UiO : Department of Informatics
University of Oslo

Keylogging of user interaction in physical and virtual environments and its implications for honeypot analysis

Stig Arild Ysterud
stigay@ifi.uio.no
Network and System Administration

Master's Thesis Spring 2014

Keylogging of user interaction in physical and virtual environments and its implications for honeypot analysis

Stig Arild Ysterud
stigay@ifi.uio.no
Network and System Administration

20th May 2014

Abstract

Computer security specialists work every day solving security problems and handling intrusions. The experts try to avoid new security threats, but the intruders are trying to find new penetration methods and sophisticated attacking methods to compromise computers. The number of intruders is increasing in the computer world today. The usage of keylogging is being used for monitoring and logging what attackers are doing when performing attacks. Keylogging can log the entered keystrokes on hosts such as remote systems and in honeypots. Collecting keystrokes is an important step towards understanding the hackers and acquire knowledge about the attacks. Honeypots can tell security researchers how data is stolen and where hackers hide their stolen data or which methods the hackers are using to take control over a remote machine.

Originally keyloggers where developed for servers with operating systems accessing the hardware directly. However, the usage of visualization and virtual machines is increasing rapidly for service providers in small and large organizations. Keylogging in bare-metal technology and in virtual technologies can be different, since the keystrokes might be interpreted differently depending on the hypervisor technology. The results of this thesis show that with respect to keylogging there are differences between bare-metal and virtual environments for Linux systems.

Acknowledgment

First and foremost I want to thank my supervisor and motivator Hårek Haugerud for his work, technical support and engagement during my master thesis.

There are many persons involved who deserves to be thank and especially I want to thank the following:

First I would like to thank Erik Hjelmås, who gave me the opportunity to be a teacher assistant at the Operating System course spring 2014.

Thanks to Torunn Gjester, that also gave me the opportunity to be a teacher assistant in computer networks in the spring 2014.

Thanks to Oslo and Akershus University College for letting me use the hardware such as servers, virtual servers, public IP's and devices to build environments at the school during my master thesis.

A big thank to the University of Oslo and Oslo & Akershus University College for giving me the opportunity to do the master thesis spring 2014.

Finally thanks to my girlfriend, family and friends all around the world, for their support.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

In a modern computer, the interpretation of a pressed key is generally left to the software. Keylogging is one of the most popular spying software in the computer history. A computer keyboard distinguishes each physical key from every other and reports all key presses to the controlling software[2]. Physical keyboards is used to type text and numbers into a word processor, text editor or other programs. In a modern computer, the interpretation of keystrokes are generally left to the software. A computer keyboard distinguishes each physical key from every other and reports all keystrokes to the controlling software. A command-line interface is a type of user interface operated entirely through a keyboard.[2] For knowing the term keylogger, and how it works, it is necessary to deeply understand the operating system architecture.[3]
The assumption is that virtual technologies are acting differently when interpreting a key stroke from user keyboard, and that depends on how the virtual machine sees its hypervisor and how the hypervisor handling and using the hardware resources, such as the keyboard. The key strokes entered on the keyboard will be necessary to detect, since one of this thesis purpose will be to log the keystrokes performed by the attacker.
In computer environment it exists both hardware keyloggers and software keyloggers. The hardware keylogger can only log from the only one physical machine the hardware keylogger is installed on. The software keylogger can log local and remote users. It will be necessary to use a software key logger in this thesis for log intruders from all over the world.
Keyloggers will be listed after the most popular keyloggers on the todays marked for Linux Ubuntu desktop 12.04, Linux Ubuntu server 12.04 and Microsoft Windows 7 platforms and then tested to look after important features such as visible or invisible and time-stamps. The description in the approach and methodology chapter, followed by testing and analysing.
Keyloggers for Linux-system are open-source there the source code is available for downloading for any interested user. Keyloggers in Windows for the most commercial, but some of the products offer a trial period for testing the current keylogger.
A keylogger with a lot of features to capture all necessary information can be used in honeypots in a honeynet. A typical honeypot is a host machine,

acting like a useful and normal host. Several honeypots in a network is called a honeynet.[4] The honeynet consist of technology for watching honeypots that are running with the primary intent of luring attackers and collect information about attacks and tracking attacking methods.[1]
In this thesis keylogging tools will be implemented, tested and analyzed in order to find out how they works and if the keyloggers works the same way for bare-metal systems and in different virtual environments, such as Xen, KVM, VMWare ESXi and Virtual Box.
Virtualization has been very useful for companies and organizations to run different services on a single virtual server. Virtualization technologies has many benefits. One virtual server enables to reduce the cost of managing more hardwares, flexibility in management, the usage of resources in more efficient ways for naming a few.
Two different platforms will be used in testing such as Microsoft Windows 7 and Linux Ubuntu 12.04 operating systems. Different operating systems can act different. Keyloggers features such as visibility, functionality and stealthiness will be tested. Keyloggers will be installed on honeypots to understandable data from the attackers from log files that will log keystrokes entered by the user or hopefully the attackers.
Since the keystrokes are fetched local or virtual, and in some cases are send over the networks, one will need a software-based keylogger[40]. Keyloggers may behave different in different environments. The keystrokes are interpreted differently by bare-metal technology as compared to virtual technologies in a virtual environment.
One other issue to take into account is to what extent keyloggers that can be used in hidden mode, being invisible for an attacker to detect. Like it is impossible to detect by looking at the running processes on a system[5, 16, 40].
For this research physical and virtual environment is set up in Oslo and Akershus University College's network. The different environments are explained in the background chapter. The hardware is thoroughly explained in the approach section.
In the computer world, a hacker is someone who seeks and exploits weaknesses in a computer system. A honeypot monitor selected hackers that get fetched in attacks to honeypot targets. The fetched attacker give us knowledge against development in the future to better handle attacks from hackers.[1]

1.1 Motivation

This section tells about the motivation for this master thesis, keylogging, and the importance around that topic. All of the following articles contains different virtual technologies, hacker attacks that are mentioned gave interest for making a proposal of problem statements to solve.
Here are two interesting cases around the topic keylogging, found in newspapers on the Internet. One article from year 2005 and the other from recently year 2014, that shows that keylogging are used for several years.

In February 2005, Joe Lopez, a businessman from Florida, filed a suit against Bank of America after unknown hackers stole $90,000 *from his Bank of America account. An investigation showed that Mr. Lopezs computer was infected with a malicious program, Backdoor. Coreflood, which records every keystroke and sends this information to malicious users via the Internet. This is how the hackers got hold of Joe Lopez user name and password.*[47]

In February 2014, an article at www.nrk.no states that the Norwegian Police Security Service(PST) ask politicians for permission to install ways to monitor data keyboards of people they have in the spotlight. This could be achieved by installing a proper keylogger secretly on the remote machine to log key strokes. [48]

Keystroke logging has become an established method used by hackers for fetching passwords and other confidential data. Not only for hackers, but also for others such as: system administrators for systems, detecting suspicious users. In research for different areas such as for research by parents for monitoring children for detecting special behaviors and criminals to name a few areas.
Keystroke logging can also be a very useful method to detect attacks and their attack mechanisms, when setting up keylogger in honeypots. An important part of this research will be to actually find out how keylogging works under different technologies and set up a honeypot to log the keystrokes, entered as commands or executable scripts entered by the attackers. With the purpose to viewing exactly what the hackers are doing. This will monitor which method that is going to be used. This may also cause successfully interaction with the hacker. To detect keystrokes might prepare against such attacks in the future.
There are several attack methods all over the world, with the purpose to harm people, groups or unknown targets. One type of attack that is interested to detect, is especially when the hacker trying to compromise the hacked computer to be a part of the bot-net.[1, 23, 40]

A virtual machine depends on the virtual technology and the underlying hypervisor. Common for all virtual technologies is that the virtual machines are running on a hypervisor that hides the physical characteristics of a computing platform from users and instead showing the abstract platform. Many hosts allow the execution of complete operating systems. The guest software executes as if it were running directly on the physical hardware, with several notable limitations. Access to physical system resources like the keyboard is generally managed at a more restrictive level than the host processor and system-memory.[22]

Some keyloggers today works on clean platform formed on bare metal machines and could maybe not work on platforms build on a virtual platform environment, since the hardware keyboard could be interpreting different that a bare-metal system. This interpreting issue of keyboard stroke signals may cause problem when trying to keylogging the attackers in a honeypot

in a virtual environment.
The situation to develop a kernel keylogger that works on virtual machines in any environment is a big motivation for this thesis. There are some research on keyloggers today at the Internet, how to install them, features with the current keylogger and issues with the installation part. It is not listed good surveys on keyloggers today, that gives a good description around the if keyloggers topic.

1.2 Problem statements

Here is the list of problem statements regarding this master thesis. Within the topic keyloggers there are several solved and unsolved questions.

There exists surveys of keylogging on bare-metal technology for Linux and Windows based systems today, but not surveys of keylogging for virtual technologies.

1. Do a survey on keyloggers on Windows- and Linux-based systems.
2. Investigate trough experiments how keyloggers function in both bare-metal and different virtual environments and weather they log any keystroke, or only keystrokes from a limited number of applications.
3. Analyze to what extent keyloggers can be detected.
4. Analyze to what extent time-stamp for keyloggers can be used to establish a time-line of the events taking place.
5. Investigate to what extent the keylogging features of Kippo facilitates the analysis of SSH attacks.

1.3 Thesis structure

One goal of this research is to investigate in keyloggers and ways to monitor detecting methods that are used in attacks trough the usage of honeypots. This is explained through a introduction in chapter one containing the motivation, problem statements and thesis structure. Chapter 2 is about the background. The Background chapter consist of information about useful tools, keystroke interpreting, the available key logger tools and the different virtual technologies behind. Related works for checking what others have been doing in this area is summaries.

The approach and methodology in chapter 3 focus on emphasizing around methods for conducting the different tests of keyloggers, how to performing the tests and honeypot analysis for ssh-attacks. The hardware and software used for this keylogging tests. Chapter 4 is showing the results. The result chapter use a explained tables for visibility and timestamps. Chapter 5 shows the analyze for the keylogger tests with visibility and time-stamp.The analyse chapter also show the analyse of the

logging attacks. After working with keyloggers and honeypots, it ends in a discussion around the topic in chapter 6. Give some future works in the future. Finally in chapter 7, the conclusion to sum up the whole research project with advantages and disadvantages.

In the end is a reference list and the appendix section in the very end.

Chapter 2

Background

For setting up keyloggers and honeypots one can use several tools and environments. The range of tools is wide within every single area. Several tools are used and tested, to find the best solution and performance regarding this project.

Within the keylogger topic there are also many tools for logging the keystrokes. The keyloggers will be listed in the keylogger section in this background chapter.

There can be as mentioned many tools in the today's computers for logging users on a machine. Many tools are easy to discover such as the tool *syslog* and *history* for Unix based systems.

The *history* command can be very informative, but the *history* command also have issues. One of the biggest issue is that the history command id typically the first item an attacker will go after and modify or delete after a penetration to a remote system. The history command will repeat the commands entered earlier in the session to a Unix system. Attackers will easily delete the history entries, after typing in commands, for easily hide eventually evidences and traces.[1]

Another feature in Unix-systems is the application *syslog*. *Syslog* can do computer message logging. *Syslog* permits separation of the software that generates messages from the system that stores them and the software that reports and analyzes them[10].

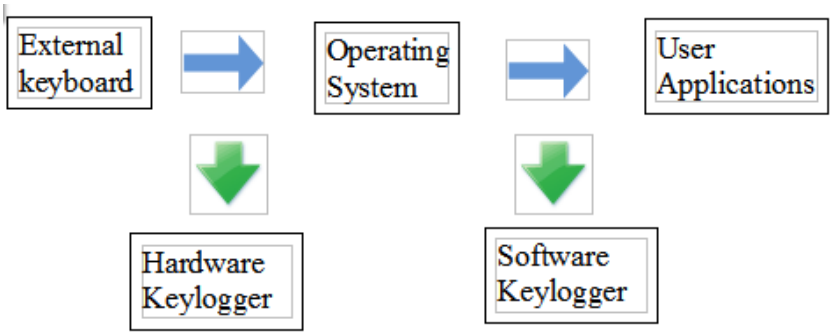

Figure 2.1: Keylogger types in a system hierarchy

2.1 Keyloggers

A keylogger known as keystroke logging or keylogging is a hardware device or a software program that records a lot of user inputs and user activity. The real time activity of a computer user including the keyboard strokes that is pressed, websites visited, programs running, instant messages as well as other computer related activities. The user might know it, or the keylogger is hidden for the user for malicious purposes.
If a keylogger in installed on a system, it can be configured to start every time the computer turns on. After the keylogger is installed on a computer system, the system can be actively monitored.
There exists two types of keyloggers. Software keyloggers and hardware keyloggers. The difference where the keyloggers detect from is showed in figure 2.1. The hardware keylogger is a device that is connected between the keyboard and the input/output(I/O) input unit on the computers hardware for logging key strokes entered in the computer. Some of hardware keyloggers works at BIOS level while some are based on keyboard level.
The hardware keyloggers does not require any driver or software and will work with all Linux based operating systems as well as with Windows operating systems. A picture of a hardware keylogger is showed in figure 2.2 on the next page. Hardware-based keyloggers do not depend upon any software being installed as they exist at a hardware level in a computer system. Hardware keyloggers are used for keystroke logging by means of a hardware circuit that is attached somewhere in between the computer keyboard and the computer, typically in line with the keyboard's cable connector. There are also USB based Hardware keyloggers as well as ones for laptop computers. More stealthy implementations can be installed or built into standard keyboards, so that no device is visible on the external cable. Both types log all keyboard activity to their internal memory, which can be subsequently accessed, for example, by typing in a secret key sequence.
A hardware keylogger has an advantage over a software keylogger solution: it is not dependent on being installed on the target computer's operating system and therefore will not interfere with any program running on the target machine or be detected by any software.[16, 24, 26, 40, 44]

Figure 2.2: Hardware keylogger

A Software keylogger in installed on a computer, directly or by remote installation. The software keylogger is invisible to the human eye, while hardware keylogger is easy to spot if a user checks what is connected to the computer. Software-based keyloggers use the target computer's operating system in various ways, including: imitating a virtual machine, hypervisor-based or virtual machine manager, acting as the keyboard driver(kernel-based), to watch keyboard strokes.
Within software keylogger there are also two different types: user-level and kernel-level keyloggers.
A kernel level-based keylogger is a program on the machine that gets administrator permissions and hides itself in the operating system, and starts intercepting keystrokes, because keystrokes always go through the kernel. A keylogger using this method can act as a keyboard device driver for example, and thus gain access to any information typed on the keyboard as it goes to the operating system.
A user level-based keylogger are the easiest to create, but also the easiest to detect.[16] This is the most common method used when creating keyloggers. The keylogger sets a global hook for all keyboard events for all threads in the system. Normal keylogging application store their data on the local hard drive, but some are can be configured to automatically transmit data over the network to a remote computer, file server or web server.
To install a keylogger on a computer system, one need to have privileged rights. In Microsoft Windows environment, administrator right are needed or root rights in a Linux Ubuntu environment. This is because a keylogger needs to interact with the hardware to a computer system, as Input/Output where the keyboard have connection to the computer.
Keyloggers are sometimes part of malicious(also called malware) packages downloaded onto computers without the owner's knowledge. Detecting the presence of a key logger on a computer can be difficult. So-called anti-

keylogging programs have been developed to *thwart* keylogging systems, and these are often effective when used properly.

There are many software based keyloggers found on the Internet, some are free for downloading while others are commercial that require a paid license for full time usage. Generally speaking, a commercial version of a key logger normally has better invisibility to prevent being detected by advanced users.
Keystroke logging can be achieved by both hardware and software means. Hardware keyloggers are attached to the keyboard cable or installed inside standard keyboards.
Software keyloggers work on the target computer's operating system and gain unauthorized access to the hardware, hook into the keyboard with functions provided by the operating system, or use remote access software to transmit recorded data out of the target computer to a remote location. Some hackers also use wireless keylogger sniffers to collect packets of data being transferred from a wireless keyboard and its receiver, and then they crack the encryption key being used to secure wireless communications between the two devices.
Most keyloggers can be fooled by alternating between typing the login credentials and typing characters somewhere else in the focus window[2, 9, 16, 27]

2.1.1 Usage of keyloggers

Both hardware keyloggers and software keyloggers have their advantages and disadvantages. It is depending on what purpose one will use the keylogger. Keyloggers are used in many different areas.
There is a lot of legitimate software which is designed to allow system administrators to track what employees do throughout the day, or to allow users to track the activity of third parties on their computers. Keyloggers are also used in information technology organizations to troubleshoot technical problems with computers and business networks. Keyloggers can also be used by a family or business to monitor the network usage of people without their direct knowledge. Malicious individuals, also called hackers may use keyloggers on public computers to steal passwords or confidential informative entered to the computer via the keyboard. Hackers are using keyloggers for cyber espionage, identity theft, fraud and several more methods. Other areas for usage are: Detecting users, parents watching children, computer cyber criminals, private detectives, law enforcement, spouses and family members, employers, system administrators and in research for different areas. Keyloggers are also using for this research to detect hackers and attackers.[16, 50] Keyloggers are also used in honeypots. For example, we can log the key strokes of an interactive session even if encryption is used to protect the network traffic.[20]

2.1.2 Visibility for keyloggers

A hardware keylogger is easy to spot if a user checks what is connected between to keyboard to the hardware on a computer, but software keyloggers are more difficult to detect, because they are software inside a computer.
A good feature for a keylogger is that the keylogger is invisible and hard to detect on the current system. Especially if the purpose is to hide the keylogger for the users.

2.1.3 Features for keyloggers

Keylogger have different performances to log the interactivity.
In Linux server environment only the keystrokes are logged. In Windows environments a lot more than keystrokes is logged.
Here is a list of features for keyloggers.

- Keystrokes Logging
  Record all the key strokes.

- Clipboard Record
  Record any words or texts which are copied and pasted on the clipboard or other file editing programs. The purpose of this is to be able to view the record in details about which user at what time have selected and copied what exact text information.

- Application Tracking
  All attempts to run any program can be logged. The purpose is to easily understand what time which user is running what applications in the computer.

- Websites Visited
  All the web activity like site titles, clicking links, visiting web-pages URLs could be monitored and recorded by Keylogger. The logs are accurate to the exact time hence you are able to know what the user was involved in the specific computer activities.

- Screen Capture
  Screen shot allows you to understand what's going on with the computer without logging key strokes. For the screen shot, you can customize with capture interval and capture quality one the screen shot taken.

- Web-camera recording
  Periodically makes web-camera pictures and stores them to log.

- Email log delivery
  Keylogger can send you recorded logs through e-mail delivery at set times.

- FTP delivery
  The keylogger can upload recorded logs through FTP delivery.
- Invisible mode
  Makes it absolutely invisible to anyone. A keylogger is usually not visible in the task bar, system tray, Windows 2000/XP/2003/Vista/Windows 7 Task Manager, process viewers (Process Explorer, WinTasks etc.), Start menu and Windows startup list.
- Time/Date tracking
  It allows you to pinpoint the exact time a window received a keystroke.
- Easy to install
- Automatic startup

2.1.4 Tools for keylogging

There is more keyloggers for Windows, than Linux. On UNIX/Linux-based systems and other operating systems, keyloggers can be easily implemented with a few lines of shell code.[33] All tools have their advantages and disadvantages. In the two next subsections that follows are lists of the keyloggers used on today's computer systems in Linux and Windows environments. How to install the Linux keyloggers is more described in the appendix A and where to download the keyloggers for Microsoft Windows in appendix B
The list below take the consideration of keyloggers, and are divided on Microsoft Windows- and Linux-based platforms. The python keylogger called *pykeylogger* are build for both Windows and Linux platforms, but are listed under both platforms since the *pykeylogger* are built and act different in both environments.

2.1.5 Keyloggers for Linux-based platforms

On GNU/Linux systems and other reasonable operating systems, simple key loggers can be easily implemented with a few lines of shell code. There are many outdated keyloggers for Linux, such as Uberkey which appears dead.
Here is a list of old and new Linux keyloggers:

- **Logkeys 0.1.1a(alpha)**
  Last updated: 2012-12-10
  Logkeys is no more advanced than other available Linux keyloggers, but is a bit more up to date.It relies on event interface of the Linux input subsystem. Once set, it logs all common character and function keys, while also being fully aware of Shift and Alt-Gr key modifiers.[32, 33]
  Logkeys are availible in the Ubuntu Software Center, a center where

applications for Ubuntu are available for download.

- **Linux Kernel Key Logger**
  Last Update: 2012-12-10
  Programming Language: C
  A Linux kernel module for logging keystrokes
  Simply its a Linux kernel module that sniffs key strokes and saves it in an in-memory buffer, and then any user space can read it from a virtual device node.

- **LKL 0.1.1**
  Last updated: 2013-04-11 in sourceforge.net
  Founded: 2005
  LKL is a userspace keylogger that runs under Linux on the x86 arch. LKL sniffs and logs everything that passes through the hardware keyboard port (0x60). It translates keycodes to ASCII with a keymap file.

- **PyKeylogger for Linux Ubuntu**
  Last updated:2009-11-29
  PyKeyLogger was founded in 2005-09-01.
  A free open source keylogger for Linux.
  PyKeylogger is a short for python keylogger and is written in the python programming language. PyKeylogger is free available as a simple python source zip. Pykeylogger is freely available for download from SourceForge file servers on the Internet.
  PyKeylogger is a proof of concept of a pure-python keylogger for Linux. It uses Xlib, that means that you must have an X connection to monitor the state of the keyboard.
  Working on platforms: Windows and Linux.
  It is primarily designed for backup purposes, but can be used as a stealth keylogger, too. It does not raise any trust issues, since it is a set of relatively short python scripts that you can easily examine.

- **THC-vlogger**
  Version: 2.1.1
  Founded: 2003-12-19.
  THC-vlogger, an advanced Linux kernel based keylogger, developed by famous hacker group THC. THC enables to log keystrokes of all root and user's sessions via console, serial and remote access such as log in from the service ssh. It can automatically detect password prompts to log only sensitive user and password information.[34]

- **Ttyrpld**
  Version: ttyrpld-2.60
  Ttyrpld is a kit to log any traffic and actions which go through any of

your Kernel's tty devices.
Ttyrpld is a multi-OS kernel-level TTY keylogger and screenlogger with asynchronous and synchronous replay support. Ttyrpld runs on Linux, Solaris, FreeBSD, NetBSD and OpenBSD.
ttyrpld is a kit to log any traffic and actions which go through any of the Kernel's tty devices.

- **Uberkey**
  Last version: uberkey-1.2.0.2
  rpmfind.net mention that uberkey was a keylogger for Red Hat Linux.
  Uberkey is a keylogger for x86 systems
  Uberkey is a keylogger which appears dead.
  Uberkey, which had over a hundred lines of code, also often repeats keys and what is worse, it makes your mouse move abruplty.

2.1.6 Keyloggers for Windows based-platforms

There is a plethora of keyloggers for Windows. There is a lot of commercial keyloggers for sale, and most of the commercial keyloggers has a free trial period from one day to one week.

- **Myjad Keylogger Pro 2.20**
  Myjad Keylogger Pro is a helping tool to better understand any desired computer activities so that one can review all the computer operation in details, such as logs sent to a desire e-mail/FTP/LAN account.
  Monitor all computer operating activities and websites visiting;
  Receive recorded logs unknowingly.
  MyJad Keylogger always runs in stealth mode. Press the hotkey to unhide the program.
  You can set password so that nobody else could enter the see what you are spying on.
  Hot key and magic word settings also allow you t2 o hide and unhidden keylogger.
  You could run keylogger by inputting the command which has been set or monitor selected users. All logs are able to be delivered to mails.
  Price: $24.95
  Last updated: Pro 2.20
  Working on platforms: Windows 8/7/Vista/XP/2003/2000 32 and 64.

- **Ardamax keylogger 4.1**
  Ardamax Keylogger is a keystroke recorder that captures user's activity and saves it to an encrypted log file. The log file can be viewed

with the powerful Log Viewer. Use this tool to find out what is happening on your computer while you are away, maintain a backup of your typed data automatically or use it to monitor your kids. Also you can use it as a monitoring device for detecting unauthorized access. Logs can be automatically sent to your e-mail address, access to the keylogger is password protected. Besides, Ardamax Keylogger logs information about the Internet addresses the user has visited.[25]
Price: 282,12 NOK
Last updated: January 22, 2014.
Last released: Version 4.1.
Working on platforms: Windows 2000, XP, 2003, Vista, 7 and Windows 8.

- **Actual Keylogger 3.2**
  If you are using the unregistered version, the limitation is no more than 40 minutes.
  Keylogger Actual Spy is capable of catching all keystrokes, capturing the screen, logging the programs being run and closed, monitoring the clipboard contents.
  Logs all keystrokes, is case sensitive (keystroke logger).
  Last updated March 20, 2014.
  Price: $59.95 USD for 1 license.
  Can be bought in many different quantities; 1 license, 2-5 licenses, 6-10 licenses, 11-20 licenses, 21-50 licenses og the last option with 51 licenses or more.

- **PyKeylogger 1.2.1 for Microsoft Windows 7**
  Last updated:2009-11-29
  Price: Cost money after the trial period on Windows.
  PyKeylogger is a short for python keylogger and is written in the python programming language. PyKeylogger is free available as a simple python source zip. Pykeylogger is freely available for download from SourceForge file servers on the Internet.
  PyKeyLogger was founded in 2005-09-01.
  Working on platforms: Windows and Linux.
  It is primarily designed for backup purposes, but can be used as a stealth keylogger, too. It does not raise any trust issues, since it is a set of relatively short python scripts that you can easily examine.

- **REFOG keylogger 8.1.2.2060**
  REFOG Free key-logger is a free software program which works like a tape recorder running in hidden mode. It captures all the typed data, username, passwords, emails, chats etc. once the computer turns on. You can block the detected website with the help of firewalls if you wish to do so.
  Price: $39.95

Trial period for 3 days.

- **Family-keylogger v5.58**
  Trial Version
  The trial version of this software may be used for evaluation purposes at the user's own risk for a period of 21 days from the date of installation.
  At the end of the trial period, the user must either purchase a license to continue using the software, or remove it from the system.

- **System Surverillance - Pro 7.2**
  SSPro uses an "Internet" based installation system which typically results in faster installs.
  Record keystrokes, programs, websites, IMs and more with SSPro.
  Logged data is only stored in the hard drive location one choose.
  Last updated: February 14, 2013

- **Argos Monitoring 1.65**
  Use a evaluation period of seven days.
  Argos logs keystrokes, log websites and capture screenshots.

Here is also a list over other commercial keyloggers for Microsoft Windows that are available on the Internet that can be bought for money, and not have free trial for download for users.

- **SoftActivity Keylogger**
  Software based keylogger. Working on platforms: Windows 98, Me, 2000, 2003, XP, Vista Windows 7 and Windows 8 (32-bit and 64-bit)
  Version: Version 7,6
  Last released: Jan 14, 2014

- **Revealer Keylogger 2.0**
  Revealer Keylogger Free ranks the second among all the keylogger programs downloaded in CNET. Logging keystrokes, multiple language support, hot-key support (default Ctrl+Alt+F9), startup settings, auto log cleanup and more advanced functions in this program. User is free to set screen shot capture and mail delivery.

- **BlackBox Express 1.0**
  BlackBox Express is a free secure monitoring program takes record on web mails, chatting tools, running applications, keystrokes, keywords typed in searching engine etc. You are optional to choose which user to monitor in the computer. BlackBox Express will generate a report that allows you to print, send email or view as HTML.

The special feature of this program is that it can monitor one local PC and up to 200 remote computers on the network.
BlackBox Express runs in the computer background and can only be unhidden from the shortcut or by running the executable file from the program file folder. User allows to set password to protect the program from being accessed. Though it will be shown in task manager but won't be visible in taksbar. Before you download the program a free account is required.

- **Spyrix Free Keylogger**
  Spyrix Free Keylogger is a free and simple program for local and remote user activity monitoring via secure web account. Spyrix Free Keylogger main features:keylogger (keystrokes logging), undetectable to antivirus software, apps activity, screenshots capture, drives and printer acivity.
  Newest version: Version 4.0.5

- **SPECTOR PRO**
  The Spectro pro keylogger records every keystroke pressed by the keyboard.
  Works on platforms: Windows and MAC.
  Once installed, no one but you will know that it's there.
  Easy-to-use (even for beginners)
  Cost: $99,95

2.2 Honeynets and Honeypots

First of all the difference of this subsubject title "Honeynets and Honeypots" is explained: Honeynet is a computer networks specifically to be attacked. The hosts that comprise a honeynet and serve as attack targets are called Honeypots.
A honeypot is a trap set to detect, deflect or in some manner, counteract attempts at unauthorized use of information systems. Generally, a honeypot consists of a computer, data, or a network site that appears to be part of a network, but is actually isolated and monitored, and which seems to contain information or a resource of value to attackers.[21, 23]
Every computer attack, whether manual or automated, has an exploratory component. When hackers or viruses go probing networks and systems they are usually able to do so unnoticed. Unless they cause a system crash or overwhelm a system, the chances of detection are pretty low. A honeypot is a system that detects unusual activity by creating false targets. In a network, for example, a simple honeypot may allocate the unused IP address space. Then if someone attempts to access an IP address that is not used, an alert can be generated. Similarly, a port-based honeypot could respond to requests on unused services on the TCP ports. Entire computers,

or even networks of computers, can be created to lure attackers. Honeypots that are build for tricking attackers, and to gather limited information. Honeypots can mainly be divided into two parts:
Research honeypots and Production honeypots.
Research honeypots are running to gather all kinds of information and are complex to deploy and maintain, capture extensive information, and are used primarily by research, military, or government organizations.These honeypots are used to research attackers and threats that an organization face every days. This might help an organization to know how to better protect against threats in the future.
Production honeypots are easy to use compared with research honeypots, because production honeypots only will capture limited information, and therefor are used primarily by companies, corporations or organizations.
Production honeypots are placed inside the production network with other production servers by an organization to improve their state of security. Normally, production honeypots are low-interaction honeypots, which are easier to deploy. They give less information about the attacks or attackers than research honeypots are doing.
Types of honeypots are based on design criteria, honeypots can be classified as:
pure honeypots, high-interaction honeypots,low-interaction honeypots.[1, 21]

2.2.1 Pure Honeypots

Pure honeypots are entirely production systems. The activities of the attacker are monitored by using a casual tap that has been installed on the honeypots link to the network. Even though a pure honeypot is useful, stealthiness of the defense mechanisms can be ensured by a more controlled mechanism.[1]

2.2.2 Low interaction Honeypots

Low-interaction honeypots simulate only the services frequently requested by attackers. Since they consume relatively few resources, multiple virtual machines can easily be hosted on one physical system, the virtual systems have a short response time, and less code is required. Example of a interaction honeypot is the low interaction honeypot: Honeyd and HoneyC.[1, 20, 21]

2.2.3 Medium interaction Honeypots

Medium interaction Honeypots are designed to log brute force attacks into a SSH connection to a Linux system and the interaction in the shell performed by the attacker. Example of a interaction honeypot is the low interaction honeypot: Kippo[20, 45]

Applications
Virtual machines
Hypervisor
Hardware

Table 2.1: Hypervisor type 1

Applications
Virtual machines
Hypervisor
Operating system
Hardware

Table 2.2: Hypervisor type 2

2.2.4 High interaction Honeypots

High-interaction honeypots pretend to have the activities of the production systems that host several services and, therefore, an attacker may be allowed a lot of services to waste his time.
High-interaction honeypots are using new technology, so by employing virtual machines, multiple honeypots can be hosted on a single physical machine. That mean if one honeypot gets compromised, it can be restored much faster. If virtual machines are not available, one honeypot must be maintained for each physical computer, which can be much more expensive. Example of a interaction honeypot is the high interaction honeypot: HoneyBow [1]

2.3 Virtual environments

Virtual environment software refers to any software or system that implements, manages and controls multiple virtual environment instances.
Virtualization means creating new virtual operating systems on a system. The idea behind virtualization systems is the usage of hardware resources between parallel running of virtual machines that are managed by special software known as Virtual Machine Monitor(VMM) also known as a hypervisor that works between the hardware and operation system.[22]
The hypervisor executes the guest operating systems with a virtual operating platform and manages the execution of the guest operating systems. Multiple instances of different operating systems may share the virtualized hardware resources.
There are two types of hypervisors. Type 1 in table 2.1 and Type 2 showed in table 2.2. A computer on which a hypervisor is running at the bottom, one or more virtual machines is defined as a host machine on the top of the hypervisor. All instructions and system call is going through the hypervisor.

Each virtual machine is called a guest machine. The hypervisor presents the guest operating systems with a virtual operating platform and manages the execution of the guest operating systems. Multiple instances of a variety of operating systems may share the virtualized hardware resources. There are many different ways to connect to the virtual machines such as remote SSH-connection, VNC, console and through locally in hypervisor using tools such as virt-viewer and virt-manager.
A virtual machine can basically have two different technologies in the bottom. The two terms is hardware virtualization(type1) and desktop virtualization(type2).[22]
Hardware virtualization refers to the creation of a virtual machine that pretend to be a real computer with an operating system. Software executed on these virtual machines is separated from the underlying hardware resources.
In hardware virtualization, the host machine is the actual machine on which the virtualization takes place, and the guest machine is the virtual machine. The words host and guest are used to distinguish the software that runs on the physical machine from the software that runs on the virtual machine. The software or firmware that creates a virtual machine on the host hardware is called a hypervisor.
Different types of hardware virtualization include:
Full-virtualization: Almost complete simulation of the actual hardware to allow software, which typically consists of a guest operating system, to run unmodified.
Partial-virtualization: Some but not all of the target environment is simulated. Some guest programs, therefore, may need modifications to run in this virtual environment.
Para-virtualization: A hardware environment is not simulated; however, the guest programs are executed in their own isolated area, as if they are running on a separate system. Guest programs need to be specifically modified to run in this environment. Such as capturing and releasing key strokes.
The virtual machine only sees keyboard devices, since the operating system in the virtual machine does not "know" that it is not running on a real computer, it expects to have full control over the keyboard. If one are running the virtual machine in full screen mode, your VM needs to share keyboard with other applications and possibly other virtual machines on current host.[22, 28]

Desktop virtualization is separating the virtual machines desktop from the physical machine.
Desktop virtualization interacting with a host computer directly via a keyboard. The host computer becomes a server computer capable of hosting multiple virtual machines at the same time for multiple users.[22, 28]

- Xen
- KVM(Kernel-based virtual machine)

- VMware ESXi
- Virtual Box

Here is an deeper explanation of the different virtual technologies Xen, KVM, VMWare ESXi and Virtual Box.

2.3.1 Xen

Xen is a hypervisor type2 showed in table 2.2 on page 19. The hypervisor on Xen delegate resources to multiple operating systems to be executed on the same computer hardware at the same time. The hypervisor is built on existing operating system, and that operating system has direct access to the hardware. Xen provides services that allow multiple computer operating systems to be executed on the same computer hardware at the same time.
The Xen community develops and maintains Xen as a open-source and a free software to use.
The Xen technology runs in a more privileged CPU state than the other software on a computer.
Xen is a type of "para-virtualization, which means a operating system whereby the operating system is aware that it is running inside a virtual machine, and so makes hyper calls directly, rather than issuing privileged instructions.[35]
Xen is the virtualization platform used for cloud computing. It is the virtualisation technology in the bottom for the Amazon EC2 cloud. Running Amazon EC2 instance, mens to launch a virtual server by using the technology Amazon EC2 that are using the virtual environment Xen.[35]

2.3.2 KVM

KVM (Kernel-based Virtual Machine) is using the hypervisor type2 showed in table 2.2 on page 19. KVM is a open source software, full virtualization solution for Linux on x86 hardware that containing virtualization extensions (Intel VT or AMD-V).
KVM is a Linux kernel module that allows a user space program to utilize the hardware virtualization features of various processors.
Using KVM, one can run multiple virtual machines running unmodified Linux or Windows images. Each virtual machine has private visualized hardware: a network card, disk, graphics adapter, etc.[17]
QEMU is the short for "Quick EMUlator".QEMU can make use of KVM when running a target architecture that is the same as the host architecture. QEMU is a hypervisor that performs hardware virtualization. For instance, when running qemu-system-x86 on an x86 compatible processor, you can take advantage of the KVM acceleration,that gives you the benefit for your host and your guest systems.

2.3.3 VMware ESXi

VMware ESXi are type 1 hypervisor that are illustrated in table 2.1 on page 19. Type 1 using a hypervisor type there the hypervisor is directly connected to the hardware at the bottom and the guest operating systems at the top. That is VMware's enterprise software hypervisors for guest virtual servers that run directly on host server hardware.
VMware ESXi use a hypervisor that are called "vmkernel".
VMWare uses the virtual machine monitor(VMM) between the operating system and the hardware for management of the resources. VMware are using a shared hardware infrastructure that offers full isolation and one can use any types of operating system for applications.
A VMWare environment do not require a additional underlying operating system.
VMware ESXi is an enterprise-level computer virtualization product offered by VMware, Inc[36, 52]

2.3.4 Virtual Box

VirtualBox is a virtualization software package that can be installed on x86 and AMD64/Intel64-based computers. Virtual Box is installed on an existing host operating system as an application. Virtual Box use the hypervisor showed in table 2.2 on page 19.
This host application allows additional guest operating systems, each known as a Guest OS, to be loaded and run, each with its own virtual environment. VirtualBox supports several operating systems including, Linux and Windows 7 as hosts and guest operating systems.
Virtual Box has an emulated environment, that means that users of VirtualBox can load multiple guest operating systems under a single host operating-system.
The administrator or users of a virtual box can configure each virtual machine and run it under either software-based virtualization or hardware assisted virtualization if the underlying host hardware supports this.[31]
The host OS and guest OSs and applications can communicate with each other through a number of mechanisms including a common clipboard and a virtualized network facility. Guest VMs can also directly communicate with each other if configured to do so.

2.4 Services and helping tools to performing and detecting network attacks for capturing keystrokes

For doing research it is very helpful to use some helping tools to perform useful results. For this research unless the honeypots and the fake SSH-server, some services are set up for attackers to make it easier to log in to a remote computer with a shell or a remote desktop. Those helping tools are mentioned in the sub sections below.

2.4.1 SSH

SSH, the Secure Shell, is a popular, powerful, software-based approach to network security. Since it needs to log into a shell with a user name and password, it is the most wanted way to hack/compromise a computer with for an attacker. Especially the brute force attack into SSH witch is a service that use port 22 to connect to.
In general SSH protocol can be used for two purposes, file transfers and terminal access. SSH is designed to provide a secure channel between two hosts, since the key strokes are encrypted by the sender and then decrypted by the receiver. In interactive mode, every individual keystroke that a user types is sent to the remote machine in a separate IP packet immediately after a key is pressed, which leaks the inter keystroke timing information of user's typing.[11, 18, 19]

2.4.2 Kojoney

Kojoney is a low level interaction honeypot that emulates an SSH server. Kojoney where used in order to catch attackers. Kojoney is released under the GNU General Public License version 2 (the GPL). The daemon is written in Python.

2.4.3 Kippo

Kippo is another implementation of fake ssh server.
Kippo are used for several platforms, and both works for Microsoft Windows and UNIX environment. Kippo is a SSH honeypot tool written in Python.
Kippo is a Python script that emulates a shell, making it a SSH Honeypot.[45]

2.4.4 Putty

Putty is a free and open-source terminal to connect to the SSH for Windows systems.

2.4.5 OpenSSH

Is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol. Open-ssh is originally written for Unix-like operating systems, but runs well under Microsoft Windows too. [18]

2.4.6 Netcat

Netcat is very powerful tool that is able to write and read data across Transmission Control Protocol(TCP) and User datagram Protocol(UDP)

network connections to or from any ports.[43]

2.4.7 Remote Desktop Protocol

Remote Desktop Protocol(RDP) is a proprietary protocol developed by Microsoft, which provides a user with a graphical interface to connect to another computer over a network connection.

2.4.8 Virtual Network Computing

VNC allows to access and control a remote desktop applications all around the world with Internet connection, to whenever IP with a VNC server installed. VNC are using the RFB(Remote Frame Buffer) protocol to control another machine. Key strokes are sent and received over a network.[46]

2.4.9 Virtual Machine Manager

Virtual Machine Manager(Virt-Manager) is a graphical user interface application for managing virtual machines through libvirt. Virtual Machine Manager are primarily used to access KVM and Xen virtual machines. Virtual Machine Manager presents a graphical summary viewing the running virtual machines with their live performance and resource utilization statistics. [59]

2.4.10 Luarm

Luarm audie engine, version: 2.4
Is a short for "Logging User Actions in Relational Mode". Luarm is an Open Source experimental audit engine that facilitates insider threat specification as well as user action computer forensic functionality for the Linux operating system.
Luarm write and log in detail the user activities into a database, such as MySQL.
Luarm is written in the PERL program language.[54]

2.5 Computer attacks through the network

There are several attack methods from intruders all over the world, with the purpose to harm people, groups or unknown targets. Attacks can be performed virtually on any layer or level of software, from network protocols to applications.
The first thing that normally occurs when attackers are trying to compromise a computer, is that the attacker will do scan on the networks huge range of IP's(Internet Protocol's). They scan for open-ports on that computer, and find out if the open-ports consist of a service that is made to log in to the computer either through log in to get a graphical user interface(GUI) or simply to get access to a command-line to enter commands or

pre-made scripts. The intruders can look for vulnerabilities to exploit software. Most software vendors release updates to patch vulnerabilities and weaknesses in their software products as fast as they are detected. Patching keeps your software updated, and that is important to help preventing infections.[18, 42]
One attack method on the Internet are bots, also referred as zombie or drones. A bot is a piece of software that is usually installed on an infected machine without the user's knowledge. A bot is controlled remotely by the attacker under a command and control structure. Several bot machines that are connected to attack a specific target is called machines in a bot net.[4, 23, 40, 42]

2.6 Rootkits

A rootkit is a type of software, typically malicious, designed to hide the existence of certain processes or programs from normal methods of detection and enable root access to a computer, with all privileged rights.
An Attacker can install a rootkit once they have got root or administrator access to a system.
Obtaining this access is a result of direct attack on a system. Such as exploiting a known vulnerability or by entering the correct password either by cracking, brute-force, or social engineering).
When a rootkit is installed, it becomes possible to hide the intrusion as well as to maintain privileged access. The key is the root/Administrator access. Rootkits may include replacements for system binaries so that the rootkit becomes impossible for the normal user to detect the presence of the intruder on the system by looking at process table or task manager.[51]

2.7 Related works to the master thesis topic

Experiment using Distributed High-Interaction Honey net(D2H)
In a master thesis from the year 2013 called "Experiment using Distributed High-Interaction Honey net(D2H)" written by Daniel Huluka from Oslo University College, are several challenges in the "future work" section. Regarding the honeynet, he recommend a complete kernel key logger tool as an important part of the research on honeynet to maximize the data collection experience made by intruders.[5]
The problem is keylogger that works on virtual machines for logging the intruders.

The honeynet project has developed a tool named "The Honeywall CDROM" whits is a boot able CD that installs onto a hard drive and comes with all the tools and functionality to implement data capture, control and analysis. The Honeywall CDROM is connected with a bridge between the honeypot and the external network. The honeywall CDROM is capable of logging key strokes using Sebek server that is loaded by default. Sebek

is a kernel module installed on the high-interaction honeypots for collecting keystrokes to give a extensive data collection. Sebek is a data capture tool secretly designed to capture attackers keystrokes on a honeypot. Sebek has no later versions after its release in 2005, and sebek is not compatible with newly updated operating system versions. The Honeywall CDROM is a software that has its latest release in May 2005, but a tool that gives enough information for capturing, controlling and analyzing attacks. Honeywall CDROM creates an architecture that allows you to deploy both low-interaction and high-interaction honeypots, but is designed primarily for high-interaction.[13, 14, 21, 23]

Another related work that has been done is an investigation into SSH activity using Kippo that is a SSH honeypot designed to log attempts on a SSH server of attackers[45]. One interesting investigation was performed from March 2013 to June 2013. The research collected and analysed behaviours and patterns detection of the attacking entities. The conclusion of the attack patterns where not consistent and there was large disparity in numbers of the attacked hosts.[45]

In 2002 a group of hackers called "The Hacker's Choice"(THC), wrote a technical paper: "Writing Linux Kernel Keylogger". The technical paper was divided into two parts, The first for: how the linux keyboard driver works, and discussed methods that can be used to create a kernel based keylogger. The second for: presents detail of THC vlogger keylogger.[29]
An "Ways Of Building Honeypots" article tells about keystroke logging that can be provide as a final monitoring tool, that allows an administrator to "read over an attacker's shoulder" by displaying on screen what the attacker sees as soon as they see it.[57]. This gives motivation to find out about keyloggers, and ways to put them in an honeypot for monitoring the attacker through a log file, that can be stored and displayed after an attack, for later review.

Chapter 3

Approach and methodology

The environment the keyloggers is tested on, are several servers with bare-metal and different virtual servers with different virtual technologies en each server for monitoring the way the keystrokes are interpreted.
A more wider test environment will gave a much better result and analyses of keyloggers.
Both the bare-metal and the virtual machines will for this research be installed on Microsoft Windows 7 and Linux Ubuntu server 12.04 LTS machines.
The keyloggers will be tested to monitor if the keyloggers work and the keyloggers performances.
A big concern will be to use a keylogger that the attacker cannot detect and how the keylogger uses time-stamps, if the keylogger has that future.

3.1 Hardware and software

The testing environments for this research project has been done on several physical servers and several virtual servers. Showed in figure 3.1 on page 28. The tests was made possible through setting up servers on the environment from HiOA and with existing virtual servers from HiOA, using Xen and KVM environments. All virtual servers and bare-metal servers where set up and installed on the Dell servers from HiOA.

3.1.1 Linux Ubuntu 12.04

The keylogger tests where running on who different operating systems. Microsoft Windows 7 and Linux Ubuntu 12.04 LTS. Linux Ubuntu 12.04 with server and desktop edition for testing all keyloggers. Both 32-bit.
The Linux distributions was Linux Ubuntu 12.04 LTS with both server and desktop versions.
Ubuntu server 12.04 is not the newest distribution, but after testing on several distributions, it seams that all of them where equal. Linux Ubuntu is a well known operating system.use the feature "LTS" which is an abbreviation for "Long Term Support".

Servers	Technology	Model	CPU	OS
Dell PowerEdge 2950	Bare-metal	Intel(R) Xeon(R) Quad Core E5335	2.00 GHz	Linux Ubuntu desktop 12.04.3 TLS
Dell PowerEdge 2950	Bare-metal	Intel(R) Xeon(R) Quad Core E5335	2.00 GHz	Linux Ubuntu server 12.04.3 TLS
Dell PowerEdge 2950	Bare-metal	Intel(R) Xeon(R) Quad Core E5335	2.00 GHz	Microsoft Windows 7
HP-blade-server	Xen	Intel(R) Xeon(R) E5440	2.83 Ghz	Linux Ubuntu desktop 12.04.3 TLS
HP-blade-server	Xen	Intel(R) Xeon(R) E5440	2.83 Ghz	Linux Ubuntu server 12.04 LTS
Dell PowerEdge 2950	Xen	Intel(R) Xeon(R) Quad Core E5335	2.00 Ghz	Linux Ubuntu server 12.04.3 LTS
HP-blade-server	KVM	Intel(R) Xeon(R) E5440	2.83 Ghz	Linux Ubuntu desktop 12.04.4 LTS
Dell PowerEdge 2950	KVM	Intel(R) Xeon(R) Quad Core E5335	2.00 Ghz	Linux Ubuntu server 12.04.3 TLS
Dell PowerEdge 2950	Vmware ESXi	Intel(R) Xeon(R) Quad Core E5335	2.00 GHz	Require no additional underlying operating system
Dell PowerEdge 2950	Virtual Box	Intel(R) Xeon(R) Quad Core E5335	2.00 Ghz	Microsoft Windows 7

Figure 3.1: Physical Servers

Linux Ubuntu 12.04 TLS was released in 2012, and will last with support i five more years, until 2017.[55]

3.1.2 Microsoft Windows 7

The keylogger tests where running on who different operating systems. Microsoft Windows 7 and Linux Ubuntu 12.04 LTS. The choice of Microsoft Windows 7 was since the newest Windows 8 is to new at the market. The version before Windows 7 was Windows XP, but Windows XP is to old, since Microsoft not release new updates or new patches for Windows XP any more. This will of security reasons make companies to change operating system, to a newer version that are Windows 7 or Windows 8.

3.2 Addressing the problem statements

Under the introduction chapter the motivation for this master thesis was described, and narrowed down to problem statements.
Here is the problem statements listed, with the intention to addressing the research question and methods to solve the problem statements.
In this section methods for trying to solve the current problem statement is mentioned.

1. `Do a survey on key loggers on Windows- and Linux-based systems.`

    - Find the most important keylogger in both environment by creating a statistics.
    - Install and doing research and testing of the characteristics of every free and trial versions of keyloggers for Windows and Linux ubuntu 12.04 systems.
    - Find the proper and the best keylogger to put in a honeypot for logging attackers.

2. `Investigate trough experiments how key loggers work in both bare-metal and different virtual environments and weather they log any keystroke, or only keystrokes from a limited number of applications.`

    - Keyloggers are tested in both bare metal and different environments to conclude if there are some differences out there.
    - If virtual machines can reads keyloggers at all.

3. `Analyze to what extent keyloggers are visible on systems.`

    One problem for the today's keylogger is that the keylogger is visible for users of a logged computer, while the purpose of the keylogger is to in most cases be hidden from others than the installer of the key logger.
    Some keyloggers can be detected in a system process viewing. Such as "ps aux" for Unix-based systems, and in "Task Manager" in Microsoft Windows systems.
    Another visible method can be that the keylogger is showed with a icon on the desktop for system with graphical user interfaces. Often one can change the setting to not show the application as a icon. And just let the administrator choose in the settings, to set or not set the current keylogger as a icon.
    The keylogger application is showed as a process on a host machine, like other running processes.
    The same for Windows host, that normal user don't need administrator privileges to monitor the running processes.

4. `Analyze to what extent time-stamp for key loggers can be used to establish a time-line of the events taking place.`

    - Check the output file that the keylogger creates or have as default output file in Linux Ubuntu.
    - For Microsoft Windows the keylogger's output file or the log in the graphical user interface showed.
    - This for checking if the commands is manually entered or running by a script created by the attackers.

5. `Investigate to what extent the keylogging features of Kippo facilitates the analysis of SSH attacks.`

- Use the Honeypot tool Kippo for logging attackers entered keystrokes.
- See section: "Using honeypot to monitor SSH attacks using Kippo" for details for logging SSH-attacks.

3.3 Testing the keyloggers

Testing the keyloggers shows to be differences between Windows 7 and Linux Ubuntu 12.04 LTS. One specific keylogger works in the Linux Ubuntu Desktop environments, but not in Linux Ubuntu Server environments. That's why both environments are tested. The installation of Linux keyloggers are showed in appendix A and where to download Windows 7 keyloggers in appendix B. Linux keyloggers should log entered keystokes by users, and hopefully incoming logins at the SSH-port. Windows keyloggers, consist of more logging features. Such as log key-strokes, mouse inputs, visited web-pages, opened applications, screen-shots and more. The most keyloggers in Windows environment are commercial, so they cost money to buy and download. Those that are tested in this research is either free or commercial, but are free for downloading a trial for seven days.
The results of Linux Ubuntu keyloggers are measured by three different states:

- 0 = The keylogger does not work and have issues to interpret on the current Operating System.
- 1 = The keylogger does work, capture every single key-stroke on the current Operating System(user-based). but not incoming SSH connections.
- 2 = The keylogger does work and capture every key stroke on the current Operating System(Kernel-based). This include the incoming SSH connections.

The results of the Linux Ubuntu keyloggers should end in the statement 1, that the keylogger does work and capture every key stroke on the current Operating System(Kernel-based). This include the incoming SSH connections.

The results of Microsoft Windows 7 keyloggers are measured by three different states:

- 0 = The keylogger does not work and have issues to interpret on the current Operating System.
- 1 = The keylogger does work, but not capture every single key-stroke on the current Operating System(user-based). This include the incoming SSH connections. Because then the keylogger will log remote connections for OpenSSH-connections.
- 2 = The keylogger does work and capture every key stroke on the current Operating System(kernel-based). This include the incoming openSSH connections.

The results of the Microsoft Windows keyloggers should end in the statement 1, that the keylogger does work and capture every key stroke

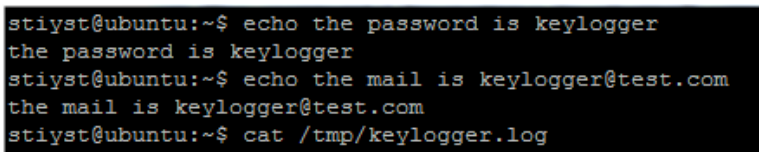

Figure 3.2: Typing in the text into the terminal for testing Linux Ubuntu keyloggers

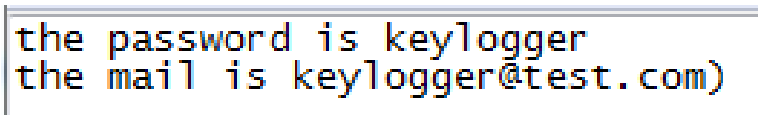

Figure 3.3: Typing in the text into notepad for testing Windows 7 keyloggers

on the current Operating System(Kernel-based). This include the incoming SSH connections. Because then the keylogger will log remote connections for ssh-connections. For this research entered key-strokes is important for the different tools. Text input is a little bit different in Linux Ubuntu 12.04 versus Windows 7, but the tests where equal on the two platforms. The test for Linux Ubuntu 12.04 was performed by the command line in the terminal, and the test for Microsoft Windows was performed in the text editor Notepad. This test where used on the two platforms to check the keyloggers: Test in Linux Ubuntu 12.04, typed in the terminal showed in 3.2

```
echo the passworddd(2*backspace) is keylogger (enter)
echo the mail is keylogger@test.com(enter)
cat "current logfile location of the keylogger"
```

Test in Windows 7: typed in notepad, showed in table 3.3.

```
the passworddd(2*backspace) is keylogger
the mail is keylogger@test.com
```

The given test was created to see whether the keylogger logged special keys as backspace and the "Alt Gr" special key:
The background for this test is if the keylogger print out the correct word after modification, or if the keylogger mention all letters entered, such as with errors and backspace for instance.
The keyloggers for Windows 7 and Linux Ubuntu 12.04 that where installed on local and distributed machines at HiOA.
One exception was made for the pykeylogger for Linux Ubuntu. That keylogger needed a graphical user interface, so Linux Ubuntu 12.04 desktop was installed for the particular keylogger. For destop keylogger was: *pykeylogger*.

Several different tools where used to interact with the keylogging tests. The tool putty where used for SSH-connection on port 22.
The tool VNC where used for accessing the graphical user interface in

Linux Ubuntu.
The virtual machines in KVM where accessed by the tool: Virtual machine manager from Linux Ubuntu Desktop.
Else the rest of environments where installed on environments on HiOa.
The test was more detailed tested by the following procedures:

1. Bare-metal
   Typing commands through the terminal in Linux Ubuntu 12.04.
   Typing through a remote ssh-connection with putty to a bare-metal machine.
2. Xen
   Typing through the terminal in Linux Ubuntu 12.04.
   Typing through a remote ssh-connection with putty to a Linux Ubuntu 12.04.
3. KVM
   Typing through the terminal in Linux Ubuntu 12.04.
   Typing via the console window from the Linux application *virtual machine manager*.
4. VMware ESXi
   Typing via the graphical user interface(GUI) through the vSphere client from a client machine.
   Typing via a remote ssh-connection through putty to the ESXi client.
5. Virtual Box
   Typing in through a local connection through the Virtual Box manager
   Typing via ssh-connection through putty.

Some of the keylogger for Linux Ubuntu needed a input device as an option input when starting the keylogger.
The keyboard devise was fetched by entering the command:
cat /var/log/Xorg.0.log | grep key or
cat /pros/bus/input/devices in the terminal.

3.4 Using honeypot to monitor SSH attacks using Kippo

In this section a medium interaction SSH honeypot Kippo is used for collection data. Kippo includes close interactions with hackers and are designed to log brute force attacks and the keystrokes performed by the attacker after the attackers have successfully logged into the system.
The SSH honeypot Kippo gather data about timestamps in attacks and the attackers interactions on the service SSH when successfully breaking in. Kippo are used for several platforms, and both works for Microsoft Windows and Linux environment. Linux environment will be used in this research.

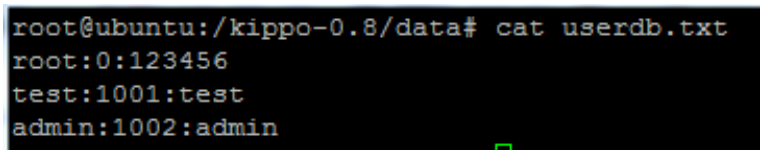

Figure 3.4: adding users to the file userdb.txt in Kippo

SSH activity can easily be logged by monitoring the Linux file: */var/log/auth.log*, that monitor only the attempts by usernames, not detailed log included timestamps and logs if attackers type after successfully logged in. Kippo was set up to detect user login and password for attacks, with timestamps on the capturing.

3.4.1 Configuring kippo

Kippo was installed on two Linux Ubuntu Servers at HiOA and on two virtual machines running at HiOA with public IPs. Four machines running Kippo to get an wide specter of different results. The kippo installation is showed in appendix C.
Expected results of the kippo tests will be many incoming connection over a amount of period. Most failed,but also successfully log ins, and monitor keystrokes for the attack,for monitoring what the hacker are typing. The user that was pre-defined to log attackers in the honeypot was: *root:1:123456*, with the meaning: username: root, groupnumber: 1 and password: 123456. Two additional users where added. Username: admin with the password admin, and the username test with the password test. This is added in the configuration file : *kippo-0.8/data/userdb.txt* showed in figure 3.4:

- root:1:1232456
- admin:1001:admin
- test:1002:test

Kippo will be executed on four different Linux Ubuntu 12.04 LTS machines, on the SSH-port 22 for logging the attackers.

Chapter 4

Results

Before testing the keyloggers it is important to find out which keylogger that is most popular among all keylogger available on the Internet today.
It is many ways to define the most important keylogger used by users.
The different keylogging tools where tested on both Linux Ubuntu machines and Windows machines, for (bare-metal) and in different virtualization technology such as: Xen, VMware ESXi,KVM and Virtual Box.
The software keyloggers for Linux Ubuntu 12.04 are summed up in table 4.3 on page 48 and for Microsoft Windows 7 is summed up in table 4.4 on page 50.
While doing the testing of keylogger in the different virtual environment, some unexpected experiences occurred. These unexpected experiences is also listed.

4.1 Statistics for Linux Ubuntu keyloggers

Before testing the keyloggers it is important to find out which keylogger that is most popular among all keylogger available on the Internet today.
Several are available, but not all are working with today computers.
It is many ways to define the most important keylogger for Linux users.
The keylogger are taken for the linux keyloggers that are both for available and unavailable on linux systems today. The keylogger that are documented outdated on the Internet, and not updated are listed with the year in parenthesis.
The criterias for this statistic are:

1. Hits on www.google.com, where the number of hits on the current keylogger is entered at www.google.com. The name of the keylogger with two obvious words where added, linux and keylogger. These were used to specify the search.

2. The next criteria was keylogger that where available for download from the github download site. GitHub is a web-based hosting service for software development projects. GitHub offers both paid

plans for private repositories, and free accounts for open source projects.

3. The third criteria was if the keylogger where available for download on sourceforge.net web site. SourceForge is also a web-based source code repository. Sourceforge acts as a centralized location for software developers to control and manage free and open-source software development.

4. The forth and last criteria are if the keylogger is available for download in the Ubuntu software center. That means that the keylogger is available for download in the ubuntu apt-get repository.

Table 4.1: Statistics of the most important keyloggers for Linux Ubuntu

Keyloggers	Google.com	Github	Sourceforge	Software Center
Linux kernel keylogger	85,200 hits	No	No	No
Pykeylogger linux keylogger	13,300 hits	Yes	No	No
Ttyrpld linux keylogger	13,000 hits	No	Yes	No
THC-vlogger linux keylogger	12,400 hits	No	No	No
LKL linux keylogger	5010 hits	Yes	Yes	No
Logkeys linux keylogger	4,920 hits	Yes	No	Yes
Uberkey linux keylogger	3690 hits	Yes	No	No

4.2 Statistics for Windows 7 keyloggers

The result is the number of hits of Windows keyloggers by search at google.com.
Before testing the keyloggers it is important to find out which keylogger that is most popular among all keylogger available on the Internet today that offers a trial period for users to get known to the product.
It is not many ways to define the most important keylogger for Windows 7 users, since the Windows keyloggers are commercial products.
The keylogger are taken for the windows keyloggers that are both for available and unavailable on windows systems today.
The criterias for this statistic are:

1. Hits on www.google.com, where the number of hits on the current keylogger is entered at www.google.com. The name of the keylogger with two obvious words where added, windows and keylogger. These were used to specify the search.

2. The next criteria was if the keylogger that where available for download from the download.cnet.com download. The search was more specified by just enable The windows 7 operating system. And the result was the number of downloads from the keylogger was uploaded to the site, if the keylogger is available on downloads.com.

Download.cnet.no provides free downloads of safe, trusted, and secure Windows software.

3. The last criteria is downloads from sourceforge.net. The measurement is from user ratings at sourceforge.org. Users are rating after ease, features, design and support. SourceForge is also a web-based source code repository. Sourceforge acts as a centralized location for software developers to control and manage free and open source software development.

Table 4.2: Statistics of the most important trail versions of keyloggers for Microsoft Windows 7

Keyloggers	Google search	Download.com	Sourceforge.net
Armadax keylogger	516,000 hits	780,066	
Actual Keylogger	460,000 hits	447,866	
REFOG keylogger	224,000 hits	156,256	
Family keylogger	185,000 hits	270,271	
Argos keylogger	80,000 hits	1,032,631	
Myjad keylogger	79,000 hits	235	
System Surveillance Pro	51,900 hits	1,032,631	
Pykeylogger	23,200 hits		4.0 of 5

4.3 Linux Ubuntu 12.04 keyloggers

Here is the testing of Linux Ubuntu 12.04 server and Linux Ubuntu 12.04 desktop. The pykeylogger for Linux Ubuntu 12.04 need a graphical user interface(GUI), so Linux Ubuntu 12.04 desktop was implemented to test this keylogger. Table 4.3 on page 48 refers to the software keylogging tools for Unix-Linux based systems. All keylogger are tested on the physical environment bare-metal. The virtual environments: Xen, VMware ESXi, KVM and Virtual Box.

4.3.1 Logkeys 0.1.1a

The output file was set by the user to: */tmp/logkeys.log*
The given test was created to see whether the keylogger logged special keys as backspace and the "Alt Gr" special key:
The test was:

```
echo the passworddd(2*backspace) is keylogger (enter)
echo the mail is keylogger@test.com(enter)
cat "/tmp/logkeys.log"
```

- **Bare-metal**

  Typing commands through the terminal in Linux Ubuntu 12.04:
  logkeys -s -o /tmp/logkeys.log

Typing the test:
Results:

```
Logging started ...
2014-05-16 15:16:57+0200 > echo the is passworddd<BckSp><BckSp> id keylogger
2014-05-16 15:17:07+0200 > echo the mail is keylogger<AltGr>@test.com
2014-05-16 15:17:17+0200 > cat<RShft>/tmp<RShft>/logkeys.log
```

Typing through a remote ssh-connection with putty to a bare-metal machine:
logkeys -s -o /tmp/logkeys.log
Typing the test:
Results:

```
Logging started ...
2014-02-15 17:50:15+0200 >
```

- **Xen**

Typing through the terminal in Linux Ubuntu 12.04:
logkeys -s -o /tmp/logkeys.log
Typing the test:
Results:

```
" "(empty)
```

Typing through a remote ssh-connection with putty to a Linux Ubuntu 12.04:
logkeys -s -o /tmp/logkeys.log
Typing the test:
Results:

```
Logging started ..., 2014-02-19 20:49:45+0100 >
" "(empty)
```

- **KVM**

Typing via the console window from the Linux application *virtual machine manager*:
logkeys -s -o /tmp/logkeys.log Typing the test:
Results:

```
2014-05-05 17:05:58+0200 > echo the passworddd<BckSp><BckSp> is keylogger
2014-05-05 17:05:59+0200 > echo the mail is keylogger<AltGr>@test.com
2014-05-05 17:05:59+0200 > cat <RShft>/tmp<RShft>/logkeys.out
```

Typing through the terminal in Linux Ubuntu 12.04:
logkeys -s -m no.map -o /tmp/logkeys.log
Typing the test:
Results:

```
Logging started ..., 2014-02-19 20:49:45+0100 >
```

- **VMware ESXi**

Typing via the graphical user interface(GUI) through the vSphere client from a client machine:
logkeys -s -o /tmp/logkeys.log
Typing the test:
Results:

```
Logging started ...\\
2014-05-05 17:05:58+0200 > <LCtrl><LAlt>q|su esq iå??
   uw???<BckSp><BckSp> y? fqrguaaqw
2014-05-05 17:06:27+0200 > esq iå<BckSp><BckSp>xåyfg<BckSp>
<BckSp>g y? eq<BckSp><BckSp>fqrguaaqw<AltGr>@eq?ev|ux
2014-05-05 17:06:46+0200 > f<BckSp>f<BckSp>guaf<Tab>
```

yping via a remote ssh-connection through putty to the ESXi client:
logkeys -s -o /tmp/logkeys.log
Typing the test:
Results:

```
Logging started ...
" "(empty file)
```

- **VirtualBox**

  Typing in through a local connection through the Virtual Box manager:
  logkeys -s -o /tmp/logkeys.log
  Typing the test:
  Results:

```
Logging started ...
2014-02-19 20:49:45+0100 > echo the passworddd<BckSp><BckSp> is keylogger
2014-02-19 20:49:55+0100 > echo the mail is keylogger<AltGr>@test.com
2014-02-19 20:50:10+0100 > cat <RShft>/home<RShft>/stiyst<RShft>/logkeys.out
```

  Typing via ssh-connection through putty:
  logkeys -s -o /tmp/logkeys.log
  Typing the test:
  Results:

```
Logging started ..., 2014-02-19 20:49:45+0100 >
" "(empty file)
```

4.3.2 Linux Kernel KeyLogger

The output file was default set to: */dev/klg*
The given test was created to see whether the keylogger logged special keys as backspace and the "Alt Gr" special key:
The test was:

```
echo the passworddd(2*backspace) is keylogger (enter)
echo the mail is keylogger@test.com(enter)
cat "/tmp/linuxkernel.log"
```

- **Bare-metal**

  Typing commands through the terminal in Linux Ubuntu 12.04:
  Starting command:
  bash klg_load.sh
  Typing the test:
  Results:

```
echo the password is keylogger\\
the mail is keylogger2test.com\\
cat 7dev7klg
```

Typing through a remote ssh-connection with putty to a bare-metal machine:
Starting command:
bash klg_load.sh
Typing the test:
Results:

```
" "(empty file).
```

- **Xen**
  Typing through the terminal in Linux Ubuntu 12.04:
  bash klg_load.sh
  Typing the test:
  Results:

```
Loading module ..
NOT WRITING TO FILE
```

  Typing through a remote ssh-connection with putty to a Linux Ubuntu 12.04:
  The linux key logger gives a error message to the user when installing the program:

```
bash Makefile
Makefile: line 1: syntax error near unexpected token ‘$(KERNELRELEASE),’
Makefile: line 1: ‘ifneq ($(KERNELRELEASE),)’
```

- **KVM**

  Typing through the terminal in Linux Ubuntu 12.04:
  The linux key logger gives a error message to the user when installing the program:

```
Loading module ..
 NOT WRITING TO FILE
```

  Typing via the console window from the Linux application *virtual machine manager*:
  bash klg_load.sh
  Typing the test:
  Results:

```
" "(empty file).
```

- **ESXi**

  Typing via the graphical user interface(GUI) through the vSphere client from a client machine:
  bash klg_load.sh
  Typing the test:
  Results:

```
echo the password is keylogger
the mail is keylogger2test.com
cat 7dev7klg
```

Typing via a remote ssh-connection through putty to the ESXi client:
Start command:
bash klg_load.sh
Typing the test:
Results:

```
" "(empty)
```

- **Virtual Box**

  Typing in through a local connection through the Virtual Box manager:
  Start command:
  bash klg_load.sh
  Typing the test:
  Results:

```
  " "(Empty logfile)
```

  Typing via ssh-connection through putty:
  Start command:
  bash klg_load.sh
  Typing the test:
  Results:

```
 " "(Empty logfile)
```

4.3.3 LKL version 0.1.1

The output file was set by the user to:
/tmp/lkl.log
First of all, lkl user space keylogger needs a keymap file.
The given test was created to see whether the keylogger logged special keys as backspace and the "Alt Gr" special key::

```
The test was:
echo the passworddd(2*backspace) is keylogger (enter)
echo the mail is keylogger@test.com(enter)
```

- **Bare-metal**

  Typing commands through the terminal in Linux Ubuntu 12.04:
  Starting command:
  lkl -l -k no.map -o /tmp/lkl.log
  Typing the test:
  Results:

```
Started to log port 0x60. Keymap is no.map.
unable to find keymap-file: No such file or directory
unable to find UPPER case keymap file, check it!
" "(Empty logfile)
```

Typing through a remote ssh-connection with putty to a bare-metal machine:
Starting command:
lkl -l -k no.map -o /tmp/lkl.log
Typing the test:
Results:

```
Started to log port 0x60. Keymap is no.map. The logfile is /tmp/lkl.log
unable to find keymap-file: No such file or directory
unable to find UPPER case keymap file, check it!
" "(Empty logfile)
```

- **Xen**

Typing through a remote ssh-connection with putty to a Linux Ubuntu 12.04:
Starting command:
lkl -l -k keymaps/it_km -o /tmp/lkl.log
Typing the test:
Results:

```
Started to log port 0x60. Keymap is keymaps/it_km.
 " "(Empty logfile)
```

Typing through the terminal in Linux Ubuntu 12.04:
Starting command:
lkl -l -k keymaps/it_km -o /tmp/lkl.log
Typing the test:
Results:

```
Started to log port 0x60. Keymap is no.map.
 " "(Empty logfile)
```

- **KVM**

Typing through the terminal in Linux Ubuntu 12.04:
lkl -l -k no.map -o /tmp/lkl.log
Typing the test:
Results:

```
Started to log port 0x60. Keymap is no.map.
 " "(Empty logfile)
```

Typing via the console window from the Linux application *virtual machine manager*:
Starting command:
lkl -l -k no.map -o /tmp/lkl.log Typing the test:
Results:

```
Started to log port 0x60. Keymap is no.map.
 " "(Empty logfile)
```

- **ESXi**

  Typing via the graphical user interface(GUI) through the vSphere client from a client machine:
  Starting command:
  lkl -l -k no.map -o /tmp/lkl.log
  Typing the test:
  Results:

```
Started to log port 0x60. Keymap is no.map. The logfile is /tmp/lkl.log
unable to find keymap-file: No such file or directory
unable to find UPPER case keymap file, check it!
 " "(Empty logfile)
```

  Typing via a remote ssh-connection through putty to the ESXi client:
  Starting command:
  lkl -l -k no.map -o /tmp/lkl.log
  Typing the test:
  Results:

```
Started to log port 0x60. Keymap is no.map. The logfile is output /tmp/lkl.log
unable to find keymap-file: No such file or directory
unable to find UPPER case keymap file, check it!
" "(Empty logfile)
```

- **VirtualBox**

  Typing in through a local connection through the Virtual Box manager:
  First create the output file:
  Starting command:
  lkl -l -k keymaps/it_km -o /tmp/lkl.log
  Typing the test:
  Results:

```
Started to log port 0x60. Keymap is keymap/it_km. The logfile is /tmp/lkl.log
After entering the test, the outputfile is empty.
```

  Typing via ssh-connection through putty:
  First create the output file:
  Starting command:
  lkl -l -k keymaps/it_km -o /tmp/lkl.log
  Typing the test:
  Results:

```
Started to log port 0x60. Keymap is keymap/it_km.
The logfile is /tmp/lkl.log
After entering the test, the outputfile is empty.
```

4.3.4 THC-vlogger

Problem with the compiling and installation.
There is insmod problems. insmod is a simple program to insert a module into the Linux kernel. The output file was set to: */tmp/thc.log*

- **Bare-metal**

  Typing commands through the terminal in Linux Ubuntu 12.04:
  Typing the test:
  Results:

```
 ./vlogctrl load
insmod: can't read '-q': No such file or directory
```

  Typing through a remote ssh-connection with putty to a bare-metal machine:

```
  ./vlogctrl load
configure: line 25: /proc/ksyms: No such file or directory
Where is the linux source build directory [/lib/modules/3.2.0-58-generic/build]:
```

- **Xen**
  Typing through a remote ssh-connection with putty to a Linux Ubuntu 12.04:

```
 ./vlogctrl load
configure: line 25: /proc/ksyms: No such file or directory
Where is the linux source build directory [/lib/modules/3.2.0-58-generic/build]:
insmod: can't read '-q': No such file or directory
```

  Typing through the terminal in Linux Ubuntu 12.04:

```
 ./vlogctrl load
configure: line 25: /proc/ksyms: No such file or directory
Where is the linux source build directory [/lib/modules/3.2.0-58-generic/build]:
 ./vlogctrl load
insmod: can't read '-q': No such file or directory
```

- **KVM**

  Typing through the terminal in Linux Ubuntu 12.04:

```
 ./vlogctrl load
./configure: 1: ./configure: cannot open /proc/ksyms: No such file
-en Where is the linux source build directory [/lib/modules/3.2.0-57-virtual/build
```

Typing via the console window from the Linux application *virtual machine manager*:

```
 ./vlogctrl load
./configure: 1: ./configure: cannot open /proc/ksyms: No such file
-en Where is the linux source build directory [/lib/modules/3.2.0-57-virtual/build]:
```

- **ESXi**

  Typing via the graphical user interface(GUI) through the vSphere client from a client machine:

```
 ./vlogctrl load
./configure: 27: cannot open /proc/ksyms: No such file
-en Where is the linux source build directory [/lib/modules/2.6.32-38-generic-pae/build]:
```

  Typing via a remote ssh-connection through putty to the ESXi client:

```
 ./vlogctrl load
./configure: 27: cannot open /proc/ksyms: No such file
-en Where is the linux source build directory [/lib/modules/2.6.32-38-generic-pae/build]:
```

- **VirtualBox**

  Typing in through a local connection through the Virtual Box manager:

```
 ./vlogctrl load
  ./configure: 1: cannot open /proc/ksyms: No such file
  -en Where is the linux source build directory [/lib/modules/3.8.0-39-generic/build]:
```

  Typing via ssh-connection through putty:

```
 ./vlogctrl load
insmod: can't read '-q': No such file or directory
```

4.3.5 PyKeylogger 1.2.1

PyKeylogger 1.2.1 for Linux Ubuntu 12.04 desktop. The python keylogger uses Xlib, that means that you must have an X connection to monitor the state of the keyboard. This is why Linux Ubuntu 12.04 desktop is installed. The output file was default files in the directory named logs, in the pykeylogger-1.2.1 directory.

The given test was created to see whether the keylogger logged special keys as backspace and the "Alt Gr" special key::
Command for read the output file:
cat logs/detailed_log/logfile.txt
The start command where:
python keylogger.pyw The test was:

```
echo the passworddd(2*backspace) is keylogger (enter)
echo the mail is keylogger@test.com(enter)
```

- **Bare-metal**
  Typing commands through the terminal in Linux Ubuntu 12.04:
  Typing starting command for the keylogger:

  Results:

  ```
  20140420|2323|
   /home/user1/pykey/pykeylogger-1.2.1|[KeyName:Return]echo the
    passworddd[KeyName:BackSpace][KeyName:BackSpace]is
     keylogger[KeyName:Return]the mail is
      keylogger[KeyName:[AltGr]]2test.com[KeyName:Return]
  ```

  Typing through a remote ssh-connection with putty to a bare-metal machine:

  Typing starting command for the keylogger:
  Results:

  ```
   " "(Empty logfile).
  ```

- **Xen**
  Logging in remotely through a GUI and using the terminal:

  Typing starting command for the keylogger:
  Results:

  ```
  20140313|1149|
   /home/user/pykey/pykeylogger-1.2.1|[KeyName:Return]
   ecdc[KeyName:BackSpace][KeyName:BackSpace]ho the[KeyName:BackSpace]
    is keylogger[KeyName:Return]the mail is
     keylogger[KeyName:Control_L]
    [KeyName:Alt_R]
     [KeyName:Shift_L]@[KeyName:Control_L]
    [KeyName:Alt_R]test.com
  ```

  Typing through a remote ssh-connection with putty to a Xen machine:
  Typing starting command for the keylogger:
  Results:

  ```
    " "(Empty logfile).
  ```

- **KVM**

  From remotely ssh-connection:
  Typing starting command for the keylogger:
  Results:

```
" "(Empty logfile).
```

  Starting command from Virtual Machine Manager:
  Typing starting command for the keylogger:
  Results:

```
20140407|0915|
   /home/user1/pykey/pykeylogger-1.2.1|[KeyName:Return]echo the
    passworddd[KeyName:BackSpace][KeyName:BackSpace]is
     keylogger[KeyName:Return]the mail is
      keylogger[KeyName:[65027]]2test.com[KeyName:Return]
```

- **ESXi**

  From vSphere console:
  Results:

```
20140405|1502|
 /home/user1/pykey/pykeylogger-1.2.1|[KeyName:Return]echo the
  passworddd[KeyName:BackSpace][KeyName:BackSpace]is
   keylogger[KeyName:Return]the mail is
    keylogger[KeyName:[65027]]2test.com[KeyName:Return]
```

  Starting command from a ssh connection:
  Results:

```
" "(Empty logfile).
```

- **Virtual Box**

  Local connection to the console into the virtual machine:

```
20140313|1106|
 /home/user1/pykey/pykeylogger-1.2.1|[KeyName:Return]echo the
  passworddd[KeyName:BackSpace][KeyName:BackSpace]is
   keylogger[KeyName:Return]the mail is
    keylogger[KeyName:[65027]]2test.com[KeyName:Return]
```

  Via ssh-connection:

```
" "(Empty logfile).
```

4.4 Summary of Linux Ubuntu 12.04 keyloggers

The interpreting of the tables for Linux Ubuntu are divided in:

- 0 = The keylogger does not work and have issues to interpret on the current Operating System.
- 1 = The keylogger does work, capture every single key-stroke on the current Operating System(user-based). but not incoming SSH connections.
- 2 = The keylogger does work and capture every key stroke on the current Operating System(Kernel-based). This include the incoming SSH connections.

Table 4.3: Software Keylogging for Linux Ubuntu 12.04

Keyloggers	Bare-metal	KVM	Xen	ESXi	Virtual Box
Logkeys-0.1.1a	1	1	0	1	1
Linux Kernel Key Logger	1	0	0	1	0
lkl	0	0	0	0	0
THC-vlogger	0	0	0	0	0
Pykeylogger-1.2.1	1	1	1	0	1

4.5 Microsoft Windows 7 keyloggers

Here is the testing of Microsoft Windows 7, the keyloggers logs from a application point of view. The keyloggers do not see the kernel, and only from the grafical user interface. That means that the keylogger not are interpreting the keyboard from the hardware, so the under lying technology or virtual environment doesn't mater. Table 4.4 on page 50 refers to the software keylogging tools for Microsoft Windows 7.
Table 4.4 on page 50 refers to the software keylogging tools for Microsoft Windows systems.
The test was performed equally in all environments. The environments was: Bare-metal, Xen, KVM, Vmware ESXi and Virtual Box.
It seams to be the same output for all five environments:
Test in Windows 7: typed in notepad:

```
echo the passworddd(2*backspace) is keylogger (enter)
the mail is keylogger@test.com(enter)
```

4.5.1 pykeylogger-.1.2.1

After typing in the test in notepad, the result was:

```
20140502|0927|noprocname|393684|group41|Untitled - Notepad|echo the
 passworddd<Backspace><Backspace> is keylogger[KeyName:Return]
 the mail is keylogger[KeyName:Lcontrol][KeyName:Rmenu]@test.com[KeyName:Return]
```

4.5.2 Myjad Keylogger Pro 2.30

After typing in the test in notepad, the result was:

```
" "(empty)
```

4.5.3 Ardamax keylogger 4.1

After typing in the test in notepad, the result was:

```
The password is keylogger the mail is keylogger2test.com
```

4.5.4 Actual Keylogger 3.2

After typing in the test in notepad, the result was: Keystrokes from the log file;

```
\verb@[@SKIFT \verb@]@The passworddd\verb@[@BkSp\verb@]@\verb@[@BkSp] is keylogger[enter]
the password is keylogger
\verb@[@Enter\verb@]@
```

4.5.5 REFOG keylogger

After typing in the test in notepad, the result was:

```
echo the password is keylogger
the mail is keyloggertest.com
```

4.5.6 Family Keylogger

After typing in the test in notepad, the result was:

```
echo the password is keylogger
the mail is keyloggertest.com
```

4.5.7 System Surveillance Pro version 7.2

After typing in the test in notepad, the result was:

```
echo the password is keylogger
the mail is keyloggertest.com
```

4.5.8 Argos monitoring

After typing in the test in notepad, the result was:

```
echo the password is keylogger
the mail is keyloggertest.com
```

4.6 Summary of Microsoft Windows 7 keyloggers

The interpreting of the tables for Microsoft Windows 7 are divided in:

- 0 = The keylogger does not work and have issues to interpret on the current Operating System.
- 1 = The keylogger does work, but not capture every single key-stroke on the current Operating System(user-based).
- 2 = The keylogger does work and capture every key stroke on the current Operating System(kernel-based). This include the incoming openSSH connections.

Keyloggers	Bare-metal	KVM	Xen	ESXi	Virtual Box
Pykeylogger 1.2.1	1	1	1	1	1
Ardamax	1	1	1	1	1
Actual Keylogger 3.2	1	1	1	1	1
Myjad 2.0	0	0	0	0	0
REFOG	1	1	1	1	1
Family-keylogger v5.58	1	1	1	1	1
System Surveillance Pro	1	1	1	1	1
Agros monitoring	1	1	1	1	1

Table 4.4: Software Keylogging in Microsoft Windows 7

4.7 Unexpected experiences when testing

Expected aunexpected experiences will occur other applications when testing the keyloggers. The results is listen is this result section, but here is a list of unexpected experiences while testing keyloggers in different environment.

1. Remote desktop Protocol(RDP)into a virtual machine on Xen When opening a Windows 7 virtual machine using Xen, through the operating system Microsoft Windows 7, some unexpected happens.
   After starting the windows 7 virtual machine through the remote desktop protocol(RDP) and starting the keylogger "Ardamax" on the

virtual machine, every keystroke on that virtual machine was logged as expected, but also from the clip board on the local computer the virtual machine is viewed from.
Expected and maybe unexpected experiences will occur other applications when testing the keyloggers.
In the options for the remote desktop connection(RDP) one can choose the devices and resources that want to be used to the remote session such as Printers and clipboard.

4.8 Visibility for keyloggers for Linux Ubuntu 12.04

On a linux host one don't have to have root privileges to monitor the running processes.

Table 4.5: Visibility on keyloggers for Linux Ubuntu 12.04

The interpreting of the tables are divided in:

- X = The keylogger is not working or have issues with the distribution
- 0 = The keylogger is not visible.
- 1 = The keylogger is visible

Keylogges	PS AUX
Pykeylogger-1.2.1	1
Logkeys-0.1.1a	1
LKL Linux KeyLogger	1
lkl	1

4.9 Visibility for keyloggers for Microsoft Windows 7

Table 4.6: Visibility on keyloggers for Microsoft Windows 7

The interpreting of the tables are divided in:

- X = The keylogger is not working or have issues with Windows 7
- 0 = The keylogger cannot be invisible.
- 1 = The keylogger can be invisible

Keylogges	Task Manager	Hidden icons in Windows
Pykeylogger	0	0
Armadax	0	1
Actual Keylogger 3.2	0	1
Myjad 2.30	1	1
REFOG keylogger	0	0
Family-keylogger v5.58	0	0
System Surveillance Pro	1	1
Argos monitoring	1	1

4.10 Time-stamps for keyloggers for Linux Ubuntu 12.04

The problem was: "Analyze to what extent time-stamp for keyloggers can be used to establish a time-line of the events taking place."
This to check if a commands is manually entered or running by a script.
For Linux Ubuntu 12.04 environments:
This is for keylogger that works.

- Logkeys:
  Take timestamps every time the user push the enter button.
- Linux kernel key-logger:
  The output file /dev/klg does not take consideration to the timestamp for key strokes.
- Pykeylogger for Linux The output file in pykeylogger collects keystrokes only every minute.
- THC-vlogger The keylogger does not work in Linux Ubuntu 12.04

4.11 Time-stamps for keyloggers for Microsoft Windows 7

The problem was: "Analyze to what extent time-stamp for keyloggers can be used to establish a time-line of the events taking place."
This to check if a commands is manually entered or running by a script.

- Armadax:
  Take timestamps every minute.
- PyKeylogger:
  Take timestamps every minute.
- System Surveillance Pro:
  Take timestamps when each section starte, and give us the total time for the operation.
  For instance a start time of an notepad operation: 11.05.2014 12:53:29

4.12 Honeypot monitoring of SSH attacks using Kippo

The medium interaction SSH honeypot Kippo was used as described in the approach chapter. Kippo includes close interactions with hackers and are designed to log timestamps, manually attacks and the keystrokes performed by the attacker when the attacker had successful managed to log

into the honeypot. Kippo was installed on two Linux Ubuntu Servers at HiOA and on two virtual machines running at HiOA with public IPs. Four machines running Kippo to get an wide specter of different results. The kippo installation is described in appendix C. By adding two users: admin with password admin and test with the password test, additional to the default user: root with the password 123456, the grade of more successful attacks would increase. The log attempt where collected in a log file, on the machine where Kippo was installed. Some log attempts where extracted before and after a succeeded attack: In table 4.7 is taken from the log file for IP 192.39.120.54. In table 4.8 is taken from the log file for IP 192.39.120.56.

Table 4.7: Log attempt in Kippo on *IP 192.39.120.54*

Timestamp	Attackers IP	Username	Password	State
2014-04-08 14:44:39	116.10.191.219	root	rootpass	failed
2014-04-08 14:44:40	116.10.191.219	root	admin123	failed
2014-04-08 14:44:40	116.10.191.219	root	123456	succeeded
2014-04-08 14:44:40	116.10.191.219	root	administrator	failed
2014-04-08 14:44:40	116.10.191.219	root	asdf1234	failed
2014-04-08 14:44:41	116.10.191.219	root	nihaoma	failed
2014-04-08 14:44:41	116.10.191.219	root	12345	failed
2014-04-08 14:44:41	116.10.191.219	root	100000	failed
2014-04-08 14:44:41	116.10.191.219	root	qwer1234	failed
2014-04-08 14:44:41	116.10.191.219	root	cisco	failed
2014-04-08 14:44:42	116.10.191.219	root	qwe.123	failed
2014-04-08 14:44:42	116.10.191.219	root	19885510	failed
2014-04-08 14:44:42	116.10.191.219	root	master123	failed
2014-04-08 14:44:42	116.10.191.219	root	q1w2e3	failed

Table 4.8: Log attempt in Kippo on *IP 192.39.120.56*

Timestamp	Attackers IP	Username	Password	State
11.05.2014 09:00:45	61.174.51.220	root	qwe.123	failed
11.05.2014 09:00:45	61.174.51.220	root	19885510	failed
11.05.2014 09:00:46	61.174.51.220	root	q1w2e3	failed
11.05.2014 09:00:47	61.174.51.220	root	258258	failed
11.05.2014 09:00:47	61.174.51.220	root	qianyue269	failed
11.05.2014 09:00:48	61.174.51.220	root	adminadmin	failed
11.05.2014 09:00:48	61.174.51.220	root	tweenion	failed
11.05.2014 09:00:49	61.174.51.220	root	master	failed
11.05.2014 09:00:49	61.174.51.220	root	daokers	failed
11.05.2014 09:00:50	61.174.51.220	root	qwe.123	failed
11.05.2014 09:00:50	61.174.51.220	admin	admin	succeeded
11.05.2014 09:00:50	61.174.51.220	root	19885510	failed
11.05.2014 09:00:51	61.174.51.220	root	master123	failed
11.05.2014 09:00:51	61.174.51.220	root	q1w2e3	failed

Two successfully attacks where extracted to show what the hackers interaction on the Kippo server. The two examples below contain the detailed version of the login attempt in table 4.7 and in table 4.8.

1. Attack 1 on *IP 192.39.120.54*

   An extracted short version of the attack:
   2014-04-08 14:44:40 [116.10.191.194] login attempt [root/123456] succeeded
   2014-04-08 14:44:40 [116.10.191.194] root authenticated with password
   2014-04-08 14:44:41 [116.10.191.194] starting service ssh-connection
   2014-04-08 14:44:41 [116.10.191.194] got channel session request
   2014-04-08 14:44:41 [116.10.191.194] channel open
   2014-04-08 14:44:41 [116.10.191.194] asking for subsystem "sftp"
   2014-04-08 14:44:42 [116.10.191.194]
   2014-04-08 14:44:42 [116.10.191.194] failed to get subsystem
   2014-04-08 14:44:42 [116.10.191.194] remote close

2. Attack 2 on *IP 192.39.120.56*

   An extracted short version of the attack:
   11.05.2014 09:00:50 [116.10.191.208] login attempt [admin/admin] succeeded
   11.05.2014 09:00:50 [116.10.191.208] admin authenticated with password
   11.05.2014 09:00:51 [116.10.191.208] starting service ssh-connection
   11.05.2014 09:00:51 [116.10.191.208] got channel session request
   11.05.2014 09:00:51 [116.10.191.208] channel open
   11.05.2014 09:00:51 [116.10.191.208] asking for subsystem "sftp"
   11.05.2014 09:00:52 [116.10.191.208]
   11.05.2014 09:00:52 [116.10.191.208] failed to get subsystem
   11.05.2014 09:00:52 [116.10.191.208] remote close

Chapter 5

Analysis

The different keyloggers are analyzed after the implementation and results from testing in the different environments.
This Analysis of the keyloggers take the consideration of analysis if the current keylogger, timestamps, visibility and other features.
Detecting a keylogger is not simple. It can be installed in many places on the computer, usually in one of the system files. There is a much easier way to detect if a keylogger is running. Right click the desktop's task bar and click Task Manager.
Keyloggers are very difficult to detect and defend.
One big features on the key loggers today, it that keystrokes i being sending to a given user by mail, if the keylogger is installed on a other host for detection. That give problems because sending the key strokes over an network can also be detectable for the attackers.

In todays computer network society there are several options for keyloggers to download for Linux Ubuntu and Windows 7 systems. The keyloggers available Linux Ubuntu keyloggers are listed in table4.1 on page 36 and keyloggers availible for Microsoft Windows 7 are listed in 4.2 on page 37. The analyse of keyloggers consist of specific information, where the output log file is saved, visibility and timestamps for current keyloggers.

5.1 Linux Ubuntu keyloggers

In the result chapter two statistics give us a wider overview over the most important keylogger available today. Linux Ubuntu keyloggers in table 4.1 on page 36 For Linux Ubuntu keyloggers one important measurement was if the keylogger gave many hits on google.com and was available under different download pages.

- **Logkeys**
  The keylogger "logkeys" dont have so many google hits, but are available for download under github and under Ubuntu Software

Center. "logkeys" is a easy keylogger to install and run. This is the only keylogger that one don't have to compile and configure in the installation process. That means the use of "apt-get install logkeys" as a administrator to install the keylogger.
Logkeys take date- and time-stamps every time the user push the enter button, but the timestamp is only for every minute. The keylogger "logkeys" are visible in the process list on the system.
Logkeys log keystrokes in: bare-metal, KVM, VMware ESXi and Virtual Box on Ubuntu server, but not incoming ssh-connections for any of the environments.
Logkeys will not log keystrokes from a Xen environment. This could be because Xen operate with a hypervisor type2 showed in table 2.2 on page 19. On Xen the hypervisor delegate resources to multiple operating systems to be executed on the same computer hardware at the same time. The hypervisor is built on existing operating system, and means several levels between the virtual machine av the hardware.
Take timestamps every time the user push the enter button. Logkeys log all keystrokes, even the back space to a pre defined file on the disk.
The sign "@" is translated as <*AltGr*>@ and the sign "/" as <*RShft*>/
For VMware ESXi trough the graphical user interface the input text is with stange sign and letters that not make sense. In the virtual environments: Xen, KVM and Virtual Box, logkeys create the output file, and start the timestamps, but logkeys will not log the entered keys.

- **Linux kernel keylogger**
  The Linux kernel keylogger have most google.com hits of this papers evaluated keyloggers. The keylogger not available on the downloaded locations. Only from the homepage for the keylogger. After stopping the keylogger with "bash klg_unload.sh, the module will be removed, and the device */dev/klg* will also be removed. The output file */dev/klg* saving keyboard strokes to an in memory buffer. The buffer is limited size and cyclic, so that not to consume your memory.
  The Linux kernel keylogger don't log backspaces or special character. Instead of logging the sign "@" the keylogger logs "2" and instead of the sign "/" the keylogger interpret it as the digit 7. That means that the keylogger only log the main letter or digit on a key, not the signs where you have to press two keys to get a special character.
  It logs the keystrokes with year, month, day and timestamps: *2014-03-21 16:43:18+0100*. In Xen is's not creating the output file, but instead gives a error message to the user.

- **LKL**
  The keylogger "LKL" don't have so many google hits. "LKL" are available for download under sourceforge. LKL have configuration prob-

lems on todays operating system and technologies. It's keymap configuration is rather awkward for a range of users.

- **THC-vlogger**
  To old and not updated keylogger. THC-vlogger receiving low score all around the web and low score of google hits. The THC-vlogger is not available for downloading on famous downloading locations.
- **pykeylogger for Linux Ubuntu 12.04 Desktop**
  The pykeylogger have average hits on the famous search engine google.com. The pykeylogger is available for download on github and sourceforge. This means that it is a attractive keylogger. The pykeylogger for Linux Ubuntu 12.04 only works on the desktop version of Linux Ubuntu 12,04.
  Create its own log file directory for: click images, detailed log and timed screenshots. The timestamp in the log file collect only keystrokes every minute.
  pykeylogger is designed for personal backup purposes, rather than stealth keylogging.
- **Uberkey**
  This keylogger does not work, on Linux Ubuntu 12.04. The keylogger has low score on google.com hits, but are available for download on github.
- **Ttyrpld**
  Ttyrpld have average hits on the famous search engine google.com. The pykeylogger is available for download on source-forge.

5.2 Microsoft Windows 7 keyloggers

In the result chapter gave statistics on windows keylogger that gave us a wider overview over the most important keylogger available today. The statistics for Microsoft Windows 7 was listed in the table 4.2 on page 37.
The interpreting measurements in table 4.4 The Windows keyloggers do not see the kernel, and only from the graphical user interface. That means that it doesn't mater which way the operating system is interpreting the keyboard. The keyloggers does not see in the operating system is build on a bare-metal or any of the virtual technologies under neat.

1. **Myjad keylogger PRO**
   - The trial version of the keylogger does not work in Windows7, as it should. One have to pay the license to get logs out of Myjad keylogger PRO.
   - This keylogger dont have so may hits at google.com, and its the less popular downloaded keylogger in this papers statistics of the most downloaded keyloggers.

2. **Ardamax 4.1**

    - Do not log backspaces, but only finally entered works.
    - Ardamax is not detecting backspace in Xen.
    - A good working keylogger and it is free for a trial period for 7 days.

3. **Actual Keylogger 3.2**

    - Allows you to create a start menu folder
    - Actual are running as hidden in the background.
    - Actual starts automatically records almost all keystrokes.
    - No time stamps
    - Create a own log report if requested.
    - Generated log files can be in encrypted form and the interface can also be protected with password.
    - One can view the reports in form of plain text or in the form of HTML.

4. **MyJad 2.30**

    - It showns to be the same output for all five environments. The environments was: Xen, KVM, Vmware ESXi, Virtual Box and Bare-metal.
    - The trial version of the keylogger will not log the keystrokes.
    - Use its own GUI for showing the log.
    - Myjad can hide and unhide the keylogger with hotkeys.
    - MyJad keylogger always runs in stealth mode.
    - MyJad is primarily designed for personal backup purposes, rather than stealth. keylogging.
    - Do not take timestamps.

5. **Pykeylogger 1.2.1**

    - Pykeylogger is only free keylogger that exist for key logging for windows today.
    - Saves the log file to: Program Files (x86)PyKeylogger
    - Pykeylogger expires after 4 days of use.
    - After downloading the free trail version of PyKeyLogger one have two ways to restore Pykeylogger's functionality.
    - That said, the only way it is visible is that the process name shows up in the task list, so it is not immediately apparent that there is a keylogger on the system.

- Donate to PyKeylogger on the sourceforge.net, and you will get a binary build of PyKeylogger without any nag-screens or expiration, by E-mail, HTTP or FTP.
- Since PyKeylogger is available on sourceforge.net, one can easily download the project source code, the supporting libraries, then find and remove the nag control. Then run PyKeylogger from source, or even build your own executable.

6. **REFOG keylogger**
    - Do not capture every keystroke as for example: @
    - View the log with the hotkeys "Shift+Ctrl+Alt+K"
    - Can give the keylogger a name, for open the keylogger i command promt.
7. **Family-keylogger v5.58**
    - Pressing the CTRL+SHIFT+ALT+F keys restores the tray icon visibility
8. **Argos Monitoring**
    - Argos Monitoring will silently start after restart (it is completely invisible, so you won't find any shortcuts, screens, etc.)
    - One can access the control panel by entering the "interface password" anywhere on your screen. This is the only way to access Argos Monitoring. Argos do not use shortcuts, which ensures that only the installer can access the program and the records.

5.3 Honeypot monitoring of SSH attacks using Kippo

The SSH honeypot was using the fake ssh-server Kippo. The purpose was how to detect a hackers attack timestamp and the interaction of what the hacker are typing.
The experiment where running in the background for four machines over a period, to collect data. Most of the log in attempts faild because of wrong password entering, but a brute force attack will normally try many combinations of password to special usernames. The first username that have been used by the attackers in my test where *root*. My next username: *admin* where also a username that where used.

In the honeypot Kippo one can detect manual and automated attacks, that will scan through a range of public IPs, and try to brute force when finding a remote host that have the SSH-port open as a service. The timestamp in the log file shows us that this is a scanned brute force attack. There are many attempts to one *IP(192.39.129.54)* per second as shown in the table 4.7 and a scanned brute force attack from the same IP to another

IP(192.39.129.54) where kippo where running as shown in table 4.8.

5.3.1 Analyse of the honeypot attacks of SSH attacks using Kippo

This section contains analyse of Kippo after collecting data in the kippo log file, of failed and successful attacks. The servers had many successful log attempts. All successful attempts was doing the same thing. After successfully logging in, the hacker ask in all cases for the application "sftp" that is a short for "secure file transfer protocol". Kippo do not have the sftp application installed by default, so when the hacker get rejected after the request of sftp, the hackers removes the connection. Its difficult to know exactly the purpose of what the hacker wants to achieve with the secure file server "sftp", but the hacker wants to steal the victims data, or upload a script, that can run and do something suspicious.

1. Attack 1
   After succeeded login into Kippo, the attacker starting a service ssh-connection. After getting channel session request, and the channel is opened, the hacker is asking for a subsystem called "stfp". When the honeypot fail to connect to the "stfp" subsystem, the attacker close the connection. All this sequence of incoming commands starts and ends in one second. That means that the attack is automatic generated.

2. Attack 2
   After succeeded login into Kippo, the attacker starting a service ssh-connection. After getting channel session request, and the channel is opened, the hacker is asking for a subsystem called "stfp". When the honeypot fail to connect to the "stfp" subsystem, the attacker close the connection. All this sequence of incoming commands starts and ends in one second. That means that the attack is automatic generated.

Chapter 6

Discussion

In this chapter, both positive and negative aspects will be discussed.
The subject keylogging is an important topic these days. It is not longer only used for malicious purposes but also to log attackers. In web sites, vendors and distributors are announcing keyloggers as a tool that everyone needs. A problem is that they don't mention if a keylogger works in a bare-metal and/or in virtual machines.
To the authors knowledge there are no research papers that have done experiments keylogging in virtual environments before. Regarding the negative results of Linux keyloggers means that to log keystrokes on a computer is a complex and difficult task. It would be even harder to log keystrokes in a virtual environment, since there is an extra abstraction level between the keyboard input of the hardware and the keylogger application, on the top of a system. How can system administrators and researcher use keylogger in a honeypots is a relevant question. In Windows Environments its possible to log keystrokes from the graphical user interface, but not other incoming ports to the system from a remote connection. The same true Linux Keyloggers, the open-source keyloggers that can be downloaded from the Internet can only be used, and not for logging keystrokes for remote connections.
Another topic wheater its safe for users to install a keylogger, without getting monitored by the vendor through the network after the users have installed the software keylogger.
Another question is that its needed to make old keyloggers work in every environments. Two options are available. re-engineer the keyloggers or extend the virtual technology to enable keylogging. The keyloggers or edit and update the virtual technologies, such as the modul KVM or edit hypervisors for virtual technologies.
Some of the Linux keyloggers are not work at all, or do not working in some virtual environments. The problem could be that for executing a keylogger, by starting it at the command-line, require a lot of arguments for the keylogger. Most of the keylogger require the argument device unit and requir a keymap for the input keys. The honeywall CDROM was capable of logging key strokes using Sebek server that was loaded by default. With considerations that Sebek in the honeywall CDROM is old software and

not updated, it was for security issues excluded from this project.
Keyloggers are also used in honeypots. For example, we can log the key strokes of an interactive session even if encryption is used to protect the network traffic.[20]

6.1 Addressing the problem statements

In the introduction chapter the problem statements for this master thesis was listed. In the Approach chapter how to address the problem statements was listed. Here is the discussion how the solution on the problem statements went.

1. `Do a survey on keyloggers on Windows7 and Linux Ubuntu-based systems.`

   A complete survey on keyloggers for Windows7 and Linux Ubuntu-based system is done in the result section. The software keyloggers for Linux Ubuntu 12.04 are summed up in table 4.3 on page 48 and for Microsoft Windows 7 is summed up in table 4.4 on page 50.

2. `Investigate trough experiments how keyloggers function in both bare-metal and different virtual environments and weather they log any keystroke, or only keystrokes from a limited number of applications.`

   The keyloggers are showed in table 4.3 and in table 4.4. Keyloggers are tested in both bare metal and different environments to conclude if there are some differences out there, such as if virtual machines can reads keyloggers.

3. `Analyze to what extent keyloggers can be detected.`

   The visibility on keyloggers are showed in table 4.5 and in table 4.6. If keylogger can be detected the user or attacker easily can stop the keylogging process if administrator or root privilege.
   If the administrator wants to hide the keylogger in a Linux environment, he can easily put the . infront of the directory. or rename the executed process to a not detectable name.

4. `Analyze to what extent time-stamp for keyloggers can be used to establish a time-line of the events taking place.`

   The time-stamps on keyloggers are showed for Linux Ubuntu in section 4.10 and for Windows 7 in section 4.11. Time-stamps are important to know to monitor if the attacks is done manually or entered automatically.

5. `Investigate to what extent the keylogging features of Kippo facilitates the analysis of SSH attacks.`

   With the results in table 4.7 and table 4.8 we can see that keylogging is very important. Keylogging can monitor what the hackers are doing after successfully logging into a system. SSH activity can easily be logged by monitoring the Linux file: */var/log/auth.log*, that

monitor only the attempts by usernames, not detailed log included timestamps and logs if attackers type after successfully logged in. Kippo are giving more relevant information in its log files, for administrators and researches to collect necessary information to detect attack methods. We can here understand that keylogging is a important part of research. By using keylogging in a honeypot will detect attack methods.

6.2 Keylogging in bare-metal technologies

Hosts with operating systems built on bare-metal hardware, do not have issues with interpreting keystrokes with updated keyloggers. New architecture and new operating systems have issues to interpret keystrokes for keyloggers. Old keyloggers was designed for old system architectures, but for using keyloggers in updated versions of operating system and updated architectures, the keylogger also have to be updated.
The distributions for Linux environments are updated and regularly renewed for the sake of new kernel versions, security issues and bug fixes. Keyloggers for Windows environment also have to be updated, in the sequence with the new patches and changing in operating systems architectures.

6.3 Keylogging in virtual technologies

Regarding the results in table 4.3 on page 48 it show that linux keyloggers are interpreting different in virtual environments. This question might be that virtual machines executes on a higher level than the bare-metal environments.
Virtual device drivers represent a particular variant of device drivers. They are used to emulate a hardware device, particularly in virtualization environments. For example, a Xen host. Instead of enabling the guest operating system to dialog with hardware, virtual device drivers take the role and emulate a piece of hardware, so that the guest operating system and its drivers running inside a virtual machine can have the illusion of accessing real hardware.
Attempts by the guest operating system to access the hardware are routed to the virtual device driver in the host operating system. The virtual device driver can also send simulated processor-level events like interrupts into the virtual machine.[2]
Another question might be how to access the keyboard from a virtual machine. The virtual machine is build on a hypervisor, that means that the virtual machine have to go through the hypervisor to fetch keyboard inputs.
One way to access the virtual machine is through a SSH-connection. One can access the virtual machine through virtual machine consoles, via remote desktop protocol(RDP), via a virtual network computing(VNC)-client.

- **Xen** Xen is not directly interpreting the keyboard from the keyboard device driver, and will not capture entered keystrokes. The results of this is showed in table 4.3 on page 48.
- **KVM** Is not directly interpreting the keyboard from the keyboard device driver, and will not capture entered keystrokes. The results of this is showed in table 4.3 on page 48. KVM are using the hypervisor type 2 that is showed in table 2.2 on page 19.
- **VMWare ESXi** VMware are using the vSphere hypervisor that is a free bare-metal hypervisor that virtualizes servers so one can built virtual machines on less hardware.[36]
  The test in table 4.3 on page 48 shows that some keyloggers that works in bare-metal systems, also works in VMware ESXi.
  This could be a possibility by that are not so many levels between the hardware device input/output(I/O) and the installed keylogger on a system.
  VMware ESXi are not using any host operating system. VMware ESXi are using a Type 1 hypervisor there the hypervisor is directly connected to the hardware at the bottom and the guest operating systems at the top. Hypervisor type 1 is showed in table 2.1 on page 19. This could be the reason why VMware ESXi works with keyloggers.
- **VirtualBox** Is not directly interpreting the keyboard from the keyboard device driver, and will not capture entered keystrokes. The results of this is showed in table 4.3 on page 48. Virtual box are using the hypervisor type 2 that is showed in table 2.2 on page 19.
  VirtualBox is interpreting the keyboard in only one of the two, your virtual machine or the rest of your computer can be the owner of the keyboard. The ownership to the keystrokes of the keyboard to your host operating system, Virtual-Box reserves a special key on the keyboard for itself: the "host key". By default, this is the right Control key on your keyboard. One can change this default in the Virtual-box Global Settings.
  In detail, all the keystrokes translates into the keyboard that is owned by the virtual machine if the virtual machine window on your host desktop has the keyboard focus. This means that if you want to type within your virtual machine, click on the title bar of your virtual machine window first.
  While the virtual machine owns the typed keystrokes on the keyboard, some key sequences (like Alt-Tab for example) will no longer be seen by the host, but will go to the guest instead. After you press the host key to re-enable the host keyboard, all key presses will go through the host again, so that sequences like Alt-Tab will no longer reach the guest. For technical reasons it may not be possible for the VM to get all keyboard input even when it does own the keyboard.[31]

6.4 How to make keyloggers work in virtual environments

The question is why keylogging in virtual environments is different from bare-metal environment. Why they not work is a unsolved question. No related works has been done in this area, has been documented at the Internet. In virtual environments there are several considerations such as: different types of hypervisors, different ways the virtual machine interprets the keystrokes.

6.5 Future Work

During the working with keyloggers and honeypots, several problems occur that could be interesting for future work. There will always be unsolved problem around the topic keyloggers and honeypots.
In this research two operating systems where used, Linux Ubuntu 12.04 and Microsoft Windows 7.

1. Check keyloggers in other operating systems and other distributions of Windows and Linux.
   Examples of other popular modern operating systems includes:
   Mac, Android, BSD, iOS, OS X, Windows Phone and z/OS.

2. Testing Windows keyloggers that are commercial, and do not offer free trial versions for downloading.

3. To create and install a keylogger on the host machine that are running a hypervisor type2, for logging the client virtual machines that are build on top of the current hypervisor.

4. To create and install a keylogger inside a virtual machine(VM), and make that keylogger to log keystrokes and capturing data from other virtual machines running on the same hypervisor.

5. To create a keylogger that works on both bare-metal and in every virtual environment.

6. To create a kernel keylogger that log every keystrokes into a host. Such as remote SSH-connection, and other incoming remote connection as well as keystrokes entered by the machine itself.

Chapter 7

Conclusion

Keyloggers are a very important tool within the computer security. Keyloggers are dangerous weapons when doing hacking and for detecting attackers on the other hand. After actually testing different keylogger in different environments, the conclusion is that one keylogger for Linux Ubuntu 12.04 servers works for bare-metal, KVM, VMware ESXi and Virtual Box, but not on Xen. Another keylogger works for bare-metal and VMware ESXi. The desktop version works in bare-metal,KVM, Xen and Virtual Box. VMware ESXi where the hypervisor is operating directly to the hardware do not work on the desktop version. Two of the Linux Ubuntu keyloggers are not updated, so do not work in todays environment. The tests in table 4.3 on page 48 shows that some keyloggers that works in bare-metal systems, also works in VMWare ESXi. This could be the reason why VMware ESXi works with keyloggers. VMware ESXi is using a Type 1 hypervisor where the hypervisor is directly connected to the hardware at the bottom and the guest operating systems at the top. Hypervisor type 1 is showed in table 2.1 on page 19. Virtual technologies that use hypervisor type 2 showed in table 2.2, will not interpret the keystrokes in the same way as type2 hypervisor or bare-metal technology. The keyloggers in Linux Ubuntu server does not work in Xen, KVM and in Virtual Box. Bare-metal has direct connection to the hardware such as a keyboard, And the same for VMware ESXi, that is using a hypervisor directly on a system hardware of interpreting the keystrokes. The other virtual technologies such as Xen and KVM and the virtual software "Virtual Box" are building on a existing operating system, so the keystrokes will not be interpreted in the same way as on bare-metal and VMware ESXi.
Microsoft Windows 7 keyloggers do not see which underlying technology the operating system is running at. Microsoft Windows 7 keyloggers interpret almost every input from the keyboard to the operating system, but not incoming keystrokes to for example OpenSSH.
After testing some important keyloggers, it shows that the keyloggers has a lot of features. As for the trial versions of keyloggers, they are often very limited in functionality and stealthiness.

Bibliography

[1] The Honeynet Project, Know your enemy: Learning about security threats. Addison-Wesley , 2004

[2] http://en.wikipedia.org/wiki/Computer_keyboard, February 2013

[3] Dieter Gollman. "Computer Security ". John. Wiley and Sons, Inc., 2011.

[4] Virtual Honeypots: From Botnet Tracking to Intrusion Detection. Addison Westley, 2008.

[5] Daniel Huluka,"Experiment using Distributed High-Interaction Honeynet(D2H), Oslo University College, Oslo, 2013.

[6] Robert Moore, Cybercrime, Investigating High Technology Computer Crime, Matthew Bender and Company, 2005.

[7] Hafez Barghouthi, Keystroke Dynamics, How typing characteristics differ from one application to another, 2009.

[8] Behaviour Logging Tool, BeLT -verktøy for logging av brukerinterasjoner, Gjøvik, May 2013.

[9] Cormac Herley and Dinei Florencio, How To Login From an Internet Cafe Without Worrying About Keyloggers, Microsoft Research, Redmond, 2006.

[10] http://en.wikipedia.org/wiki/Syslog, April 2014.

[11] Timing Analysis of Keystrokes and Timing Attacks on SSH, Dawn Xiaodong Song,David Wagner, Xuqing Tian ,University of California,Berkeley, April 2014

[12] Kirk P.H. Sullivan, Eva Lindgren, Computer keystroke logging and writing : methods and applications

[13] Samuel Feshazion Afeworki, Comparative Analysis of Network Attacks Against FQDN Using Honeynet, January 2014

[14] Honeywall, http://projects.honeynet.org/, April 2014

[15] Irfan Habib, 2008, Virtualization with KVM, http://www.linuxjournal.com/article/9764, April 2014

[16] http://www.securelist.com/en/analysis/, April 2014

[17] www.linux-kvm.org, "Kernel-based Virtual Machine", April 2014

[18] Daniel J. Barrett, Richard E. Silverman and Robert G. Byrnes, SSH The Secure Shell, The Definitive Guide, 2005

[19] Daniel Cid, "SSH Brute Force" The 10 Year Old Attack That Still Persists, 2013.

[20] http://www.honeyd.org/background.php, Mars 2014.

[21] Andreas M. Antonopoulos,Network World,Honeypots for hacker detection http://www.networkworld.com/columnists/2010/070610antonopoulos.html, 2006

[22] http://en.wikipedia.org/wiki/Hardware_virtualization, 2010.

[23] Bill McCarty, Botnets: big and bigger, EEE SECURITY and PRIVACY, 2003.

[24] Nikolay Grebennikov, Securelist, Keyloggers: How they work and how to detect them, 2007

[25] http://www.ardamax.com/keylogger/, April 2014

[26] Invisible Key Logger [Online]. Available: http://www.invisiblekeylogger.com/ invisible-keylogger.html

[27] http://www.scamwatch.gov.au/content/index.phtml/tag/SpywareKeyloggers

[28] http://en.wikipedia.org/wiki/Virtualization, April 2014

[29] Phrack Inc., Writing Linux Kernel Keylogger, June 19th, 2002

[30] http://www.linuxjournal.com/article/1080 The Linux keyboard driver

[31] https://www.virtualbox.org/manual, April 2014

[32] http://askubuntu.com/questions/14312/how-to-run-logkeys

[33] The keylogger logkeys, http://code.google.com/p/logkeys/

[34] The hacker's choise, http://tch.org.

[35] http://en.wikipedia.org/wiki/Xen, April 2014

[36] "ESX Server Architecture". Vmware.com. Archived from the original on 2009-11-07. Retrieved 2009-10-22.

[37] Detecting Bots Based on Keylogging Activities, Yousof Al-Hammadi and Uwe Aickelin Department of Computer Science and Information Technology, The University of Nottingham

[38] Stefano Ortolain, Cristiano Giuffrida, and Bruno Crispo, Bait your Hook: a Novel Detection Technique for Keyloggers.

[39] pyHook, http://sourceforge.net/, 16 August 2009

[40] http://en.wikipedia.org/wiki/Keystroke_logging, April 2014

[41] http://en.wikipedia.org/wiki/Virtual_keyboard, April 2014

[42] Wm. Arthur Conklin, Gregory White. Principles of Computer Security third edition. 2012

[43] T Armstrong - Netcat - The TCP/IP Swiss Army Knife - 2001

[44] Keyghost, http://www.keyghost.com/sx/, 2009

[45] SSH - somewhat secure Host, Craig Valli , Security Research Institute, Edith Cowan University, Australia, 2012

[46] Daniel Stødle, John Markus Bjørndalen, Otto J. Anshus, Decentralizing the VNC Model for Improved Performance on Wall-Sized, High-Resolution Tiled Displays, 2007

[47] http://searchfinancialsecurity.techtarget.com/news/1294508/Customer-vs-Bank-of-America-Whos-to-blame

[48] http://www.nrk.no/norge/pst-vil-overvake-datatastaturer-1.11583286, 2014

[49] Jinho Hwang,Sai Zeng and Frederick y Wu,Timothy Wood. A Component-Based Performance Comparison of Four Hypervisors, 2013.

[50] http://www.spycop.com/ebookkeylogger.pdf

[51] "Rootkits, Part 1 of 3: The Growing Threat". McAfee. 2006-04-17.

[52] Lee B. and Brooks D., Accurate and efficient regression modeling for microarchitectural performance and power prediction. In Proceedings of the 12th international conference on Architectural support for programming languages and operating systems, New York, USA, 2006.

[53] Craig Valli, PriyaRabadia and Andrew Woodwar, Edith Cowan University ,Security Research Institute Perth, Australia, An Investigation into SSHActivity Using Kippo Honeypots, 2013

[54] George Magklaras Steven Furnell and Maria Papadaki, LUARM ? An audit engine for insider misuse detection, Center for Security, Communications and Networks Research, School of Computing and Mathematics, University of Plymouth

[55] https://wiki.ubuntu.com/LTS, 2013-10-23.

[56] ukessays.com, http://www.ukessays.com/essays/computer-science/server-honeypot-based-detection-for-keylogger-computer-science-essay.php.

[57] Ways to build a honeypot, http://web2.clarkson.edu/projects/itl/honeypot/buildinghon 2011

[58] http://www.securelist.com/en/threats/vulnerabilities?chapter=38, February 2014.

[59] http://virt-manager.org/, April 2014

Appendix A

How to install keyloggers in Linux Ubuntu 12.04

There are many location on the Internet today to download keyloggers and other applications, but not all locations are safe. Especially for Linux keyloggers that are distributed in open-source there users can modify the source code. Hackers can easily modify the source code for a keylogger so that the keystrokes are being sent to the hackers as well.
Here is a list over locations one can download and how to install and compile the current Linux Ubuntu keyloggers.

1. Logkeys 0.1.1a This Linux keylogger can be downloaded by installing logkeys from the ubuntu software center by "sudo apt-get install logkeys" or download the package and compile it as described below.

    - To be sudo on the system:
      sudo su
    - Update, upgrade and install a necessary software one your system:
      apt-get update
      apt-get upgrade
      apt-get install build-essential
    - Download the application:
      wget http://logkeys.googlecode.com/files/logkeys-0.1.1a.tar.gz
    - Open the package:
      gunzip logkeys-0.1.1a.tar.gz
      tar xvf logkeys-0.1.1a.tar
    - Change directory to the extracted directory:
      cd logkeys-0.1.1a
    - Install the keylogger:
      cd logkeys_0.1.1a
      ./configure
      make install

- Start the keylogger:
  logkeys -s -o /tmp/output.log
- Stopp the keylogger:
  logkeys -k
- Look at the created log file:
  cat /tmp/output.log

2. Linux Kernel Key Logger

   - To be sudo on the system:
     sudo su
   - Update and upgrade the system:
     sudo apt-get update
     sudo apt-get upgrade
   - Install required software:
     sudo apt-get install build-essential
   - Download the application:
     Download the file:key-logger.zip from the *http://downloads.sourceforge.net/project/linux*
     site
     or directly with wget and change the output filename:
     wget -O key-logger.zip http://downloads.sourceforge.net/project/linuxkernelkeyl/key-logger.zip?r=http%3A%2F%2Fsourceforge.net%2Fprojects%2Flinuxkernelkeyl%2Ffiles%2Flates
   - unzip the downloaded file:
     unzip key-logger.zip
   - Change directory to the extracted directory:
     cd key-logger
   - Compile and install the keylogger:
     make
     bash Makefile
   - Start the keylogger:
     bash klg_load.sh
   - Stopp the keylogger:
     bash klg_unload.sh
   - Look at the default log file:
     cat /dev/klg

3. LKL version 0.1.1

   - To be sudo on the system. *sudo su*
   - Update, upgrade and install a necessary software one the system:
     apt-get update
     apt-get upgrade
   - Install required software
     apt-get install build-essential

- Download the application:
  wget http://downloads.sourceforge.net/project/lkl/lkl-0.1.1/lkl-0.1.1/lkl-0.1.1.tar.gz
- Unzip the downloaded LKL keylogger:
  gunzip lkl-0.1.1.tar.gz
  tar xvf lkl-0.1.1.tar
- Change directory to the extracted directory:
  cd lkl-0.1.1
- Compile and install the LKL keylogger:
  ./configure
  make
  make install
- Download a proper keymap for your keyboard. My example is for Norway:
  wget http://wiki.logkeys.googlecode.com/git/keymaps/no.map
- Create the output file name:
  touch /tmp/lkl.output
- Test the keylogger:
  ./lkl -l -k keymaps/us_kmUP -o /tmp/lkl.output
- Look at the log:
  cat /tmp/lkl.output

4. PyKeylogger 1.2.1
   This installation work only on desktop versions of Linux.
   - To be sudo on the system:
     sudo su
   - Update and upgrade the system:
     apt-get update
     apt-get upgrade
   - Install required software:
     apt-get install build-essential
     apt-get install python-xlib
     apt-get install python-configobj
     apt-get install python-pyx
     apt-get install python-gtk2
     apt-get install python-imaging
     apt-get install python-tk
   - Download the PyKeylogger source zip archive:
     wget -O pykeylogger-1.2.1_src.zip http://downloads.sourceforge.net/project/pykeylogger/pykeylogger/1.
     1.2.1_src.zip?r=http%3A%2F%2Fsourceforge.net%2Fprojects%2Fpykeylogger%2Ffiles%2Fpykeylogger%2F
     ams

- Unzip the downloaded file:
  unzip pykeylogger-1.2.1-src.zip
- Change directory to the extracted directory:
  cd pykeylogger-1.2.1
- Start the keylogger:
  python keylogger.pyw

5. THC-vlogger

   - To be sudo on the system:
     sudo su
   - Update and upgrade the system:
     apt-get update
     apt-get upgrade
   - Install required software:
     apt-get install build-essential
   - Download the application:
     wget https://www.thc.org/download.php?t=r&f=vlogger-2.1.1.tar.gz
   - Unzip the downloaded file:
     gunzip vlogger-2.1.1.tar.gz
     tar xvf vlogger-2.1.1.tar
   - Change directory to the extracted directory:
     cd vlogger-2.1.1.tar
   - Configuring and compiling:
     ./configure
     make
   - Manually install appropriate paramerters to the vlogger module:
     ./vlogconfig

     (a) Pleace choose magic password for logmode switching(echoed):
     (b) Pleace choose timezone (offset to GMT, from -12 to 13):)
     (c) Pleace choose log method: (local file or network):
     (d) Pleace choose default log mode: (nolog, dumb, smart) :
     (e) In which directory to save the log data:
     (f) Autohide vlogger module after loaded(cannot remove vlogger after that):
   - Start the keylogger:
     ./vlogctrl load
   - Stopp the keylogger:
     ./vlogctrl unload vlogger

Appendix B

From which location to download the keyloggers in Windows 7

There are many different locations on the Internet to download keyloggers from. Most of the locations are safe to download from, but on can also download a modified keylogger from untrusted Internet sites that are modified by hackers or other users with dangerous purposes.
These keylogger versions are commercial, but have a short trial period witch is specified in the background chapter.
It's strait forward to Install Windows keyloggers. Only download the current keylogger, run it by double click it. Than the installation process starts, and users just click next on the upcoming questions. Most of the keylogger uses a setup wizard where it is described what to do, and what will happends.

1. Myjad Keylogger Pro 2.30
   Download the keylogger from:
   http://www.myjad.com/keylogger-pro.html
2. Ardamax keylogger 4.1.2
   Download the keylogger from:
   http://www.ardamax.com/download.html
3. PyKeylogger 1.2.1
   Download the binary(executable) file for sourceForge file servers from:
   http://sourceforge.net/projects/pykeylogger/files/pykeylogger/1.2.1/pykeylogger-1.2.1_win32_installer.exe/download
4. Actual keylogger 3.2
   Download the zip file for the keylogger from:
   http://www.mediafire.com/download/7kf91964kjzy2gy/actualkeylogger.zip
5. REFOG keylogger
   Download the binary file from the *http://www.refog.com/download.html*

site named Keylogger 3-day Trial with the file: *keylogger.exe* from the location:
http://monitoring-software.s3-website-us-east-1.amazonaws.com/?p=rkl&_ga=1.262476559.2050

6. Argos Monitoring 1.65 Download the binary file from argosafe.com
http://argos-monitoring.en.lo4d.com/download/mirror-ex1

7. Family-keylogger v5.58
Download the fkl-setup.zip file:
http://www.kmint21.com/familykeylogger/fkl-setup.zip
And open the zip file with the password "2013" or "2012"

8. System Surverillance - Pro 7.2 Download the binary file from SoftonicDownload site.
http://system-surveillance-pro.en.softonic.com/universaldownloader-launch

Appendix C

How to install Kippo in Linux Ubuntu 12.04

This appendix consist of my experiences for install Kippo on a Linux Ubuntu 12.04. The installation is executed as a normal user on a system and become root only when necessary. Kippo runs normal on port 2222, but to make the kippo attacks realistic, its needed to run Kippo on port 22. If the honeypot machine is running on a remote locate, the administrator needs to connect remotely to the machine through the SSH-port. The SSH-port and the Kippo port can then easily change port nummer.

(a) Update and upgrade the system:
sudo apt-get update
sudo apt-get upgrade

(b) Install required software
sudo apt-get install python-twisted-conch sudo apt-get install python-twisted

(c) Download the application:
wget http://kippo.googlecode.com/files/kippo-0.8.tar.gz

(d) unzip the downloaded file:
tar xfz kippo-0.8.tar.gz

(e) Add iptables rules to a make the attacks easier:
Kippo is by default running on port 2222, so a modification in the iptables rules need to be done to let Kippo run at the default SSH-port 22 instead.
Also otherwise to let the administrator log in at monitor the attacks for remote connection on port 22.
sudo iptables -t nat -A PREROUTING -i eth0 -p tcp –dport 2222 -j REDIRECT –to-port 22
sudo iptables -t nat -A PREROUTING -i eth0 -p tcp –dport 22 -j REDIRECT –to-port 2222

(f) Start kippo from the kippo directory:
./start.sh

(g) Check to log files in
cat /home/your_user_name/kippo-0.8/log/kippo.log