SRM Institute of Science and Technology
Ramapuram Campus
College of Science & Humanities
Department of Computer Science and Applications (MCA)

LAB MANUAL

PCA20D02J CYBER SECURITY

For

P.G. Degree Programme

Batch (2023– 2025)

MCA (1st Semester)

Academic year 2023-24 Odd Semester

Regulations-2020

Prepared By

Dr. S. SUBBAIAH

Approved By

Dr. J. DHILIPAN

INDEX

PCA20D02J CYBER SECURITY LAB MANUAL

LIST OF PROGRAMS

Lab 1 : Cyber security attacks case study Submission

Lab 2: Cyber security attacks case study Submission

Lab 3: TCP scanning using NMAP Port scanning using NMAP

Lab 4 : TCP / UDP connectivity using Netcat

Lab 5: TCP / UDP connectivity using Netcat

Lab 6 : Perform an experiment to demonstrate sniffing of router traffic by using the tool Wireshark

Lab 7: Demonstrate how to provide secure data storage, secure data transmission and for creating digital signatures (GnuPG)

Lab 8: Demonstrate how to provide secure data storage, secure data transmission and for creating digital signatures (GnuPG)

Lab 9: Perform an experiment to sniff traffic using ARP Poisoning

Lab 10: Perform an experiment how to use dumpsec

Lab 11: Perform an experiment how to use dumpsec

Lab 12: Implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) network protocols

Lab13: Setup a honey pot on network

Lab14: Monitor the honey pot on network

Lab15: Demonstrate intrusion detection system (ids) using any tool (snort or any other software)

1: Cyber security attacks case study Submission

Aim: To create case study on Cyber security attacks.

Case Study:

Research and Background Information

Chatter's recent cyber security incident

A staff member left their laptop on the train while commuting home. The laptop was picked up by someone and they were able to gain access to it. Fortunately, the member of staff had reported it missing and the laptop was remotely wiped. Chatter cannot be sure if any data was accessed before the laptop was remotely wiped.

Important Government Regulations

GDPR - General Data Protection Regulation

As of Spring 2018, changes to GDPR came into force, designed to better protect consumer and personal data. Any organisation holding data must:

● Gain consent from the consumer to process their data

● Anonymise the data collected to protect privacy

● Provide data breach notifications

● Safely handle the transfer of data across borders. Transferring data outside Europe. The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third-party countries or international organisations, to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

● Require certain companies to appoint a data protection officer to oversee GDPR compliance. If these rules are not followed, then companies face hefty fines of up to €20million.

PwC's Cyber Security Teams

Core Advisory

We help organisations from all sectors operate securely in the digital world. Our expertise enables clients to resist, detect and respond to cyber-attacks. Our Core Advisory team, works globally to support clients across the public, private and financial sectors, helping them to understand and reduce their cyber risks.

Some of the services offered to clients include:

- Assessing and measuring their exposure to cyber security risk
- Developing a strategy and vision for tackling cyber security
- Designing and implementing the secure IT systems a client needs to be secure
- Designing and putting in place security training and awareness programmes
- Gaining experience of security operations and incident response

Ethical Hackers

The ethical hacking team will work within the boundaries defined to legally penetrate the company with their permission. This exercise is designed to help companies understand their technical security weaknesses, to provide specific recommendations to clients to help them keep hackers out.

- Ethical hacking to expose vulnerabilities in client IT systems
- Identifying and monitoring malicious activity on client networks
- Actively tracking and disrupting cyber threat actors and seeking out new ones
- Investigating networks which attackers have compromised and removing threat actors.

Crisis Team

Cyber crisis team help companies prepare for, respond to and recover from a cyber-security crisis. A crisis may include events that prevent the business from operating.

This team works with their people, to define these plans or understand what work has already been done to prepare for these types of events. The team also facilitate exercises to help companies test their approach, helping the team to practise for real events and can turn up to help you ‘steady the ship’ when under attack.

Benefits of this service include:

● Help companies consider what they would do when under attack. The team may help simulate this and ensure non-technical members of staff know how to respond.

● Help companies to understand and develop key access controls to their critical systems and assets during a crisis or active cyber threat.

● Helping the company to 'steady the ship' when under attack.

Cyber Threat Team

This team tracks and gathers information on cyber threats across the globe that could target the industry or type of company. The team uses various methods to gain a well-rounded view of the company's threat landscape, and can help them to understand those that could be motivated to attack the company.

● Threat intelligence - look into political situations and try and detect threat actors e.g. hacking groups.

● Track and gather intelligence to share with companies.

● Analyse the virus and malware used for information.

Identity and Access Management

Companies often grant access to information and assets to staff even if it is not relevant to that member of staff's role. It is important for companies to follow the principle of least privilege - only granting access to the systems necessary for each member of staff's role. This helps to reduce the risk of attackers gaining access to critical systems by compromising a less protected user account used in another area in the business. If all user accounts only have access to what they need, this should help contain compromises to their area of origin, to help prevent them from spreading throughout the business.

● Help companies to understand who in their company has access to what information

- Help them to improve their governance and management of their access granted throughout the business.

Facebook security breach: upto 50m accounts attacked

Facebook says almost 50 million of its users were left exposed by a security flaw.

The company said attackers were able to exploit a vulnerability in a feature known as “View As” to gain control of people's accounts. The breach was discovered on Tuesday, Facebook said, and it has informed police. Users that had potentially been affected were prompted to re-log-in on Friday.

The flaw has been fixed, wrote the firm’s vice-president of product management, Guy Rosen, adding all affected accounts had been reset, as well as another 40 million "as a precautionary step". Facebook - which saw its share price drop more than 3% on Friday - has more than two billion active monthly users.

The company has confirmed to reporters that the breach would allow hackers to log in to other accounts that use Facebook's system, of which there are many. This means other major sites, such as AirBnB and Tinder, may also be affected. The firm would not say where in the world the 50 million users are, but it has informed Irish data regulators, where Facebook's European subsidiary is based. The company said the users prompted to log-in again did not have to change their passwords. "Since we’ve only just started our investigation, we have yet to determine whether these accounts were misused or any information accessed. We also don’t know who’s behind these attacks or where they’re based. He added: "People’s privacy and security is incredibly important, and we’re sorry this happened." The company has confirmed that Facebook founder Mark Zuckerberg and its chief operating officer Sheryl Sandberg were among the 50 million accounts affected.

Web Link to full article:

https://www.bbc.co.uk/news/technology-45686890

Millions of people could not use their games consoles for a second day as disruption on the Xbox Live and Sony Playstation networks continued after an apparent cyber-attack. A group calling itself Lizard Squad claimed responsibility for bringing down both networks on Christmas Eve, which could have affected nearly 160 million gamers. Even an intervention by eccentric internet entrepreneur Kim Dotcom, who offered the hackers free lifetime use of his file storage service, does not appear to have ended the attack. Known as a distributed denial of service, or DDOS, the attack is overloading the systems of both services by generating fake access requests…..…Sony has not responded to requests for comment. Its official Twitter account repeatedly responded to users’ complaints with the same message, but did not acknowledge an attack:

“We are aware that some users are unable to access at the moment. Our technicians are working to fix this issue.” The official PSN status was listed as “offline” at the time of writing, while Xbox Live is “limited”.

Microsoft would not comment on the cause of network problems but a spokesman told the Guardian: “We are aware some users are unable to sign in to Xbox Live. Our teams are working to resolve the issue. Visitxbox.com/support for status updates.”

The news is damaging for Microsoft but particularly for Sony, which suffered a high profile hack in early December by a group called Guardians of Peace. Stolen emails were leaked and published, revealing embarrassing exchanges between executives and celebrities, while stolen files and even film scripts left the company so exposed it has reportedly reverted to using fax machines and paper in its offices….

Web Link to the full article:

https://www.theguardian.com/technology/2014/dec/26/xbox-live-and-psn-attack-christmas-ruined-for-millions-of-gamers

Superdrug has advised its online customers to change their passwords after the high street chain was targeted by hackers claiming to have stolen the personal details of thousands of people. The health and beauty retailer told customers it had been contacted by a group on Monday evening claiming to have obtained the details of 20,000 customers, including names, addresses, dates of birth and phone numbers.

Superdrug said in the email to customers the company had only seen evidence so far that 386 of the accounts had been compromised.

A spokeswoman said: “The hacker shared a number of details with us to try to prove he had customer information – we were then able to verify they were Superdrug customers from their email and log-in.”... ...Superdrug is the latest high street retailer to report a data breach. Last month Dixons Carphone said personal data belonging to 10 million customers may have been accessed illegally last year, nearly 10 times as many as the firm initially thought. The electronics retailer had estimated the attack – one of the biggest-ever data breaches – involved 1.2m personal records when it first reported the breach in June.

Web Link to the full article:

https://www.theguardian.com/business/2018/aug/22/superdrug-targeted-by-hackers-who-claim-to-have-20000-customer-details

‘Fraudsters exploited my angry tweet' By Kevin Peachey. 28 November 2018 A bank customer was tricked into transferring money by fraudsters who pretended to be responding to his angry Twitter post about poor service. Writer Mike Tinmouth was furious with the process and time taken to open a business account with Barclays. He expressed his frustration in a public tweet - which was seized on by fraudsters who posed as the bank in an attempt to trick him out of £8,000. Fraud experts say con-artists are becoming skilled at impersonation…

... [In the Twitter post] he even posted an email that he received from the bank which he felt was unprofessional and had to confirm was genuine. The bank urged him to delete this public post. All this information, together with some personal details that were already available about him online, was enough for fraudsters to mimic the bank and appear to know details of the case. Soon after the Twitter exchange, he received another email apologising for the poor service and offering to deal with his case. This time the message was from a fraudster posing as his bank.

After various exchanges, he was provided with details of his "new" account, and he started to transfer money from his personal current account with a different bank. The transfer was blocked, saving Mr Tinmouth from losing the £8,000 he intended to move between the two accounts. Barclays said that customers should always be careful about posting details in public, and that it had a system of ensuring customers dealt with the bank's social media teams on private channels. No-one should transfer money to a new account without having all the relevant paperwork and full control of the account.

Web Link to the full article: https://www.bbc.co.uk/news/business-46309561

Result: We have understood the cyber attacks through case study.

****

2: Cyber security attacks case study Submission

Aim: To Understand the cyber security attacks and its solutions.

Challenge

A leading private hospital must ensure sensitive patient data is always suitably protected. It has gained confidence after subscribing to Kroll Responder, Kroll's award-winning managed detection and response (MDR) service, for proactive network and endpoint monitoring. The hospital now has peace of mind, knowing it is doing all it can to protect patient data and maintain operational resilience.

Few organizations need to process large volumes of sensitive and private data like those in the health care sector. It is no exaggeration to describe the hospital's need for operational resilience as critical.

Like all hospitals, this company must manage and maintain a large range of specialist systems, including life-saving medical equipment. Ensuring that these systems are always operational, and that personal patient data can be accessed and shared across a network instantaneously to facilitate medical care, is paramount. Simultaneously, a strict duty exists to ensure that such sensitive and personal information does not end up in the wrong hands.

The organization must also ensure that it is compliant with the requirements of the GDPR, NIS Directive and CQC, which mandate that personal data is suitably protected and breaches are promptly detected, responded to and, when necessary, reported.

The hospital had firewalls and antivirus software but wanted to improve visibility of events inside its network to detect advanced threats capable of evading these controls. At the hospital, security is viewed as a sub-function of the IT department, but the team of six just didn't have the resources to manage the technologies required to perform 24/7 security monitoring alongside other day-to-day responsibilities. The hospital's Head of IT says, "Our patients trust us to protect their personal information and by working with Kroll, we extend that trust to them."

Solution

Knowing that the hospital needed a managed service to provide the capabilities required for proactive network monitoring, the Head of IT for the hospital spent considerable time researching suitable providers to find a solution

that met his requirements. Kroll and its MDR service, Kroll Responder, stood out from the crowd, offering a high level of specialist security expertise and technology, plus support to manage cyber incidents.

Combining 24/7/365 security professionals, best-in-class network and endpoint detection tools, and up-to-the-minute industry intelligence, Kroll Responder helps the organization identify, contain and respond to cyber threats, ensuring the continual protection of its systems and data.

The Kroll Responder deployment comprises a leading SIEM technology and Carbon Black Response. Combining these two solutions enables Kroll to achieve wide visibility of events across the hospital's network and endpoints to detect and respond swiftly to malicious activity whenever it occurs. The network and endpoints are strengthened with detection and monitoring geared towards identifying a wide range of threats, from malware and ransomware to suspicious account activity.

The Impact

Quick and Hassle-free Technology Deployment

When deploying Kroll Responder, Kroll's engineering team worked hand in hand with the hospital's IT team to design and deploy a solution that is needs-driven and provides maximum threat visibility. The technology underpinning the solution was installed and then configured to meet the team's exacting requirements.

24/7 Network and Endpoint Monitoring

Kroll's global security operations centre (SOC) professionals monitor the company's infrastructure around the clock and investigate, analyse and triage security alerts generated by the underlying technologies. In the first six months following the deployment of the service, the hospital's systems generated over 6,200 security alerts. The team at Kroll triaged every one of these alerts to remove false positives and ensure that only genuine incidents were reported for remediation.

Swift Incident Response

Kroll's global SOCs are always on hand to not only report threats but help the hospital respond to them. On one occasion, it was on the receiving end of an advanced persistent malware attack that targeted multiple endpoints and sought to harvest user credentials and exfiltrate data. Using Carbon Black Response, the Kroll team was able to quickly identify infected endpoints, isolate them from the network and analyze the chain of events associated with the attack to help prevent similar attacks. Had Kroll Responder not been engaged at this time, it's likely that the attack would have caused significant damage to the hospital's systems.

Clear Remediation Support

Following the detection of incidents, Kroll's SOC analysts provide all the advice and support that the hospital needs to quickly address issues and minimize any potential disruption. Kroll's Redscan threat management platform enables the SOCs to communicate securely with the company's in-house team.

Sideways Integration with the In-house IT Team

The Head of IT describes Kroll's SOC professionals as an extension of his in-house team. He's on first-name terms with Kroll's analysts and relies on their assistance to not just detect threats but also respond quickly and effectively to them.

Total Reporting Coverage

Kroll provides weekly and monthly reports that help the management team stay abreast of the hospital's security posture. The reports help demonstrate compliance with the GDPR, CQC and NIS Directive to give confidence that appropriate controls are in place.

Cost Effective

The hospital is very happy with the value of the service, which offers a huge savings compared to the cost of maintaining an in-house team to provide an equivalent threat monitoring and detection capability. Kroll Responder ensures that the hospital doesn't need to make a large capital investment in resources, recruit and train staff, or regularly invest in new security technologies.

Result: We understood the cyber security attacks and its solutions through case study.

****

3:TCP scanning using NMAP Port scanning using NMAP

Aim: To study the TCP & Port Scanning using NMAP

Procedure:

1. TCP scanning using NMAP Port scanning using NMAP

Port Scanning Techniques By Using Nmap

Nmap is a security auditing tool used in the security field to actively enumerate a target system/network. It is one of the most extensively used tools by network administrators and conversely attackers for reconnaissance (enumeration), the first step in the 5 phases of hacking. Nmap is used to actively probe the target network for active hosts (host discovery), port scanning, OS detection, version details, and active services running on the hosts that are up. For this, Nmap uses the technique of sending packets and analyzing the responses.

Port Scanning is one of the features of Nmap wherein the tool detects the status of the ports on active hosts in a network. The status of the ports can be open, filtered, or closed. Type Nmap in the command line to run Nmap. Add necessary switches according to the scanning type to initiate a specific scan technique.

Example: nmap -sS 192.168.0.1-192.168.0.52

This command runs Nmap in TCP SYN scan type (-sS) and scans the given IP address range for active hosts and services.

Types of Port Status:

Open: The open status means that the given port is open and is actively running a service.

Filtered: The filtered status means that the respective port might be hidden behind a firewall and its status remains unknown.

Closed: The closed state represents a given port is closed on the host machine.

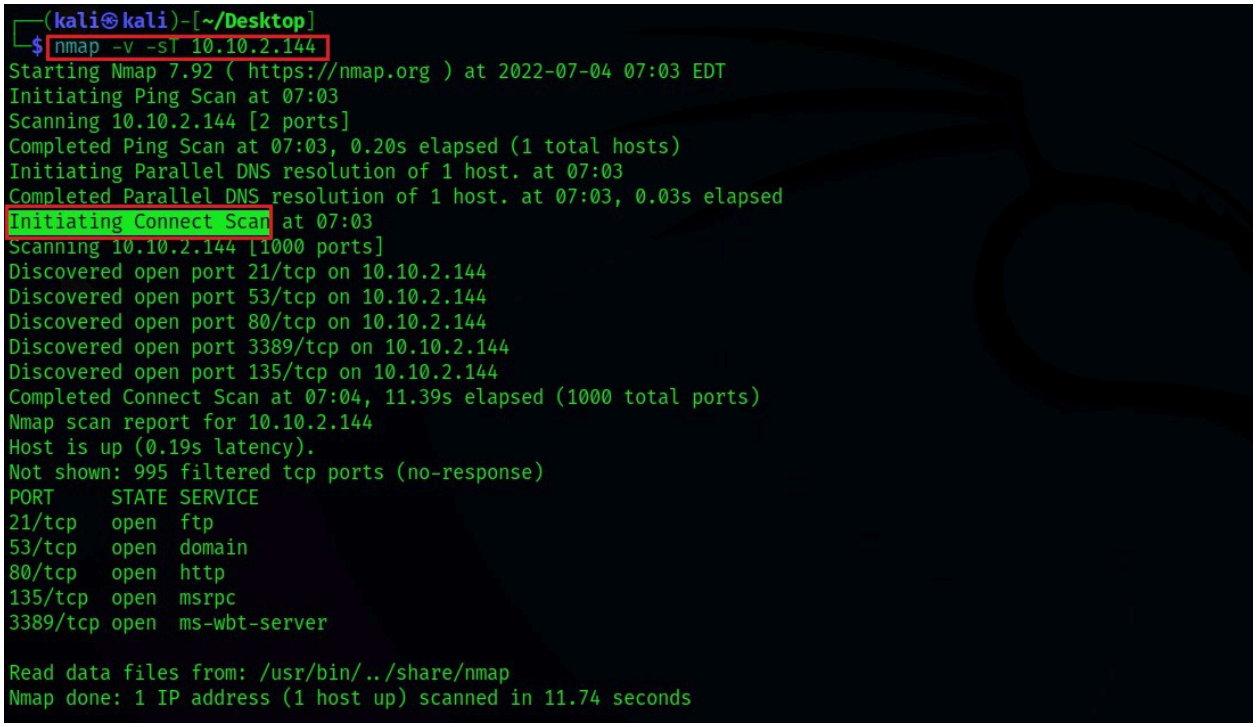
Different Port Scanning Techniques in Nmap:

The following are the extensively used scanning techniques in Nmap:

1. TCP Connect Scan (-sT): TCP Connect scan uses the concept of a full three-way handshake to discover whether a given port is open, filtered, or closed according to the response it receives. Nmap sends a TCP request packet to each and every port specified and determines the status of the port by the response it receives. RFC 793 says,

If the connection does not exist (CLOSED) then a reset is sent in response to any incoming segment except another reset. In particular, SYNs addressed to a non-existent connection are rejected by this means.

- What it essentially means is that if Nmap sends a TCP request to a closed port with its SYN flag set, then it receives a TCP packet with its RESET FLAG set from the target server. This tells Nmap that the specified port is "closed".
- Otherwise, if the port is actually "open", then Nmap receives a response with SYN/ACK flags set responding to the packet sent by Nmap with its SYN flag set.
- The third possibility is that if a port is filtered, most of the server's firewalls are configured to just drop incoming packets. Nmap doesn't receive any response back. This essentially means that the given port is running behind a firewall (i.e "filtered").

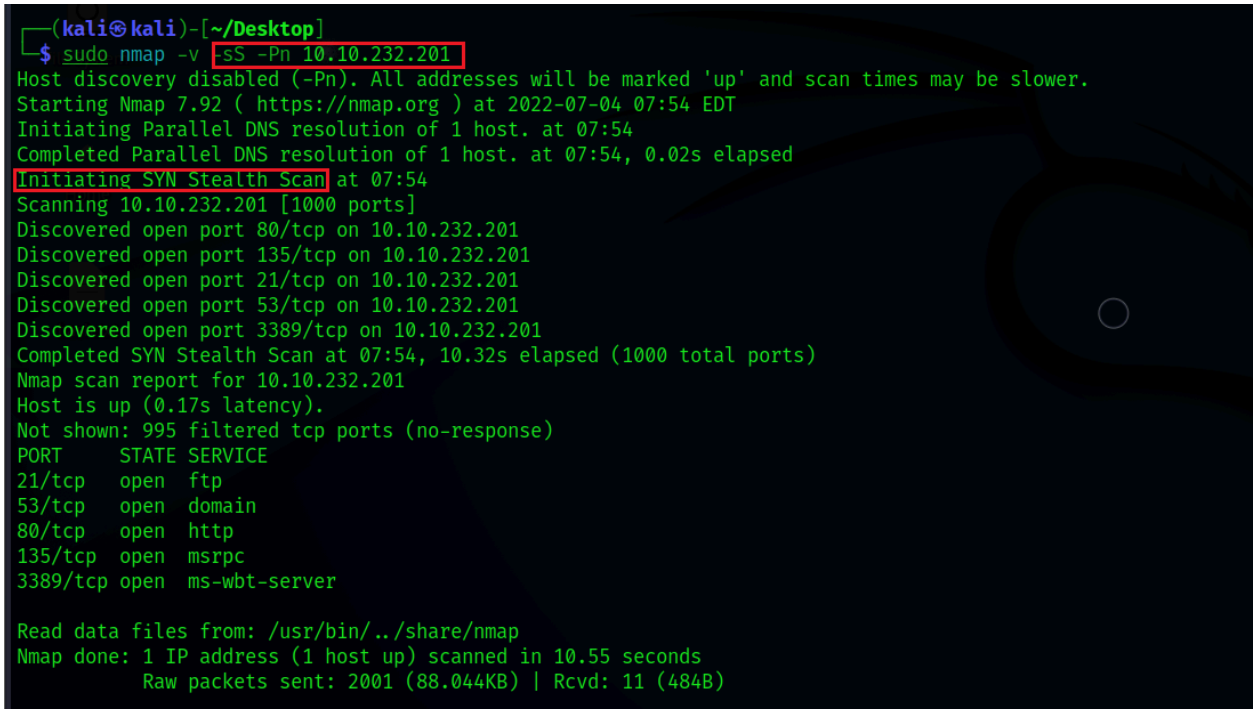


2. **TCP SYN Scan (-sS):**

SYN scans are often called “Half-open” or “Stealth” scans. SYN scan works the same way as TCP Connect scan with closed and filtered ports i.e receives a RST packet for closed port and no response for filtered ports. The only difference is in the way they handle the open ports. SYN scan sends a response packet to the server with its RESET FLAG set (but not ACK which is usually the default in the actual three-way handshake) after receiving SYN/ACK from the target server. This is to avoid the server from continuously making requests to establish a connection and thereby reduce the scan time.

This scan type is referred to as a stealth scan due to the following advantages:

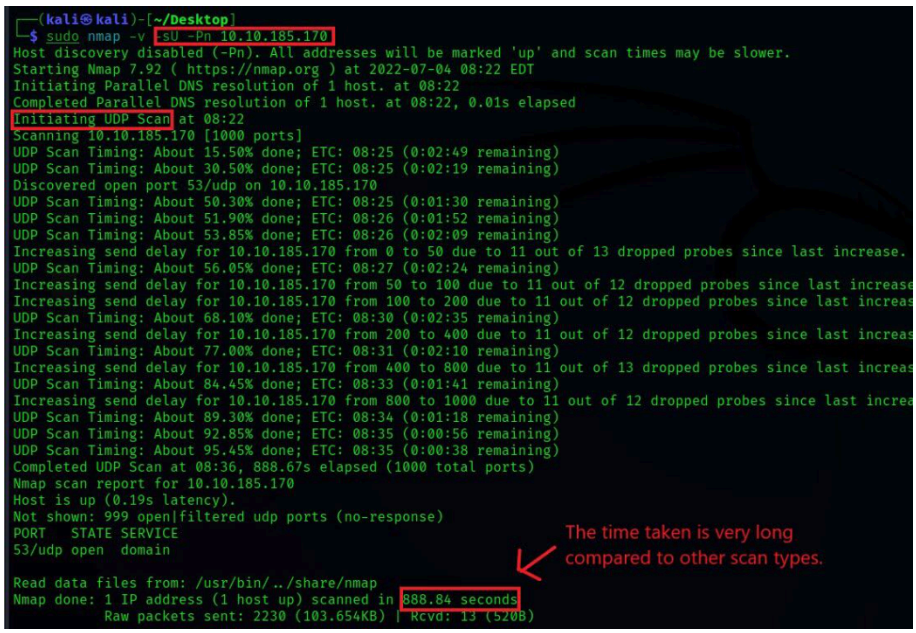
- Faster because it doesn’t have to complete the full three-way handshake.
- Some applications often log only those connections that are fully established. So applications listening on open ports do not log these connections which makes SYN scan “stealthy”.



3. **UDP Scan (-sU):**

UDP unlike TCP, doesn't perform a handshake to establish a connection before sending data packets to the target port but rather sends the packets hoping that the packets would be received by the target port. That is why UDP connections are often called "stateless". This type of connection is more efficient when speed dwarfs quality, like in video sharing. As there will be no acknowledgment from the target port whether it has received the packet, UDP scans become more difficult and very much slower.

- When there's no response from the target port after sending a UDP packet, it often times means that the port is either "open" or is running behind a firewall i.e "filtered" in which case the server would just drop the packet with no response.
- UDP scan can effectively identify closed ports as the target UDP port responds with an ICMP packet with a message that the port is unreachable.



Result: We have studied the TCP scanning using NMAP.

****

4:TCP / UDP connectivity using Netcat

Aim: To study the TCP/UDP connectivity using Netcat

Procedure:

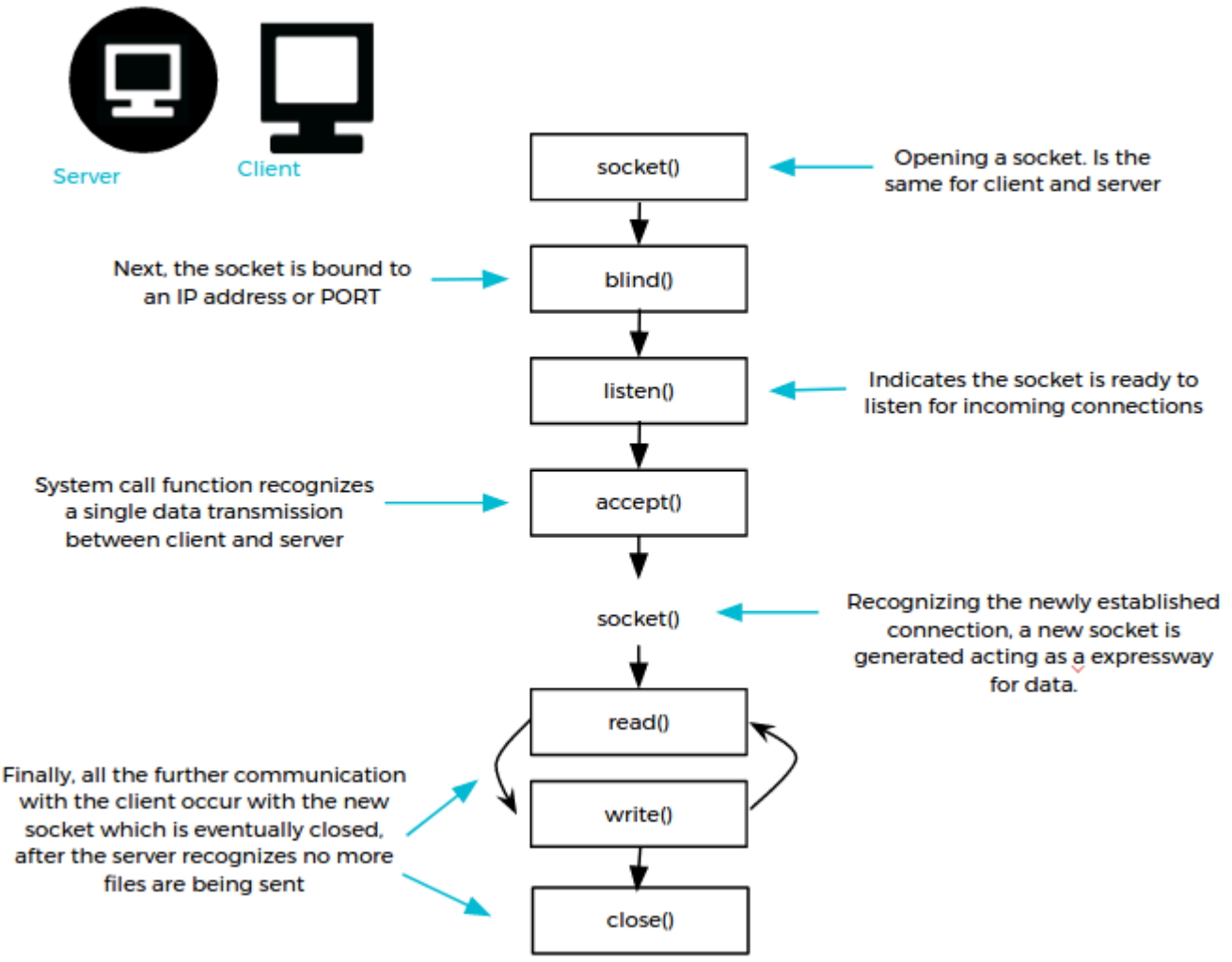
What is Netcat?

Netcat is a featured networking utility which reads and writes data across network connections, using the TCP/IP protocol. Designed to be a reliable "back-end" tool, Netcat can be used directly with other programs and scripts to send files from a client to a server and back. At the same time, it is a feature-rich network debugging and exploration tool that can specify the network patameters while also establishing a connection to a remote host via a tunnel.

Although **Netcat** can do many things, its main purpose and most desirable function is to:

1. Create an initial socket to establish a connection from server to the client.
2. Once connected, Netcat will automatically generate a second socket to transmit files from the server to the client and visa versa. (This is the really cool part.)

Reference below for a diagram of the data Netcat protocol architecture.



Something so simple happens to be extraordinarily powerful and flexible as you will see below. For simplicity, local connections are used, although, of course, they can be used between different machines.

Syntax

nc [-options] hostname port[s] [ports]
nc -l -p port [-options] [hostname] [port]

Basic parameters

- **-l**: set the "listen" mode, waits for the incoming connections.
- **-p**: local port
- **-u**: set the UDP mode

Test your Netcat understanding as a client-server

Open two computer terminals, the first will act as the server and the second will be the client.

TCP client

With **Netcat** your PC can be converted in a server, you want to begin as a server that listens at port **2399**:

```
$ nc -l 2399
```

In addition, we can use the server to connect to the port (**2399**) recently opened, from the **client** side:

```
$ nc localhost 2399
```

As you can see on the image below, the connection is established:

With the connection established you are now able to write to the **server** from the **client**:

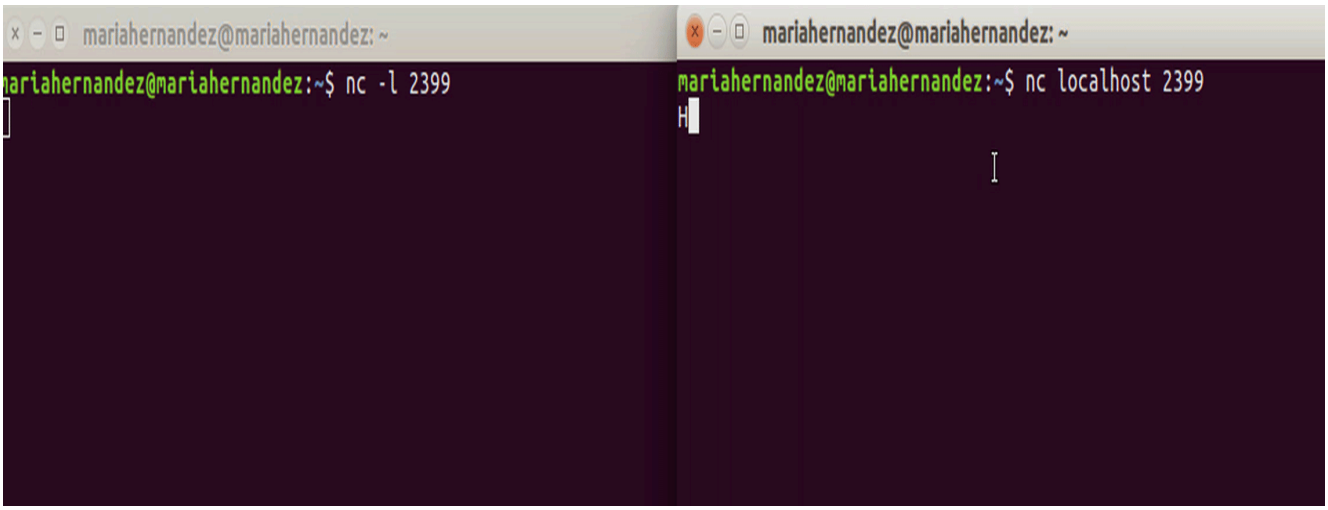
```
$ nc localhost 2399

Hello Server
```

In the terminal where the **server** is running, your text files will appear seamlessly.

```
$ nc -l 2399
```

```
Hello Server
```



UDP client

By default **Netcat** uses the **TCP** protocol for its communications, but it can also **UDP** using the **-u** option.

As we mentioned at the previous step, **Netcat** lets you convert your PC in a server. In this case we're going to establish the connection between the server and the client but using UDP.

From the **server** side, run the command below. As you can see, the command establishes the **UDP** connection just requires the **-u** to be added to the command:

```
$ nc -u -l 2399
```

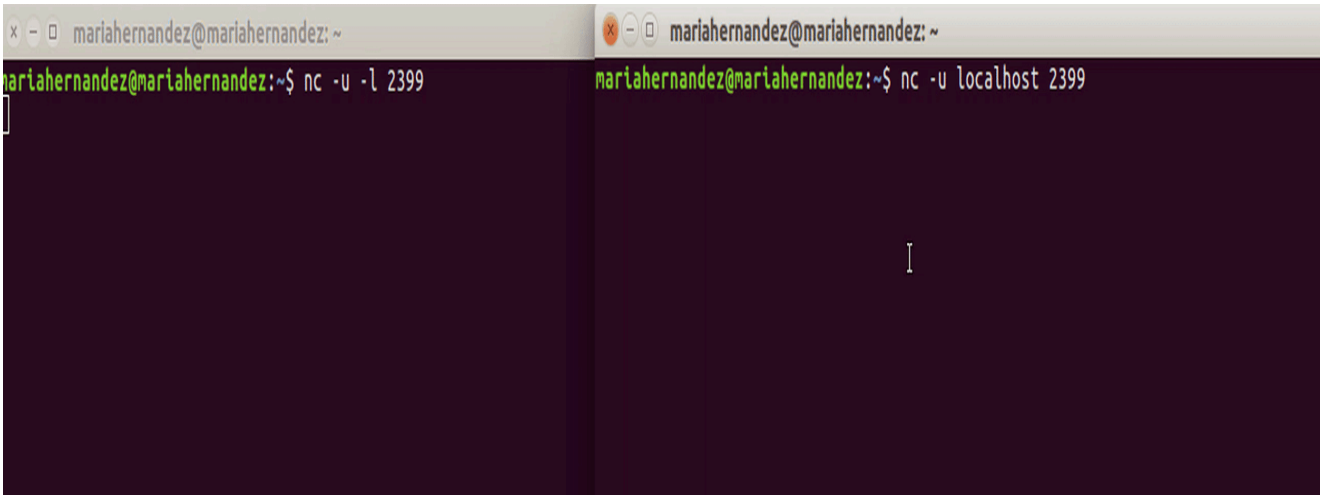
Once you start the server, establish the connection with the **client**:

```
$ nc -u localhost 2399
```

Now the client and the server are using **UDP** protocol for their communication. You can verify commincation using the **netstat** command in a new (3rd) computer terminal.

```
$ netstat | grep 2399
udp 0 0 localhost:2399 localhost:57508  ESTABLISHED
```

As you can see in the images below, the message is received by the server, and the transmission is verified by the connection:



With this introduction to Netcat, you now have a better understanding of this advanced tool to send data quickly and efficiently between client and server.

Result: We have executed the TCP and UDP connectivity using Netcat successfully.

****

5 : TCP / UDP connectivity using Netcat

Aim: To study the TCP/UDP connectivity using Netcat

Procedure:

General Syntax

By default, netcat operates by initiating a TCP connection to a remote host.

The most basic syntax is:

```
1. netcat [options] host port
2.
```

This will attempt to initiate a TCP connection to the defined host on the port number specified. This functions similarly to the old Linux telnet command. Keep in mind that your connection is entirely unencrypted.

If you would like to send a UDP packet instead of initiating a TCP connection, you can use the -u option:

```
1. netcat -u host port
2.
```

You can specify a range of ports by placing a dash between the first and last:

```
1. netcat host startport-endport
2.
```

- This is generally used with some additional flags.
- On most systems, we can use either netcat or nc interchangeably. They are aliases for the same command.

How To Use Netcat for Port Scanning

- One of the most common uses for netcat is as a port scanner.
- Although netcat is probably not the most sophisticated tool for the job (nmap is a better choice in most cases), it can perform simple port scans to easily identify open ports.
- We do this by specifying a range of ports to scan, as we did above, along with the -z option to perform a scan instead of attempting to initiate a connection.

For instance, we can scan all ports up to 1000 by issuing this command:

```
1.  netcat -z -v domain.com 1-1000
2.
```

- Along with the -z option, we have also specified the -v option to tell netcat to provide more verbose information.

  The output will look like this:

```
Output
nc: connect to domain.com port 1 (tcp) failed: Connection refused
nc: connect to domain.com port 2 (tcp) failed: Connection refused
nc: connect to domain.com port 3 (tcp) failed: Connection refused
nc: connect to domain.com port 4 (tcp) failed: Connection refused
nc: connect to domain.com port 5 (tcp) failed: Connection refused
nc: connect to domain.com port 6 (tcp) failed: Connection refused
nc: connect to domain.com port 7 (tcp) failed: Connection refused
. . .
Connection to domain.com 22 port [tcp/ssh] succeeded!
. . .
```

- As you can see, this provides a lot of information and will tell you for each port whether a scan was successful or not.

- If you are actually using a domain name, this is the form you will have to use.

- However, your scan will go much faster if you know the IP address that you need.

  You can then use the -n flag to specify that you do not need to resolve the IP address using DNS:

```
1.  netcat -z -n -v 198.51.100.0 1-1000
2.
```

The messages returned are actually sent to standard error (see our I/O redirection article for more info). We can send the standard error messages to standard out, which will allow us to filter the results easier.We will redirect standard error to standard output using the 2>&1 bash syntax. We will then filter the results with grep:

```
1.  netcat -z -n -v 198.51.100.0 1-1000 2>&1 | grep succeeded
2.
```

```
Output
Connection to 198.51.100.0 22 port [tcp/*] succeeded!
```

Here, we can see that the only port open in the range of 1–1000 on the remote computer is port 22, the traditional SSH port.

How To Communicate through Netcat

- Netcat is not restricted to sending TCP and UDP packets. It also can listen on a port for connections and packets. This gives us the opportunity to connect two instances of netcat in a client-server relationship.
- Which computer is the server and which is the client is only a relevant distinction during the initial configuration. After the connection is established, communication is exactly the same in both directions.
- On one machine, you can tell netcat to listen to a specific port for connections.
- We can do this by providing the -l parameter and choosing a port:

```
1.  netcat -l 4444
2.
```

- This will tell netcat to listen for TCP connections on port 4444. As a regular (non-**root**) user, you will not be able to open any ports under 1000, as a security measure.
- On a second server, we can connect to the first machine on the port number we chose.
- We do this the same way we've been establishing connections previously:

```
1.  netcat domain.com 4444
2.
```

- It will look as if nothing has happened. However, you can now send messages on either side of the connection and they will be seen on either end.
- Type a message and press ENTER. It will appear on both the local and remote screen. This works in the opposite direction as well.

- When you are finished passing messages, you can press CTRL-D to close the TCP connection.

How To Send Files through Netcat

Building off of the previous example, we can accomplish more useful tasks.

Because we are establishing a regular TCP connection, we can transmit just about any kind of information over that connection. It is not limited to chat messages that are typed in by a user. We can use this knowledge to turn netcat into a file transfer program.

Once again, we need to choose one end of the connection to listen for connections. However, instead of printing information onto the screen, as we did in the last example, we will place all of the information straight into a file:

```
1. netcat -l 4444 > received_file
2.
```

The > in this command redirects all the output of netcat into the specified filename.

On the second computer, create a simple text file by typing:

```
1. echo "Hello, this is a file" > original_file
2.
```

We can now use this file as an input for the netcat connection we will establish to the listening computer. The file will be transmitted just as if we had typed it interactively:

```
1. netcat domain.com 4444 < original_file
2.
```

We can see on the computer that was awaiting a connection, that we now have a new file called received_file with the contents of the file we typed on the other computer:

```
1. cat received_file
2.
```

```
Output
Hello, this is a file
```

- As you can see, by piping things, we can easily take advantage of this connection to transfer all kinds of things.

- For instance, we can transfer the contents of an entire directory by creating an unnamed tarball on-the-fly, transferring it to the remote system, and unpacking it into the remote directory.
- On the receiving end, we can anticipate a file coming over that will need to be unzipped and extracted by typing:

```
1. netcat -l 4444 | tar xzvf -
2.
```

- The ending dash (-) means that tar will operate on standard input, which is being piped from netcat across the network when a connection is made.
- On the side with the directory contents we want to transfer, we can pack them into a tarball and then send them to the remote computer through netcat:

```
1. tar -czf - * | netcat domain.com 4444
2.
```

This time, the dash in the tar command means to tar and zip the contents of the current directory (as specified by the * wildcard), and write the result to standard output.

This is then written directly to the TCP connection, which is then received at the other end and decompressed into the current directory of the remote computer.

This is just one example of transferring more complex data from one computer to another. Another common idea is to use the dd command to image a disk on one side and transfer it to a remote computer. We won't be covering this here though.

How To Use Netcat as a Simple Web Server

We've been configuring netcat to listen for connections in order to communicate and transfer files. We can use this same concept to operate netcat as a very simple web server. This can be useful for testing pages that you are creating.

First, let's make a simple HTML file on one server:

```
1. nano index.html
2.
```

Here is some simple HTML that you can use in your file:

index.html

```
<html>
    <head>
        <title>Test Page</title>
    </head>
    <body>
        <h1>Level 1 header</h1>
        <h2>Subheading</h2>
        <p>Normal text here</p>
    </body>
</html>
```

Save and close the file.

Without root privileges, you cannot serve this file on the default web port, port 80. We can choose port 8888 as a regular user.

If you just want to serve this page one time to check how it renders, you can run the following command:

```
1. printf 'HTTP/1.1 200 OK\n\n%s' "$(cat index.html)" | netcat -l 8888
2.
```

Now, in your browser, you can access the content by visiting:

```
http://server_IP:8888
```

Result: We have executed the TCP and UDP connectivity using Netcat successfully.

6 : Perform an experiment to demonstrate sniffing of router traffic by using the tool Wireshark

Aim: To perform sniff operation for router traffic using wireshark network analyzer.

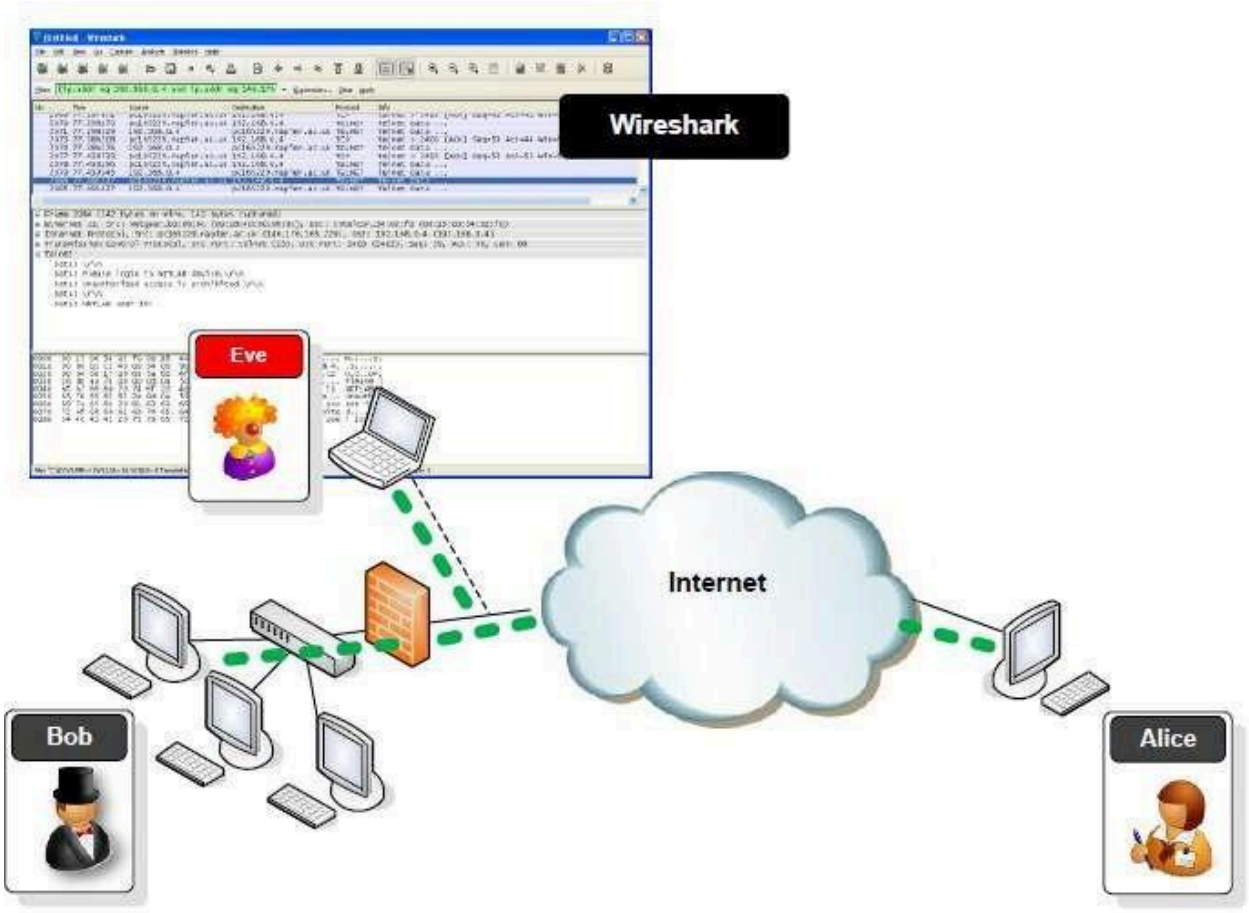
Procedure:

Packet Capture (Packet Sniffing)

A packet sniffer is an application which can capture and analyse network traffic which is passing through a system's Network Interface Card (NIC). The sniffer sets the card to promiscuous mode which means all traffic

is read, whether it is addressed to that machine or not. The figure below shows an attacker sniffing packets from the network, and the Wiresharkpacket sniffer/analyser (formerly known as ethereal).

Diagram



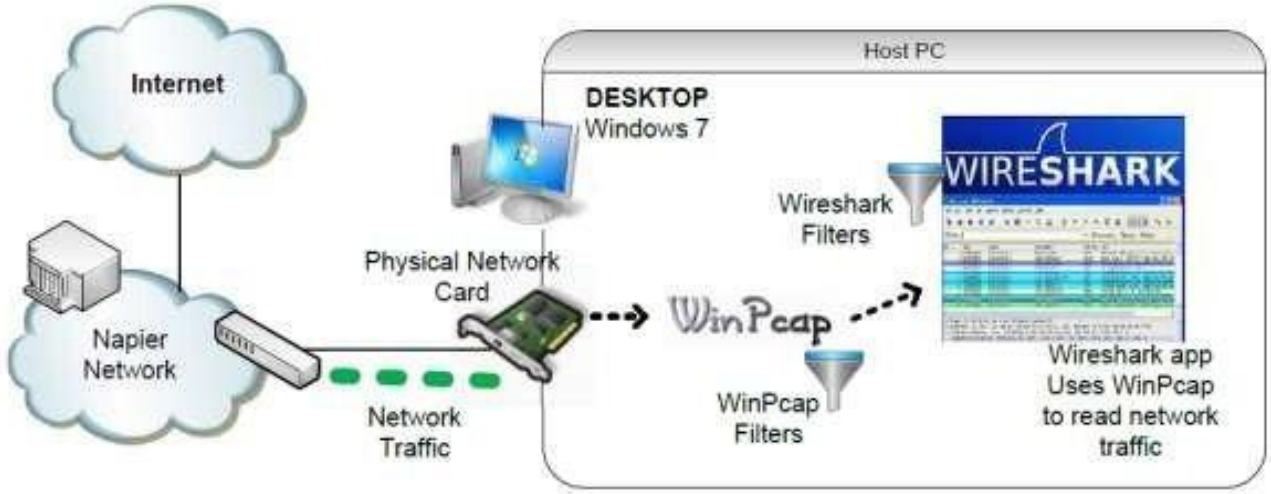
Packet Analysis

Wireshark is an open-source cross-platform packet capture and analysis tool, with versions for Windows and Linux. The GUI window gives a detailed breakdown of the network protocol stack for each packet, colorising packet details based on protocol, as well as having functionality to filter and search the traffic, and pick out TCP streams. Wireshark can also save packet data to files for offline analysis and export/import packet captures to/from other tools. Statistics can also be generated for packet capture files. Wireshark can be used for network troubleshooting, to investigate security issues, and to analyse and understand network protocols. The

packet sniffer can exploit information passed in plaintext, i.e. not encrypted. Examples of protocols which pass information in plaintext are Telnet, FTP, SNMP, POP, and HTTP.

Wireshark is a GUI based network capture tool. There is a command line-based version of the packet capture utility, called TShark. TShark provides many of the same features as it's big brother, but is console-based. It can be a good alternative if only command line access is available, and also uses less resources as it has no GUI to generate.

Using Wireshark to Capture Traffic



Select a Network Interface to Capture Packets through.

Start the Wireshark application. When Wireshark is first run, a default, or blank window is shown. To list the available network interfaces, select the Capture->Interfaces menu option.

Wireshark should display a popup window such as the one shown in Figure 2. To capture network traffic click the **Start** button for the network interface you want to capture traffic on. Windows can have a long list of virtual interfaces, before the Ethernet Network Interface Card (NIC).

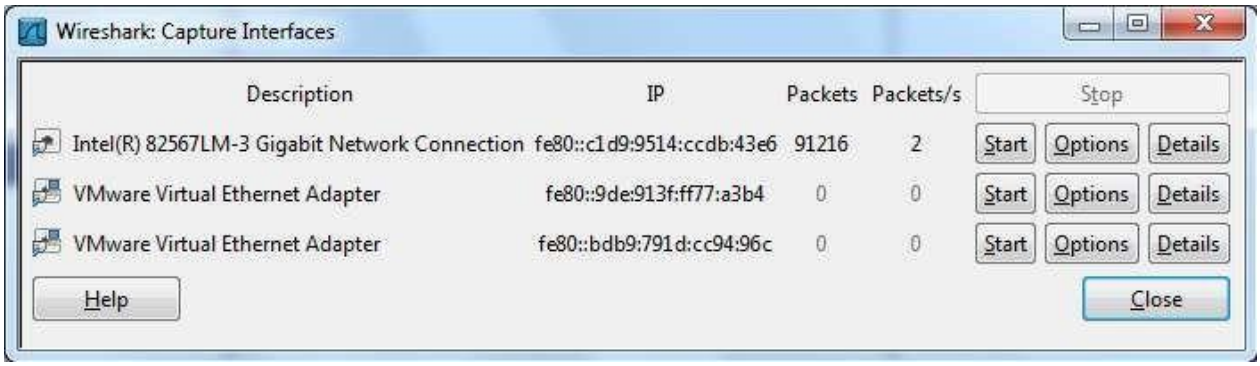


Figure 2 - Wireshark Interfaces Window

Generate some network traffic with a Web Browser, such as Internet Explorer or Chrome. Your Wireshark window should show the packets, and now look something like.

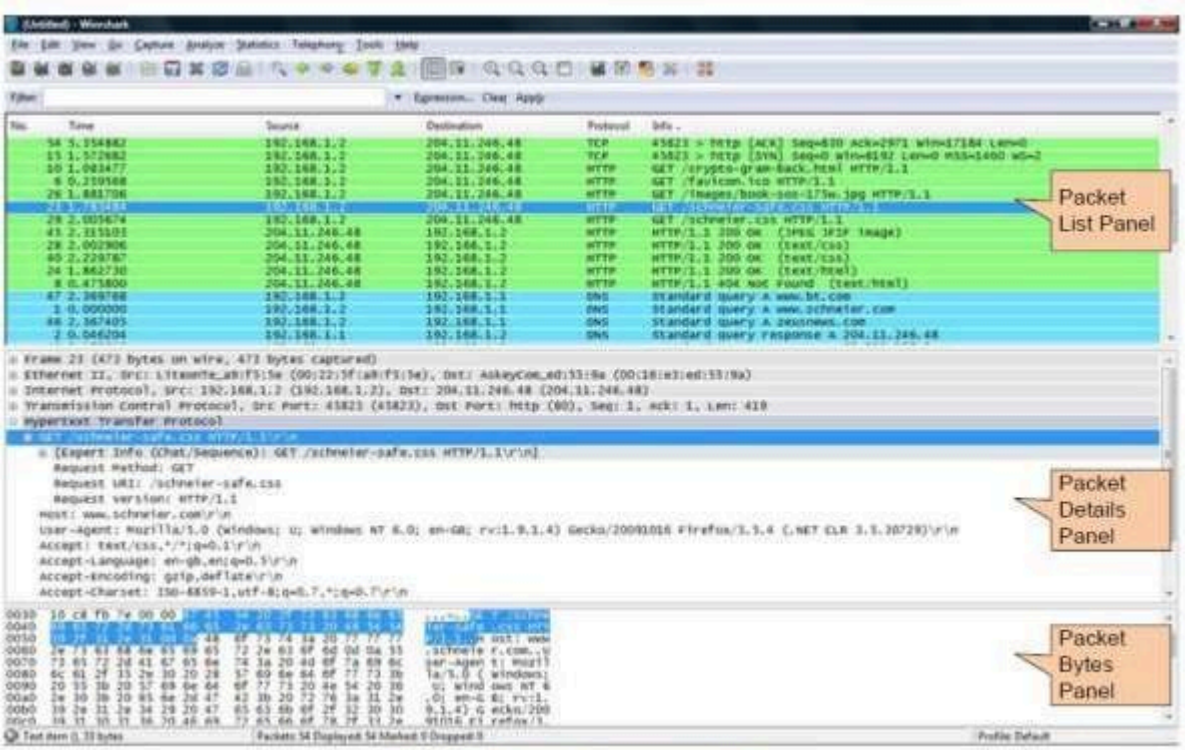


Figure 3 - Wireshark capuring traffic

To stop the capture, select the **Capture->Stop** menu option, Ctrl+E, or the Stop toolbar button. What you have created is a Packet Capture or ***„pcap'***, which you can now view and analyse using the Wireshark interface, or save to disk to analyse later.

The capture is split into 3 parts:

1. **Packet List Panel –** this is a list of packets in the current capture. It colours the packets based on the protocol type. When a packet is selected, the details are shown in the two panels below.
2. **Packet Details Panel –** this shows the details of the selected packet. It shows the different protocols making up the layers of data for this packet. Layers include Frame, Ethernet, IP, TCP/UDP/ICMP, and application protocols such as HTTP.
3. **Packet Bytes Panel –** shows the packet bytes in Hex and ASCII encodings.

To select more detailed options when starting a capture, select the **Capture->Options** menu option, or **Ctrl+K**, or the Capture Options button on the toolbar (the wrench). This should show a window such as shown in Figure 4.

Some of the more interesting options are:

□ ***Capture Options > Interface*** **-** Again the important thing is to select the correct Network Interface to capture traffic through.

□ ***Capture Options > Capture File*** **–** useful to save a file of the packet capture in real time, in case of a system crash.

□ ***Display Options > Update list of packets in real time*** **–** A display option, which should be checked if you want to view the capture as it happens (typically switched off to capture straight to a file, for later analysis).

□ ***Name Resolution > MAC name resolution*** **–** resolves the first 3 bytes of the MAC Address, the Organisation Unique Identifier (OUI), which represents the Manufacturer of the Card.

□ ***Name Resolution > Network name resolution*** **–** does a DNS lookup for the IP Addresses captured, to display the network name. Set to off by default, so covert scans do not generate this DNS traffic, and tip off who's packets you are sniffing. Make sure the MAC name resolution is selected. Start the capture, and generate some Web traffic again, then stop the capture.

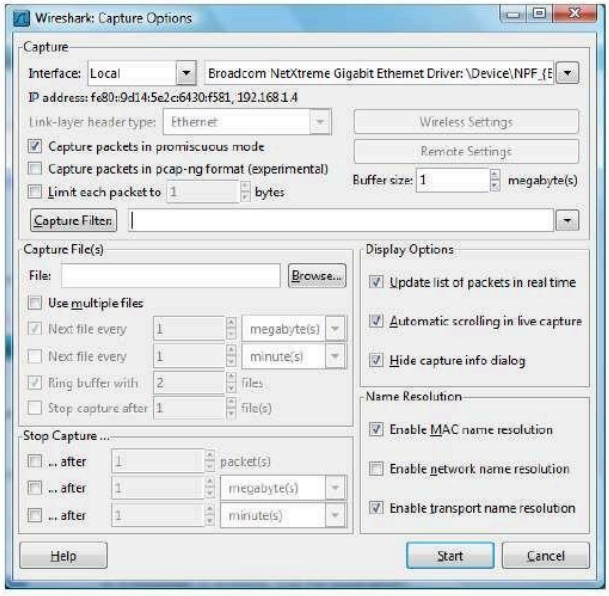


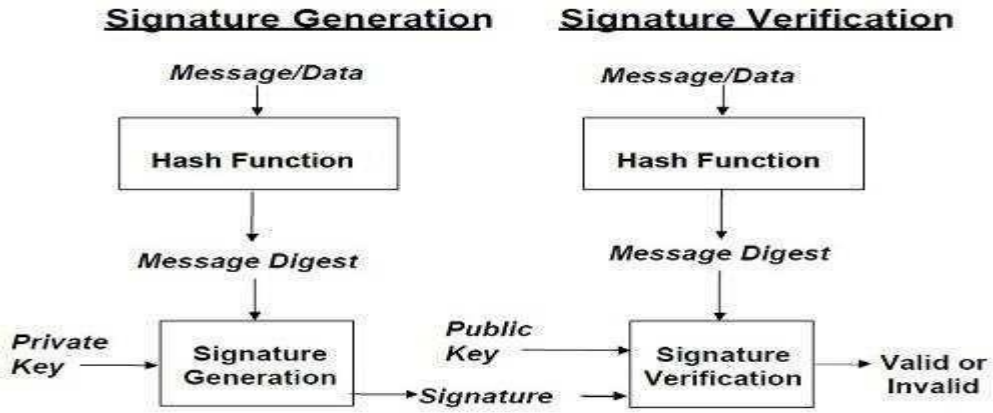
Figure 4 - Wireshark Capture Options

Result: - Thus, the sniff operation for router traffic using wireshark network analyzer executed successfully.

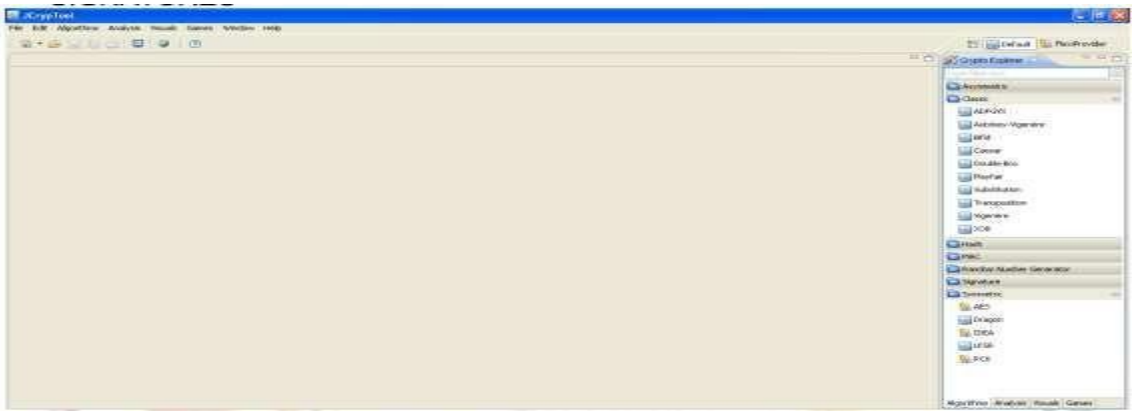
7. Demonstrate how to provide secure data storage, secure data transmission and for creating digital signatures (GnuPG) - IMPLEMENT THE SIGNATURE SCHEME

Aim: To implement the signature scheme - Digital Signature Standard using SNORT Tool.

Methodology:



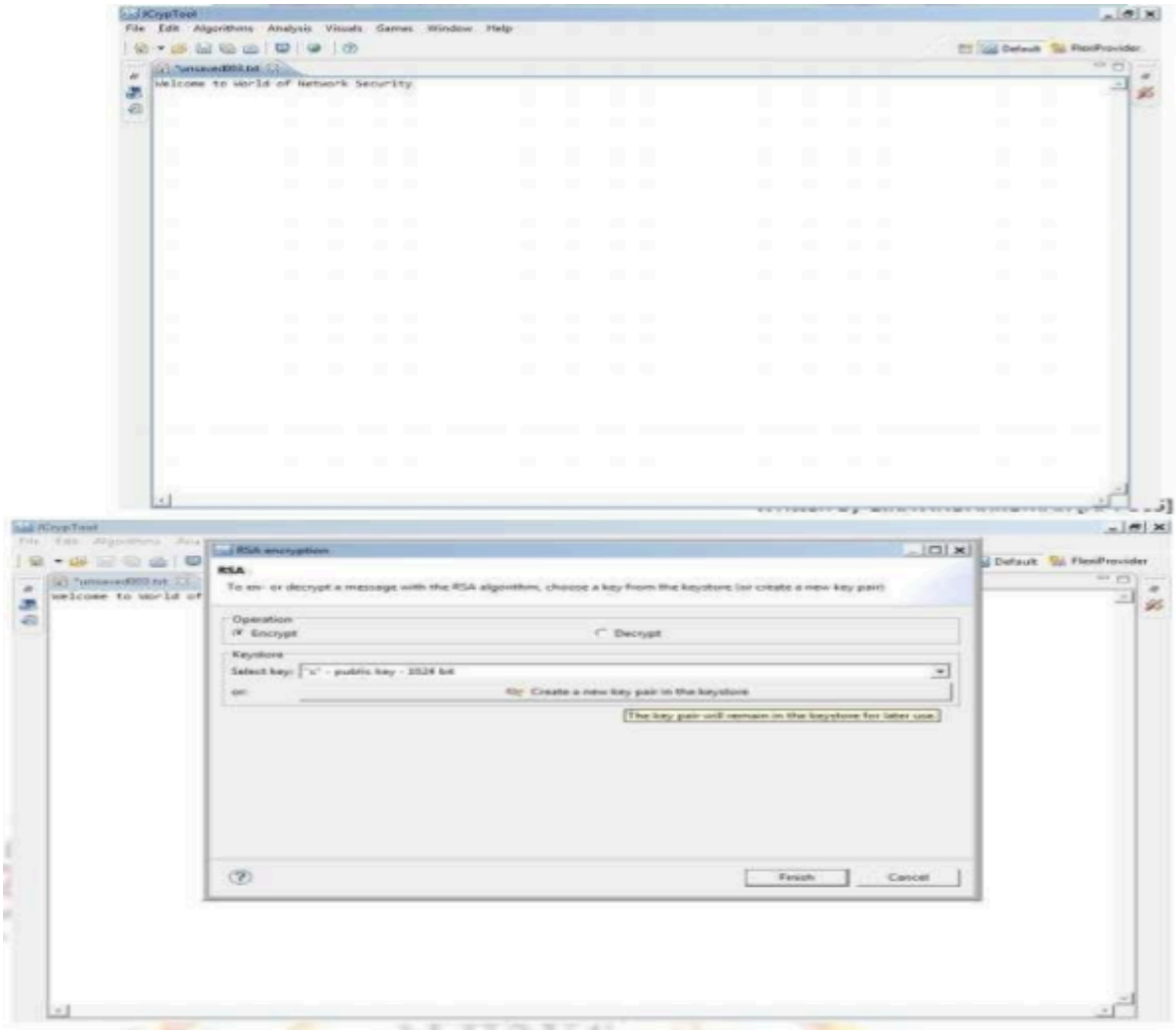
PROCEDURE:



ASYMMETRIC ALGORITHM

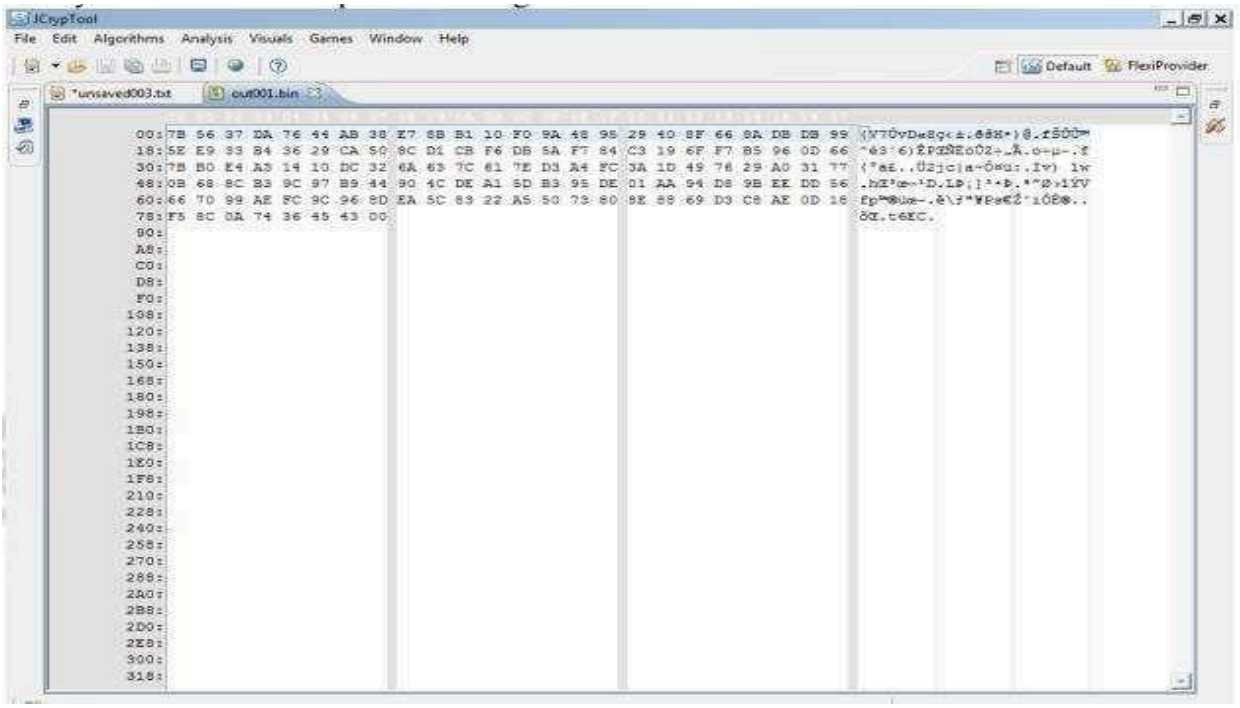
o Download Jcrypt tool from Cryptool Website and Install

o Open Jcrypt Software and Click on NEW text editor, type the text information into it



Click on the Algorithm menu bar and Select Asymmetric algorithm RSA for encryption.

1. Click create a New KeyPair and type in the contact name[xxxxx] and enter the password and confirm password, then Click finish again.



The same output bin file to decrypt select RSA Algorithm and Click on Decrypt, Select keyname you have declared earlier and Click Finish.

3. Enter the password to Decrypt and see the output with original Decrypted text on the Screen.

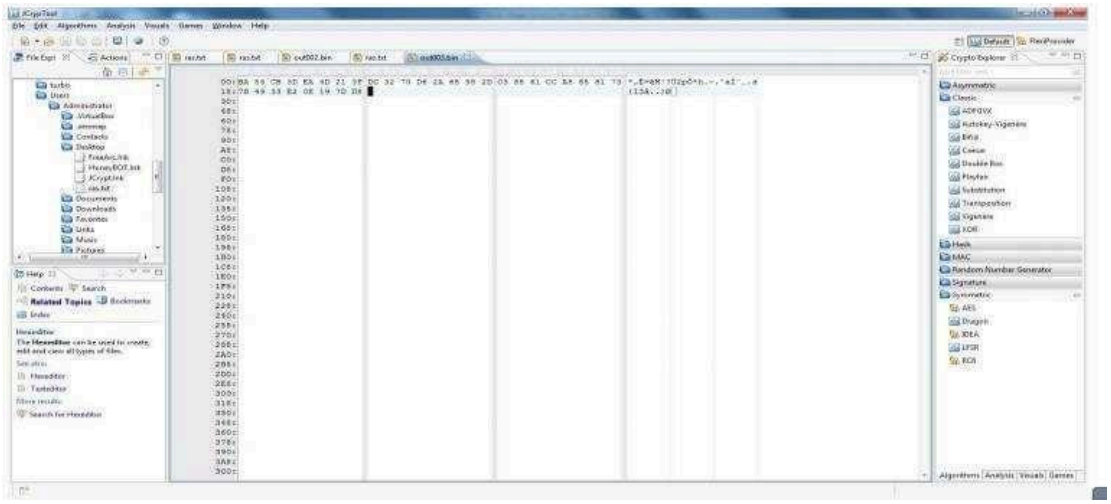
SYMMETRIC ALGORITHM

- Click on Algorithm Menu bar Select Symmetric AES and Click on it.
- Click on create a new key, type contact name and enter the password and confirm, Click Finish
- Click finish again.
- Enter the password to open the output file.
- To Decrypt Select Algorithms Symmetric Select the key which you have created and
- Click Finish.

- Enter the password and see the result in output bin file with hexadecimal values and plain
- text. HASH GENERATION
- Click on Algorithms, Click on Hash Select MD5 Click Finish.
- Now view the output bin file HASH generated.
- Practice using SHA and SHA3 and verify the result on the screen.

DIGITAL SIGNATURE

- Click on algorithms, Click on Signature, Select DSA and Click on it.
- Select sign operation and Click on create a new key.
- Enter the password and save the file and Click finish.
- To verify Click on Algorithm, Click on Signature and Click DSA.
- Select verify operation, Click open and type the password and Click finish.
- The Signature file is opened and verified.



RESULT: Thus, the SNORT Tool is installed and Implementation of the signature scheme - Digital Signature Standard is done and verified successfully.

8. Demonstrate How To Provide Secure Data Storage, Secure Data Transmission And For Creating Digital Signatures (GnuPG)

Aim: To provide secure data storage, secure data transmission for creating digital signatures.

Procedure:

GPG & its Benefits:

GPG (Gnu Privacy Guard) is a system for encryption of data that afterwards can be transmitted through open communication channels and kept in not protected storage. Open communication channels are email, cloud storage, instant messengers, and many others you probably use daily. These tools don't provide any dependable data protection.

GPG is available in almost all repositories and Linux distributives. It is used for creating digital signatures and files encrypting. GPG is an open source analog of PGP (Pretty Good Privacy).

GPG shield is quite reliable. It's not possible to hack it using simple tools since it uses 2048- bit keys and it is very resistant to the most complex hacking algorithms. For transferring sensitive information it's enough to compress the data using the gpg utility. After that it can be transferred using any convenient method regardless of its built-in security means. Besides compressing data GPG can also be used for files signing to confirm the file authorship.

Procedure:

Basic Workflow:

In order to encrypt the file, the sender should have a private open key of the person to whom the file is going to be sent. The open key is used by the sender to encrypt the data and cannot be used to decrypt it. This is why the open key can be sent using open communication channels. The recipient can decrypt the file using his private secret key and a passphrase. It is extremely important to keep both the private key and the passphrase or you won't be able to decrypt the file.

Keys:

The main components of GPG are a private (secret) and public (open) keys. The private key should be safely kept only by its owner and it can be used for signing data and decryption of encrypted files. In all operations where the private key is used you should provide the passphrase as well. A public key can be used for checking a digital signature and for encrypting files. It can be made available for various users you communicate with. Thus, if we would like to send somebody encrypted sensitive data you should take that person's public key and use it to encrypt your data. After receiving that data the person should use his private key to decrypt it. If you would like to send an email with your digital signature you should use your private key to generate it. The recipient of such a signed email can use your public key to validate your signature and make sure the email has been sent by you personally.

Generating & Managing Keys Generating Keys

You can generate both the private and the public keys using the following command: gpg –gen-key

It will ask you about the kind of key you would like to have, its length, and period of validity. For start choose defaults. Now you should enter your details:

User: PEC

Email: hello@gmail.com

Passphrase: My top-secret phrase for decryption

Note that in commands below where you have to refer to the keys you can either use the username

“PEC” or the email “hello@gmail.com”.

Importing Keys

You can import keys from files. Later we will show how to generate such files. Public and private:

gpg –import gll.prv.key

Public only (you also may need to change the level of trust for this key): gpg –import gll.pub.key

Private only:

gpg –allow-secret-key-import –import gll.prv.key

Exporting Keys

Public:

gpg –export –a “Giant Leap Lab” > gll.pub.key && cat gll.pub.key Private:

gpg –export-secret-key –a “Giant Leap Lab” > gll.prv.key && cat gll.prv.key

Checking if a Key is Installed

Show the public key: gpg –list-key

Show all private keys: gpg –list-secret-keys

Removing Keys

Public:

gpg –delete-keys ‘Giant Leap Lab’

Private:

gpg –delete-secret-keys ‘Giant Leap Lab’

Trust Levels

GPG allows editing level of trust for public keys. This level reflects how high is trust to a particular user and his ability to properly sign his files. Sometimes for example when importing a key you also can get the following warning message:

gpg: WARNING: This key is not certified with a trusted signature! gpg: There is no indication that the signature belongs to the owner.

In order to fix this and set proper trust levels use the following command:

gpg –edit-key ‘Giant Leap Lab’

then type:

gpg> trust

and you’ll get the following options to choose from:

1 = Don’t know

2 = I do NOT trust

3 = I trust marginally 4 = I trust fully

s = please show me more information m = back to the main menu

As an alternative you can sign this key with your secret key. Method 1 and Method 2

Transferring an Encrypted File:

Encrypting & Sending:

Let's say we have a really sensitive data in a file called top_secret_file.txt. In order to send it

by email to a user whose email is user@mail.com use the following command:

gpg –r user@mail.com –e top_secret_file.txt

(We assume user@mail.com email has been used to generate the private key of the recipient that you should have. You can also use his name instead of the email after the "-r" argument).

This will create a file called top_secret_file.txt.gpg that can be sent by email or transferred using other open communication channels.

If you add the "-a" option the content of the generated encrypted file (top_secret_file.txt.asc) can be sent as text for example through an instant messenger.

Receiving & Decrypting:

Keep in mind that the recipient should have the private key for the user@mail.com email address and should have the passphrase for that key. Run the following command to decrypt the received file:

gpg –o top_secret_file.txt –d top_secret_file.txt.gpg

This will restore the original top_secret_file.txt file from top_secret_file.txt.gpg.

Signing Files:

Sometimes it might be necessary to add a digital signature to a file to confirm its authorship. The command below creates a digital signature for the signGLL.txt file. The signature is saved as a separate file sign GLL.txt.sig (detached signature). The "-u" argument defines what key should be used for generating the signature.

gpg –u user@mail.com –detach-sign signGLL.txt

Instead of " – detach-sign" you can also use "-b":

gpg –u user@mail.com –b signGLL.txt

You can also compress the file so that it includes the signature:

gpg –u user@mail.com –s signGLL.txt

Then the received signGLL.txt.gpg file can be decrypted using this command: gpg –output signGLL.txt –decrypt signGLL.txt.gpg

In order to verify a signature use the command below. Note that the original file should be in the same folder as the validated signature.

gpg –verify signGLL.txt.sig

If the file named differently, you can add his name:

gpg –verify signGLL.txt.sig lincense.txt.

Result: Thus, secured data storage, secure data transmission for creating digital signatures is completed successfully.

9. Perform an experiment to sniff traffic using ARP Poisoning

Aim: To perform an experiment to sniff traffic using ARP poisoning

Procedure:

What is IP and MAC Addresses

IP Address is the acronym for Internet Protocol address. An internet protocol address is used to uniquely identify a computer or device such as printers, storage disks on a computer network. There are

currently two versions of IP addresses. IPv4 uses 32-bit numbers. Due to the massive growth of the internet, IPv6 has been developed, and it uses 128-bit numbers.

IPv4 addresses are formatted in four groups of numbers separated by dots. The minimum number is 0, and the maximum number is 255. An example of an IPv4 address looks like this;

127.0.0.1

IPv6 addresses are formatted in groups of six numbers separated by full colons. The group numbers are written as 4 hexadecimal digits. An example of an IPv6 address looks like this;

2001:0db8:85a3:0000:0000:8a2e:0370:7334

In order to simplify the representation of the IP addresses in text format, leading zeros are omitted, and the group of zeros is completed omitted. The above address in a simplified format is displayed as;

2001:db8:85a3:::8a2e:370:7334

MAC Address is the acronym for media access control address. MAC addresses are used to uniquely identify network interfaces for communication at the physical layer of the network. MAC addresses are usually embedded into the network card.

A MAC address is like a serial number of a phone while the IP address is like the phone number.

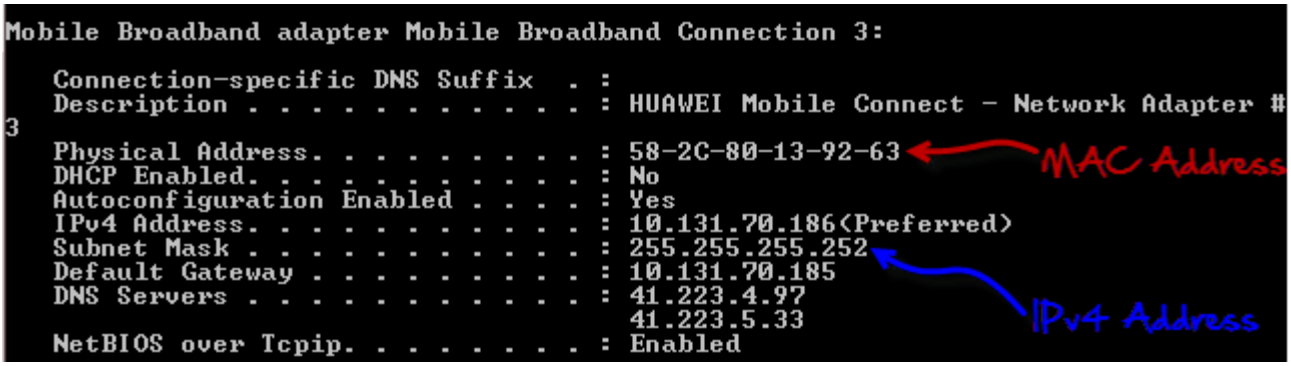
Exercise

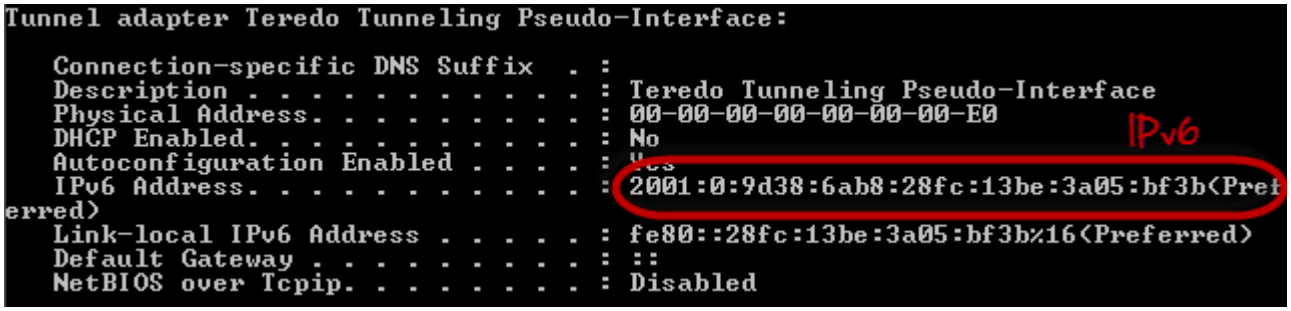
We will assume you are using windows for this exercise. Open the command prompt.

Enter the command

ipconfig /all

You will get detailed information about all the network connections available on your computer. The results shown below are for a broadband modem to show the MAC address and IPv4 format and wireless network to show IPv6 format.





What is ARP Poisoning?

ARP is the acronym for Address Resolution Protocol. It is used to convert IP address to physical addresses [MAC address] on a switch. The host sends an ARP broadcast on the network, and the recipient computer responds with its physical address [MAC Address]. The resolved IP/MAC address is then used to communicate. **ARP poisoning is sending fake MAC addresses to the switch so that it can associate the fake MAC addresses with the IP address of a genuine computer on a network and hijack the traffic**.

ARP Poisoning Countermeasures

Static ARP entries: these can be defined in the local ARP cache and the switch configured to ignore all auto ARP reply packets. The disadvantage of this method is, it's difficult to maintain on large networks. IP/MAC address mapping has to be distributed to all the computers on the network.

ARP poisoning detection software: these systems can be used to cross check the IP/MAC address resolution and certify them if they are authenticated. Uncertified IP/MAC address resolutions can then be blocked.

Operating System Security: this measure is dependent on the operating system been used. The following are the basic techniques used by various operating systems.

- **Linux based**: these work by ignoring unsolicited ARP reply packets.
- **Microsoft Windows**: the ARP cache behavior can be configured via the registry. The following list includes some of the software that can be used to protect networks against sniffing;

    - **AntiARP**– provides protection against both passive and active sniffing
    - **Agnitum Outpost Firewall**–provides protection against passive sniffing

- **XArp**– provides protection against both passive and active sniffing
- **Mac OS**: ArpGuard can be used to provide protection. It protects against both active and passive sniffing.

Hacking Activity: Configure ARP entries in Windows

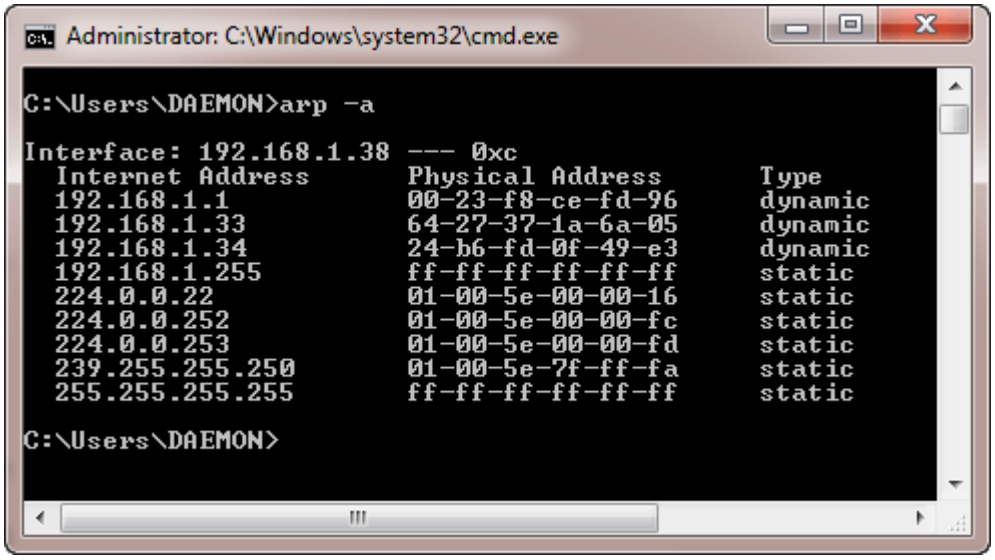
We are using Windows 7 for this exercise, but the commands should be able to work on other versions of windows as well.

Open the command prompt and enter the following command

arp –a
HERE,

- **arp**calls the ARP configure program located in Windows/System32 directory
- **-a** is the parameter to display to contents of the ARP cache

You will get results similar to the following

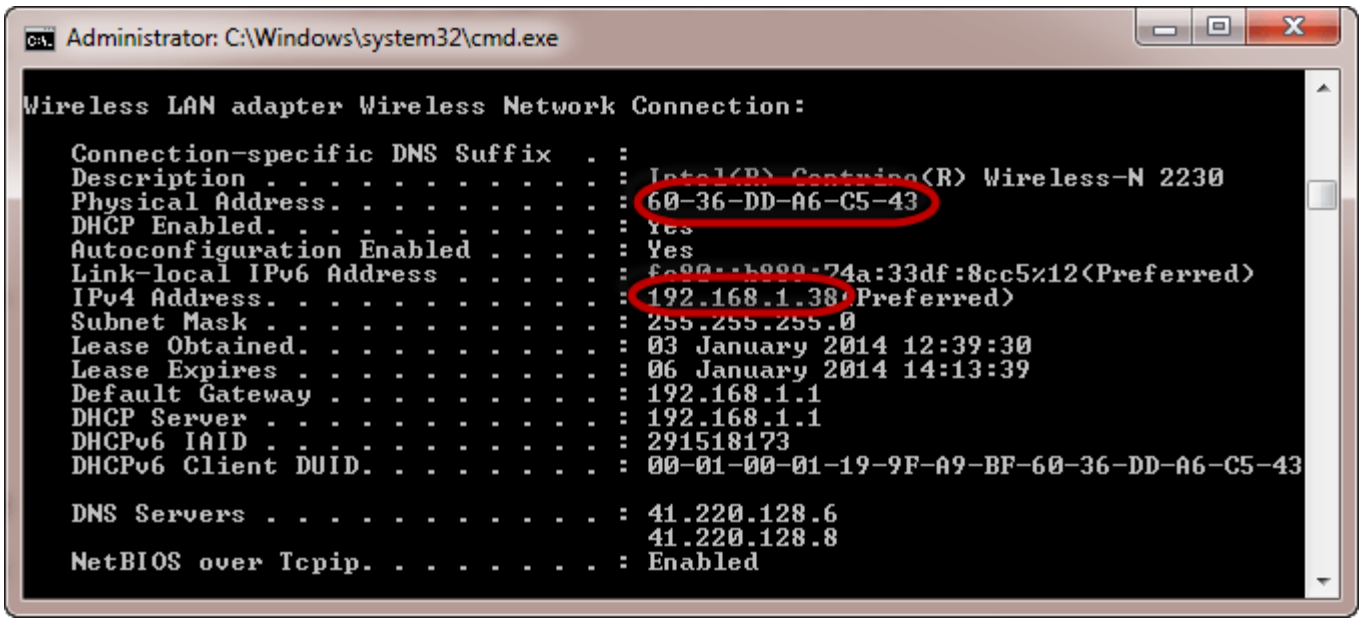


***Note**: dynamic entries are added and deleted automatically when using TCP/IP sessions with remote computers.*

Static entries are added manually and are deleted when the computer is restarted, and the network interface card restarted or other activities that affect it.

Adding static entries

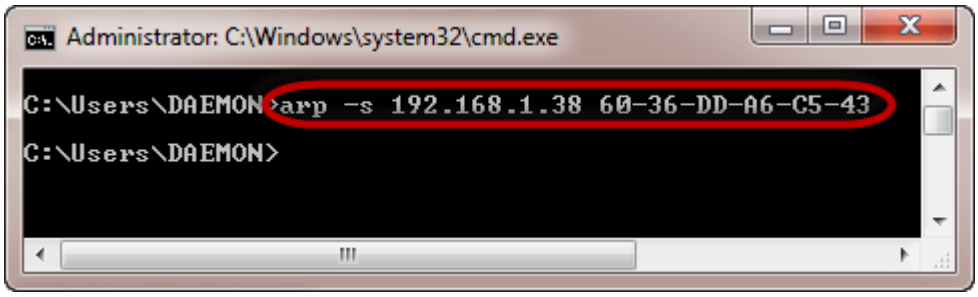
Open the command prompt then use the ipconfig /all command to get the IP and MAC address



The MAC address is represented using the Physical Address and the IP address is IPv4Address

Enter the following command

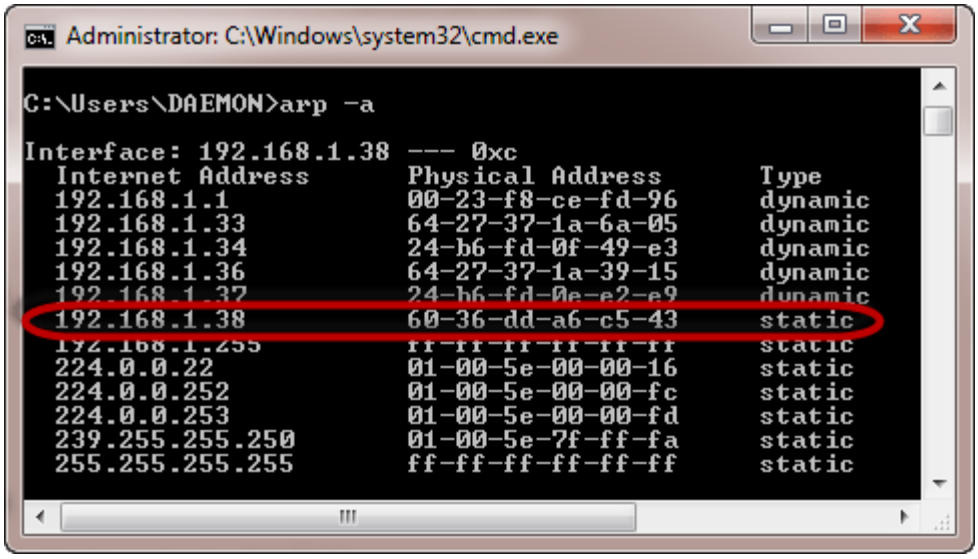
arp –s 192.168.1.38 60-36-DD-A6-C5-43



Note: The IP and MAC address will be different from the ones used here. This is because they are unique.

Use the following command to view the ARP cache

arp –a
You will get the following results

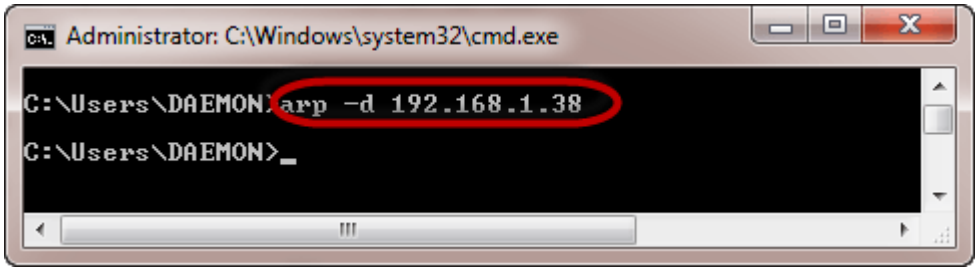


Note the IP address has been resolved to the MAC address we provided and it is of a static type.

Deleting an ARP cache entry

Use the following command to remove an entry

arp –d 192.168.1.38



P.S. ARP poisoning works by sending fake MAC addresses to the switch

Result: Thus, the experiment was completed successfully.

10. Perform an Experiment How To Use Dumpsec

Aim: To understand and install Dumpsec tool for Security.

Procedure:

To do this, press the Windows key + R at the same time and then type 'appwiz.cpl'. Then find Somarsoft DumpSec in the list of installed programs and uninstall this application. A most useful application that was especially created in order to help systems administrators who work with Windows NT infrastructures SOFTPEDIA.

DumpSec is a security auditing program for Microsoft Windows NT/XP/200x. It dumps the permissions (DACLs) and audit settings (SACLs) for the file system, registry, printers and shares in a concise, readable format, so that holes in system security are readily apparent. DumpSec also dumps user, group and replication information. Windows contains a variety of system utilities that are useful, but well-hidden. Some are buried deep in the Start menu, while others you can access only if you know the right command to run. You can launch most of these tools pretty easily if you know their names—just search your start menu for the name of the tool, and you're good to go. On Windows 8, you may have to select the Settings category on the search screen to have the actual tool show up in the search results. Regardless of how you launch them, these tools can help you do everything from diagnose crashes to examine system performance to improve security.

Windows Memory Diagnostic

RELATED:How to Test Your Computer's RAM for ProblemsWindows includes a Memory Diagnostic tool that restarts your computer (so nothing is loaded into memory) and tests your memory for defects—much like the popular MemTest86 application. If you want to check your computer's memory for errors, you don't need a third-party tool—just run the Windows Memory Diagnostic tool by searching for it on your Start menu.

RELATED:10+ Useful System Tools Hidden in Windows

The Resource Monitor app offers a detailed look at your computer's resource usage. You can view computer-wide CPU, disk, network, and memory graphics, or drill down and view per-process statistics for each type of resource.You can see which processes are using your disk or network heavily, which are communicating with Internet addresses, and more. The Resource Monitor provides much more detailed resource statistics than the Task Manager does.You can launch the Resource Monitor by opening the Task Manager, clicking the "Performance" tab, and selecting "Resource Monitor" or by just searching for "resource monitor" on your Start menu.

Performance Monitor

RELATED:Geek School: Learning Windows 7 – Monitoring, Performance and Keeping Windows Up To DateThe Performance Monitor app can collect performance data from hundreds of different sources. You can use it to log performance data over time—letting you determine how system changes affect performance—or to monitor the performance of a remote computer in real-time.

Computer Management and Administrative Tools

The Performance Monitor is actually one of many Microsoft Management Console (MMC) tools. Many of these can be found in the "Administrative Tools" folder in the Control Panel, but you can also access them through a single window by opening the Computer Management application. Just hit Start and type "computer management" in the search box.Among other things, this window contains the following tools:RELATED:What Is the Windows Event Viewer, and How Can I Use It?

Task Scheduler: A tool that allows you to view and customize the scheduled tasks on your computer, in addition to creating your own custom scheduled tasks.

Event Viewer: A log viewer that allows you to view and filter system events—everything from software installation to application crashes and blue screens of death.

Shared Folders: An interface that displays the folders shared over the network on your computer, useful for viewing what folders are being shared at a glance.

Device Manager: The classic Windows Device Manager that allows you to view the devices connected to your computer, disable them, and configure their drivers.

Disk Management: A built-in partition manager you can use without downloading any third-party tools.

Services: An interface that allows you to view and control the background services running in Windows.

Advanced User Accounts Tool

Windows contains a hidden User Accounts utility that provides some options not present in the standard interface. To open it, hit Start (or press Windows+R to open the Run dialog), type either "netplwiz" or "control userpasswords2," and then press Enter.RELATED:Using Local Users and Groups to Manage User Passwords in Windows 7The "User Accounts" window also contains a shortcut to launch the"Local Users and Groups" tool, which offers more user management tasks, but isn't available on the Home editions of Windows.

Disk Cleanup

RELATED:7 Ways To Free Up Hard Disk Space On WindowsWindows' Disk Cleanup utility isn't quite as hidden as some of the other utilities here, but not enough people know about it—or how to use it to its fullest potential. It scans your computer for files that can be safely deleted—temporary files, memory dumps, old system restore points, leftover files from Windows upgrades, and so on.Disk Cleanup does the same job a PC cleaning utility does, but it's free and doesn't try to extract any money from you. Advanced users may prefer CCleaner, but Disk Cleanup does a decent job.Access it by searching for "Disk Cleanup" on your Start menu.

Local Group Policy Editor

The Local Group Policy Editor is only available on Professional or Ultimate editions of Windows—not the standard or Home editions. It provides a wide variety of settings that are designed for use by system administrators to customize and lock down PCs on their networks, but the Local Group Policy Editor also contains settings that average users might be interested in. For example, in Windows 10, you can use it to hide personal information on the sign in screen.

Microsoft Dumpsec Utility Download

To open the Local Group Policy Editor, type“gpedit.msc” at the Start menu or Run dialog box, and then press Enter.

Registry Editor

Sure, everyone knows about Registry Editor—but it’s still hidden, with Microsoft not even providing a Start menu shortcut to it. To launch it, you must type “regedit” into the Start menu search or Run dialog box.Many tweaks that you can make using the Local Group Policy Editor have equivalent tweaks that can be made in Registry Editor if you don’t have a Professional or Enterprise edition of Windows. For example, users with the Home edition of Windows can’t prevent specific users from shutting down Windows using group policy—but they can with a few Registry tweaks. In addition, there are all kinds of Registry tweaks that have no equivalent in group policy at all—like customizing the manufacturer support information on your PC. RELATED: Learning to Use the Registry Editor Like a ProFair warning, though: Registry Editor is a complex and powerful tool. It’s easy to damage your installation of Windows, or even render Windows inoperable if you’re not careful. If you’ve never worked with the Registry before, consider reading about how to use the Registry Editor before you get started. And definitely back up the Registry (and your computer!) before making changes. And stick to well-documented Registry tweaks from a source you trust.

System Configuration

System Configuration is another classic tool that many people don’t know about. Prior to Windows 8 and 10, which feature a startup-program manager built into Task Manager, System Configuration was the only included way of controlling startup programs on Windows. It also allows you to customize your boot loader, which is particularly useful if you have multiple versions of Windows installed.Launch it by typing “msconfig” into the Start menu search box or Run dialog.

System Information

The System Information utility displays all kinds of information about your PC. You can find out things like the exact version of Windows you’re running, what kind of motherboard your system contains, how much RAM (and what kind) you have, what graphics adapter you’re sporting, and a whole lot more.RELATED:Find Detailed Hardware Information with SpeccySystem Information doesn’t provide the slickest interface, nor does it provide all the information a third-party system information tool like Speccy

does, but it will display a lot of system information without forcing you to install another program.Open it by searching for “System Information” at your Start menu.Once you know these utilities exist, you can do more with the tools built into Windows. These tools are available on any Windows computer (with the lone exception that Local Group Policy Editor isn’t available on Home editions of Windows), so you can always use them without downloading and installing third-party software.

Result: Thus, the experiment was completed successfully.

11. Perform an Experiment How To Use Dumpsec

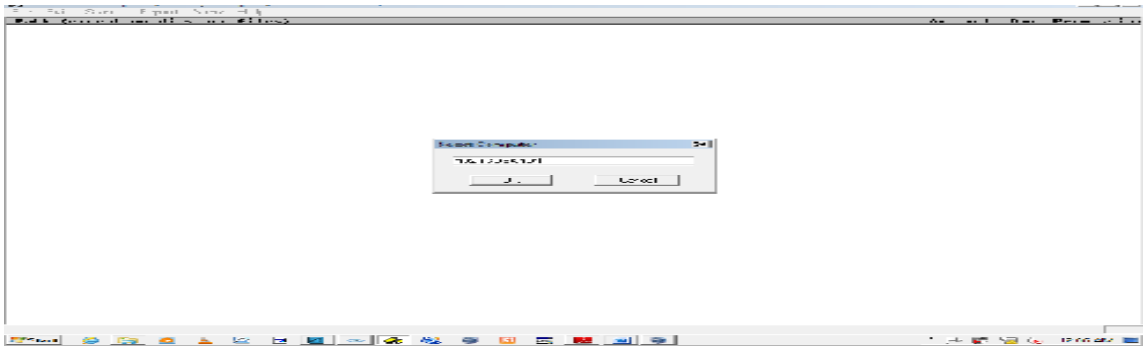
Aim: To operate Dumpsec tool for Security.

Procedure:

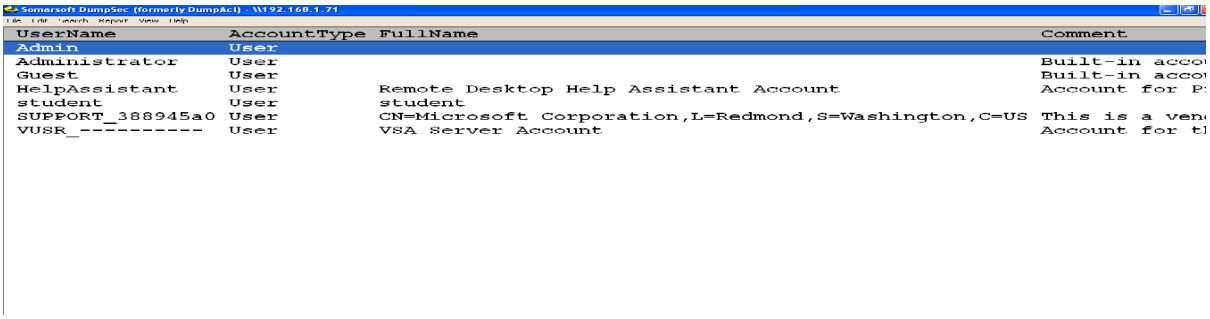
SomarSoft's Dumper is a (free) security auditing program for Microsoft Windows NT/2000. It dumps the permissions (DACLs) and audit settings (SACLs) for the file system, registry, printers and shares in a concise, readable format, so that holes in system security are readily apparent. DumpSec also dumps user, group and replication information. DumpSec is a must have product for Windows NT systems administrators and computer security auditors.

1. Download & install dumpsec.

2. Open dumpsec and select computer

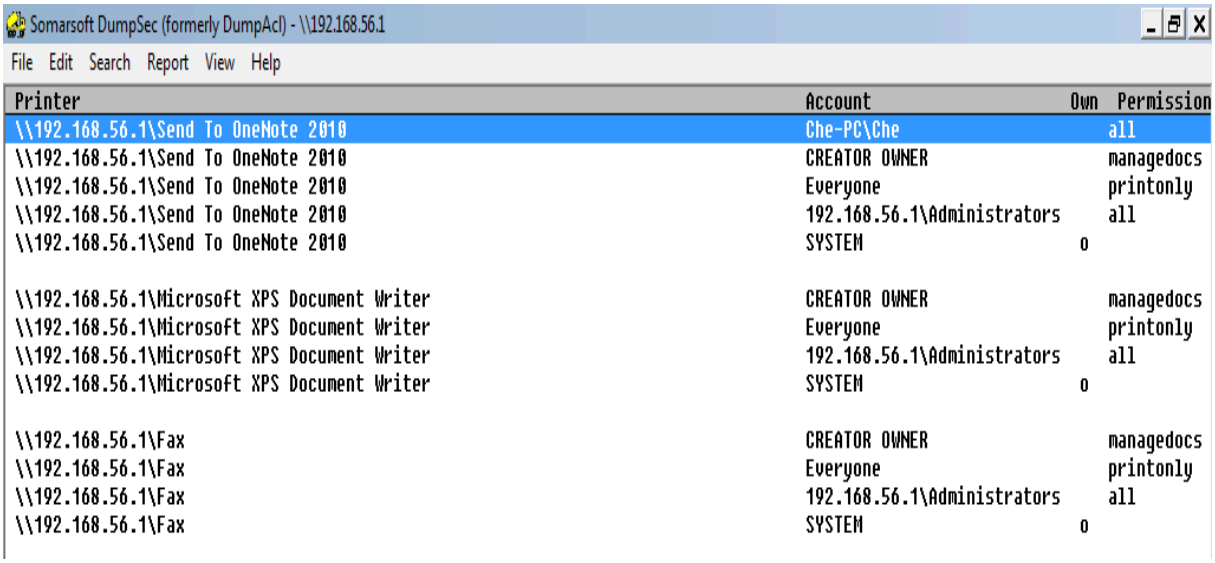


2. Now select report=> dump users as table and click ok.



UserName	AccountType	FullName	Comment
Admin	User		
Administrator	User		Built-in acco
Guest	User		Built-in acco
HelpAssistant	User	Remote Desktop Help Assistant Account	Account for P
student	User	student	
SUPPORT_388945a0	User	CN=Microsoft Corporation,L=Redmond,S=Washington,C=US	This is a ven
VUSR_----------	User	VSA Server Account	Account for t

Printer Sharing Report

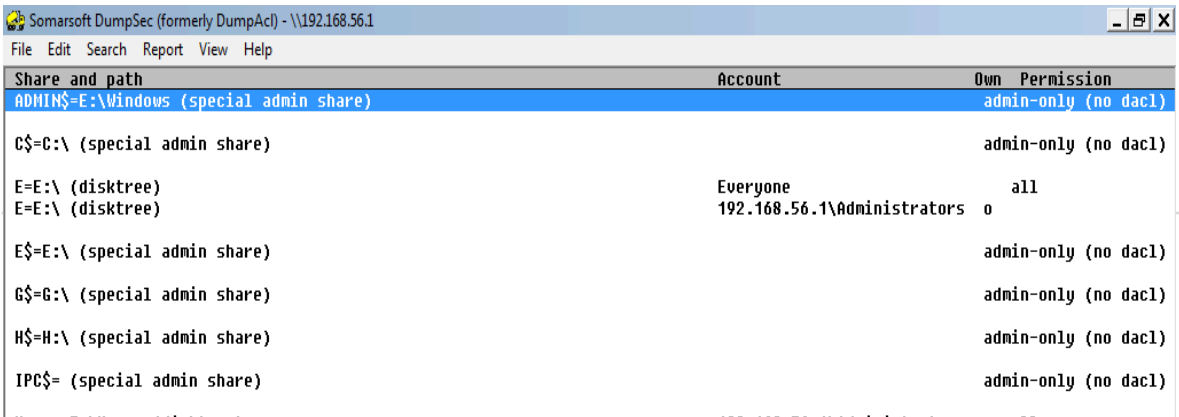


Somarsoft DumpSec (formerly DumpAcl) - \\192.168.56.1

File Edit Search Report View Help

Printer	Account	Own	Permission
\\192.168.56.1\Send To OneNote 2010	Che-PC\Che		all
\\192.168.56.1\Send To OneNote 2010	CREATOR OWNER		managedocs
\\192.168.56.1\Send To OneNote 2010	Everyone		printonly
\\192.168.56.1\Send To OneNote 2010	192.168.56.1\Administrators		all
\\192.168.56.1\Send To OneNote 2010	SYSTEM	o	
\\192.168.56.1\Microsoft XPS Document Writer	CREATOR OWNER		managedocs
\\192.168.56.1\Microsoft XPS Document Writer	Everyone		printonly
\\192.168.56.1\Microsoft XPS Document Writer	192.168.56.1\Administrators		all
\\192.168.56.1\Microsoft XPS Document Writer	SYSTEM	o	
\\192.168.56.1\Fax	CREATOR OWNER		managedocs
\\192.168.56.1\Fax	Everyone		printonly
\\192.168.56.1\Fax	192.168.56.1\Administrators		all
\\192.168.56.1\Fax	SYSTEM	o	

Permission on Shares:



Somarsoft DumpSec (formerly DumpAcl) - \\192.168.56.1

File Edit Search Report View Help

Share and path	Account	Own	Permission
ADMIN$=E:\Windows (special admin share)			admin-only (no dacl)
C$=C:\ (special admin share)			admin-only (no dacl)
E=E:\ (disktree)	Everyone		all
E=E:\ (disktree)	192.168.56.1\Administrators	o	
E$=E:\ (special admin share)			admin-only (no dacl)
G$=G:\ (special admin share)			admin-only (no dacl)
H$=H:\ (special admin share)			admin-only (no dacl)
IPC$= (special admin share)			admin-only (no dacl)

Result: Thus, the experiment was executed successfully.

12. Implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) network protocols

Aim: To implement the secure socket layer and transport layer security network protocols

Procedure:

Before diving into the many benefits and uses of SSL Certificates, it may help understand the underpinning technology. This article provides a brief history lesson on how Secure Socket Layer (SSL) has evolved into Transport Layer Security (TLS) and a simple explanation of how they provide security for both Public Internet and Enterprise Intranet connections.

In particular, the aim is to give you a complete overview of the Secure Socket Layer (SSL) protocol and certificates to help you make the best decisions regarding certificate management for your enterprise.

What is SSL?

SSL is the original name of the cryptographic protocol for authenticating and encrypting communications over a network. Officially, SSL was replaced by an updated protocol called TLS some time ago.

SSL to TLS Timeline

The following is a timeline of how SSL has changed over time:

SSL is a security protocol developed by Netscape in the 90s for encrypting and securing communications over the internet. SSL v1.0 was never released due to security issues.

In 1995, Netscape released SSL v2.0, but it still had many flaws.

SSL v3.0 released in 1996 and addressed the problems of SSL v2.0. This version offered incredible improvements and forever changed the way the internet works. However, as of 2015, SSL 3.0 and prior versions have been deprecated.

TLS was developed by the Internet Engineering Task Force (IETF) as an improvement on SSL; TLS v1.0 released in 1999 and based on SSL v3.0, with minor security improvements still significant enough that SSL v3.0 and TLS v1.0 did not interoperate.

TLS v1.1 came out seven years later in 2006 and was replaced by TLS v1.2 shortly afterward, in 2008. That hurt TLS v1.1 adoption as many websites upgraded from TLS v1.0 directly to TLS v1.2. 11 years later, we are now at TLS v1.3.

TLS v1.3 finalized in 2018 and after nearly 30 IETF drafts. TLS v1.3 makes significant improvements over its predecessors. Microsoft, Apple, Google, Mozilla, Cloudflare, and Cisco all have deprecated TLS v1.0 and TLS v1.1 as of March 2020. TLS v1.2 and TLS v1.3 are now the only SSL protocols still available.

So, in reality, TLS is simply a newer version of SSL. However, most people still say SSL instead of TLS. SSL and TLS serve the same purpose, protecting sensitive information during transmission, but under the hood, the cryptography has changed a lot from the original SSL to the latest TLS v1.3.

Digital certificates are the core of the SSL protocol; they initiate the secure connections between servers (e.g., websites, intranets, or VPN) and clients(e.g., web browsers, applications, or email clients).

SSL certificates offer adequate protection against phishing and eavesdropping of transmissions and automatic authentication of a server, such as a website domain. If a website asks for users' sensitive

information, it needs to have an SSL certificate to encrypt it during transmission. If there is no SSL certificate, then that connection should not be trusted with any private information.

How does it Work?

The primary purpose of SSL is to provide a secure transport-layer connection between two endpoints, the server and the client. This connection is typically between a website server and the client's browser, or a mail server and the client's email application, such as Outlook.

SSL comprises two separate protocols:

The Handshake protocol authenticates the server(and optionally the client), negotiates crypto suites, and generates the shared key.

The Record protocol isolates each connection and uses the shared key to secure communications for the remainder of the session.

The Handshake Protocol

The SSL handshake is an asymmetric cryptography process for establishing a secure channel for server and client to communicate — HTTPS connections always begins with the SSL handshake.

A successful handshake takes place behind the client's browser or application, instantly and automatically — without disturbing the client user experience. However, A failed handshake triggers the termination of the connection, usually preceded by an alert message in the client's browser.

Provided the SSL is valid and correct, the handshake offers the following security benefits:

Authentication: The server is always authenticated for as long as the connection is valid.

Confidentiality: Data sent via SSL is encrypted and only visible to the server and client.

Integrity: Digital Certificate Signatures ensure the data has not been modified during the transfer.

In summary, SSL certificates fundamentally work using a blend of asymmetric cryptography and symmetric cryptography for communications over the internet. There are also other infrastructures involved in achieving SSL communication in enterprises, known as Public Key Infrastructures.

How do SSL Certificates Work?

When you receive the SSL certificate, you install it on your server. You can install an Intermediate certificate that establishes your SSL certificate's credibility by chaining it to your CA's root certificate.

Root certificates are self-signed and form the basis of an X.509-based Public-Key Infrastructure (PKI). The PKI supporting HTTPS for secure web browsing and electronic signature schemes depends on root certificates. In other applications of X.509 certificates, a hierarchy of certificates certifies a certificate's issuance validity. This hierarchy is called a certificate "Chain of Trust."

Chain of Trust

The Chain of Trust refers to your SSL certificate and its link to a trusted certificate authority. For an SSL certificate to be trusted, it must trace back to a trusted root CA. A Chain of Trust ensures privacy, trust, and security for all parties involved.

At the core of every PKI is the root CA; it serves as the trusted source of integrity for the entire system. The root certificate authority signs an SSL certificate, thus starting the Chain of Trust. If the root CA is publicly trusted, then any valid CA certificate chained to it is trusted by all major internet browsers and operating systems.

How is a Trust Chain Verified?

The client or browser inherently knows the Public-Keys of a handful of trusted CAs and uses these keys to verify the server's SSL certificate. The client repeats the verification process recursively with each certificate in the Trust Chain until tracing it back to the beginning, the root CA.

What does an SSL Certificate do?

In unsecured HTTP connections, hackers can easily intercept messages between client and server and read them in plain text. Encrypted connections scramble communication until the client can decrypt it with the other session key.

When installed on a web server, SSL certificates use a public/private key pair system to initiate the HTTPS protocol and enable secured connections for users and clients to connect.

For the Internet: What do SSL certificates do for websites?

When a signed SSL certificate secures a website, it proves that the organization has verified and authenticated its identity with the trusted third party; since the browser trusts the CA, the browser now trusts that organization's identity too.

The easiest way to check if the website has an SSL installed is to look at your browser; see if the website URL starts with "HTTPS:" as this shows if it has an SSL certificate installed on the server. If so, click the padlock icon in the address bar to view the certificate information.

Web browsers use HyperText Transfer Protocol (HTTP) to connect to web servers that listen on TCP port 80 by default. HTTP is a plain-text protocol, which means it is relatively easy for a hacker to intercept and read the transit data. It is not adequate for any application that requires confidentiality.

SSL uses port number 443, encrypting data exchanged between the browser and the server and authenticating the user. Therefore, when the communications between the web browser and server need to be secure, the browser automatically switches to SSL — that is, as long as the server has an SSL certificate installed.

Establishing a connection with a server with a certificate signed by a trusted CA takes place without additional difficulties for the user. When an internet user visits an SSL-secured website, they are more willing to submit their contact information or shop with their credit card. Furthermore, having an SSL certificate on your website increases your ranking position, making it easier for users and customers to find your site.

SSL certificate attests to the reliability of a website, but with more advanced certificates, the entire company can be SSL certified.

For Intranets: What do SSL certificates do for applications in an enterprise environment?

Although SSL's original purpose was for the World Wide Web, enterprises use SSL certificates to secure a wide variety of internal and external connections. The most common use cases for Enterprise SSL certificates include:

Virtual Private Networks (VPN)

Single sign-on

Internet of Things(IoT)

If properly configured, all these applications run atop of SSL protocol. We'll take a closer look at these examples in the following section:

Network Access

Employees who connect wireless devices to the corporate network have a need for ease of access, while at the same time, the network must prevent unauthorized access to corporate resources. Employees may use SSL certificates to access and encrypt files from their devices, corporate servers, or even cloud servers for approved individuals.

Avoid the need to remember/reset long, difficult to remember passwords that change every 90 days by replacing it with a digital identity. Place a digital identity into the Windows or Mac desktop, server, or WiFi access points, so only authorized devices can connect to your corporate network.

Single Sign-On

Today's enterprise employees have access to a wide variety of Identity service or federation products. Enterprises often use a Web Single Sign-on product to access all its resources in the corporate portal or cloud services.

Internet of Things

A digital identity can be installed in your IoT device and the user's device or application to ensure that only trusted IoT devices could connect to your network. The IoT device takes instructions from or sends data to authorized applications, and users possess a digital identity.

SSL VPN

A Secure Sockets Layer Virtual Private Network (SSL VPN) is a virtual private network (VPN) created using the Secure Sockets Layer (SSL) IT departments can scale both the solution and its required infrastructure services. SSL VPN enables granular control over managed application access to enterprise web applications. Perhaps the most significant benefits of SSL VPN come from the gained efficiency and productivity of freeing up IT resources by enabling all digital certificates to be accessed remotely.

Code, document, and email signing

A Secure Sockets Layer Virtual Private Network (SSL VPN) is a virtual private network (VPN) created using the Secure Sockets Layer (SSL) IT departments can scale both the solution and its required infrastructure services. SSL VPN enables granular control over managed application access to enterprise web applications. Perhaps the most significant benefits of SSL VPN come from the gained efficiency and productivity of freeing up IT resources by enabling all digital certificates to be accessed remotely.

Many people don't realize that code, document, and email signing certificates are not SSL certificates. Even though they are all facilitated by PKI x.509 certificates, the key-usage function makes all the difference. Read "Difference Between Code Signing and SSL certificate" or "Difference Between Digital certificate and Digital Signature" to learn more on the subject**.**

Procedure to generate password hashes with openssl

1. The Open SSL is command line binary can perform a wide range of cryptographic operation.

2. Install Open SSL setup file on to the default location.

3. Perform Full installation and Click Next.

4. Create Document shortcuts in start menu and Click Next

5. Complete the installation.

6. Execute the Open SSL from command prompt available at

C:\ProgramFiles\GnuWin32\OpenSSL\openssl.exe

7. openssl> (This is the Open SSL prompt)

8. Now execute the command as follows for password generation.

9. Passwd –crypt [type your password] This is limited to 8 characters password generator.

10. Passwd -1 [your password] This allows you to insert password length beyond 8 characters.

11. Type this command to generate 10-12 characters passwords of TEN numbers.

Result: Thus, the experiment was completed successfully.

13. Setup a Honey Pot on Network

Aim: To setup a honey pot on network

Procedure:

Honey Pot is a device placed on Computer Network specifically designed to capture malicious network traffic. KF Sensor is the tool to setup as honeypot when KF Sensor is running it places a siren icon in the windows system tray in the bottom right of the screen. If there are no alerts then green icon is displayed.

STEPS:

1. Install winpcap library (mandatory for kfsensor)

2.Download kfsensor and install

3.Then restart your pc. Configure properly no change needs to do now go to setting option and configure according to your attack.

4.Now go to your home screen of kf sensor

5.You will get some logs about clients and it will start working

KFSensor

- Windows based honeypot known as KF Sensor
- It detects an incoming attack or port scanning and reports it to you
- A machine running KFSensor can be treated as just another server on the network, without the need to make complex changes to routers and firewalls.

How KFSensor Works?

- KFSensor is an Intrusion Detection System.
- It performs by opening ports on the machine it is installed on and waiting for connections to be made to those ports.

- By doing this it sets up a target, or a honeypot server, that will record the actions of a hacker.

Components: KFSensor server

- KFSensor Server- Performs core functionality
- It listens to both TCP and UDP ports on the server machine and interacts with visitors and generates events.

A daemon that runs at the background (like Unix daemon)

Components: KFSensor Monitor

- Interprets all the data and alerts captured by server in graphical form.
- Using it you can configure the KFSensor Server and monitor the events generated by the KFSensor Server.

Sim Server

- Sim server is short for simulated server.
- It is a definition of how KFSensor should emulate real server software.
- There is no limit to the number of Sim Servers that can be defined.
- There are two types of Sim Server available; the Sim Banner and the Sim Standard Server.

Setting Up a HoneyPot

• You can get educational License from Keyfocus.

• Install WinPCap – A industry standard network packet capturing library

• Install KFSensor

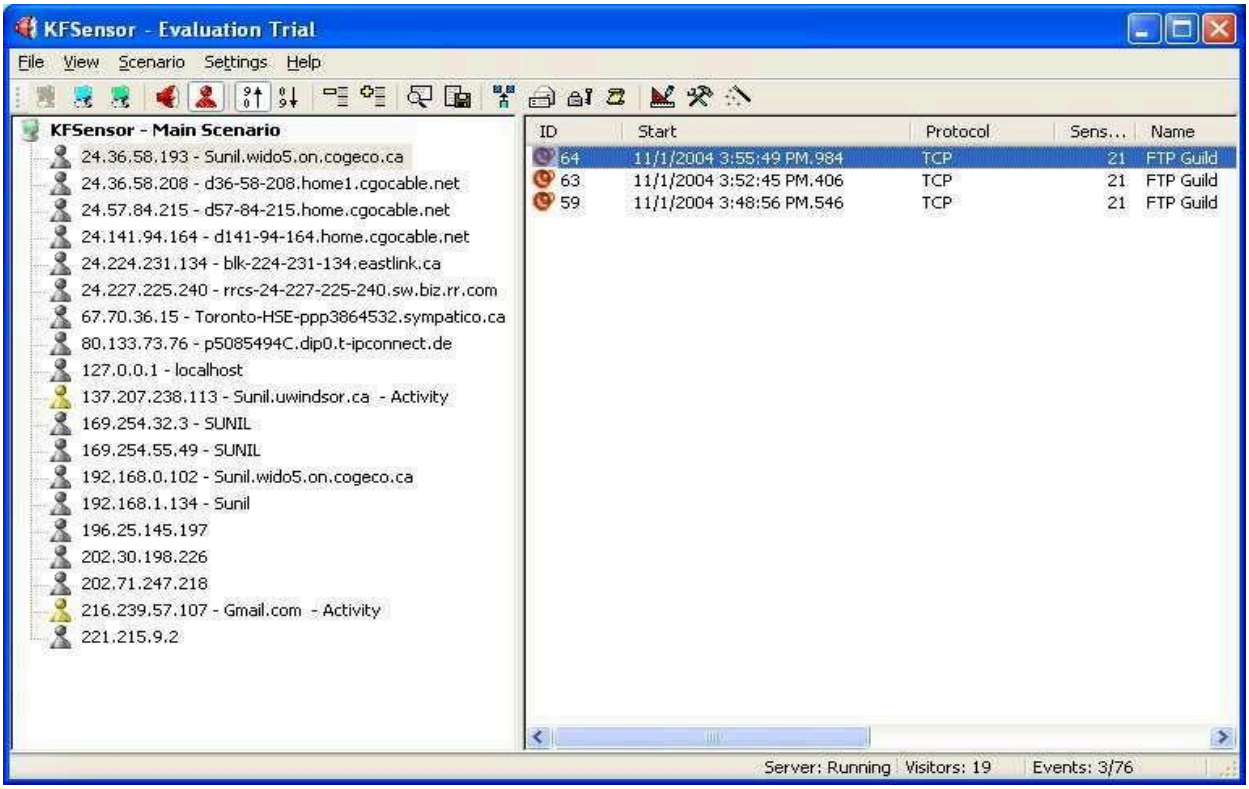
RESULT: Thus, the program was executed and verified successfully.

14. Monitor the Honey Pot on Network

Aim: To monitor the honey pot on network

Procedure:

KFSensor Monitor



Terminology

Visitor

A visitor is an entity that connects to KFSensor.

Event

• Visitors could be hackers, worms, viruses or even legitimate users that have stumbled onto KFSensor by mistake.

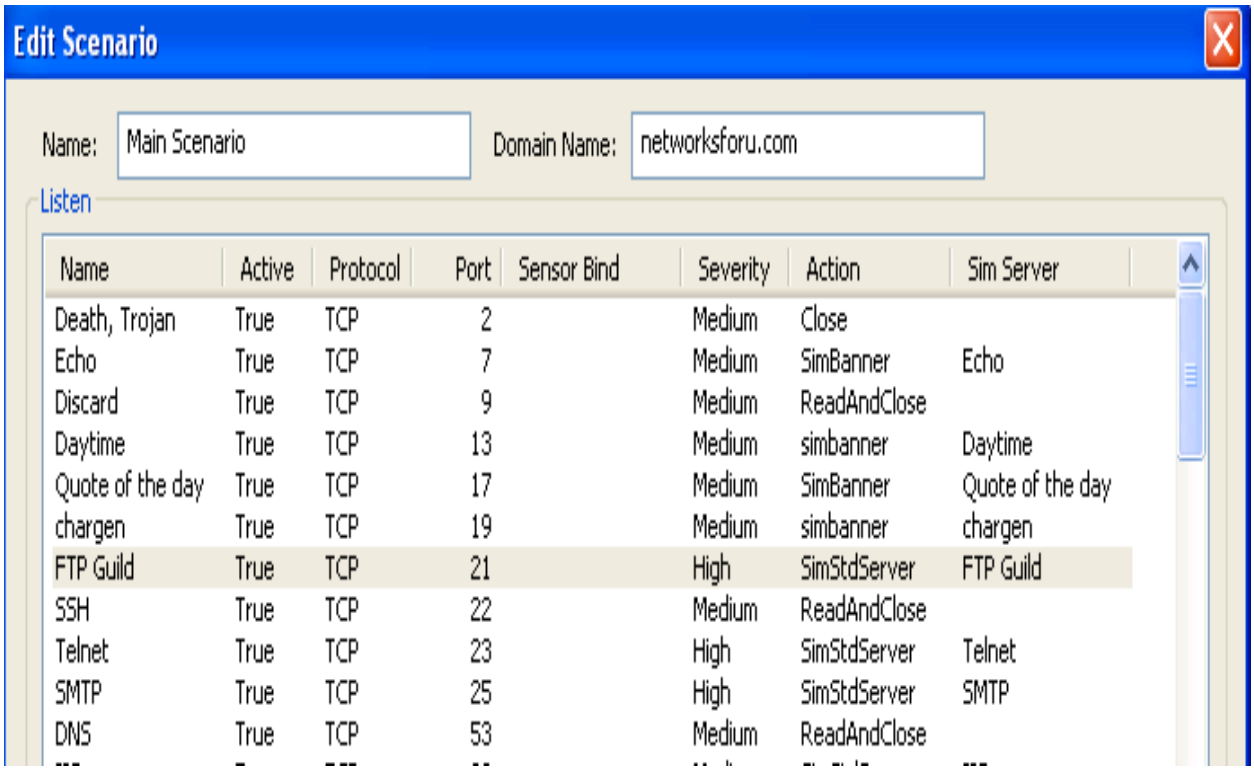
• Visitors can also be referred to as the clients of the services provided by KFSensor.

• An event is a record of an incident detected by the KFSensor Service.

• For example, if a visitor attempts to connect to the simulated web server then an event detailing the connection is generated.

• Events are recorded in the log file and displayed in the KFSensor monitor.

Editing Scenario



Name	Active	Protocol	Port	Sensor Bind	Severity	Action	Sim Server
Death, Trojan	True	TCP	2		Medium	Close	
Echo	True	TCP	7		Medium	SimBanner	Echo
Discard	True	TCP	9		Medium	ReadAndClose	
Daytime	True	TCP	13		Medium	simbanner	Daytime
Quote of the day	True	TCP	17		Medium	SimBanner	Quote of the day
chargen	True	TCP	19		Medium	simbanner	chargen
FTP Guild	True	TCP	21		High	SimStdServer	FTP Guild
SSH	True	TCP	22		Medium	ReadAndClose	
Telnet	True	TCP	23		High	SimStdServer	Telnet
SMTP	True	TCP	25		High	SimStdServer	SMTP
DNS	True	TCP	53		Medium	ReadAndClose	

Terminology – Rules

• KFSensor is rules based.

• All of the data that was produced was the result of KFSensor detecting certain types of activity and then using a rule to determine what type of action should be taken.

• We can easily modify the existing rules or add your own.

Edit Active Scenario

• To create or modify rules,

– Scenario menu ->select the Edit Active Scenario command ->you will see a dialog box which contains a summary of all of the existing rules.

– either select a rule and click the Edit button to edit a rule, or you can click the Add button to create a new rule.

Adding a rule

• Click the Add button and you will see the Add Listen dialog box.

– The first thing that this dialog box asks for is a name. This is just a name for the

rule.

– Pick something descriptive though, because the name that you enter is what will

show up in the logs whenever the rule is triggered.

Download Link

• http://www.keyfocus.net/kfsensor/free-trial/

• Write to support@keyfocus.net and request for educational license

Installing KFSensor

1.Download and install winpcap

2.Download and install KFSensor

3. Enable Telnet client, server, Internet Information server in Control Panel-> Programs-> Turn windows features on/off

- Check Telnet client, Telnet server, IIS-> FTP (both options),

Convert to Native Service

1. Convert the stroked off services as native services.

*Select Scenario ->Edit Active Scenario

* Choose the respective service listed in the dialog box opened and press convert to native button and ok.

Setting up Server

1. To start the server

• Settings-> Set Up Wizard

• Go through the wizard, give fictitious mail ids when they are asked and start the server running by pressing the finish button.

2. Kfsensor now start showing the captured information in its window.

FTP Emulation

1. Open command prompt

2. Type

Ftp ipaddress

Enter user name anonymous

Enter any password

Get any file name with path

3. Monitor this ftp access in KFSensor monitor

4. Right click KFSensor entry, select Event details, see the details captured by the server

5. Create visitor rule by right clicking the FTP entry and check either ignore / close under actions

in the dialog box that opened.

6. Now redo the above said operations at the command prompt and see how the emulation

behaves.

7. You can see/ modify the created rules in Scenario->edit active visitor rules.

SMTP Emulation

1. open command prompt

2. Type

telnet ipaddress 25

Helo

Mail from:<mail-id>

Rcpt to:<mail-id>

Data

type contents of mail end that with . in new line

3. Check the kfsensor for the captured information.

IIS emulation

1. Create an index.html, store it in c:\keyfocus\kfsensor\files\iis7\wwwroot

2. Select scenario->edit simserver

1. Choose iis and edit

2. Make sure index.html is in first place in the listed htm files in the dialog box

3. Check the kfsensor for the captured information.

DOS attack

1. Settings-> DOS attack settings modify (reduce) values in general tab, ICMP and other tabs. Press ok.

2. Open command prompt and type

Ping ipaddress –t or

Ping –l 65000 ipaddress –t

1. Check the kfsensor for the DOS attack alerts, open event details in right click menu for further details.

RESULT: Thus, the program was executed and verified successfully.

15. Demonstrate Intrusion Detection System (IDS) using any tool (snort or any other software)

Aim: To Demonstrate Intrusion Detection system.

Procedure:

SNORT can be configured to run in three modes:

1. Sniffer mode

2. Packet Logger mode

3. Network Intrusion Detection System mode

Sniffer mode snort –vPrint out theTCP/IPpackets header on thescreen

Snort –vd show theTCP/IPICMPheaderwith application data in transit.

PacketLogger mode snort–dev –l c:\log[createthis directoryin theC drive]and snort will

automatically know to go into packet logger mode, it collects every packet it sees and places it in logdirectory.snort –dev –l c:\log–hipaddress/24 This rule tells snort thatyou want to printout thedata link and TCP/IPheaders as wellasapplication data into the logdirectory.snort –l c:\log–b This is binarymodelogseverythinginto asinglefile.

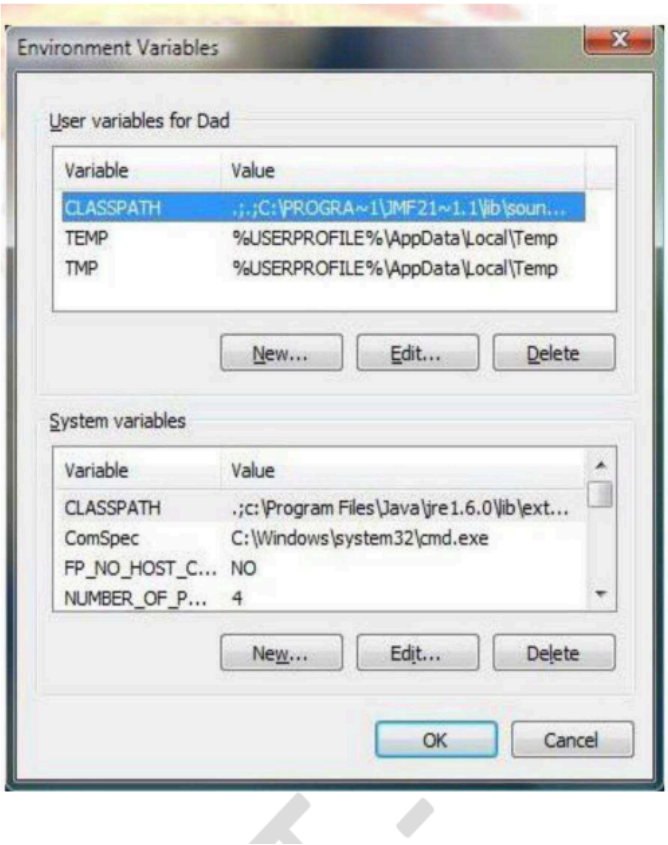
Network Intrusion Detection System mode snort –d c:\log–h ipaddress/24–csnort.conf This is a configuration file applies ruleto each packet to decide it an action based upon the rule typein the file. Snort –d –h ipaddress/24 –l c:\log–csnort.conf This will configuresnortto run in its most basic NIDS form, loggingpackets that trigger rules specifies in the snort.conf

- Download SNORT fromsnort.org
- Install snort with or without database support.

1. Select all the components and Click Next. Install and Close.

2. Skip the Win Pcap driver installation

3. Add the path variable in windows environment variable by selecting new class path. Create a path variable and point it at snort.exe variable namepath and apath variable and point it at snort.exe variable namepath and variable valuec:\snort\bin.



4. Click OKbutton and then close alldialogboxes.

5.Open command prompt and type the following commands:

Result: Thus, demonstration of IDS is completed successfully.

16. Installation of Kali Linux in Virtualbox

Aim: To install kali linux in virtualbox

Procedure:

Kali Linux is a Debian-derived Linux distribution designed for penetration testing. With over 600 preinstalled penetration-testing programs, it earned a reputation as one of the best-operating systems used for security testing. As a security-testing platform, it is best to install Kali as a VM on VirtualBox. Kali has a rolling release model, ensuring up-to-date tools on your system. Also, there is an active community of users providing ongoing support.

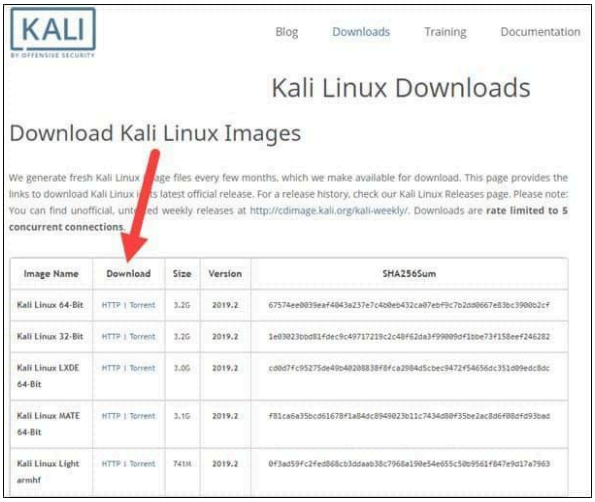
Steps For Installing Kali Linux on VirtualBox

Since these instructions take you through the installation process in a virtual environment, you need to ensure you have one set up on your system. In this article, we are using VirtualBox, as it is a simple to use, open-source virtualization solution. In case you do not have VirtualBox installed, use this step-by-step VirtualBox installation guide.

Step 1: Download Kali Linux ISO Image

On the official Kali Linux website downloads section, you can find Kali Linux .iso images. These images are uploaded every few months, providing the latest official releases.

Navigate to the Kali Linux Downloads page and find the packages available for download. Depending on the system you have, download the 64-Bit or 32-Bit version.

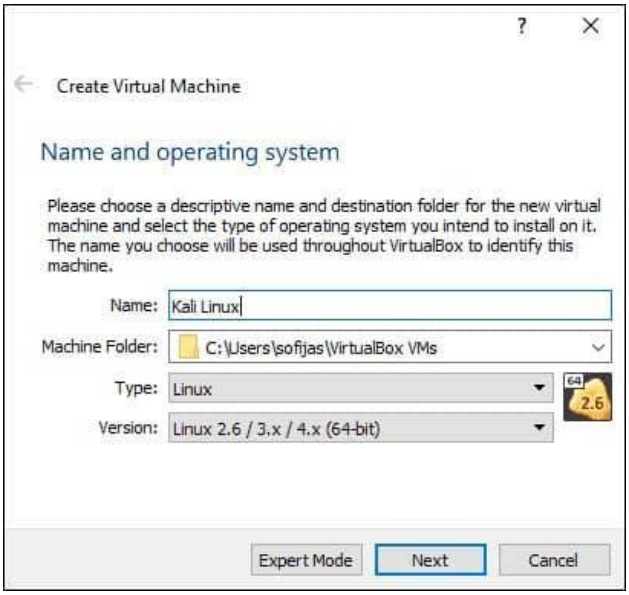


Step 2: Create Kali Linux VirtualBox Container

After downloading the .iso image, create a new virtual machine and import Kali as its OS.

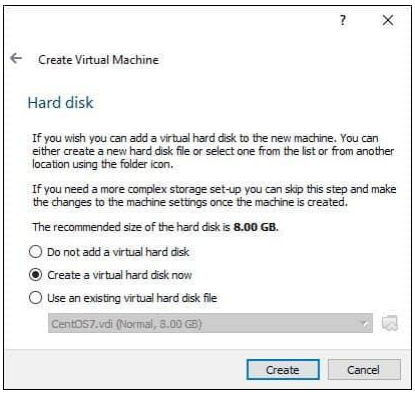
1. Launch VirtualBox Manager and click the New icon.

2. Name and operating system. A pop-up window for creating a new VM appears. Specify a name and a destination folder. The Type and Version change automatically, based on the name you provide. Make sure the information matches the package you downloaded and click Next.



3. Memory size. Choose how much memory to allocate to the virtual machine and click Next. The default setting for Linux is 1024 MB. However, this varies depending on your individual needs.

4. Hard disk. The default option is to create a virtual hard disk for the new VM. Click Create to continue. Alternatively, you can use an existing virtual hard disk file or decide not to add one at all.

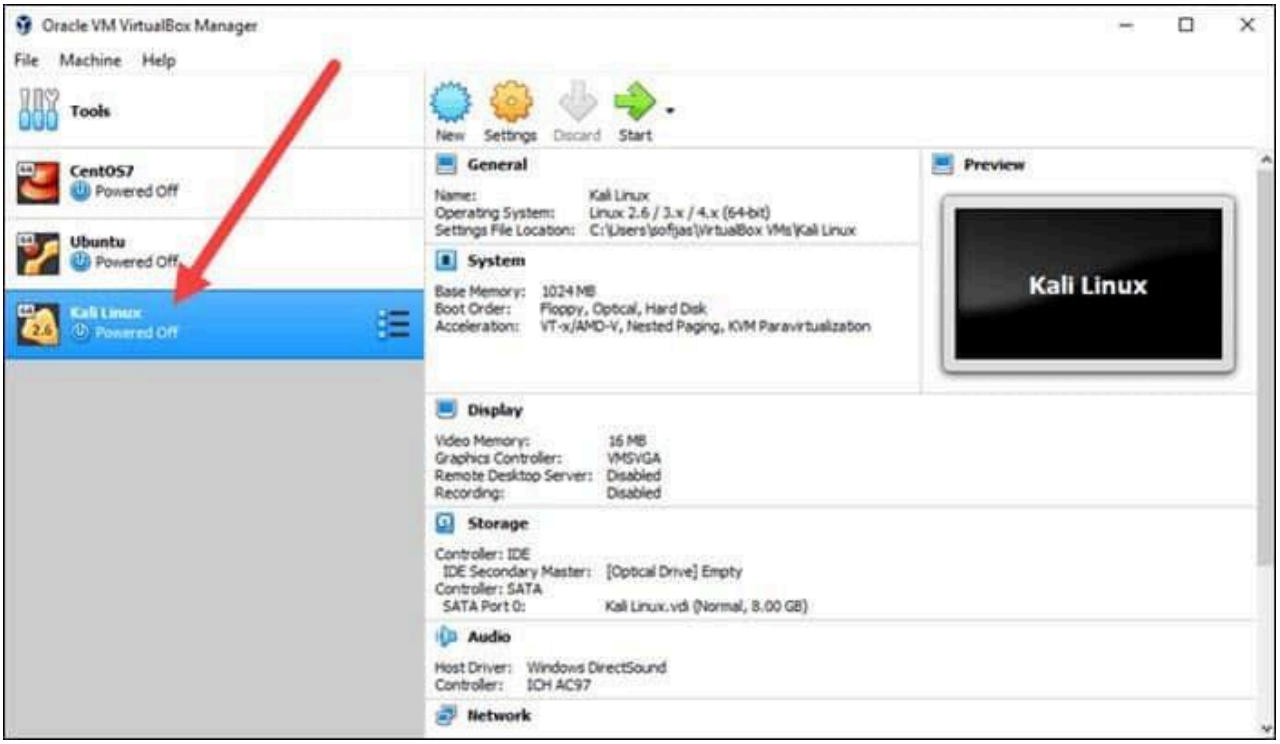


5. Hard disk file type. Stick to the default file type for the new virtual hard disk, VDI (VirtualBox Disk Image). Click Next to continue.

6. Storage on a physical hard disk. Decide between Dynamically allocated and Fixed size. The first choice allows the new hard disk to grow and fill up space dedicated to it. The second, fixed size, uses the maximum capacity from the start. Click Next.

7. File location and size. Specify the name and where you want to store the virtual hard disk. Choose the amount of file data the VM is allowed to store on the hard disk. We advise giving it at least 8 gigabytes. Click Create to finish.

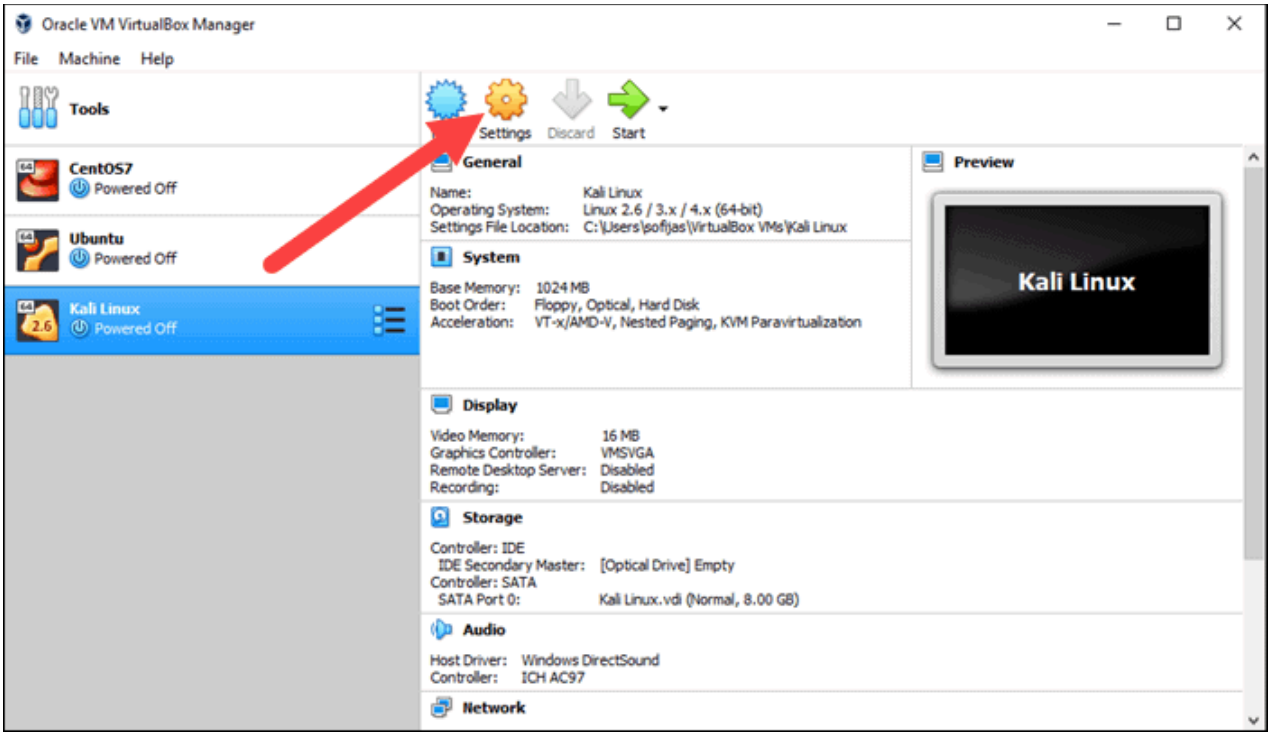
Now you created a new VM. The VM appears on the list in the VirtualBox Manager.



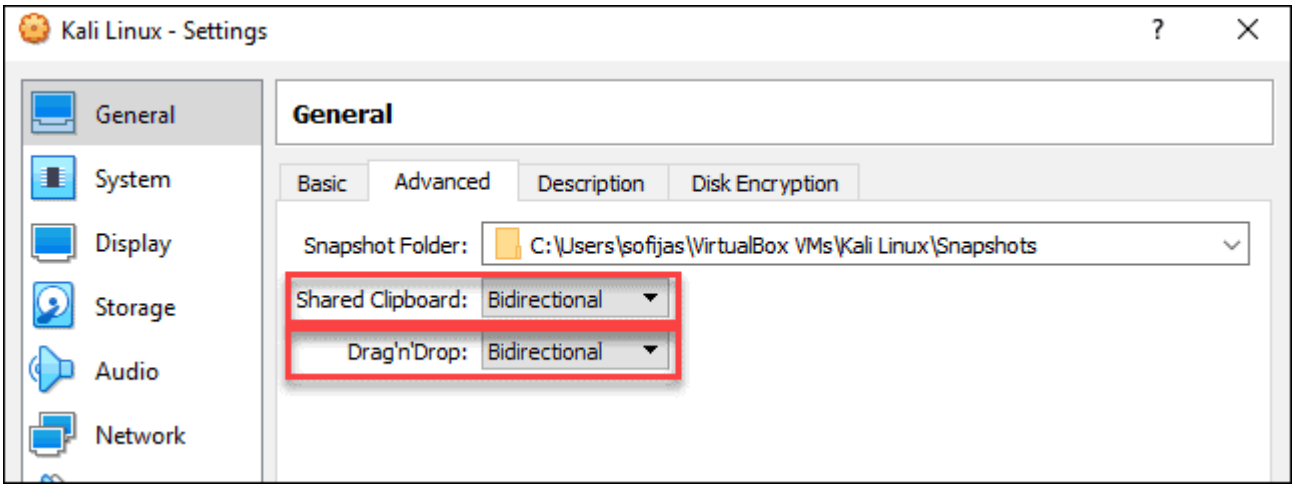
Step 3: Configure Virtual Machine Settings

The next step is adjusting the default virtual machine settings.

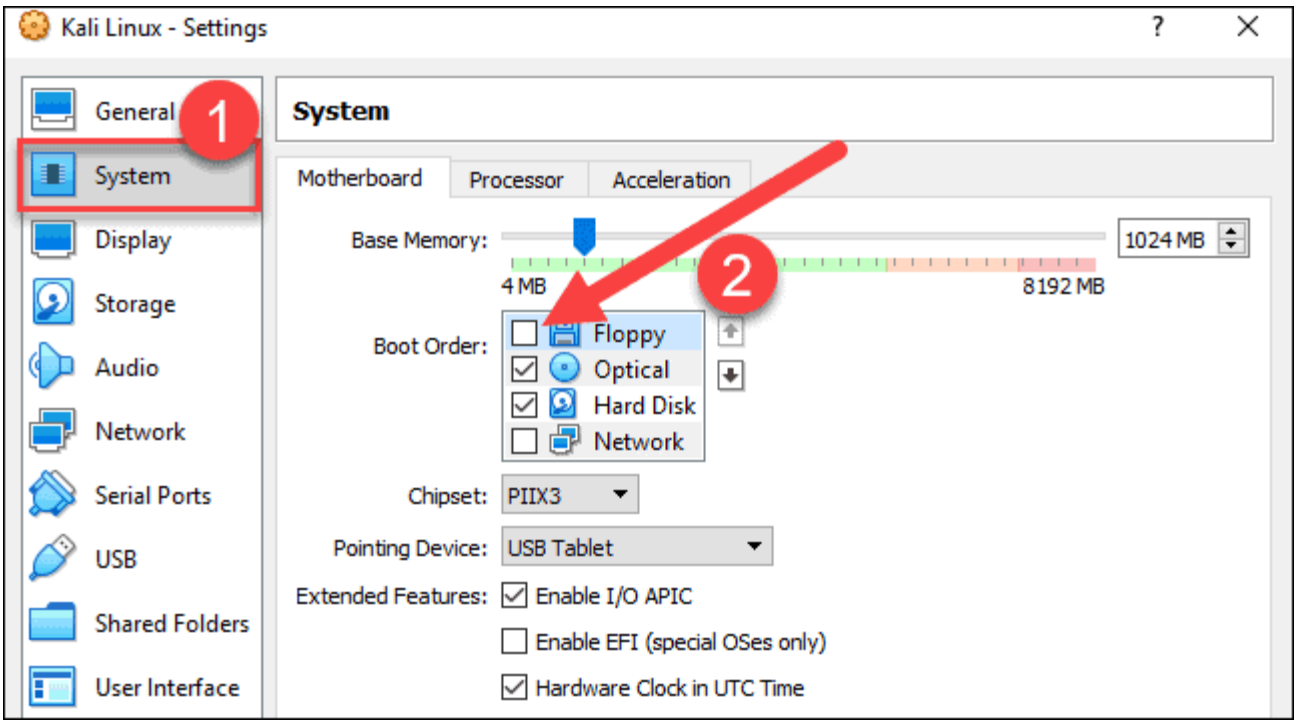
1. Select a virtual machine and click the Settings icon. Make sure you marked the correct VM and that the right-hand side is displaying details for Kali Linux.



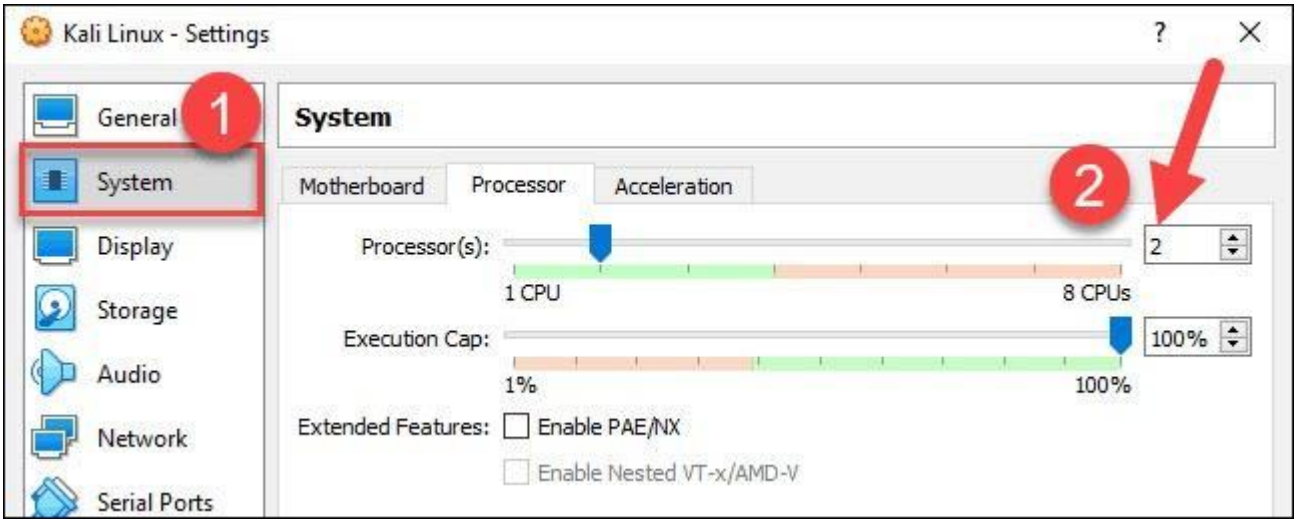
2. In the Kali Linux – Settings window, navigate to General > Advanced tab. Change the Shared Clipboard and Drag'n'Drop settings to Bidirectional. This feature allows you to copy and paste between the host and guest machine.



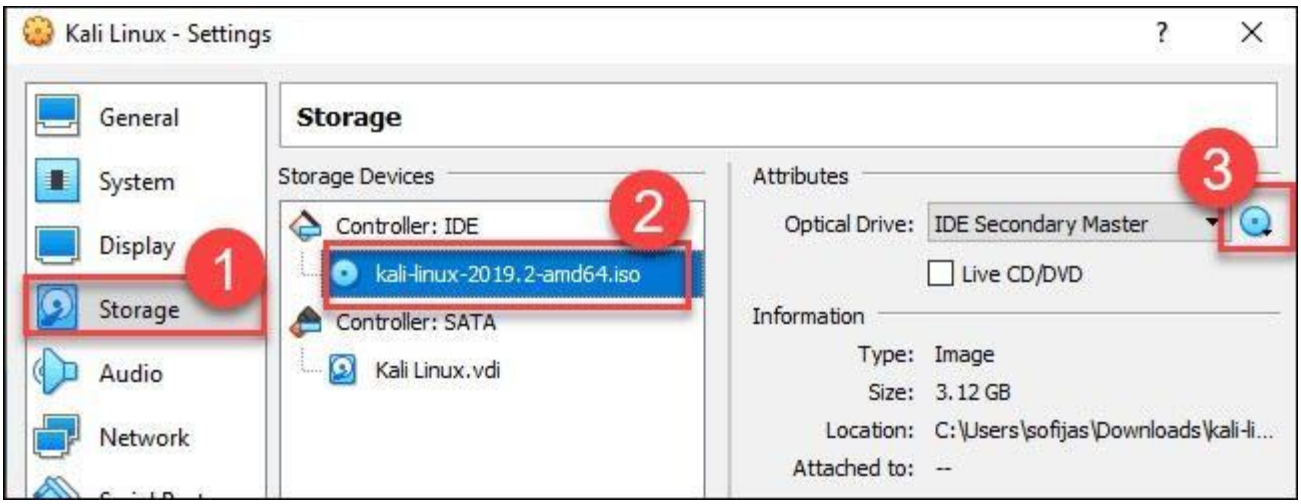
3. Go to System > Motherboard. Set the boot order to start from Optical, followed by Hard Disk. Uncheck Floppy as it is unnecessary.



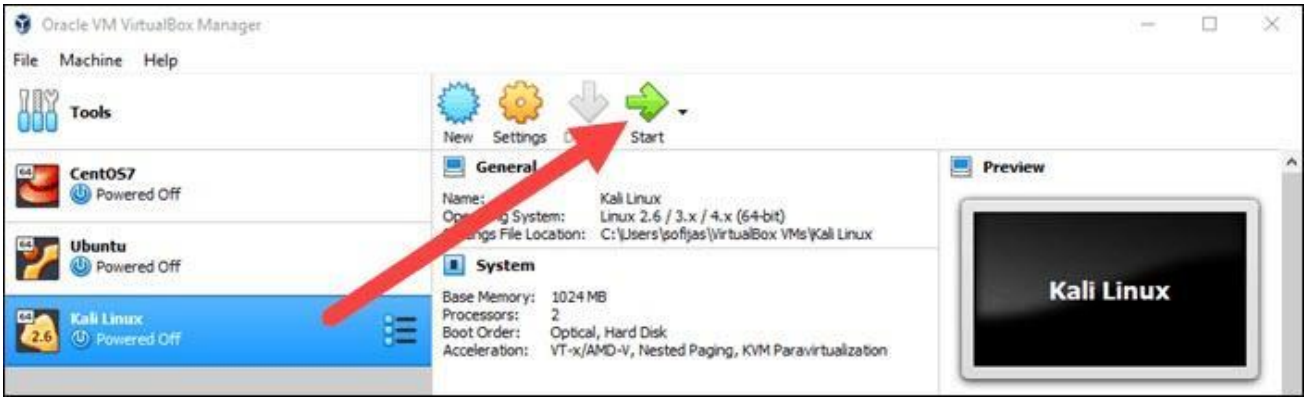
4. Next, move to the Processor tab in the same window. Increase the number of processors to two (2) to enhance performance.



5. Finally, navigate to Storage settings. Add the downloaded Kali image to a storage device under Controller: IDE. Click the disk icon to search for the image. Once finished, close the Settings window.



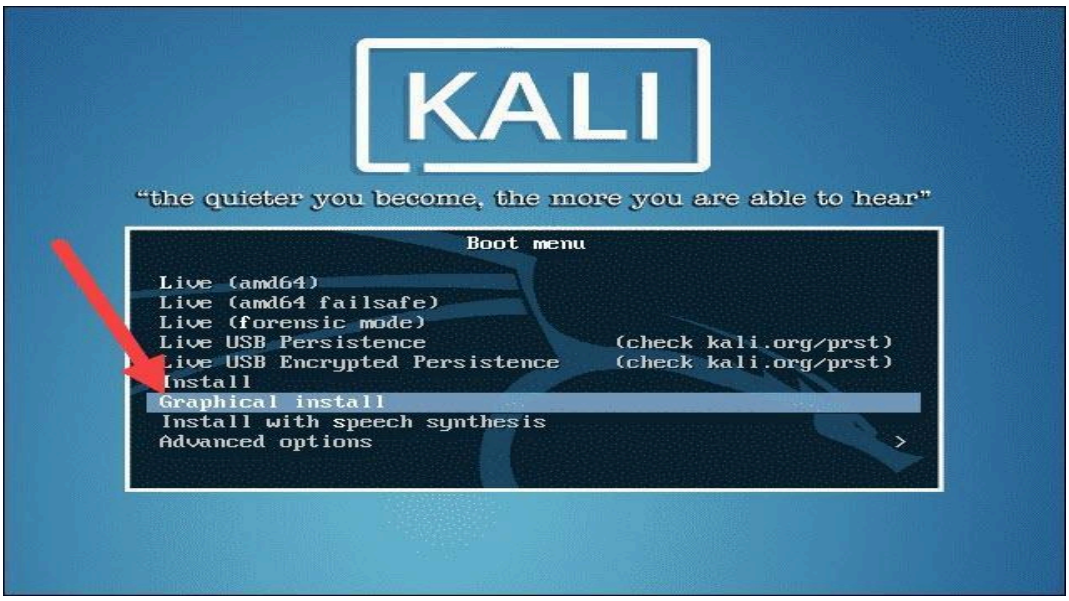
6. Click the Start icon to begin installing Kali.



Step 4: Installing and Setting Up Kali Linux

After you booted the installation menu by clicking Start, a new VM VirtualBox window appears with the Kali welcome screen.

Select the Graphical install option and go through the following installation steps for setting up Kali Linux in VirtualBox.



1. Select a language. Choose the default language for the system (which will also be the language used during the installation process).

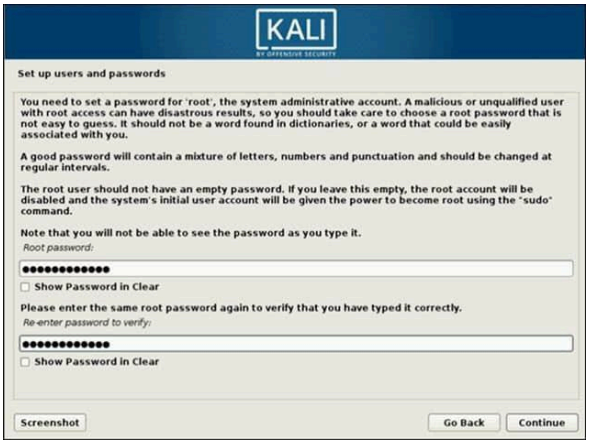
2. Select your location. Find and select your country from the list (or choose "other").

3. Configure the keyboard. Decide which keymap to use. In most cases, the best option is to select American English.

4. Configure the network. First, enter a hostname for the system and click Continue.

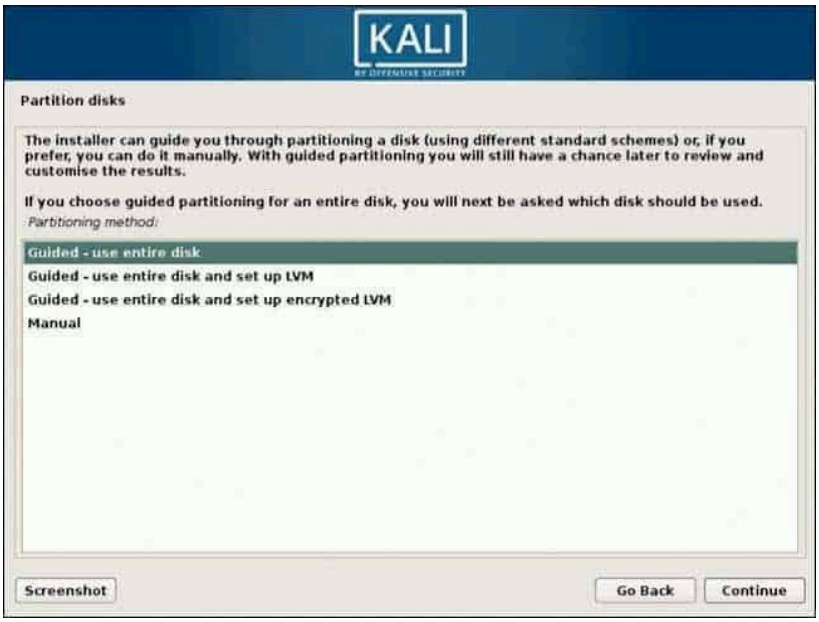
5. Next, create a domain name (the part of your internet address after your hostname). Domain names usually end in .com, .net, .edu, etc. Make sure you use the same domain name on all your machines.

6. Set up users and passwords. Create a strong root password for the system administrator account.



7. Configure the clock. Select your time zone from the available options.

8. Partition disks. Select how you would like to partition the hard disk. Unless you have a good reason to do it manually, go for the Guided –use entire disk option.



9. Then, select which disk you want to use for partitioning. As you created a single virtual hard disk in Step 3: Adjust VM Settings, you do not have to worry about data loss. Select the only available option – SCSI3 (0,0,0) (sda) – 68.7 GB ATA VBOK HARDDISK (the details after the dash vary depending on your virtualization software).

10. Next, select the scheme for partitioning. If you are a new user, go for All files in one partition.

11. The wizard gives you an overview of the configured partitions. Continue by navigating to Finish partitioning and write changes to disk. Click Continue and confirm with Yes.

12. The wizard starts installing Kali. While the installation bar loads, additional configuration settings appear.

13. Configure the package manager. Select whether you want to use a network mirror and click Continue. Enter the HTTP proxy information if you are using one. Otherwise, leave the field blank and click Continue again.

14. Install the GRUB boot loader on a hard disk. Select Yes and Continue. Then, select a boot loader device to ensure the newly installed system is bootable.

15. Once you receive the message Installation is complete, click Continue to reboot your VM.

With this, we have successfully installed Kali Linux on VirtualBox. After rebooting, the Kali login screen appears. Type in a username (root) and password you entered in the previous steps.

Finally, the interface of Kali Linux appears on your screen.

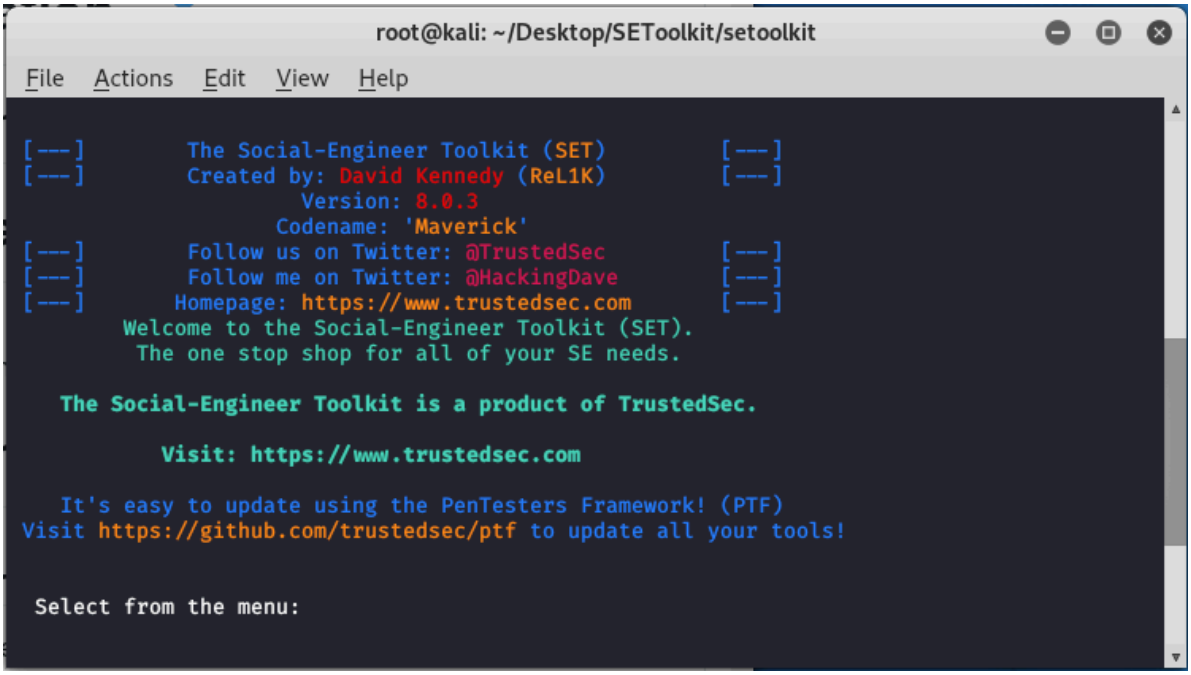
Result: Thus, the installation of kali linux is completed successfully.

17. Installation of Social Engineering Toolkit in Kali Linux

Aim: To install social engineering toolkit in kali linux.

Procedure:

Social engineering toolkit is a free and open-source tool that is used for social engineering attacks such as phishing, faking phone numbers, sending SMS, etc. it's a free tool available in Kali Linux or you can directly download and install it from Github. The Social Engineering Toolkit is designed and developed by a programmer named Dave Kennedy. This tool is used by security researchers, penetration testers all around the globe for checking cybersecurity flaws in systems. Social engineering toolkit targets to perform attacking techniques on their machines. This tool kit also offers website vector attacks or custom vector attacks by which you can clone any website and can perform phishing attacks. There are various features of the social engineering toolkit some of them are given below.



Features of Social Engineering toolkit:

- SET is free and Open Source
- SET is already installed in your Kali Linux however you can also download and install it from Github.
- SET is portable, which means you can easily change attack vectors.
- SET is a Multi-platform tool: It can run on Linux, Unix, and Windows.
- SET Supports integration with third-party modules.

- SET Includes access to the Fast-Track Penetration Testing platform
- SET provides many attack vectors such as Spear-Phishing Attacks, Website Attacks, Infection Media Generator etc.

Uses of Social Engineering Toolkit:

Phishing Attacks: Social Engineering Toolkit allows you to perform phishing attacks on your victim. By using SET you can create phishing pages of many websites such as Instagram, Facebook, Google, etc. SET will generate a link of the option that you have chosen, and then you can send that URL to the victim once the victim open that URL and he /she will see a legitimate webpage of a real website which is actually a phishing page .once he/she entered his/her id password then you will get that id password on your terminal screen this is how phishing attack using SET works.

Web Attack: Web Attack is a module in SET. This module combines different options for attacking the victim remotely by using this module you can create a payload and can deliver payload onto your victim browser using Metasploit browser exploit. web attack has Credential Harvester method using which you can clone any website for a phishing attack and can send the link of that webpage to the victim to harvest the information from user and password fields.

Create a Payload and Listener: when you will first run the Social Engineering Toolkit. You will see the 4th option which is to create a payload and listener by using that module of SET you'll be able to create malicious payloads for Windows, including Shell Reverse_TCP, Reverse_TCP Meterpreter, Shell Reverse_TCP X64, and Meterpreter Reverse HTTPS. You can use these payloads in the same way how you use payloads from metasploitable.

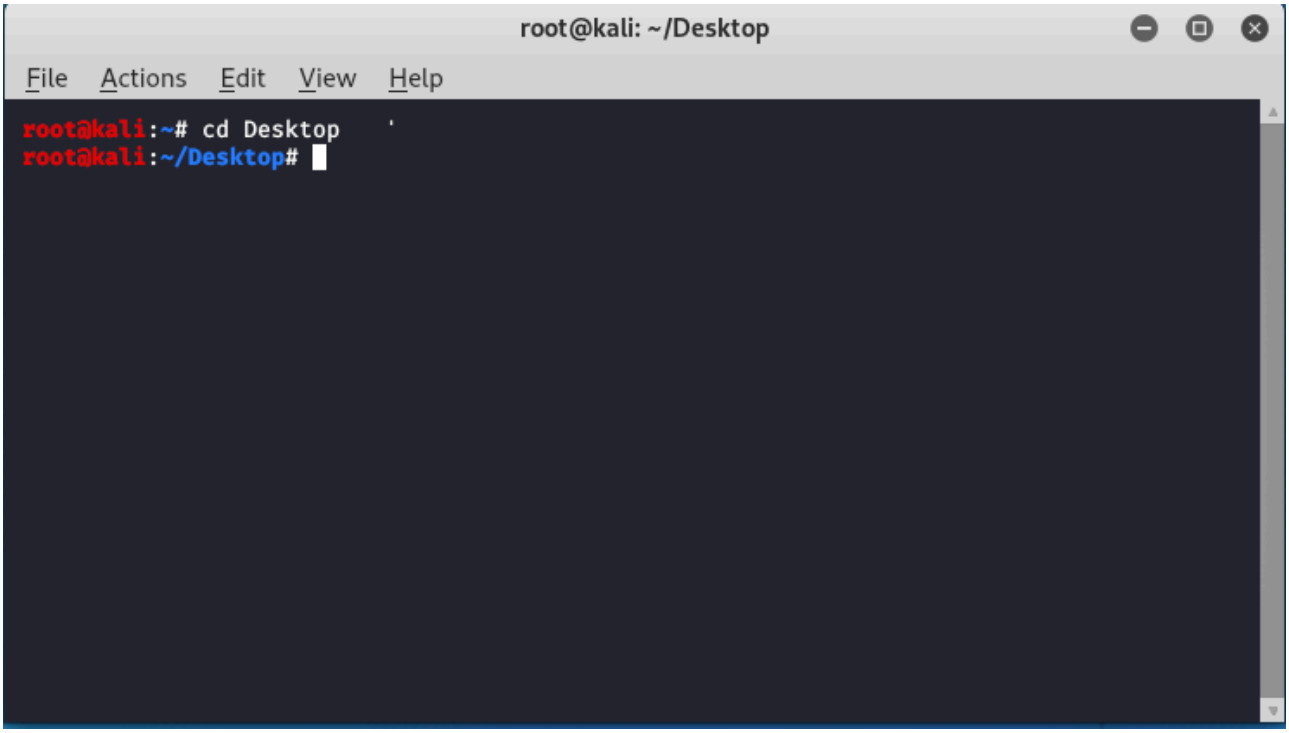
Mass Mailer Attack: mass mailer attack is a module in the social engineering toolkit that is used for bombarding emails on target mail account for that you can use your own Gmail account also or you can own a server for that.

These were some attack vectors that you can perform using Social Engineering Toolkit .when you will run the SET you will feel fun because using SET is very easy now we will see how you can install Social Engineering Toolkit and how you can use it for phishing attack.

Installation of Social engineering toolkit :

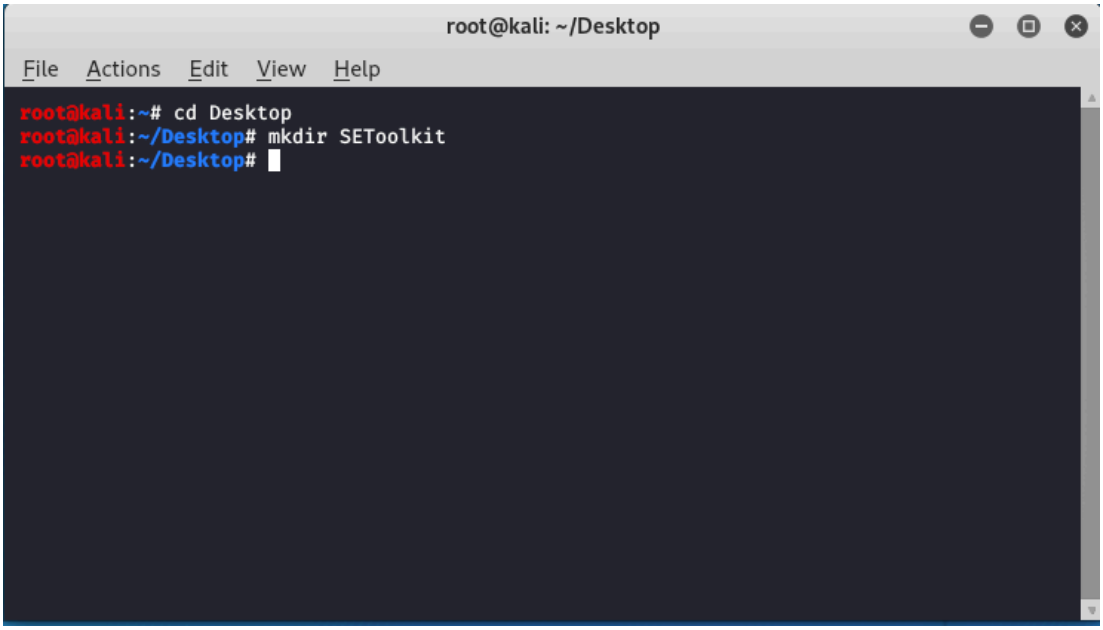
Step 1: Open your Kali Linux Terminal and move to Desktop

cd Desktop



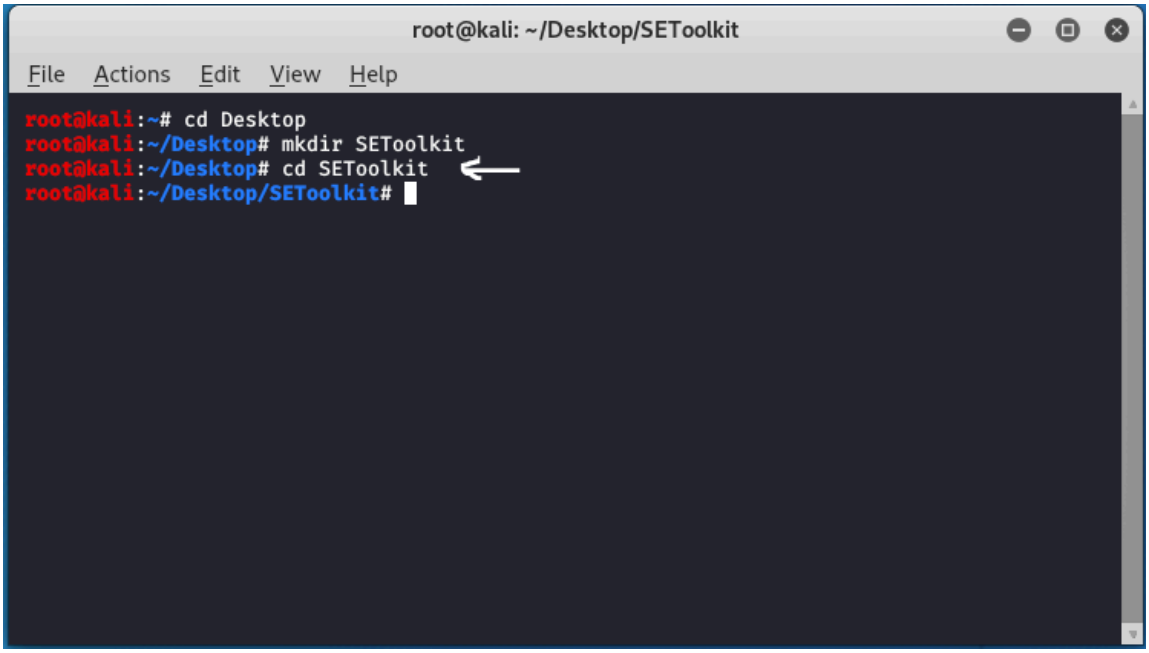
Step 2: As of now you are on a desktop so here you have to create a new directory named SEToolkit using the following command.

mkdir SEToolkit



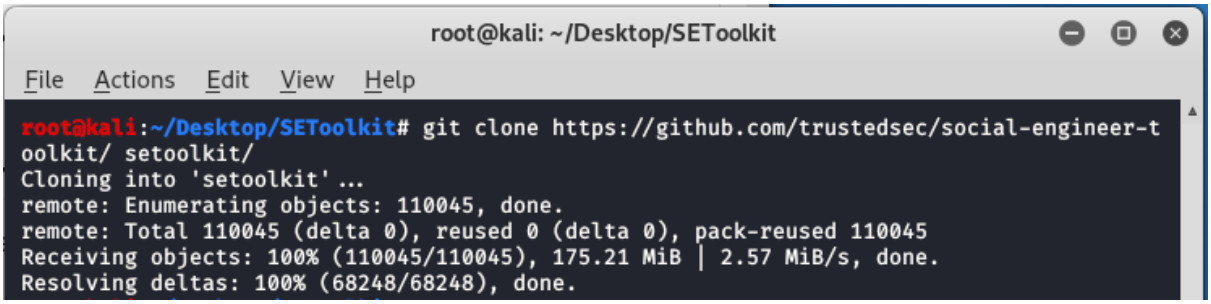
Step 3: Now as you are in the Desktop directory however you have created a SEToolkit directory so move to SEToolkit directory using the following command.

cd SEToolkit



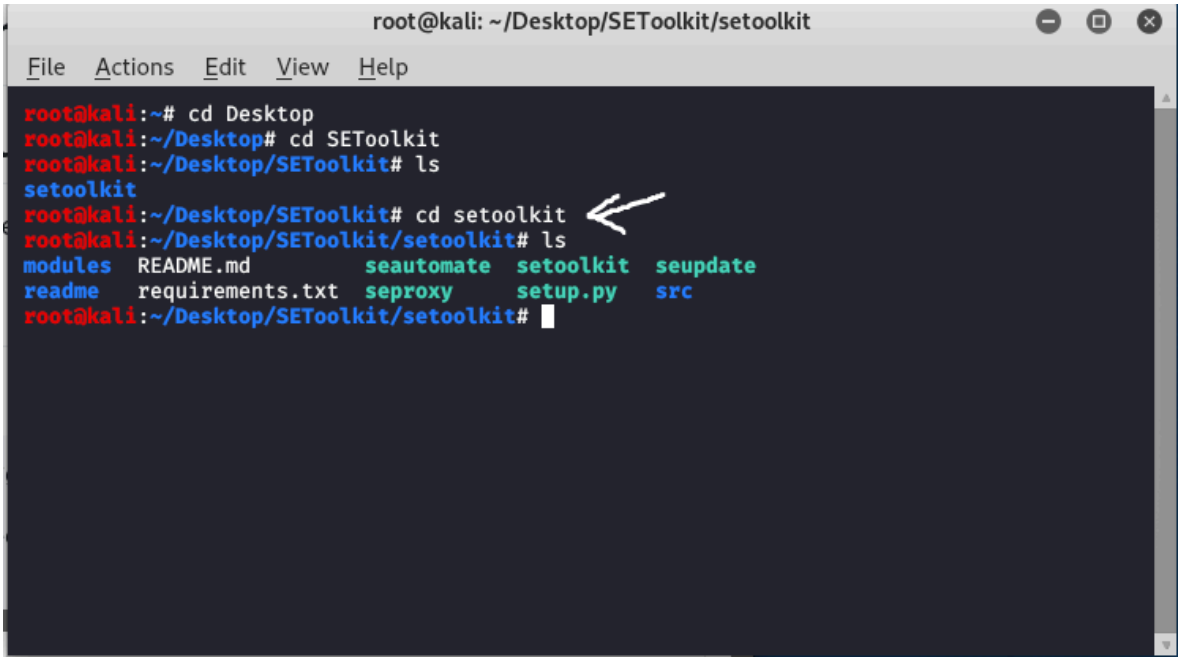
Step 4: Now you are in SEToolkit directory here you have to clone SEToolkit from GitHub so you can use it.

git clone https://github.com/trustedsec/social-engineer-toolkit setoolkit/



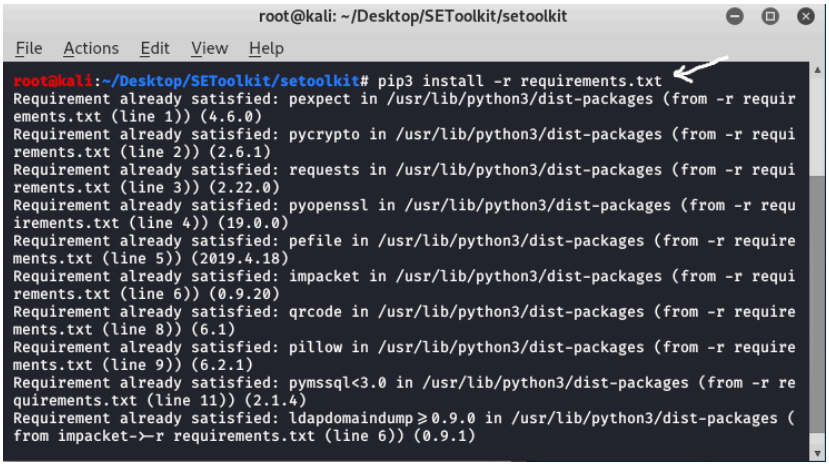
Step 5: Social Engineering Toolkit has been downloaded in your directory now you have to move to the internal directory of the social engineering toolkit using the following command.

cd setoolkit



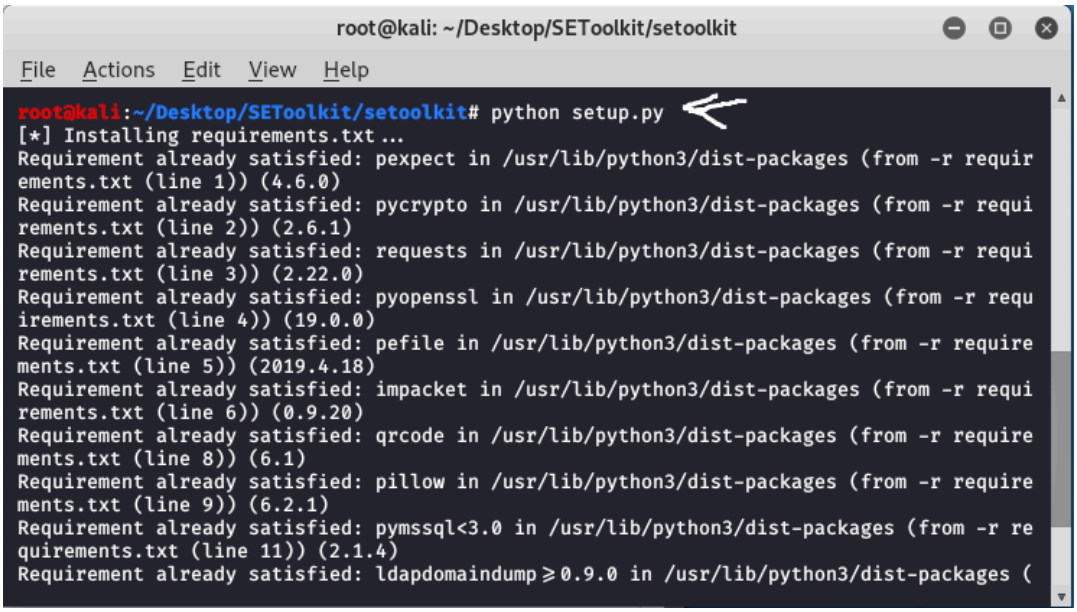
Step 6: Finally, the social engineering toolkit in your directory SEToolkit has been downloaded. Now it's time to install requirements using the following command.

pip3 install -r requirements.txt



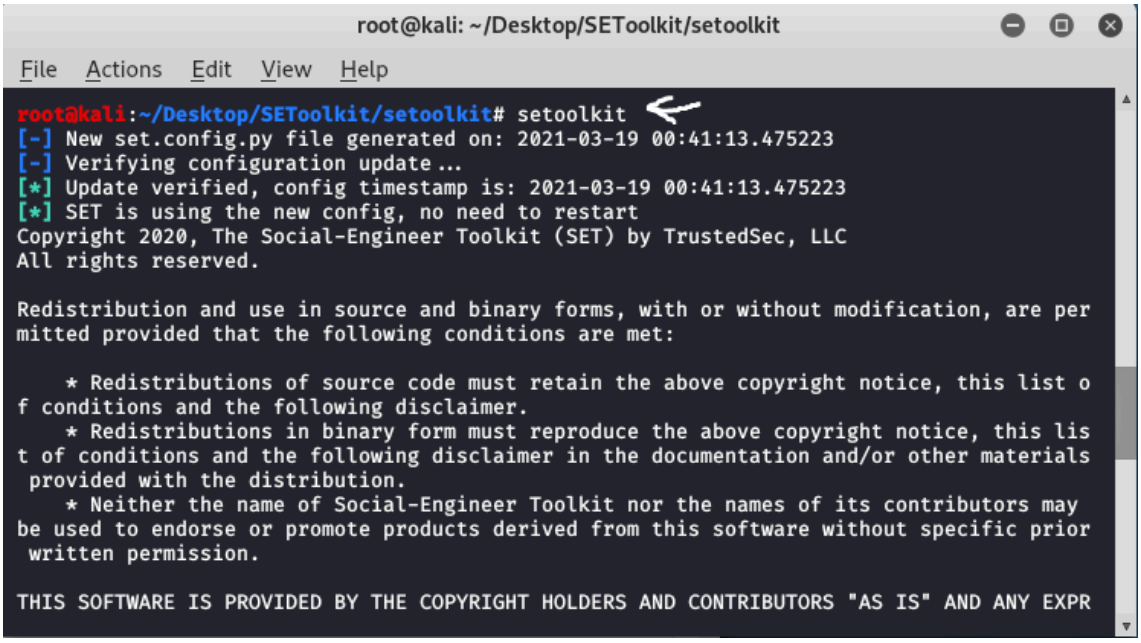
Step 7: All the requirements have been downloaded in your setoolkit. Now it's time to install the requirements that you have downloaded

python setup.py



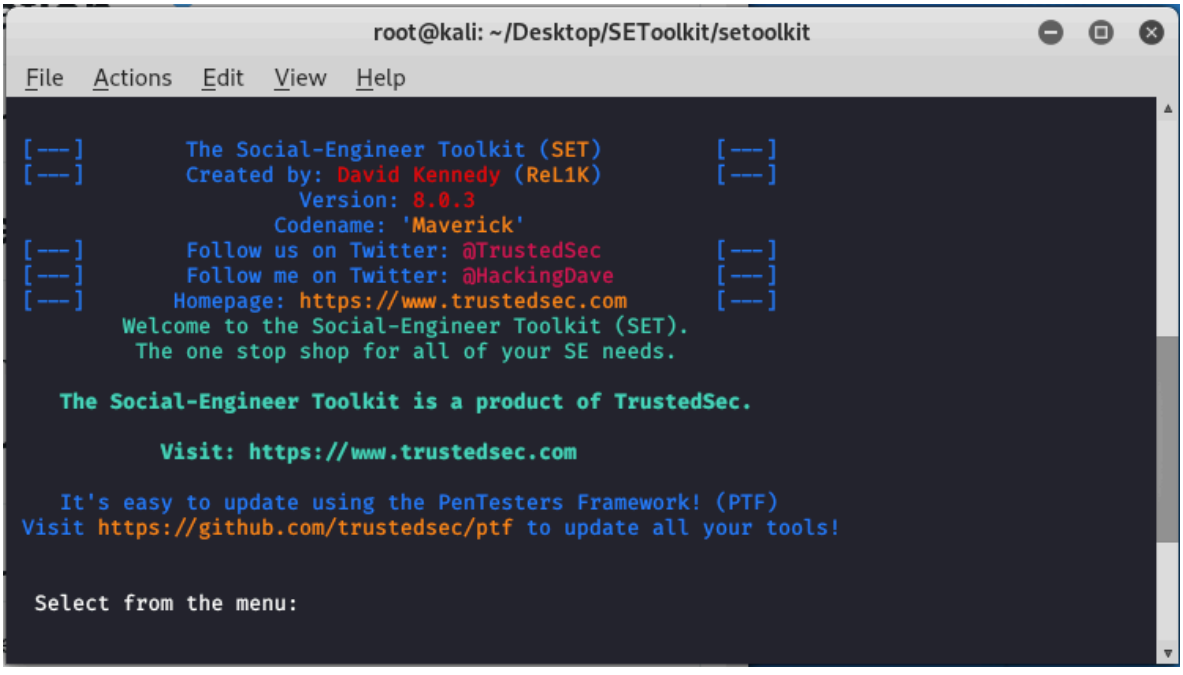
Step 8: Finally all the processes of installation have been completed now it's time to run the social engineering toolkit .to run the SEToolkit type following command.

Setoolkit



Step 9: At this step, setoolkit will ask you (y) or (n). Type y and your social engineering toolkit will start running.

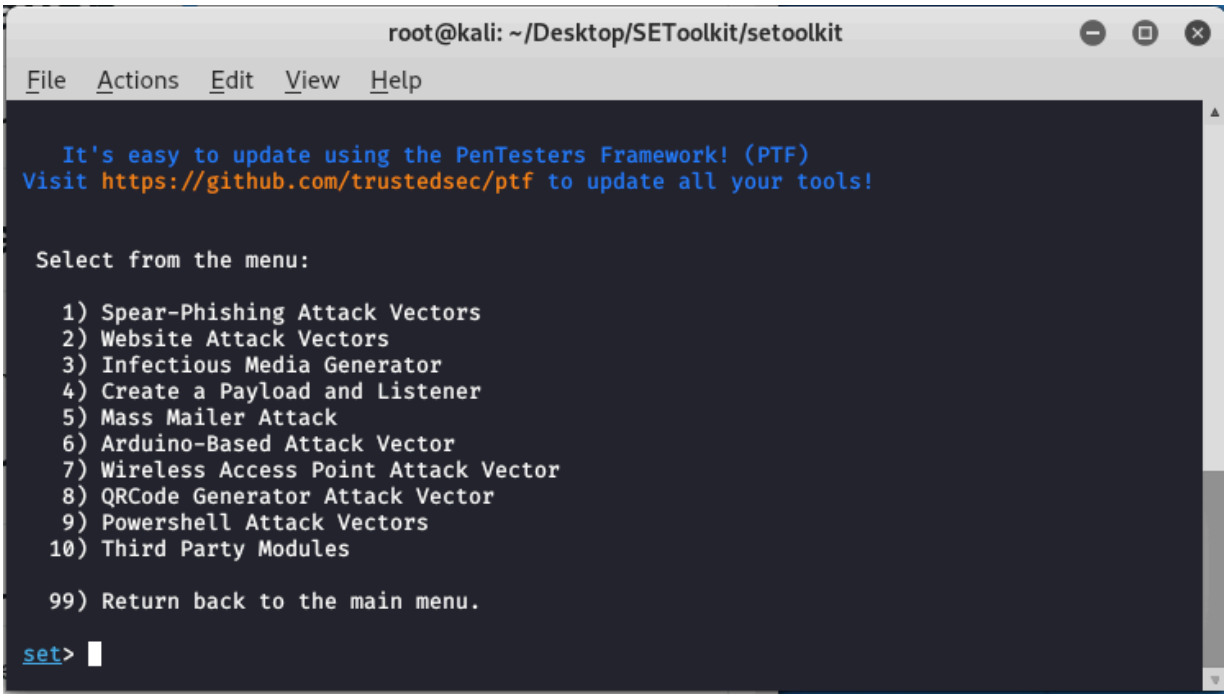
Y



Step 10: Now your setoolkit has been downloaded into your system now it's time to use it .now you have to choose an option from the following options .here we are choosing option 2

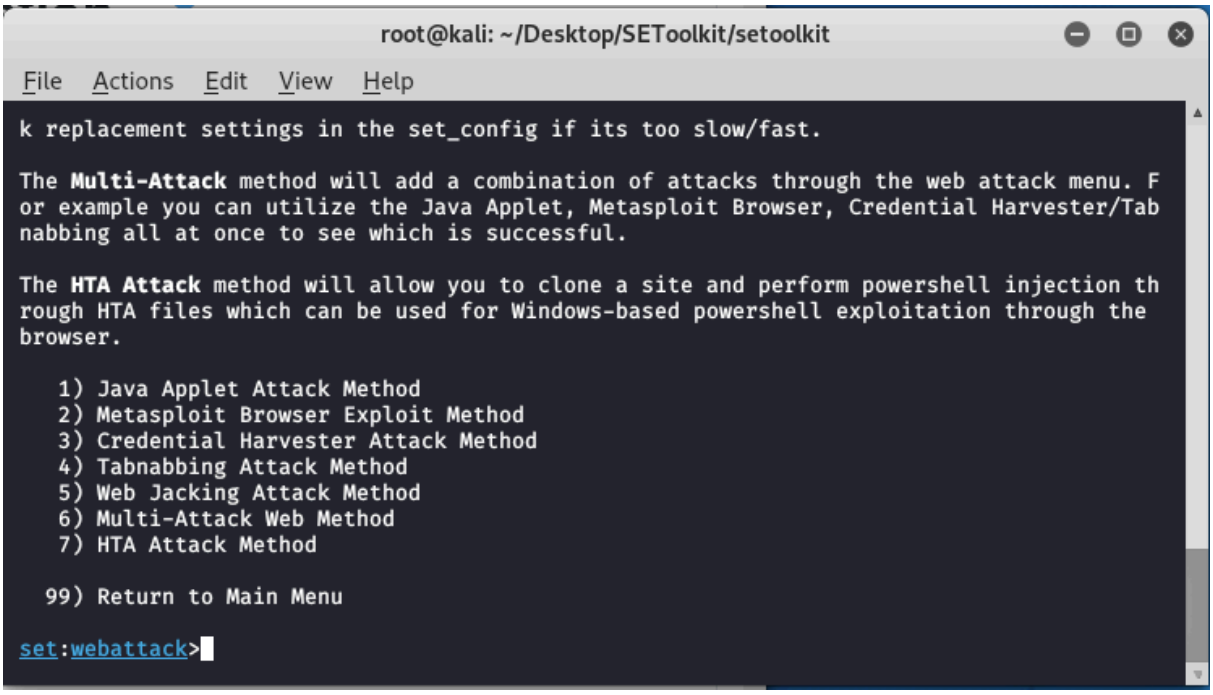
Website Attack Vectors:

option : 2



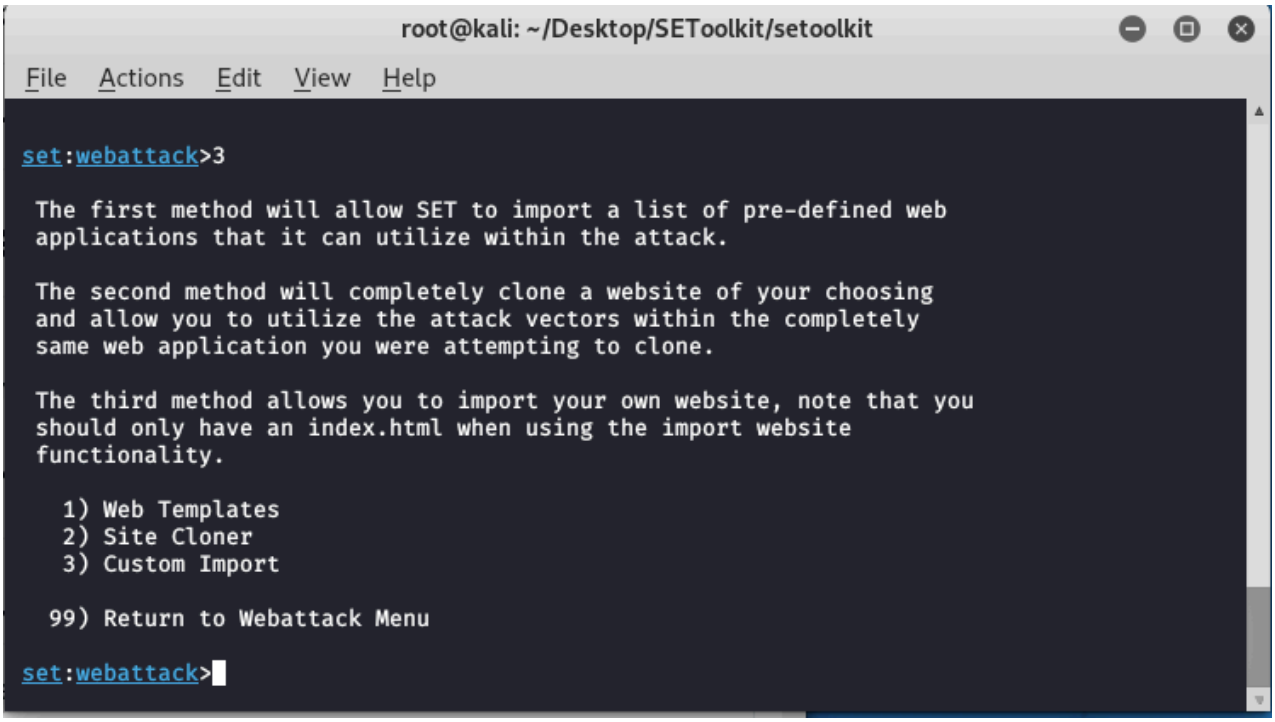
Step 11: Now we are about to set up a phishing page so here we will choose option 3 that is the credential harvester attack method.

Option : 3

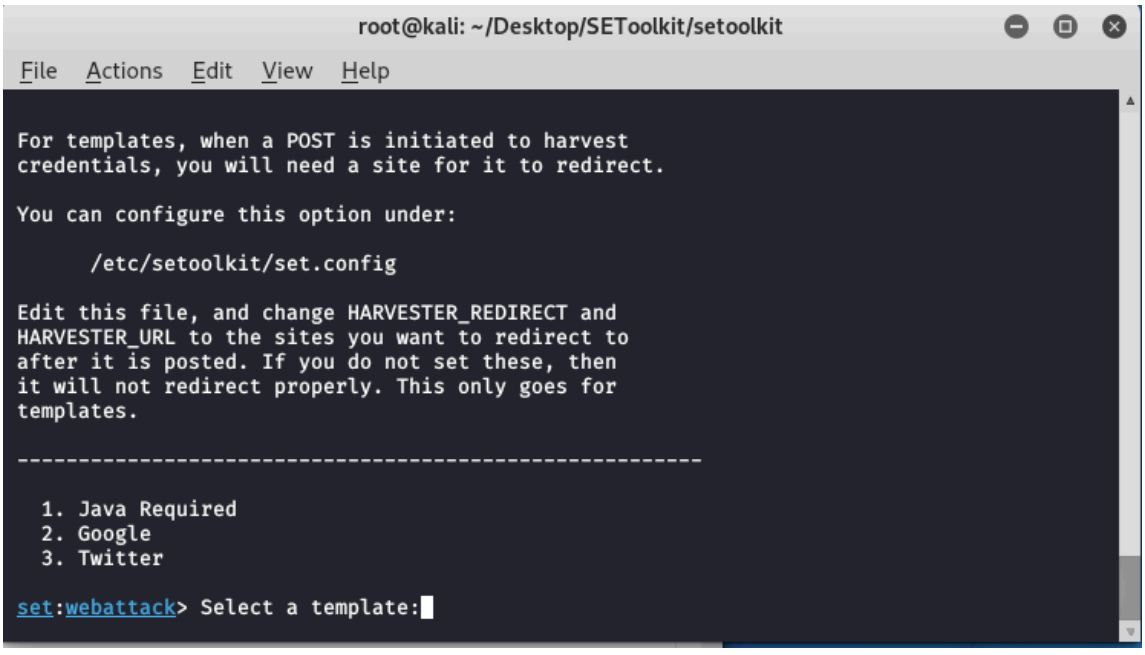


Step 12: Now since we are creating a Phishing page so here we will choose option 1 that is web templates.

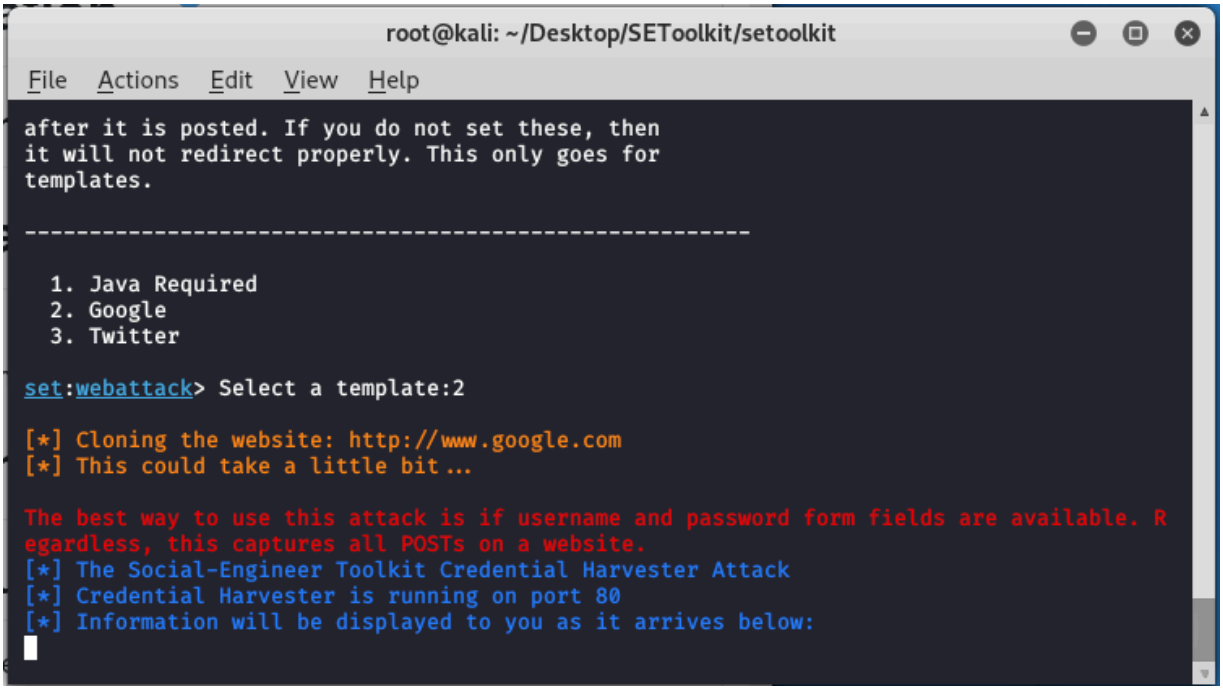
option 1



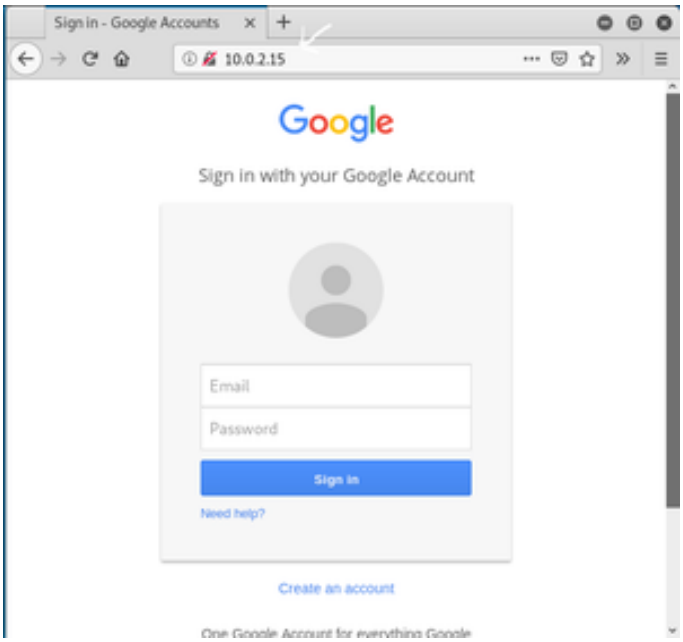
Step 13: At this time the social engineering tool will generate a phishing page at our localhost.



Step 14: Create a google phishing page so choose option 2 for that then a phishing page will be generated on your localhost.



Step 15: Social engineering toolkit is creating a phishing page of google.



As you can see on our localhost means on our IP address setoolkit created a phishing page of google. This is how the social engineering toolkit works. Your phishing page will be created by social engineering toolkit. Once the victim types the id password in the fields the id password will be shown on your terminal where SET is running.

Result: Thus, the social engineering toolkit has been installed and verified successfully.