Enumeration is fundamentally checking. An attacker sets up a functioning associated with the objective host. The weaknesses are then tallied and evaluated. It is done mostly to look for assaults and dangers to the objective framework. Enumeration is utilized to gather usernames, hostname, IP addresses, passwords, arrangements, and so on. At the point when a functioning connection with the objective host is set up, hackers oversee the objective framework. They at that point take private data and information. Now and again, aggressors have additionally been discovered changing the setup of the objective frameworks. How the connection is set up to the host decides the information or data the attacker will have the option to get to.

What is Enumeration?

Enumeration is the process of scanning a target system, network, or application and collecting information on it while in the process. This step is critical in the reconnaissance phase of ethical hacking or penetration testing where the aim is to find out some of the weaknesses within the target. Enumeration includes asking the system questions to get information such as usernames, machine names, shares, services, and other assets. The information that can be collected during the enumeration phase can be utilized by an attacker to understand the structure and security of the targeted system so that the attacker would understand what comes next.

Types Of Enumeration

In this section, we will be discussing the various types of Enumerations.

1. NetBIOS(Network Basic Input Output System) Enumeration

- NetBIOS name is an exceptional 16 ASCII character string used to distinguish the organization gadgets over TCP/IP, 15 characters are utilized for the gadget name and the sixteenth character is saved for the administration or name record type.
- Programmers utilize the NetBIOS enumeration to get a rundown of PCs that have a place with a specific domain, a rundown of offers on the individual hosts in the organization, and strategies and passwords.

- NetBIOS name goal isn’t supported by Microsoft for Internet Protocol Version 6.
- The initial phase in specifying a Windows framework is to exploit the NetBIOS API. It was initially an Application Programming Interface(API) for custom programming to get to LAN assets. Windows utilizes NetBIOS for document and printer sharing.
- A hacker who finds a Windows OS with port 139 open, can verify what assets can be gotten to or seen on the far off framework. In any case, to count the NetBIOS names, the distant framework probably empowered document and printer sharing. This sort of enumeration may empower the programmer to peruse or keep in touch with the distant PC framework, contingent upon the accessibility of offers, or dispatch a DoS.
- NetBIOS name list:

Name	NetBIOS Code	Type
<host name>	<00>	UNIQUE
<domain>	<00>	GROUP

<host name>	<03>	UNIQUE
<username>	<03>	UNIQUE
<host name>	<20>	UNIQUE
<domain>	<1D>	GROUP
<domain>	<1B>	UNIQUE

- Nbtstat Utility: In Windows, it shows NetBIOS over TCP/IP (NetBT) convention insights, NetBIOS name tables for both the neighborhood and distant PCs, and the NetBIOS name reserve. This utility allows a resuscitate of the NetBIOS name cache and the names selected with Windows Internet Name Service. The sentence structure for Nbtstat:

```
nbtstat [-a RemoteName] [-A IPAddress] [-c] [-n] [-r] [-R] [-RR] [-s] [-S] [Interval]
```

The table appeared beneath shows different Nbtstat boundaries:

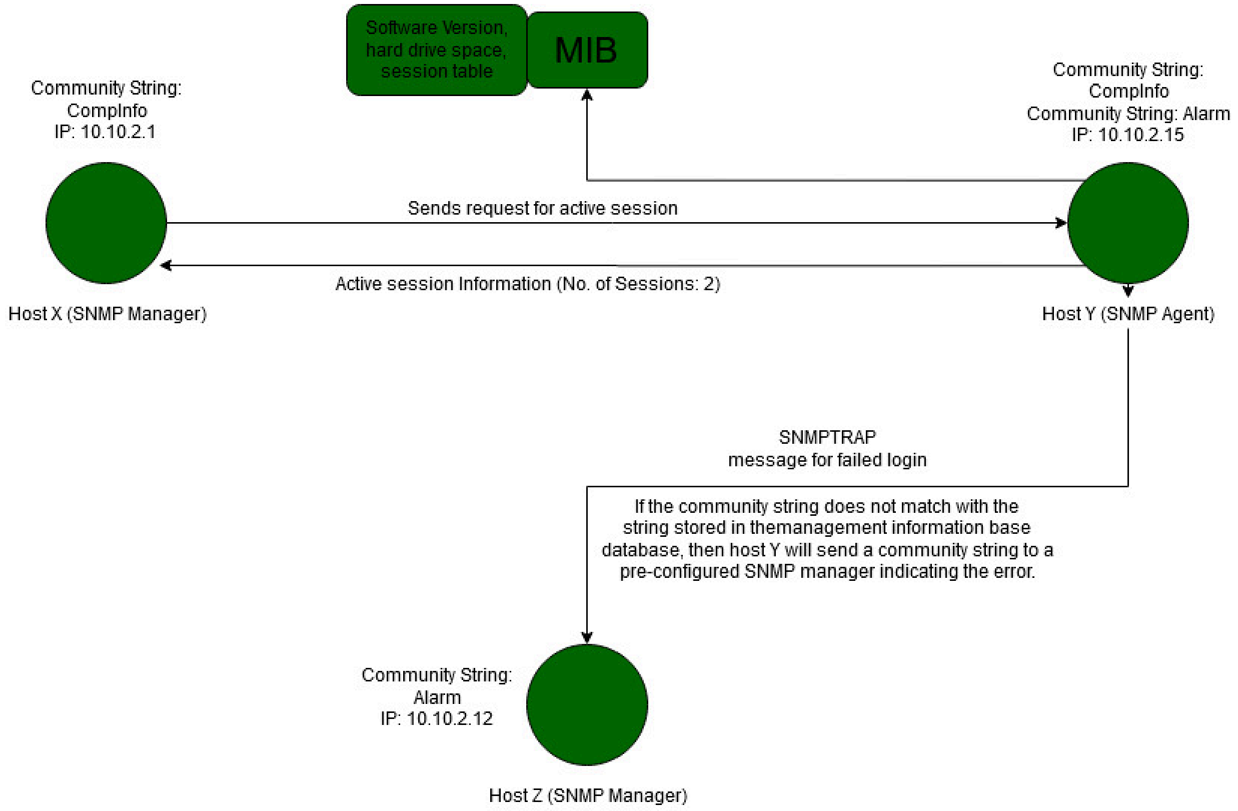
Parameters
-a RemoteName
-A IPAddress
-c
-n
-r
-RR

-s
-S
Interval

2. SNMP(Simple Network Management Protocol) Enumeration:

- SNMP enumeration is a cycle of specifying client records and gadgets on an objective framework utilizing SNMP. SNMP comprises a manager and a specialist. Specialists are inserted on each organization gadget, and the trough is introduced on a different PC.
- SNMP holds two passwords to get to and design the SNMP specialist from the administration station. Read Community String is public of course, permits review of gadget/framework setup. Read/Write people group string is private of course, permits far off altering of arrangement.
- Hackers utilize these default network strings to remove data about a gadget. Hackers list SNMP to remove data about organization assets, for example, has, switches, gadgets, shares, and so on, and network data, for example, ARP tables, directing tables, traffic, and so forth.
- SNMP utilizes dispersed engineering containing SNMP agents, managers, and a few related parts. Orders related with SNMP include: GetRequest, GetNextRequest, GetResponse, SetRequest, Trap.

Given below is the communication between the SNMP agent and manager:


Software Version, hard drive space, session table
MIB
Community String: CompInfo IP: 10.10.2.1
Community String: CompInfo Community String: Alarm IP: 10.10.2.15
Sends request for active session
Active session Information (No. of Sessions: 2)
Host X (SNMP Manager)
Host Y (SNMP Agent)
SNMPTRAP message for failed login
If the community string does not match with the string stored in themanagement information base database, then host Y will send a community string to a pre-configured SNMP manager indicating the error.
Community String: Alarm IP: 10.10.2.12
Host Z (SNMP Manager)

- SNMP Enumeration tools are utilized to examine a solitary IP address or a scope of IP addresses of SNMP empowered organization gadgets to screen, analyze, and investigate security dangers. Instances of this sort of instruments incorporate NetScanTolls Pro, SoftPerfect Network Scanner, SNMP Informant, and so forth

3. LDAP Enumeration:

- Lightweight Directory Access Protocol is an Internet Protocol for getting to dispersed registry administrations.
- Registry administrations may give any coordinated arrangement of records, regularly in a hierarchical and sensible structure, for example, a corporate email index.

- A customer starts an LDAP meeting by associating with a Directory System Agent on TCP port 389 and afterward sends an activity solicitation to the DSA.
- Data is sent between the customer and the worker utilizing Basic Encoding Rules.
- Programmer inquiries LDAP administration to assemble information such as substantial usernames, addresses, division subtleties, and so on that can be additionally used to perform assaults.
- There are numerous LDAP enumeration apparatuses that entrance the registry postings inside Active Directory or other catalog administrations. Utilizing these devices, assailants can identify data, for example, substantial usernames, addresses, division subtleties, and so forth from various LDAP workers.
- Examples of these kinds of tools include LDAP Admin Tool, Active Directory Explorer, LDAP Admin, etc.

4. NTP Enumeration:

- Network Time Protocol is intended to synchronize clocks of arranged PCs.
- It utilizes UDP port 123 as its essential method for correspondence.
- NTP can check time to inside 10 milliseconds (1/100 seconds) over the public web.
- It can accomplish correctness of 200 microseconds or better in a neighborhood under ideal conditions.
- Executives regularly disregard the NTP worker regarding security. Be that as it may, whenever questioned appropriately, it can give important organization data to the programmers.
- Hackers inquiries NTP workers to assemble significant data, for example, a list of hosts associated with NTP workers, Clients' IP addresses in an organization,

their framework names and Oss, and Internal IPs can likewise be gotten if NTP worker is in the demilitarized zone.

- NTP enumeration tools are utilized to screen the working of SNTP and NTP workers present in the organization and furthermore help in the configuration and confirmation of availability from the time customer to the NTP workers.

5. SMTP Enumeration:

- Mail frameworks ordinarily use SMTP with POP3 and IMAP that empowers clients to spare the messages in the worker letter drop and download them once in a while from the mainframe.
- SMTP utilizes Mail Exchange (MX) workers to coordinate the mail through DNS. It runs on TCP port 25.
- SMTP provides 3 built-in commands: VRFY, EXPN, RCPT TO.
- These servers respond differently to the commands for valid and invalid users from which we can determine valid users on SMTP servers.
- Hackers can legitimately associate with SMTP through telnet brief and gather a rundown of substantial clients on the mainframe.
- Hackers can perform SMTP enumeration using command-line utilities such as telnet, netcat, etc., or by using tools such as Metasploit, Nmap, NetScanTools Pro, etc.

6. DNS Enumeration using Zone Transfer:

- It is a cycle for finding the DNS worker and the records of an objective organization.
- A hacker can accumulate significant organization data, for example, DNS worker names, hostname, machine names, usernames, IPs, and so forth of the objectives.

- In DNS Zone Transfer enumeration, a hacker tries to retrieve a copy of the entire zone file for a domain from the DNS server.
- In order to execute a zone transfer, the hacker sends a zone transfer request to the DNS server pretending to be a client, the DNS then sends a portion of its database as a zone to you. This zone may contain a ton of data about the DNS zone organization.

7. IPsec Enumeration:

- IPsec utilizes ESP (Encapsulation Security Payload), AH (Authentication Header), and IKE (Internet Key Exchange) to make sure about the correspondence between virtual private organization (VPN) end focuses.
- Most IPsec-based VPNs use the Internet Security Association and Key Management Protocol, a piece of IKE, to establish, arrange, alter, and erase Security Associations and cryptographic keys in a VPN climate.
- A straightforward checking for ISAKMP at the UDP port 500 can demonstrate the presence of a VPN passage.
- Hackers can research further utilizing an apparatus, for example, IKE-output to identify the delicate information including encryption and hashing calculation, authentication type, key conveyance calculation, and so forth.

8. VoIP(Voice over IP) Enumeration:

- VoIP uses the SIP (Session Initiation Protocol) protocol to enable voice and video calls over an IP network.
- SIP administration by and large uses UDP/TCP ports 2000, 2001, 5050, 5061.
- VoIP enumeration provides sensitive information such as VoIP gateway/servers, IP-PBX systems, client software, and user extensions.

- This information can be used to launch various VoIP attacks such as DoS, Session Hijacking, Caller ID spoofing, Eavesdropping, Spamming over Internet Telephony, VoIP phishing, etc.

9. RPC Enumeration:

- Remote Procedure Call permits customers and workers to impart in disseminated customer/worker programs.
- Counting RPC endpoints empower aggressors to recognize any weak administrations on these administration ports.
- In networks ensured by firewalls and other security establishments, this portmapper is regularly sifted. Along these lines, hackers filter high port reaches to recognize RPC administrations that are available to coordinate an assault.

10. Unix/Linux User Enumeration:

- One of the most vital steps for conducting an enumeration is to perform this kind of enumeration. This provides a list of users along with details like username, hostname, start date and time of each session, etc.
- We can use command-line utilities to perform Linux user enumeration like users, rwho, finger, etc.

11. SMB Enumeration:

- SMB list is significant expertise for any pen-tester. Prior to figuring out how to count SMB, we should initially realize what SMB is. SMB represents server message block.

- It’s a convention for sharing assets like records, printers, by and large, any asset which should be retrievable or made accessible by the server. It fundamentally runs on port 445 or port 139 relying upon the server.
- It is quite accessible in windows, so windows clients don’t have to arrange anything extra as such other than essential set up. In Linux in any case, it is somewhat extraordinary. To make it work for Linux, you have to introduce a samba server since Linux locally doesn’t utilize SMB convention.
- Clearly, some kind of confirmation will be set up like a username and secret word, and just certain assets made shareable. So dislike everybody can get to everything, a solid confirmation.
- The main evident defect is utilizing default certifications or effectively guessable and sometimes even no verification for access of significant assets of the server. Administrators should make a point to utilize solid passwords for clients who need to get to assets utilizing SMB. The subsequent blemish is the samba server. Samba servers are infamous for being hugely vulnerable.

Mitigation Of Different Types Of Enumeration

There are several countermeasures which can be taken into account for the mitigation of several kinds of enumeration:

1. NetBIOS Enumeration:

- Disable SMB and NetBIOS.
- Use a network firewall.
- Prefer Windows firewall/ software firewalls.
- Disable sharing.

2. SNMP Enumeration:

- Eliminate the specialist or shut off the SNMP administration.

- In the event that stopping SNMP isn't a choice, at that point change the default network string names.
- Move up to SNMP3, which encodes passwords and messages.
- Actualize the Group Policy security alternative.

3. LDAP Enumeration:

- Utilize SSL technology to encrypt the traffic.
- Select a username unique in relation to your email address and empower account lockout.

4. NTP Enumeration:

- Configure MD5 Layer.
- Configure NTP Authentication.
- Upgrade NTP version.

5. SMTP Enumeration:

- Ignore email messages to unknown recipients.
- Disable open relay feature.
- Breaking point the number of acknowledged associations from a source to forestall brute force exploits.
- Not to include sensitive mail server and localhost information in mail responses.

6. DNS Enumeration Using Zone Transfer:

- Incapacitate the DNS Zone moves to the untrusted hosts.
- Make sure that the private hosts and their IP addresses are not published in DNS zone files of the public DNS server.

- Use premium DNS regulation services that hide sensitive information such as host information from the public.
- Utilize standard organization administrator contacts for DNS enlistment to maintain a strategic distance from social designing assaults.
- Avoid publishing Private IP address information into the zone file.
- Disable Zone Transfer for untrusted hosts.
- Hide Sensitive information from public hosts.

7. IPsec Enumeration:

- Preshared keys utilized with both fundamental and forceful mode IKE key trade components are available to sniffing and disconnected savage power granulating assaults to bargain the shared mystery. You should utilize advanced testaments or two-factor validation components to refute these dangers.
- Pre-shared keys and forceful mode IKE uphold is a catastrophe waiting to happen. On the off chance that you should uphold forceful mode IKE, utilize advanced declarations for verification.
- Forcefully firewall and channel traffic coursing through VPN encrypted tunnel so that, in case of a trade-off, network access is restricted. This point is particularly significant while giving versatile clients network access, instead of branch workplaces.
- Where conceivable, limit inbound IPsec security relationship to explicit IP addresses. This guarantees that regardless of whether an aggressor bargains a preshared key, she can only with significant effort access the VPN.

8. VoIP (Voice over IP) Enumeration:

- This hack can be smothered by actualizing SIPS (SIP over TLS) and confirming SIP queries and reactions (which can incorporate uprightness insurance).
- The utilization of SIPS and the verification of reactions can stifle many related hacks including eavesdropping and message or client pantomime.
- The utilization of digest confirmation joined with the utilization of TLS between SIP telephones and SIP intermediaries can give a station through which clients can safely validate inside their SIP domain.
- Voicemail messages can be changed over to message records and parsed by ordinary spam channels. This can just shield clients from SPIT voicemails.

9. RPC Enumeration:

- Try not to run rexd, users, or rwalld RPC administrations, since they are of negligible utilization and give aggressors both valuable data and direct admittance to your hosts.
- In high-security conditions, don't offer any RPC administrations to the public Internet. Because of the unpredictability of these administrations, almost certainly, zero-day misuse contents will be accessible to assailants before fixed data is delivered.
- To limit the danger of inner or confided in hacks against vital RPC administrations, (for example, NFS segments, including statd, lockd, and mountd), introduce the most recent seller security patches.
- Forcefully channel egress traffic, where conceivable, to guarantee that regardless of whether an assault against an RPC administration is effective, an associate back shell can't be brought forth to the hacker.

10. Unix/Linux User Enumeration:

- Keep the kernel fixed and refreshed.
- Never run any service as root except if truly required, particularly the web, information base, and record mainframes.
- SUID digit ought not to be set to any program which lets you getaway to the shell.
- You should never set SUID cycle on any record supervisor/compiler/mediator as an aggressor can undoubtedly peruse/overwrite any documents present on the framework.
- Try not to give sudo rights to any program which lets you break to the shell.

11. SMB Enumeration:

- Impair SMB convention on Web and DNS mainframes.
- Debilitate SMB convention web confronting mainframes.
- Handicap ports TCP 139 and TCP 445 utilized by the SMB convention.
- Restrict anonymous access through the RestrictNull Access parameter from the Windows Registry.

How Enumeration Gives an Attacker Access to Sensitive Data?

Enumeration is a strong tool in the context of an adversary since the latter gets the possibility to collect as many specific data as possible in relation to the object under attack. Once a connection with the target host is established, the attacker can extract sensitive data such as:

- Usernames and Passwords: Sometimes, through gaining knowledge of the passwords and username, an attacker can easily penetrate into several systems.
- Network Shares and Resources: Knowledge about shared folder, files and devices is good news to the attacker as they can take advantage of that or even gain further hold.

- Configuration Settings: Additional, one may discover misconfigurations in security settings that gives the attackers, potential points of entry.
- System Architecture Details: Getting to know the actual structure of the used system allows the attacker to better adapt in his actions.

The Enumeration Step of Security Testing

In security testing especially in penetration testing enumeration is an important phase that follows reconnaissance. In this phase, which often involves whistle blowing, testers escalate their function and seek to obtain as much information about the target system as they can. The end product is to look for the blind spots that can be exploited by a malicious user in order to compromise the system.

Key activities in the enumeration phase include:

- Identifying User Accounts: Finding legitimate usernames and if possible, the passwords to go with them.
- Mapping Network Resources: Identifying hidden resources, services and device on the network.
- Extracting Configuration Data: They involve collecting information on the settings of the system, established security policies as well as the security measures in place.
- Detecting Running Services: Gleaning service running and open ports which are potential gateway for an attack.

Conclusion

Gathering is the identification of targets and giving valuable data about their security state, which is a significant step in the evaluation of security. It is a useful resource for ethical hackers and security personnel to monitor for likely risks but at the same time is dangerous if employed by crooks. When enumeration is used and understood well and efforts are made to prevent unauthorized access to such information, then most systems cannot be compromised. Proper configuration management and some security tests such as penetration testing should be frequently done in order to secure such vital resources.

Types of Enumeration -FAQs

What is the difference between reconnaissance and enumeration?

What is NetBIOS Enumeration?

NetBIOS is an acronym that stands for Network Basic Input Output System. It enables computer communication over a LAN and the sharing of files and printers. TCP/IP network devices are identified using NetBIOS names (Windows). It must be network-unique and limited to 16 characters, with 15 reserved for the device name and the 16th reserved for identifying the type of service running or name record type.

Uses of NetBIOS Enumeration:

An attacker who discovers a Windows OS with port 139 open can investigate what resources are accessible or viewable on the remote system. To enumerate the NetBIOS names, the remote system must have file and printer sharing enabled. Depending on the availability of shares, NetBIOS enumeration may allow an attacker to read or write to the remote computer system or launch a (Dos).

NetBIOS Enumeration Tools:

NetBIOS's enumeration tools explore and scan the network for security loopholes or flaws in networked systems within a given range of IP addresses and computer lists. In addition, these tools list the operating system, users, password policies, groups, service packs and hotfixes, services, NetBIOS shares, discs, transmits, sessions, SIDs and security event logs.

Netstat:

Netstat is a utility for obtaining protocol statistics, NetBIOS name table, name cache information and current TCP/IP connections over NBT (NetBIOS over TCP/IP), assisting in the resolution of NetBIOS name resolution issues. Name resolution is normally performed when NetBIOS over TCP/IP is operational.

Netstat Parameters and their respective functions :

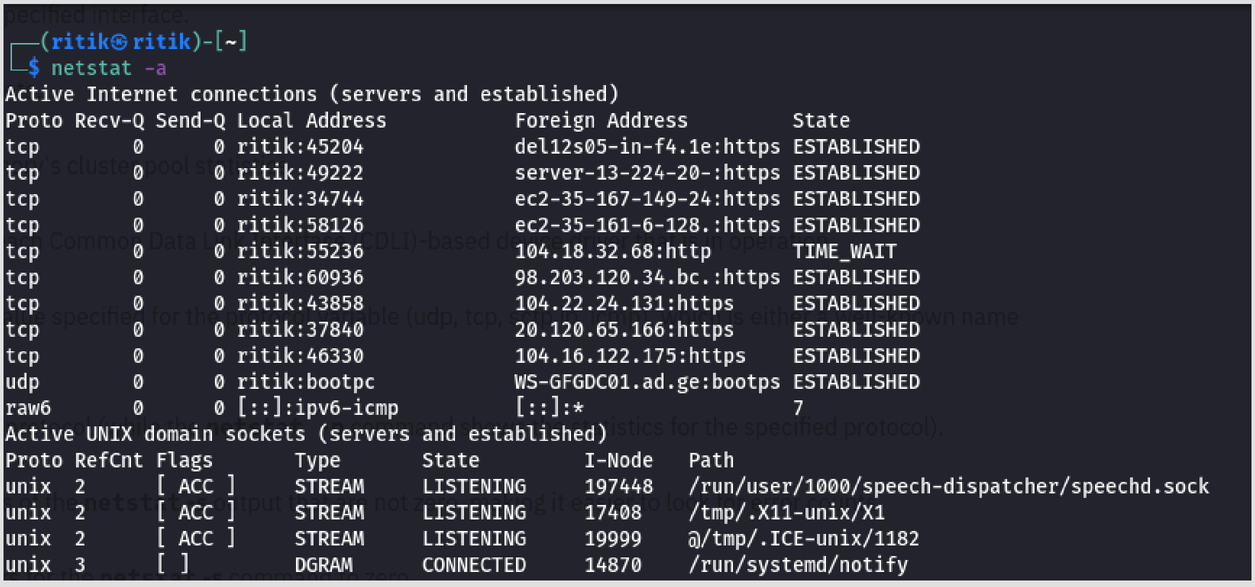
Nbtst Parameters	Functions
-a RemoteName	Displays the NetBIOS name table of a remote computer, where RemoteName is the remote computer’s NetBIOS computer name.
-A IPAddress	Displays the NetBIOS name table of a remote computer, as specified by the remote computer’s IP address (in dotted decimal notation).
-c	The contents of the NetBIOS name cache, as well as the table of NetBIOS names and their resolved IP addresses, are listed.
-n	Displays the names that NetBIOS applications, such as the server and redirector, have registered locally.
-r	Displays the total number of names resolved by a broadcast or WINS server.

-R	Removes all #PRE entries from LMHOSTS and clears the name cache.
-RR	All names are released and reregistered with the name server.
-s	The NetBIOS sessions table is listed, with destination IP addresses converted to computer NetBIOS names.
-S	Lists the current NetBIOS sessions, along with their status and IP addresses.
Interval	Displays selected statistics again, pausing for the amount of time specified in Interval between each display.

Examples:

1. To display the NetBIOS name table of a remote computer

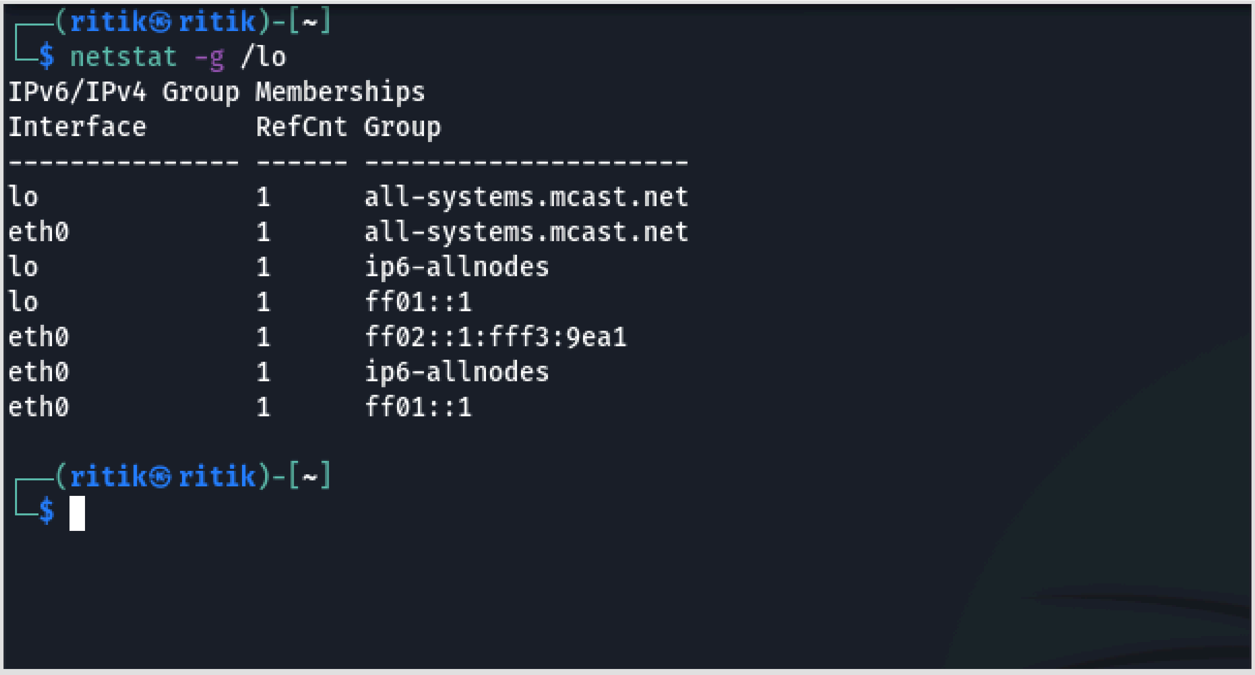
```
Netstat -a
```



```
┌──(ritik㉿ritik)-[~]
└─$ netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 ritik:45204             del12s05-in-f4.1e:https ESTABLISHED
tcp        0      0 ritik:49222             server-13-224-20-:https ESTABLISHED
tcp        0      0 ritik:34744             ec2-35-167-149-24:https ESTABLISHED
tcp        0      0 ritik:58126             ec2-35-161-6-128.:https ESTABLISHED
tcp        0      0 ritik:55236             104.18.32.68:http       TIME_WAIT
tcp        0      0 ritik:60936             98.203.120.34.bc.:https ESTABLISHED
tcp        0      0 ritik:43858             104.22.24.131:https     ESTABLISHED
tcp        0      0 ritik:37840             20.120.65.166:https     ESTABLISHED
tcp        0      0 ritik:46330             104.16.122.175:https    ESTABLISHED
udp        0      0 ritik:bootpc            WS-GFGDC01.ad.ge:bootps ESTABLISHED
raw6       0      0 [::]:ipv6-icmp          [::]:*                  7
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     STREAM     LISTENING     197448   /run/user/1000/speech-dispatcher/speechd.sock
unix  2      [ ACC ]     STREAM     LISTENING     17408    /tmp/.X11-unix/X1
unix  2      [ ACC ]     STREAM     LISTENING     19999    @/tmp/.ICE-unix/1182
unix  3      [ ]         DGRAM      CONNECTED     14870    /run/systemd/notify
```

2. To see IPv4/IPv6 Group Memberships

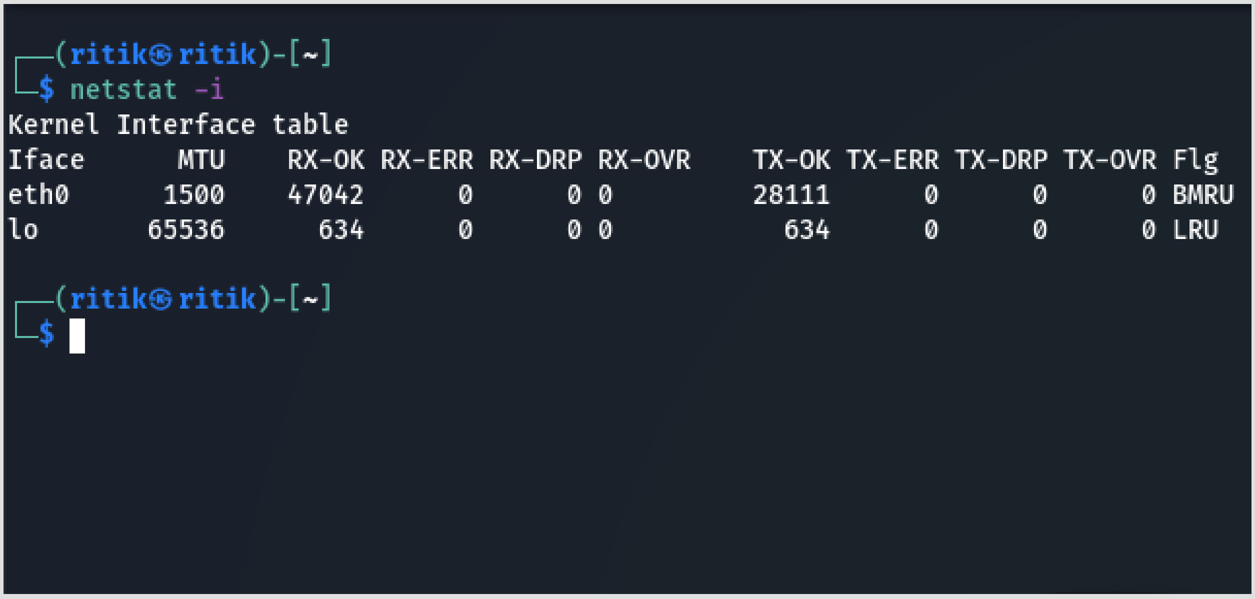
Netstat -g



```
┌──(ritik㉿ritik)-[~]
└─$ netstat -g /lo
IPv6/IPv4 Group Memberships
Interface       RefCnt Group
--------------- ------ ---------------------
lo              1      all-systems.mcast.net
eth0            1      all-systems.mcast.net
lo              1      ip6-allnodes
lo              1      ff01::1
eth0            1      ff02::1:fff3:9ea1
eth0            1      ip6-allnodes
eth0            1      ff01::1

┌──(ritik㉿ritik)-[~]
└─$ 
```

3. To display kernel interface

Netstat -i



```
┌──(ritik㉿ritik)-[~]
└─$ netstat -i
Kernel Interface table
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0      1500    47042      0      0 0         28111      0      0      0 BMRU
lo       65536      634      0      0 0           634      0      0      0 LRU

┌──(ritik㉿ritik)-[~]
└─$ 
```

Hyena:

Windows operating systems are managed and secured by Hyena. For all operations, it employs a Windows Explorer-style interface. Users, groups (both local and global), shares, domains, computers, services, devices, events, files, printers, print jobs, sessions, open files, disc space, user rights, messaging, exporting, job scheduling, processes, and printing are all supported. It displays Windows server and domain controller shares and user log on names.

It shows a graphical representation of Microsoft Terminal Services, Windows Network, Web Client Network, and so on.

Features:

1. Active Task Matching Options – Active Directory update tasks, a key match option has been added to Active Task. When updating directory objects, the new key option allows any unique directory characteristic to be employed as a 'match' field.
2. Group Member Matrix – in a simple grid all members of multiple groups, including direct, indirect (nested), and primary membership.

3. Active Editor Enhancements – The new Hyena release includes new Editor feature enhancements such as account expiration date, support for multivalued attributes, and multi-selection and update capabilities.

PsExec:

PsExec is a lightweight telnet replacement that can execute processes on other systems, complete with full interactivity for console applications, without the need for manual client software installation. PsExec's most powerful applications include launching interactive command prompts on remote systems and remote-enabling tools such as Ipconfig, which would otherwise be unable to display information about remote systems.

PsFile:

PsFile is a command-line utility which displays a list of files that have been opened remotely on a system and can close opened files by name or file identifier. PsFile's default behaviour is to list the files on the local system that have been opened by remote systems. Typing a command followed by "-" showcases details about the command's syntax.

PsGetSid:

PsGetSid converts SIDs to display names and vice versa. It is compatible with built-in accounts, domain accounts, and local accounts. It also displays the SIDs of user accounts and translates a SID into its corresponding name. It can query SIDs remotely across the network.

PsKill:

PsKill is a kill utility that can end processes and kill processes on remote systems. When you run PsKill with a process ID, it will kill the process with that ID on your local computer. If you define a process name, PsKill will kill all processes with that name. PsKill does not require the installation of a client on the targeted device to terminate a remote process.

SuperScan :

SuperScan is a free proprietary graphical application tool for enumerating Windows machines for Windows which was built by Foundstone and later acquired by McAffe. This tool is no longer available for download from the McAffe website.

NET VIEW:

NET VIEW is a command-line tool for locating shared network resources. NetBIOS is required for the NET VIEW command. When NetBIOS is disabled, greatest modern networks will return an incomplete list of nearby computers, or none at all. It is used in.

1. net view \\<computername> – Where<computername> is the name of the computer whose resources you wish to view.
2. net view /workgroup:<workgroupname> – Where <workgroupname>is the name of the workgroup from which you want to view the shared resources.

NetBIOS Protection Ways:

A security hole in the NetBIOS protocol allows a Windows VPS with this service enabled to be used in an amplification DDoS attack. The following security controls are in place to prevent NetBIOS enumeration attacks:

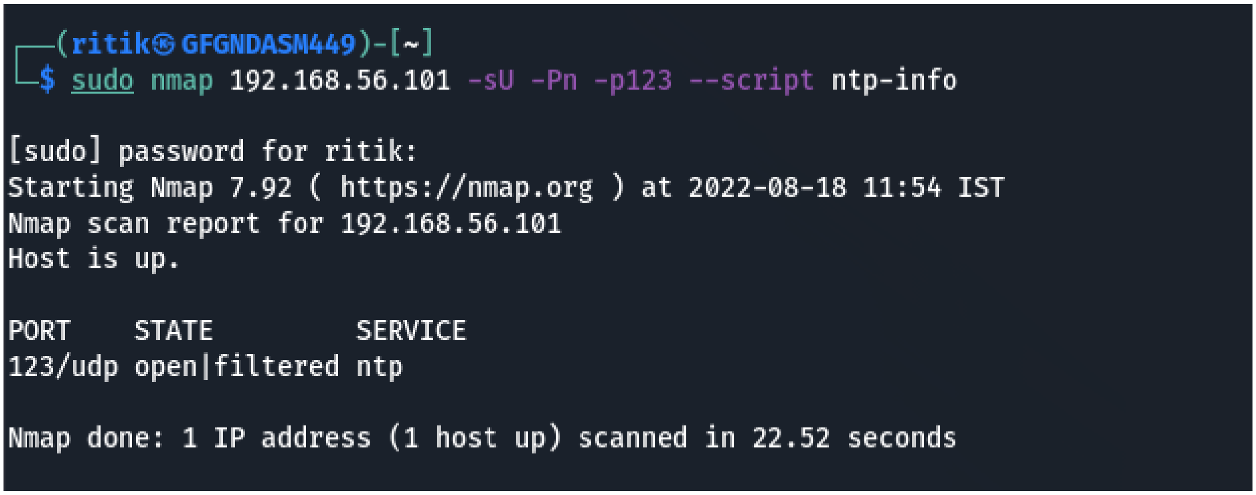
- Reduce the attack surface by removing unnecessary services such as Server Message Block (SMB).
- On Windows, disable file and printer sharing.

What is NTP Enumeration?

NTP Enumeration is a process by which an attacker can discover NTP servers on the network. This information can then be used to find vulnerable NTP servers, or simply to further enumerate the network. Servers that are allowed access from the internet usually have a much higher chance of being exploitable. An attacker will often use both DNS and brute force methods to find these servers, as well as using Shodan.io or Censys to find unprotected devices.

Exploit Vulnerability:

While NTP servers are typically given special access to the network, they do not always have to be on the same network. For example, an attacker may compromise a server with an open port and use NTP to take a list of hosts that are connected to him/her. The attacker can then send that list to scanners that scan for vulnerable hosts. The difference between this and other types of vulnerability is the amount of research involved and harder exploitation options. This can be used against wireless networks because many manufacturers will disable wireless access from their default factory settings. There are also less obvious ways to use it as well, such as traffic mirroring.



```
┌──(ritik㉿GFGNDASM449)-[~]
└─$ sudo nmap 192.168.56.101 -sU -Pn -p123 --script ntp-info

[sudo] password for ritik:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-18 11:54 IST
Nmap scan report for 192.168.56.101
Host is up.

PORT    STATE         SERVICE
123/udp open|filtered ntp

Nmap done: 1 IP address (1 host up) scanned in 22.52 seconds
```

Properties:

- Since NTP can be used to enumerate many hosts on a network, some basic checks should be done before using it as an alternative route.
- “-NTP only” and “-NTP enabled” are easy checks that can often be done on a simple server to identify if they are vulnerable or not.
- A “ping sweep” is another easy test that can often reveal which servers may or may not be vulnerable, simply by sending packets from the attacker and recording the reply from his/her victim.
- Many of these tests can also be automated with ping with tcpdump. There are also many programs available for Nessus and OpenVAS that can scan for vulnerabilities in NTP configurations.

- Nessus is a network security scanner available for most Operating Systems. This program will run checks against a range of services. NTP should be added to this list and the vulnerabilities will be identified by a plugin or rule. This can often cause a short outage if downtime is required for maintenance, updating software, repairing, etc.
- OpenVAS is an open-source vulnerability scanner that can scan networks for common known vulnerabilities. It can also scan for many more obscure vulnerabilities like NTP Enumeration and other issues that are not yet documented in the official documentation.
- Several applications are available online that will automate vulnerability scanning on OpenVAS (Stratumnscan, ASVScan).

NTP Security Model:

- NTP runs over UDP and TCP. NTP can also be sent via IP multicast, as well as running on Layer 2 (Ethernet).
- NTP uses symmetric encryption with a shared key between each server and client.
- There are two types of keys, Autokey, and Symmetric keys. Autokey is used for broadcast communication. The source of the time message is known as a "stratum 1" server, but since this system has been deprecated, many NTP servers no longer use it. All modern servers use a Symmetric key for communication between clients and servers.
- It uses only one type of packet, the NTP packet. The only difference between the NTP and UDP and TCP packets is how they're encrypted.
- The symmetric key is used for every packet sent by a client, it also allows multicast communication, however multicast packets are less efficient because of this.

- A client should use the local unicast IP address to identify itself in packets (not the MAC address).
- The NTP packets contain a checksum and port number which is sent once, upon connection.
- Firewalls need to be configured to allow NTP to operate properly.
- NTP can operate in non-authenticated or authenticated mode.

Important Points:

- In practice, the whole network is not required to be controlled by NTP; only the first level of infrastructure.
- NTP should not be used in parallel to DNS.
- Network time can often be disabled in wrong configured devices, or over-ridden in clients and servers.
- Servers should use different time sources, and clients should use the NTP options to set their own source (otherwise the client might be vulnerable).

LDAP Enumeration

Before continuing reading, read about the LDAP in general. Lightweight Directory Access Protocol (LDAP) is an internet protocol that works on TCP/IP, used to access information from directories. The LDAP protocol is used to access an active directory. LDAP enumeration is a technique used to enumerate the active directory. This service mainly runs on TCP ports 389 and 639 as default. LDAP enumeration can help enumerate usernames, addresses, and much juicy information that can be later used for other attacks including social engineering attacks.

LDAP queries can be used to enumerate various things like usernames, groups, and much more stuff.

Tools Used For LDAP Enumeration:

- Nmap
- enum4linux

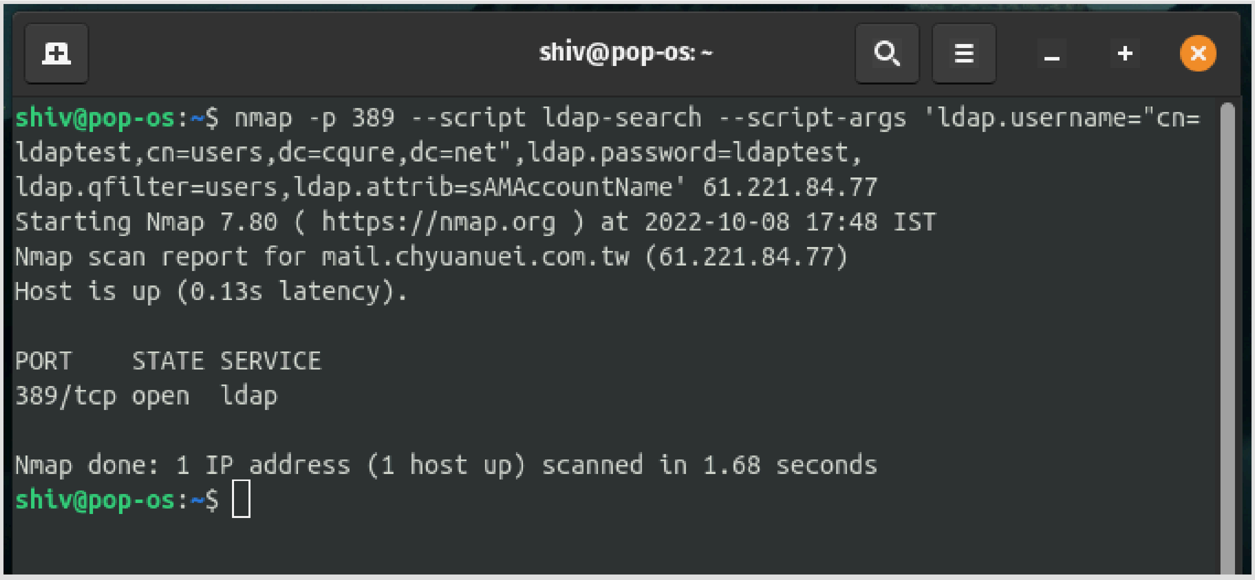
- windapsearch
- ldapsearch
- Jxplorer

LDAP Enumeration using Nmap:

By using Nmap’s LDAP-search NSE script we can scan for the LDAP service, and then we can try other arguments for this script like LDAP.searchattrib, also you can use the LDAP-brute script, and when you don’t have any valid credentials.

```
$ nmap -p 389 --script ldap-search --script-args
'ldap.username="cn=ldaptest,cn=users,dc=cqure,
dc=net",ldap.password=ldaptest,
ldap.qfilter=users,ldap.attrib=sAMAccountName' <IP address>
```

```
$ nmap -p 389 --script ldap-search --script-args
'ldap.username="cn=ldaptest,cn=users,
dc=cqure,dc=net",ldap.password=ldaptest,
ldap.qfilter=custom,ldap.searchattrib="operatingSystem",
ldap.searchvalue="Windows *Server*",ldap.attrib=
{operatingSystem,whencreated,OperatingSystemServicePack}' <host>
```

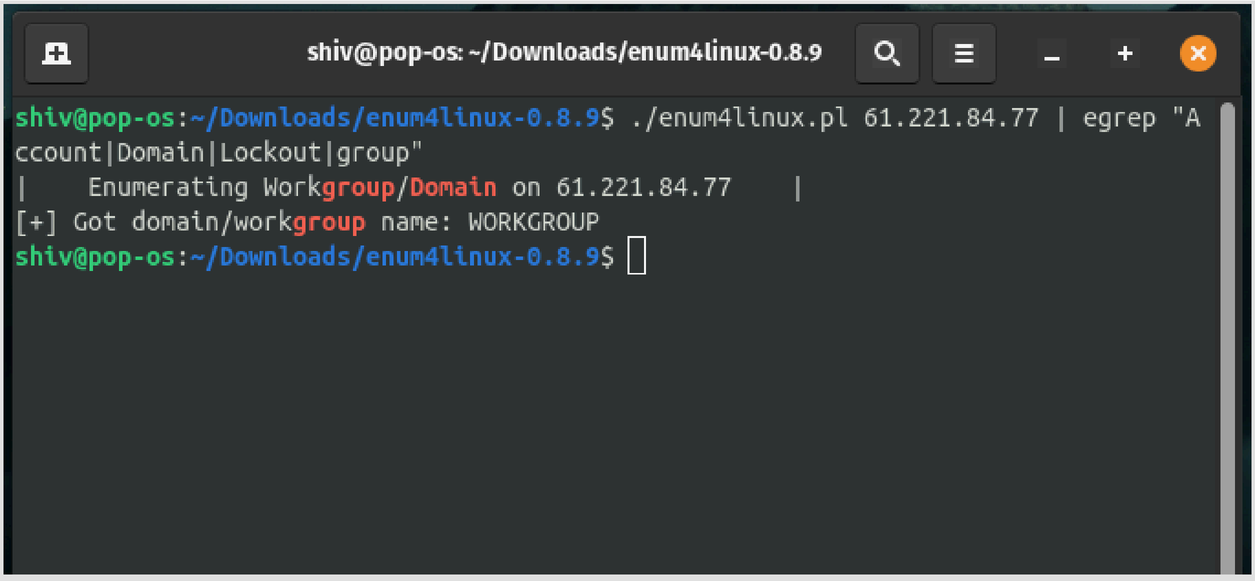


```
shiv@pop-os:~$ nmap -p 389 --script ldap-search --script-args 'ldap.username="cn=
ldaptest,cn=users,dc=cqure,dc=net",ldap.password=ldaptest,
ldap.qfilter=users,ldap.attrib=sAMAccountName' 61.221.84.77
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-08 17:48 IST
Nmap scan report for mail.chyuanuei.com.tw (61.221.84.77)
Host is up (0.13s latency).

PORT    STATE SERVICE
389/tcp open  ldap

Nmap done: 1 IP address (1 host up) scanned in 1.68 seconds
shiv@pop-os:~$ 
```

LDAP Enumeration Using enum4linux:

Enum4linux is a great tool that is used in windows enumeration, hence we are going to look at this tool's usage. Using the below command, you can enumerate the accounts and groups.

```
$ enum4linux <IP address> |
egrep "Account|Domain|Lockout|group"
```



```
shiv@pop-os:~/Downloads/enum4linux-0.8.9$ ./enum4linux.pl 61.221.84.77 | egrep "A
ccount|Domain|Lockout|group"
|    Enumerating Workgroup/Domain on 61.221.84.77    |
[+] Got domain/workgroup name: WORKGROUP
shiv@pop-os:~/Downloads/enum4linux-0.8.9$
```

LDAP Enumeration Using Windapsearch:

Windapsearch is a python script that is used to enumerate users, groups, and computers from a windows domain by taking the leverage of LDAP queries.

```
#for computers
python3 windapsearch.py --dc-ip
<IP address> -u <username>
-p <password> --computers

#for groups
python3 windapsearch.py --dc-ip <IP address>
-u <username> -p <password> --groups

#for users
python3 windapsearch.py --dc-ip <IP address>
-u <username> -p <password> --da
```

```
#for privileged users
python3 windapsearch.py --dc-ip <IP address>
-u <username> -p <password> --privileged-users
```

LDAP Enumeration Using Ldapsearch:
LDAP search makes a connection to an LDAP server, and it executes a search by using different paraments. The filter conforms to the string representation for search filters as defined in RFC 4515 else it uses (objectClass=*).

Below are some commands that can be used for checking and verifying the credentials.

```
#To check null credentials
$ ldapsearch -x -H ldap://<IP address>
 -D '' -w '' -b "DC=<1_SUBDOMAIN>,DC=<TLD>"
```

```
#to validate the credentials
$ ldapsearch -x -H ldap://<IP address>
-D '<DOMAIN>\<username>' -w '<password>'
-b "DC=<1_SUBDOMAIN>,DC=<TLD>"
```

SMTP Enumeration
SMTP (Simple Mail Transfer Protocol) is a set of communication guidelines that allow web applications to perform communication tasks over the internet, including emails. It is a part of the TCP/IP protocol and works on moving emails across the network. SMTP enumeration allows us to identify valid users on the SMTP server. This is done with the built-in SMTP commands using them. VRFY – This command is used to authenticate the user. EXPN – This command displays the actual mailing address for aliases and mailing lists. RCPT TO – It identifies the recipient of the message. SMTP enumeration is a technique used to enumerate the SMTP service that is running on the target server.

Pre-Defined Commands:

- **VRFY**: It is used to validate the user on the server.
- **EXPN**: It is used to find the delivery address of mail aliases
- **RCPT TO**: It points to the recipient’s address.

Test for SMTP Enumeration:

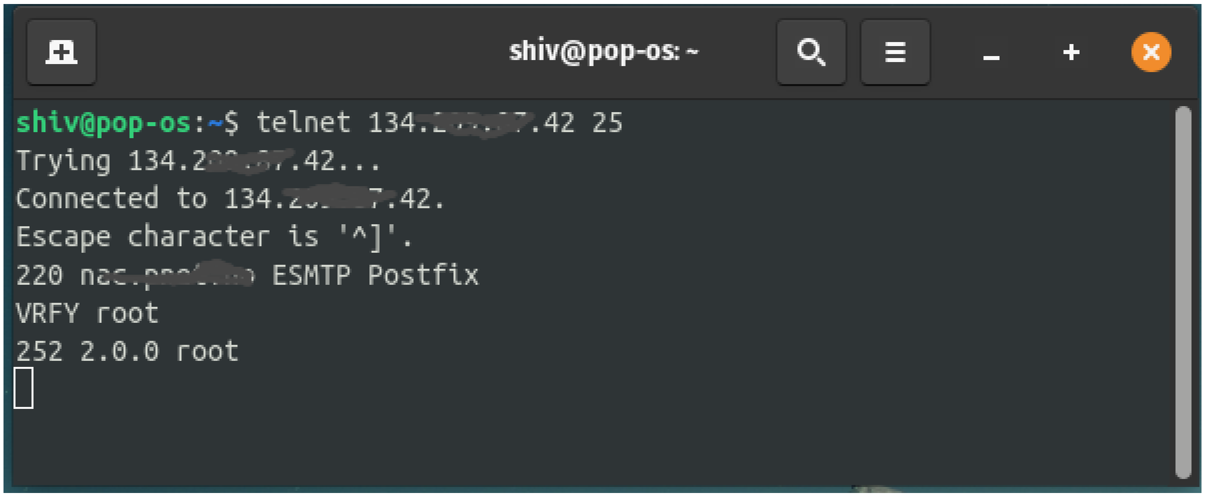
SMTP enumeration can be performed by using different tools and scripts like **telnet**, **Nmap**, and **smtp-user-enum.**

1. Using Telnet for SMTP enumeration:

Telnet comes in handy in SMTP enumeration as it provides a communication channel with the host.

```
$ telnet <domain name/ip> <port no.>
```

Example:



```
shiv@pop-os:~$ telnet 134.[redacted].42 25
Trying 134.2[redacted].42...
Connected to 134.[redacted].42.
Escape character is '^]'.
220 na[redacted] ESMTP Postfix
VRFY root
252 2.0.0 root
```

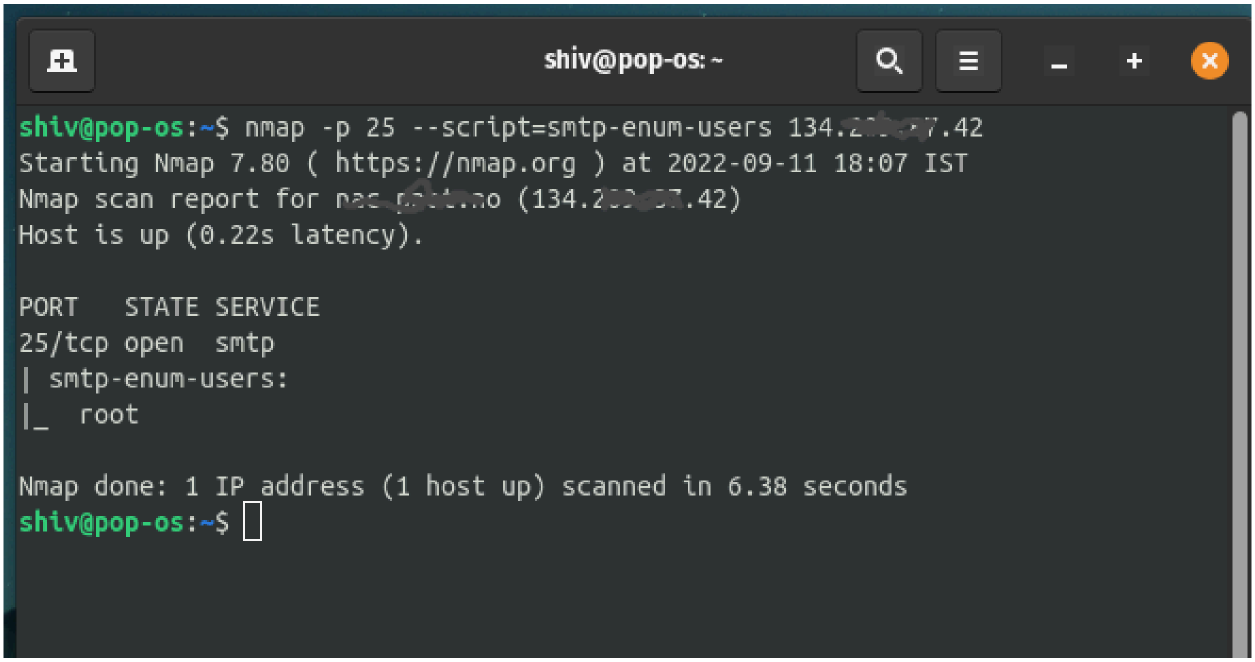
later you can use EXPN, MAIL FROM, and RCPT TO after connecting to the target host.

2. Using Nmap for SMTP enumeration:

Nmap is a powerful tool and is used in different enumeration phases. Nmap provides special scripts for SMTP enumeration. smtp-enum-users is one of the scripts that is provided by Nmap.

```
$sudo nmap -p 25 --script =
 smtp-enum-users <target Domain/IP>
```

Example:



```
shiv@pop-os:~$ nmap -p 25 --script=smtp-enum-users 134.[redacted].42
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-11 18:07 IST
Nmap scan report for [redacted] (134.[redacted].42)
Host is up (0.22s latency).

PORT   STATE SERVICE
25/tcp open  smtp
| smtp-enum-users:
|_  root

Nmap done: 1 IP address (1 host up) scanned in 6.38 seconds
shiv@pop-os:~$ 
```

SMTP enumeration using Nmap

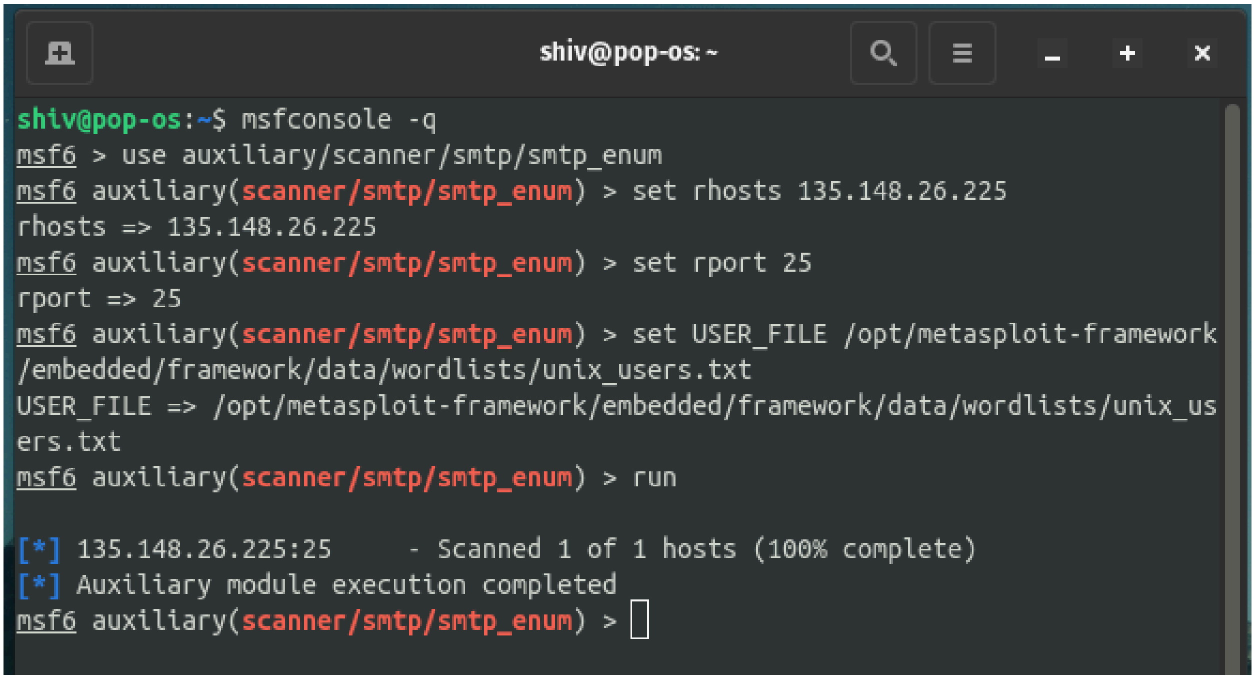
3. Using Metasploit for SMTP Enumeration:

Metasploit provides two SMTP auxiliary Modules i.e., smtp_enum and smtp_version. Both are used for SMTP enumeration and provide adequate information about the SMTP server.

smtp_enum:

```
msf > use auxiliary/scanner/smtp/smtp_enum
msf auxiliary(smtp_enum) set RHOSTS <IP address/target>
msf auxiliary(smtp_enum) > set rport 25
msf auxiliary(smtp_enum) set USER_FILE <address of file>
msf auxiliary(smtp_enum) run
```

Example:



```
shiv@pop-os:~$ msfconsole -q
msf6 > use auxiliary/scanner/smtp/smtp_enum
msf6 auxiliary(scanner/smtp/smtp_enum) > set rhosts 135.148.26.225
rhosts => 135.148.26.225
msf6 auxiliary(scanner/smtp/smtp_enum) > set rport 25
rport => 25
msf6 auxiliary(scanner/smtp/smtp_enum) > set USER_FILE /opt/metasploit-framework
/embedded/framework/data/wordlists/unix_users.txt
USER_FILE => /opt/metasploit-framework/embedded/framework/data/wordlists/unix_us
ers.txt
msf6 auxiliary(scanner/smtp/smtp_enum) > run

[*] 135.148.26.225:25     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) > 
```

What is DNS Enumeration?

Domain Name System(DNS) is nothing but a program that converts or translates a website name into an IP address and vice versa.

Example: A user enters www.geeksforgeeks.org in a browser, now the DNS will intercept this request and will fetch the corresponding IP address and connect the user to that fetched IP address.

***DNS Enumeration** is a technique used for Reconnaissance for better understanding of surface area of the **Target systems**(i.e. IP addresses).*

- The process of DNS Enumeration returns various important information about the target like DNS record types, host names, IP addresses and much more depending upon the configuration of that target system.

- To perform DNS enumeration there are various open source tools, scripts available like Nmap, DNS recon etc.

Importance and Impacts:

Importance:

- It helps in discovering the various services and hosts that are running on the domain.
- It makes the target surface larger as we enumerate further.
- Furthermore, it exposes the critical information about the target.

Impact:

- The attacker can read about the system data and also can modify it.
- It can also lead to various other potential DNS attacks.
- It gives the Threat actor very critical details about the system that the attack can leverage to other attacks.

Steps of DNS Enumeration:

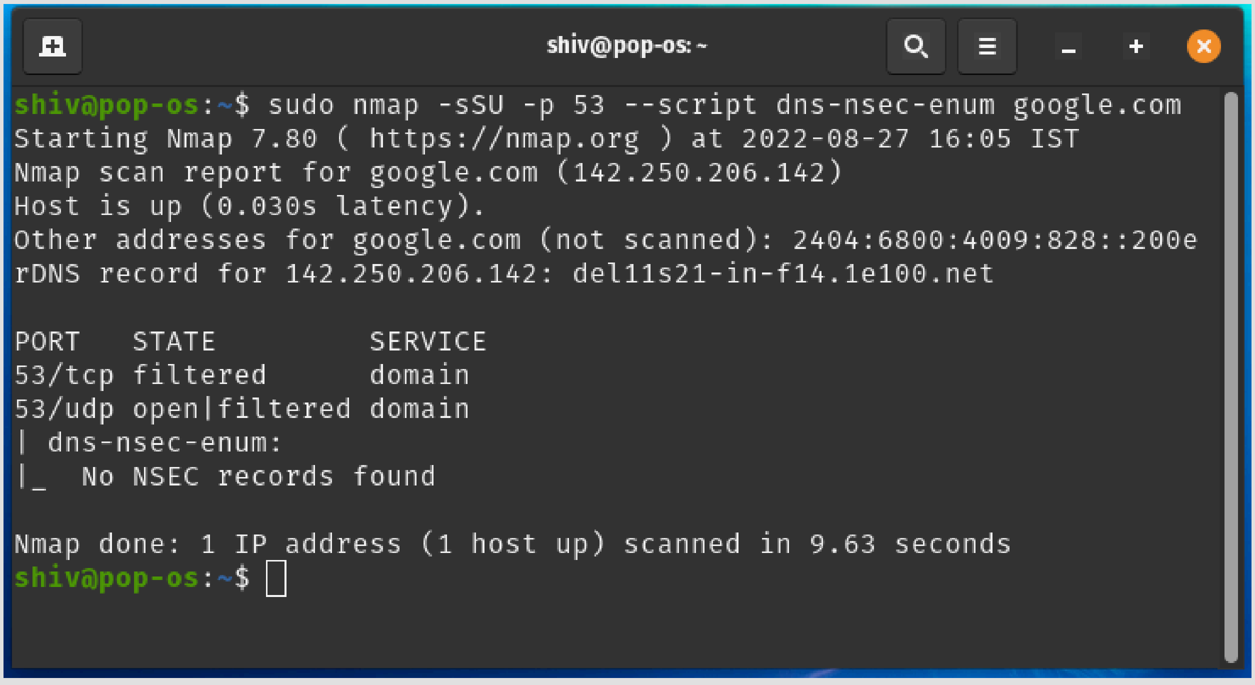
There are various tools to do DNS Enumeration, you are free to explore them by doing a simple web search about DNS Enumeration tools, but here we are going to use Nmap as an example:-

Nmap:

It is a tool used to discover host and services that are currently running of a computer network. Nmap provides an extensive Script by the name dns-nsec-enum.

Command Usage:

```
nmap -sSU -p 53 --script dns-nsec-enum -
-script-args dns-nsec-enum.domains=example.com
<target>
```



```
shiv@pop-os:~$ sudo nmap -sSU -p 53 --script dns-nsec-enum google.com
Starting Nmap 7.80 ( https://nmap.org ) at 2022-08-27 16:05 IST
Nmap scan report for google.com (142.250.206.142)
Host is up (0.030s latency).
Other addresses for google.com (not scanned): 2404:6800:4009:828::200e
rDNS record for 142.250.206.142: del11s21-in-f14.1e100.net

PORT     STATE         SERVICE
53/tcp   filtered      domain
53/udp   open|filtered domain
| dns-nsec-enum:
|_  No NSEC records found

Nmap done: 1 IP address (1 host up) scanned in 9.63 seconds
shiv@pop-os:~$ 
```

Output:

In the above result, we didn't find any NSEC records, but you can try different other scripts like dns-brute. nse, dns-cache-snoop. nse, and dns-check-zone. nse for more DNS Enumeration.

Prevention:

- By restricting Zone Transfer by untrusted hosts.
- By auditing regularly the DNS record to avoid the availability of unused DNS record.
- Never that your private host remain private and doesn't use public IP address.

What is System Hacking in Ethical Hacking?

System hacking is the process of exploiting vulnerabilities in electronic systems for the purpose of gaining unauthorized access to those systems. Hackers use a variety of techniques and methods to access electronic systems, including phishing, social engineering, and password guessing.

Purpose of System Hacking:

Generally, the motive of the hackers behind System Hacking is gaining access to the personal data of an individual or sensitive information belonging to an organization in order to misuse the information and leak it which may cause a negative image of the organization in the minds of people, Privilege Escalation, Executing malicious applications to constantly monitor the system.

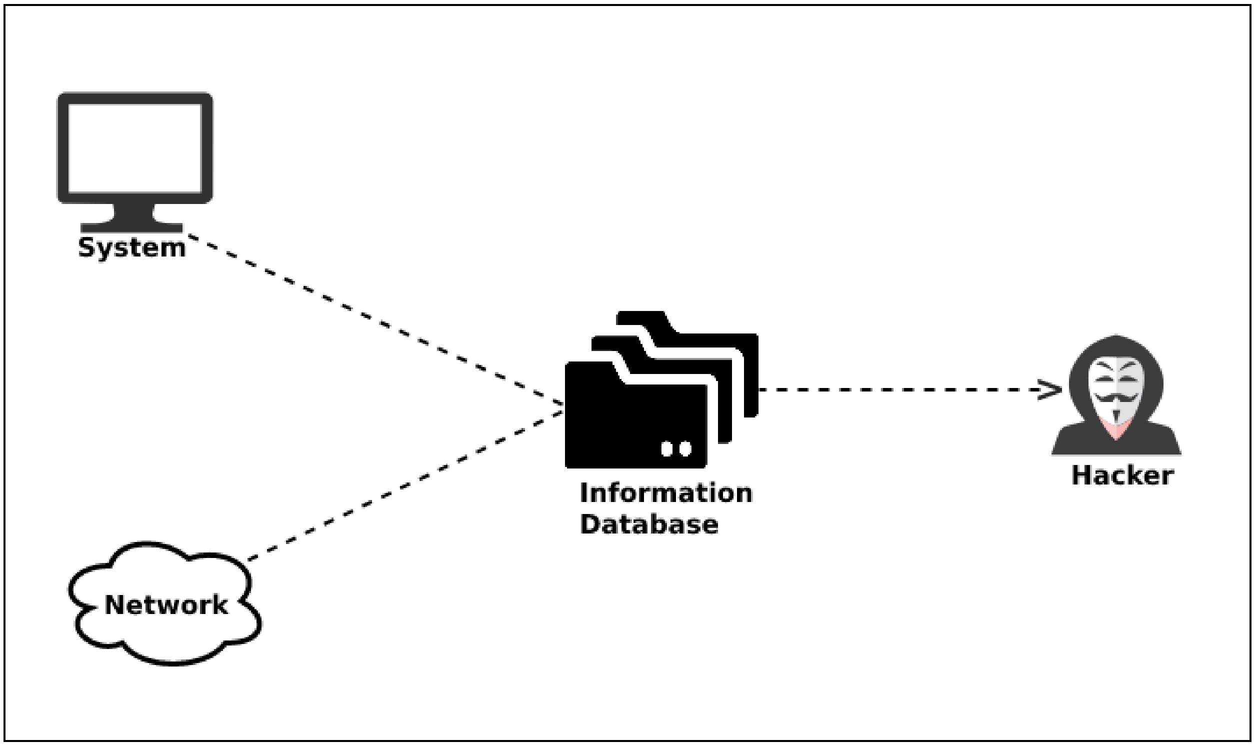
How this is carried out?

This type of hacking is generally done by a Hacker who has a lot of information regarding the System security, network, software, and how the system communicates with others in the network, often called Footprinting and Reconnaissance. Then these hackers try numerous ways to carry out the attack but the common ways are:

- By deploying Viruses, Worms, Malware, Trojans
- Using phishing techniques
- Social Engineering
- Identifying and exploiting Vulnerability

Steps:

1. Reconnaissance: The first step in this type of Hacking is collecting information regarding the System's infrastructure, working, system's network. This step is very important as after this step the Hacker knows what attack to perform and how to gain access without leaving a trace.



2. Scanning: This step involves scanning the target System, which includes:

- **Vulnerability Scanning:** Checking vulnerabilities in the targeted system that can be exploited to gain access.
- **Mapping of Network:** Finding the working of the network, firewalls, routers, and systems connected to it.
- **Port Scanning:** Scanning the open ports, and services running over the System/Server.

3. Gaining Access: This is the phase in which the hacker breaks into the system and gains unauthorized access to the System/Network and then elevates his privileges to that of Administrator or SuperUser so he can play with the System files that a normal/Guest user is unable to access.

4. Maintaining the Access: After the Hacker enters the System he tries to maintain the connection with it in the background until he accomplishes the goal with which he entered it.

To know more about the phases of hacking please refer to the article 5 Phases of Hacking.

Prevention from Hacking:

- Using Firewall.
- Installing Anti-Virus and Anti-Spyware packages.
- Keeping the system up-to-date as security patches updates comes regularly.
- Be Aware of various phishing techniques.

What is Vulnerability Assessment?

Last Updated : 20 Aug, 2024

[redacted]

Living in a world with more and more complex threats posted by cybercriminals, it is imperative that you shield your networks. A vulnerability scanning is done to understand areas that are prone to an attack by the invader before they exploit the system. The above measures not only protect data and guard against data leakage but also help meet security requirements and strengthen risk management. In this article, we'll look at what vulnerability assessment is, why it is important, and how it stands from penetration testing. We will also outline how the assessment is conducted, the provided tool, and key advantages and disadvantages.

What is a Vulnerability Assessment?

A vulnerability assessment is a procedure that is employed in an information system to determine and rate potential risks. It seeks to identify vulnerabilities that can be leveraged by an attacker to compromise the system and to employ tools and techniques that ensure that data confidentiality, integrity, and availability are achieved. This systematic review assists organizations in identifying security issues like cross-site scripting (XSS) and SQL injection before they can be leveraged.

Importance of Vulnerability Assessments

Vulnerability assessments are very important in the protection of information systems and data. They help by:

- **Preventing Data Breaches:** Directing single and exclusive attention to every risk in line with time and noticing the recurrent threats so as to treat them before they bring about expensive security invasions.
- **Ensuring Regulatory Compliance:** Conformity to the laws and evasion of the law.
- **Managing Risks:** Risk priority and risk control to improve the general shareholder's risk evaluation.
- **Enhancing Security Posture:** Periodic evaluations enhance security by making provisions of security to cater for emerging threats.
- **Cost-Effective Security:** This solution lowers the expensive costs associated with security incidents that occur when the vulnerabilities are not tended to as soon as they are identified.

Types of Vulnerability Assessments

- **Host Vulnerability Assessment:** Conducts analysis on the servers and host systems so as to expose and contain backend attacks.
- **Database Vulnerability Assessment:** Provides for the prevention of unauthorized access of data within the database in terms of confidentiality, integrity and availability.

- **Network Vulnerability Assessment:** Evaluates the security of networks with the aim of attainable protection against oncoming and existing network complexity.
- **Application Scan Vulnerability Assessment:** Scans application code for application level vulnerabilities in frontend and backend auto-mated tools.

Vulnerability Assessments vs Penetration Tests

Parameter	**Vulnerability assessments**	**Penetration tests**
Objective	Identification and evaluation of potential vulnerabilities	Real world attacks are simulated to exploit vulnerabilities
Methodology	Usage of manual techniques and automated systems to scan systems	Ethical hackers are involved who attempt to exploit vulnerabilities
Scope	Various aspects of the system are covered	Target specific vulnerabilities and attack vectors

Frequency	Conducted regularly as part of an ongoing strategy	Less frequent and is performed when needed
Focus	Gives a broader perspective of potential issues	Gives deeper insight into the impact of exploiting vulnerabilities
Approach	Proactive approach which helps prevent potential issues	Reactive approach which assess the effectiveness of existing security measures

How Does a Vulnerability Assessment Work?

- **Planning and Scoping:** Identify the parameters, aims and objectives and target system of the assessment.
- **Discovery:** Collect general information about the system: hosts, ports, and software, etc. Collect it with using specialized software and through manual assessment.
- **Scanning:** Make a scan to each host in order to detect open ports, mistakes or problems in configurations.
- **Analysis:** Analyze scan information to identify imperatives and determine their potential vulnerability.

- **Reporting:** Record exploits, their consequences and rank suggestions for insurance.
- **Remediation:** Apply remedies, modify settings and work on the fortification of the architecture.
- **Follow-Up:** Ensure fix and verify that fix is correct & look for new vulnerability.

How Does Vulnerability Assessment Help?

It helps any organization safeguard itself from cyber attacks by identifying the loopholes in advance. Here are some threats that we can prevent if we use vulnerability assessment.

- Injection attacks like XSS and SQL injection
- Authentication faults that lead to unidentified access to important data
- Insecure settings and weak defaults

The Process of Vulnerability Assessment

The process of Vulnerability Assessment is divided into four stages. Let us discuss them one by one.

- **Testing or Vulnerability Identification:** All the aspects of a system like networks, servers, and databases are checked for possible threats, weaknesses, and vulnerabilities. The goal of this step is to get a list of all the possible loopholes in the security of the system. The testing is done through machines as well as manually and all parameters are kept in mind while doing so.
- **Analysis:** From the first step, we get a list of vulnerabilities. Then, it is time that these are analyzed in detail. The goal of this analysis is to identify where things went wrong so that rectification can be done easily. This step aims at finding the root cause of vulnerabilities.

- **Risk Assessment:** When there are many vulnerabilities, it becomes important to classify them on the basis of risks they might cause. The main objective of this step is to prioritize vulnerabilities on the basis of data and systems they might affect. It also gauges the severity of attacks and the damage they can cause.
- **Rectification:** Once if have a clear layout of the risks, their root cause, and their severity, we can start making corrections in the system. The fourth step aims at closing the gaps in security by introducing new security tools and measures.

Tools for Vulnerability Assessment

Manually testing an application for possible vulnerabilities might be a tedious job. There are some tools that can automatically scan the system for vulnerabilities. A few such tools include:

- Simulation tools that test web applications.
- Scanners that test network services and protocols.
- Network scanners that identify malicious packets and defects in IP addresses.

Advantages of Vulnerability Assessment

- Detect the weakness of your system before any data breach occurs.
- A list of all possible vulnerabilities for each device present in the system.
- Record of security for future assessments.

Disadvantages of Vulnerability Assessment

- Some advanced vulnerabilities might not be detected.
- Assessment tools might not give exact results.

What is Vulnerability Assessment? – FAQs

How do a vulnerability assessment and a risk assessment differ?

Vulnerability assessment provides information on numerous flaws of a system while risk assessment determines severity of the vulnerability and the probability of it being exploited.

How precise should the assessments be and how often should they take place?

The vulnerabilities should be scanned at frequent intervals like at least quarterly, or annually and always after some system or software changes.

Are the vulnerability assessments adequate enough for achieving total and complete security?

No, vulnerability assessments are a part of a total security management. They should be accompanied by such strategies as penetration testing and continuous monitoring, for instance.

Is it possible to automate the vulnerability assessments?

To an extent, the procedures of vulnerability assessments can be automated to streamline work and increase the efficacy of particular tools; nevertheless, it is crucial to include a manual check of the data obtained by particular tools and platforms.

What is a Vulnerability Assessment?

Vulnerability assessment is the process of identifying the threats or weaknesses in computer systems, networks, and software, along with the inherent risks they introduce.

Vulnerability assessments done by performing black box or grey box security testing simulate real-life scenarios of how hackers attack applications. After all every application is a black box from a hacker's perspective and they just brute force various attack types using sophisticated scanners.

Vulnerability Assessment and Penetration Testing(VAPT) helps organizations figure out where they might be at risk to prioritize remediation based on the severity level.

What Is a Vulnerability?

Vulnerabilities refer to errors or weaknesses within a system's security protocols, structure, execution, or internal management that could potentially breach the system's security policies.

How to Perform Vulnerability Assessments?

To identify code or security vulnerabilities in advance, performing a SAST or a DAST scan and integrating these tools in your CI/CD pipeline is recommended. These vulnerability scanners use databases of known vulnerabilities to detect potential weaknesses across applications, systems, data, and other elements.

The vulnerability scanner performs a thorough scan across all dimensions of your technology. It examines the target system for known security issues, misconfigurations, outdated software, and potential entry points that attackers could exploit. Once the scans finish, the tool presents a report detailing all uncovered problems and proposes measures to counter potential threats.

More comprehensive tools could go further by providing SIEM Integration. With this integration, the data from vulnerability scanner can be pushed into a SIEM (Security Information & Event Management), enhancing the scope of threat analysis.

Asset discovery and monitoring is a valuable attribute of Indusface WAS, facilitating the creation of a complete asset inventory and enforcing consistent security monitoring for all assets.

Vulnerability Assessment vs. Penetration Testing

Vulnerability assessment is more focused on identifying vulnerabilities and weaknesses, while penetration testing involves actively exploiting those vulnerabilities to assess their real-world impact. Vulnerability assessments help organizations identify areas that need attention and prioritize fixes, while penetration testing helps organizations understand the potential consequences of successful attacks and improve their incident response capabilities.

Key features of a vulnerability assessment:

- Scanning: Automated tools are used to scan the target system for known vulnerabilities.
- Identifying Weaknesses: The assessment identifies security weaknesses and provides a prioritized list of vulnerabilities.
- No Exploitation: Vulnerability assessment does not involve actively exploiting vulnerabilities; it focuses on identification and reporting.
- Remediation Recommendations: The assessment results typically include recommendations for remediation and mitigation.

Key features of penetration testing:

- Active Exploitation: Penetration testing involves actively attempting to exploit vulnerabilities to assess their impact.
- Realistic Scenarios: Testers simulate real-world attack scenarios to identify potential entry points and the extent of damage that could occur.
- Manual and Automated Testing: Both manual techniques and automated tools are used to identify and exploit vulnerabilities.
- Limited Scope: Penetration testing usually focuses on specific target systems or components.
- Actionable Insights: Penetration testing provides actionable insights into the effectiveness of security measures and the potential impact of successful attacks.

Vulnerability Assessment Types

Several types of vulnerability assessments can be conducted, including:

1. Network-Based Vulnerability Assessment

A network-based vulnerability assessment identifies vulnerabilities in network devices such as routers, switches, firewalls, and other network infrastructure components. The primary goal of a network-based vulnerability assessment is to identify weaknesses in the network that attackers could exploit to gain unauthorized access, steal data, or launch attacks.

Network-based vulnerability assessments typically involve specialized software tools and techniques that scan the network for vulnerabilities. These tools may use various methods to identify vulnerabilities, such as port scanning, vulnerability scanning, password cracking, and network mapping.

2. Application-Based Vulnerability Assessment

An application vulnerability assessment is a process of reviewing security weaknesses in software applications(Layer 7) including websites, mobile apps and APIs. It examines if the apps are susceptible to known vulnerabilities and assigns severity/criticality levels to those vulnerabilities, recommending remediation or mitigation if and whenever needed.

These assessments typically involve testing the application for common vulnerabilities, such as SQL injection, cross-site scripting (XSS), and other OWASP Top 10 vulnerabilities. Application vulnerability assessments can be performed using both automated and manual methods.

OWASP consistently compiles a list of the most critical application vulnerabilities, updated periodically. In its latest OWASP Top 10 risks 2021 ranking, the following vulnerabilities demand attention:

- A01:2021-Broken Access Control
- A02:2021-Cryptographic Failures
- A03:2021-Injection
- A04:2021-Insecure Design
- A05:2021-Security Misconfiguration
- A06:2021-Vulnerable and Outdated Components
- A07:2021-Identification and Authentication Failures
- A08:2021-Software and Data Integrity Failures
- A09:2021-Security Logging and Monitoring Failures
- A10:2021-Server-Side Request Forgery

3. API-Based Vulnerability Assessment

API vulnerability assessment is conducted to identify and mitigate potential security risks in APIs. This process identifies vulnerabilities and weaknesses in the API’s design, implementation, and deployment. The goal is to ensure that the API is secure, reliable, and resilient to attacks.

The following OWASP API Top 10 vulnerabilities require specific attention in vulnerability assessment process to ensure the security and integrity of API interactions:

- API1:2023 Broken Object Level Authorization
- API2:2023 Broken Authentication
- API3:2023 Broken Object Property Level Authorization
- API4:2023 Unrestricted Resource Consumption
- API5:2023 Broken Function Level Authorization (BFLA)
- API6:2023 Unrestricted Access to Sensitive Business Flows
- API7:2023 Server-Side Request Forgery (SSRF)
- API8:2023 Security Misconfiguration
- API9:2023 Improper Inventory Management
- API10:2023 Unsafe Consumption of APIs

4. Host-Based Vulnerability Assessment

A host-based vulnerability assessment identifies vulnerabilities in individual host systems, including servers, workstations, and laptops.

These assessments typically involve scanning the host system for known vulnerabilities, such as missing security patches or outdated software. Host-based vulnerability assessments can be performed using both automated and manual methods.

5. Wireless Network Vulnerability Assessment

A wireless network vulnerability assessment focuses on identifying vulnerabilities in wireless networks, including Wi-Fi networks. These assessments typically involve testing the wireless network for common vulnerabilities, such as weak encryption, default passwords, and rogue access points.

Wireless network vulnerability assessments can be performed using specialized software tools and techniques.

6. Physical Vulnerability Assessment

A physical vulnerability assessment identifies vulnerabilities in physical security measures, such as locks, surveillance cameras, and access control systems. These assessments typically involve physical inspections of the facility and its security measures.

7. Social Engineering Vulnerability Assessment

A social engineering vulnerability assessment identifies vulnerabilities in human behaviour, such as phishing attacks and other social engineering techniques.

This vulnerability assessment type typically involves simulated attacks against employees to test their awareness of security threats and their ability to identify and respond to them.

8. Cloud-Based Vulnerability Assessment

A cloud-based vulnerability assessment identifies vulnerabilities in cloud infrastructure and services, such as Amazon Web Services (AWS) and Microsoft Azure.

These assessments scan the cloud infrastructure for known vulnerabilities and test the security of cloud applications and services.

What Types of Threats Does Vulnerability Assessment Find?

Here are some of the most common types of threats that can be prevented through vulnerability assessment methods:

1. Malware Infections

Malware infections are among the most common cyber threats, which can devastate organizations. Malware is typically delivered through attack vectors such as phishing emails, malicious websites, and software vulnerabilities.

2. Denial of Service (DoS) Attacks

DoS attacks are a type of cyberattack that aims to overwhelm a targeted system or network with traffic or other resources, causing it to crash or become unavailable to legitimate users. Vulnerability assessment can identify vulnerabilities in the network or systems that attackers could exploit to launch DoS attacks.

3. Data Breaches

Data breaches occur when attackers gain unauthorized access to sensitive data, such as personal information, financial data, or intellectual property.

4. Insider Threats

Insider threats are threats that originate from within an organization. These threats could come from current or former employees, contractors, or business partners who can access an organization’s IT resources.

Vulnerability assessment can identify vulnerabilities in applications, systems, and network devices that insiders could exploit to steal data or cause damage to an organization’s IT infrastructure.

5. Phishing Attacks

Phishing attacks are a cyberattack that uses social engineering techniques to trick users into sharing sensitive information, such as login credentials or financial data.

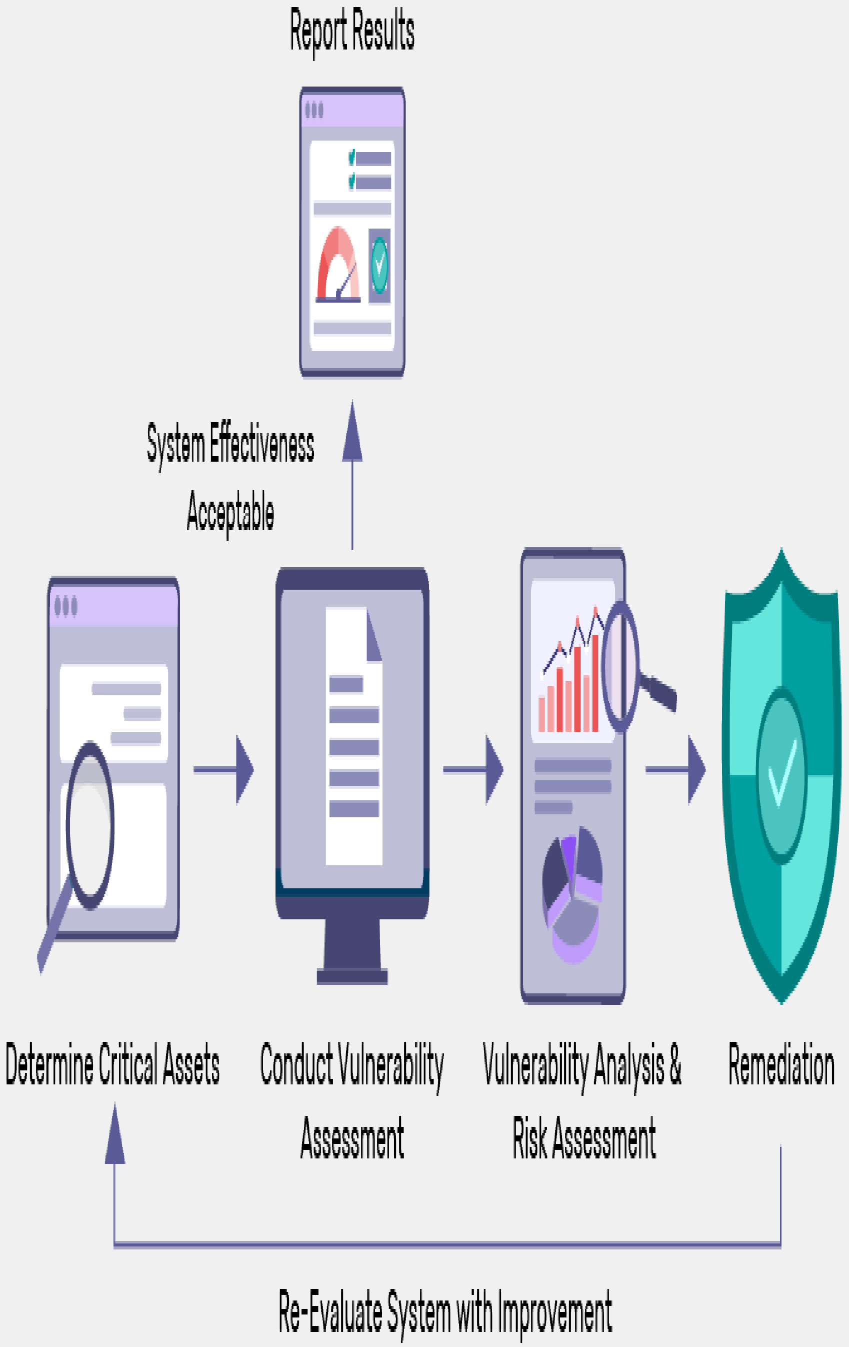
6. Web Application Attacks

Web application attacks are a cyberattack that targets web application vulnerabilities, such as SQL injection or cross-site scripting (XSS) attacks. Application vulnerability assessment can identify vulnerabilities in web applications and help organizations prioritize patching these vulnerabilities.

Vulnerability Assessment Methodology

Vulnerability Assessment steps include identifying the critical assets, performing in-depth security scans and pentests, ranking the vulnerabilities in the descending order of risk posed and finally remediation.

Vulnerability Assessment Methodology Flow Chart



Report Results

System Effectiveness Acceptable

Determine Critical Assets

Conduct Vulnerability Assessment

Vulnerability Analysis & Risk Assessment

Remediation

Re-Evaluate System with Improvement

1. Determine Critical and Attractive Assets

The first step in vulnerability assessment is understanding your entire ecosystem and determining which networks and systems are more critical to your business operation.

The attacker's objectives might vary from your perspective. Review each asset from an attacker's perspective and rank them based on attractiveness.

2. Conduct Vulnerability Assessment

Actively scan your entire network or system through automated tools to identify security flaws and weaknesses. The critical and attractive assets should be termed "targets," which requires further analysis, including testing with real-time scenarios to find and assess perceived security weaknesses. The assessments should rely on vendor vulnerability announcements, asset management systems, vulnerability databases, and threat intelligence feed.

The vulnerability assessment is complete if the overall network or system effectiveness meets the defined security requirements. If vulnerabilities are identified, you should proceed to the next phase.

3. Vulnerability Analysis and Risk Assessment

The next phase in the vulnerability assessment methodology is identifying the source and root cause of the security weakness identified in phase two. It offers a coherent view of remediation. It involves assigning the severity score or rank to each susceptibility based on factors like.

- What data are at risk?

- Which network or system is affected?
- The severity of the possible attacks
- Ease of compromise
- Potential damage if an attack happens

4. Remediation

The main objective of this phase is the closing of security gaps. For each identified vulnerability, determine the remediation actions. Certain remediation actions might include:

- Update all the configuration or operational changes
- Develop and implement vulnerability patches
- Implement new security measures, procedures, or tools

5. Mitigation

Not all vulnerabilities can be resolved completely; this is where mitigation comes into play. Mitigation focuses on lowering the chances of a vulnerability being exploited or minimizing the impact of its exploitation.

A practical approach, known as virtual patching, involves promptly applying a patch to the identified vulnerability without making any changes to the actual source code or components.

This virtual patch creates a protective barrier that prevents malicious actors from exploiting the vulnerability, effectively buying time until a permanent patch or code fix can be implemented.

6. Re-Evaluate System with Improvements

During this phase, the system’s security posture is reassessed using similar methods as the initial assessment, which may include vulnerability testing, penetration testing, code reviews, and other relevant techniques. The focus, however, is shifted toward determining whether the previously identified vulnerabilities have been successfully mitigated or reduced to an acceptable level.

The assessment also aims to identify any new vulnerabilities that have emerged due to the applied changes or configurations.

7. Report Results

The final phase in the security vulnerability assessment methodology is reporting the assessment result understandably.

The main goal of reporting is to clearly defining the system’s effectiveness and recommending potential solutions if the current security measure seems ineffective.

A comprehensive vulnerability assessment report will include additional factors like:

- Which system is impacted?
- The level of simplicity in attacking or compromising the system
- The potential business consequences resulting from a successful breach
- Whether the vulnerability can be accessed via the Internet or demands physical proximity
- The age of the identified vulnerability
- Any regulatory obligations your organization adheres to
- The expense associated with a data breach in your specific industry

Upgrade your vulnerability assessment process with our 15 key point vulnerability assessment checklist.

The Benefits of Ongoing Vulnerability Assessments

What is the recommended frequency for conducting vulnerability assessments?
We're proud to be recognized among
India's Great Places 2022
It has become a leading finance rate.

1. Spotting Vulnerabilities Ahead

This is one of the biggest benefits of vulnerability assessment when done routinely. When you regularly conduct vulnerability scanning using automated tools, you can find all known vulnerabilities (SQLi, XSS, CSRF, malware, etc.), security misconfigurations, and weaknesses (weak passwords, un-updated parts, etc.) in your network, applications, third-party components, codes, perimeter systems and so on. You have the first-mover advantage in closing the vulnerability window before the attackers see it.

2. Syncing Security and Change

Say you conduct vulnerability assessment on a half-yearly basis and vulnerability scanning on a weekly basis. Or you conduct vulnerability assessment once, including remediation, and leave it there.

What happens?

The business processes, applications, devices, networks, etc., change in the current dynamic IT architecture. There are lots of moving parts. The various third-party components used in applications, such as chatbots and software, etc., keep evolving, and updates keep getting released.

Many vulnerabilities may have arisen in your IT architecture, the severity of vulnerabilities may have changed, and risks may have evolved.

The larger the gaps between vulnerability assessments, the more vulnerable you are.

When we say regular vulnerability assessment, we mean

- Vulnerability scanning on a daily basis and after significant changes in the systems or business processes
- Ongoing risk assessments and remediation
- Continuous documentation
- Quarterly or half-yearly security audits and pen tests to evaluate and analyze vulnerabilities and their exploitability

3. Eliminating Mistakes Early

To ensure vulnerability assessment best practices, it’s essential to conduct assessments early in the Software Development Lifecycle (SDLC). This helps businesses ensure that misconfigurations and vulnerabilities are identified and remediated as soon as possible.

For instance, it allows you to detect any vulnerable sections of code, frameworks, plug-ins, and so on, even before the application is launched for public use.

The information gathered from vulnerability assessments can serve as valuable training material for developers. This includes emphasizing the importance of adopting secure coding practices, conducting thorough reviews of source code, and ensuring a robust security architecture during the development process. Businesses that do so are likely to encounter fewer vulnerabilities when the application is launched

4. Shifting Employee Mindsets

Regular vulnerability assessments and communication of results show your employees how serious you are about cybersecurity. Thus, helping you to transform their mindset about security.

5. Offering Insights into the Risks

To build a solid security posture, organizations need to know where they stand regarding risks. Regular vulnerability assessments offer real-time insights into the organization’s risks, enabling them to act quickly.

Further, the practice allows to evaluate the strength of the security defenses and promptly detect cracks in the Armor – on the human, network, application, and systems fronts.

This way, an organization can instantly strengthen its defenses and protect its data, mission-critical assets, and infrastructure. It helps organizations maximize the efficiency of their security systems.

6. Keeping Track of Assets

The attack surface is ever-expanding with several moving parts, shared services, third-party components, and software. Organizations must be aware of their assets. With an ongoing vulnerability assessment process, organizations can create and keep updating their asset inventory.

The automated vulnerability assessment tools particularly those equipped with asset discovery capability, make this process quick, accurate, and efficient. So they can gain real-time visibility into their attack surface and identify the areas of exposure before attacks can locate and gain access to them.

7. Prioritizing Business-Critical Assets

Ongoing vulnerability assessments also tell organizations about the position and condition of each asset/system/device connected to the network, its purpose, and related systems. Based on this, assets can be prioritized, and greater efforts can be directed toward business-critical assets.

8. Making Informed Decisions

From real-time, actionable insights to thorough reporting and documentation, an ongoing vulnerability assessment equips organizations to make the right decisions at the right time, prepare solid incident response plans, and formulate robust strategies and strong security controls.

Organizations are not basing their strategy and decisions on dated information and reports but on the latest insights. This helps strengthen their security posture.

9. Building Trust with Customers

Routine vulnerability assessments reassure customers and foster trust in your business. It shows customers that you care about data security and privacy. Businesses that are victims of data breaches face large-scale customer attrition. This loss of customer confidence and trust is an uphill task for businesses.

Vulnerability Assessment Best Practices

The extensive vulnerability assessment and management task can be time-intensive, particularly when handling a broad spectrum of assets. Consider these approaches to manage the process effectively:

- Know Your Assets – Identify and categorize all assets in your environment. Understanding what you need to protect is crucial for an effective assessment.
- Automation – Leverage automated tools for scanning and identifying vulnerabilities. Automation speeds up the assessment process and ensures consistent results.
- Formulate KPIs – Define Key Performance Indicators (KPIs) to measure the success and effectiveness of your vulnerability assessment program. KPIs provide valuable insights into the program's impact.
- Build a Vulnerability Management Database – Maintain a centralized database to track and manage identified vulnerabilities. This database aids in tracking remediation efforts and monitoring progress.
- Prioritization – Rank vulnerabilities based on severity, potential impact, and exploitability to focus on the most critical issues.
- False Positive Verification – Verify identified vulnerabilities to eliminate false positives and ensure accuracy.

- Documentation – Thoroughly document assessment findings, including vulnerabilities, evidence, and potential risks.
- Remediation Recommendations – Provide clear and actionable recommendations for addressing identified vulnerabilities.
- Collaboration – Involve different teams, such as IT, security, and development, to ensure a holistic assessment.
- Integration with Other Security Protocols –Integrate vulnerability assessment into your broader security strategy. Coordinate with intrusion detection, incident response, and other security practices for a cohesive defense.
- Share Executive Reports – Prepare summarized reports for organizational leadership, providing an overview of assessment findings, risks, and recommended actions. This promotes informed decision-making.

Escalating Privileges

Privileges dictate the access a user or device gets on a network. Hackers who access these privileges can create tremendous damage. But there are ways to keep your networks safe

Types of privilege escalation attacks

Privilege escalation attacks fall into two broad categories:

1. **Horizontal privilege escalation.** The attacker, after successfully gaining access to an existing user or device account, uses that passage to hack into another account. While this tactic doesn't necessarily result in the hacker obtaining additional privileges, it can cause harm to the new victim if the hacker harvests the target's personal data and other resources. Vulnerabilities in websites can enable cross-site scripting, cross-site request forgery and other

types of attacks to capture another user's login credentials or authentication data and gain access to the account.

2. **Vertical privilege escalation.** This is usually the second phase of a multistage cyber attack. Attackers look to exploit system misconfigurations, vulnerabilities, weak passwords and inadequate access controls to gain administrative permissions through which they can continue to access other resources on the network. Once armed with more powerful privileges, attackers can install malware and ransomware, change system settings and steal data. They can even delete logs so their presence on the network goes unnoticed. This is the more dangerous category of escalation attack as the attacker may be able to take control of the entire network.

How privilege escalation attacks work

The following are common methods malicious hackers use to carry out privilege escalation attacks -- the first two methods are used in horizontal privilege escalation attacks, but depending on the ultimate goal of the attacker, the compromised accounts may be used to try and elevate privileges vertically.

- **Social engineering.** Social engineering attacks -- including phishing, watering hole and pharming -- are commonly used to trick users into divulging their account credentials. With these types of attacks, there is no need to mount a complex campaign to bypass a system's security defenses.
- **Weak credentials.** Weak, reused or shared passwords represent an easy way for an attacker to gain unauthorized access to an account. If the account has

administrative privileges, the network is in immediate danger of being seriously compromised.

- **System misconfigurations.** Network resources where security settings have not been locked down can provide opportunities for attackers to obtain greater privileges than intended; for example, consider cloud storage buckets with public access. Incorrectly configured network defenses, such as firewalls and open and unprotected ports, as well as default passwords on important accounts and insecure defaults on newly installed applications -- both particularly common occurrences on IoT devices -- all open a path for an attacker to obtain additional privileges.
- **Malware.** Malware, such as keyloggers, memory scrapers and network sniffers, can steal passwords. Once introduced into the network and depending upon the privileges of the compromised account, the malware can trigger far more dangerous attacks.
- **System vulnerabilities.** Any publicly accessible vulnerability in the design, implementation or configuration of a system may give attackers the ability to obtain account privileges by executing malicious code to gain shell access.

Privilege escalation exploits vulnerabilities in services and applications running on a network, particularly those with weak access controls. Privilege escalation is a key phase in a comprehensive cyber attack.

6 ways to prevent a privilege escalation attack

Like any cyber attack, privilege escalation exploits vulnerabilities in services and applications running on a network, particularly those with weak access controls. Privilege escalation is a key phase in a comprehensive cyber attack. Security controls aimed at preventing these types of attacks have to be strong and maintained on a regular basis.

Here are six best practices to help ensure your network is protected.

1. Keep accounts up to date with comprehensive privilege account management

Enforcing the principle of least privilege to limit users' and services' access rights to the bare minimum reduces an attacker's chances of obtaining administrative-level privileges.

The security team and HR must work together to guard against unnecessary privilege creep and ensure the user account inventory accurately records who, what, where and why an account exists and the privileges it has been granted. Minimizing the number and scope of privileged accounts, while monitoring and logging their activities, also helps flag any potential misuse.

2. Patch and update software

Reducing the chances an attacker can find an exploitable vulnerability is the single best way to stop any type of cyber attack. A comprehensive patch management policy makes it harder for any attacker to take advantage of system and application vulnerabilities; in particular, keep browsers and antivirus software updated.

3. Perform vulnerability scans

Regularly scanning all the components in the IT infrastructure for vulnerabilities makes it tougher for an attacker to gain a foothold in the network. Vulnerability scans find misconfigurations, undocumented system changes, unpatched or insecure OSes and applications, and other flaws before potential attackers can exploit them.

4. Monitor network traffic and behavior

If an attacker does succeed in obtaining a network user's credentials, the intruder's presence can go undetected unless the network is constantly monitored for unusual traffic or user behavior. User and entity behavior analytics software can create a baseline of legitimate behavior and flag activities that deviate from the norm and indicate a potential compromise.

5. Institute a strong password policy

A password policy is the most effective way to prevent a horizontal privilege escalation attack, particularly if it's combined with multifactor authentication (MFA). Password management tools can help users generate and safely store unique and complex passwords that meet security policy rules. All accounts with administrative privileges should require MFA. Digital credentials used in machine authentication should be rotated on a regular basis.

6. Conduct security awareness training

People are usually the weakest link in any organization's security. They can unwittingly aid an escalation attack by using weak passwords, clicking malicious links or attachments, and ignoring warnings regarding dangerous websites. Regular security awareness trainings ensure new threats can be explained, as well as keep security policies fresh in employees' minds. Emphasize the dangers and risks of sharing accounts and credentials.

Privilege escalation attacks are among the most serious. A well-rehearsed incident plan is critical. If a privilege escalation incident is discovered, the compromised account must be quickly isolated, have its password changed and then disabled. The security team must then conduct an in-depth investigation to discover the extent of the intrusion and identify the resources compromised.