**MODULE no 4**

**Enumeration**

What is Enumeration?

Enumeration is the process of extracting **user names, machine names, network resources, shares, and services** from a system, and its conducted in an intranet environment.

* **Get user names using email IDs :-** Most of the time username are hidden in email Ids , or full name or organization name are there in email ID
* **Get information using default passwords:-** Many online resource provide default credential If user doen’t change their credential . so by from that we can take access.
* **Get user names using SNMP :-** Attacker can easily guess snmp string like read-only or read-write string by tool.
* **Brute force AD:-**
* **- Get user groups from Windows**
* **Get information using DNS zone transfers :-** If DNS server is not configured properly by administrator than it is a very effective method of gaining information of Organization’s network.

In this phase, the attacker creates an active connection to the system and performs directed queries to gain more information about the target. The gathered information is used to identify the vulnerabilities or weak points in system security and tries to exploit in the System gaining phase.

**Basic login information**

**finger** --> This tool declare that who is currently logged in, when and where.

**Use**:- finger -s

* Login Name Tty Idle Login Time Office Office Phone
* kali Kali tty7 10:09 Sep 1 14:14 (:0)

**w** --> Show who is logged on and what they are doing.

00:27:15 up 9:32, 1 user, load average: 0.06, 0.09, 0.09

USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT

kali tty7 :0 14:16 10:11m 30.26s 2.09s xfce4-session

* **ps aux**

to see the root service

Linux credential : /store 🡨 etc/passwd | etc/shadow

**SNMP Enumeration**

**Simple network management protocol**

**Simple Network Management Protocol** (SNMP) is a networking protocol used for the management and monitoring of network-connected devices like routers, switches, in Internet Protocol networks.

So we enumerate here for user account and devices which are available on the network

**SNMP enumeration is the process of enumerating the users accounts and devices on a SNMP enabled computer.**

Attackers enumerate SNMP to extract information about network resources such as hosts, routers, devices, share Network information such as ARP tables, routing tables, device specific information and traffic statistics.

* **Runs on Port 161 UDP**
* **Management Information Base** (MIB) - database that stores information
* SNMP service comes with two passwords, which are used to configure and access the SNMP agent from the management station (MIB):
  1. **Read community string**
  2. **Read/Write community string**
* These strings (**passwords**) come with a **default value**, which is same for all the systems.
* **They become easy entry points for attackers if left unchanged by administrator**.

Perform snmp enumeration with snmp-check

Command :- nmap -sU 192.168.1.242

Check port 161 is open or not if it is open lets enumerate

Command :- snmp-check 192.168.1.242

another tool is **onesixtyone -c (wordlist) $ip**

**Metaploit have auxillary** scanner which enumerate the snmp.

Use:- auxiliary/scanner/snmp/snmp\_enum

**SMB Enumeration**

**command & tool:**

* nmap -p 139,445 $ip
* nbtstat -r $ip
* nmblookup -A $ip
* smbmap -H $ip
* nmap --script smb-enum-shares.nse -p 139,445 192.168.1.18

> to check directory login way

* smbclient -L \\$ip\\

Sam file store in window , where all password are stored in encrypted formate.

**SAM Database** - file where all local passwords are stored (encrypted)

* + Stored in C:\Windows\System32\Config

**NetBIOS Enumeration**

**Network Basic Input Output**

* NetBIOS provides name servicing, connectionless communication and some Session layer stuff
* The browser service in Windows designed to host information about all machines within domain or TCP/IP network segment
* NetBIOS name is a **16-character ASCII string** used to identify devices

**This is window tool for NetBios enumeration.**

***nbtstat****displays protocol statistics and current TCP/IP connections using NetBIOS over TCP/IP.*

* **nbtstat** gives your own info
* **nbtstat -a** list the remote machine's name table given its **name**
* **nbtstat -A**- list the remote machine's name table given its **IP address**
* **nbtstat -n** gives local table
* **nbtstat -c** gives cache information

*C:\Users\IEUser>nbtstat -A 10.20.20.10*

*Local Area Connection 2:*

*Node IpAddress: [10.20.20.10] Scope Id: []*

*NetBIOS Remote Machine Name Table*

*Name Type Status*

*---------------------------------------------*

*IE8WIN7 <00> UNIQUE Registered*

*WORKGROUP <00> GROUP Registered*

*IE8WIN7 <20> UNIQUE Registered*

*MAC Address = 08-00-27-99-B1-5F*

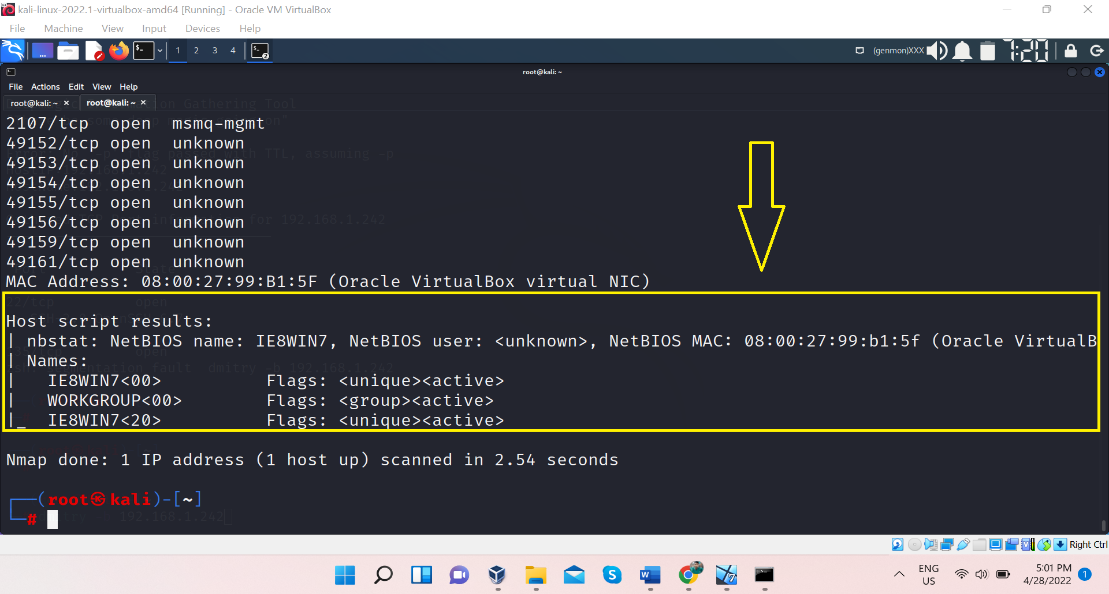
| *Code* | *Type* | *Meaning* |
| --- | --- | --- |
| *<1B>* | *UNIQUE* | *Domain master browser* |
| *<1C>* | *UNIQUE* | *Domain controller* |
| *<1D>* | *GROUP* | *Master browser for subnet* |
| *<00>* | *UNIQUE* | *Hostname* |
| *<00>* | *GROUP* | *Domain name* |
| *<03>* | *UNIQUE* | *Service running on system* |
| *<20>* | *UNIQUE* | *Server service running* |

**Netbios Enumeraion with nmap**

Basically we run nmap script which is nbtstat.nse

Command:- nmap --script nbstat.nse 192.168.1.242

We will got the all netBios result



**DNS enumeration**

**Domain name system**

DNS enumeration is process in which we get all possible dns record of a target Domain.

In the section of Footprintig we had seen the DNS Footprinting , unaware of dns enumeration we had done much enumeration at that time only like we had seen all possible Dns record from tool , NSLOOKUP

Let see another tool for DNS enumeration

**DNSrecon:**-

Command :- dnsrecon -d craw.in

**DNSenum:-**

Command :- dnsenum craw.in

command :- host $domain

host -t ns $domain

## SMTP Enumeration

## Simple Mail Transfer Protocol

## By the word we already get much info about this port system , this port help user to send mail or message.

* **Ports used**:
  + **SMTP: TCP 25**
* In simple words: **users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail.**

**Enumerating with nmap**:

we can enumerate first that it smtp port 25 is open or not

**Command :- nmap -p25 --script smtp-enum-users <target IP>**

PORT STATE SERVICE

25/tcp open smtp

| smtp-commands: WIN-J83C1DR5CV1.ceh.global Hello [10.10.10.10], TURN, SIZE 2097152, ETRN, PIPELINING, DSN, ENHANCEDSTATUSCODES, 8bitmime, BINARYMIME, CHUNKING, VRFY, OK,

|\_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH TURN ETRN BDAT VRFY

Nmap done: 1 IP address (1 host up) scanned in 0.86 seconds

**Other tools**:

* smtp-user-enum
  + Username guessing tool primarily for use against the default Solaris SMTP service. Can use either EXPN, VRFY or RCPT TO.

**command**:- smtp-user-enum -M VRFY -U /usr/share/wordlists/unix\_users.txt -t $ip

This tool enumerate the server gives all the user of servers

**SMTP enum by Metasploit**

There are various auxillary scanner , but let focus on the important scanner

*auxiliary/scanner/smtp/smtp\_version*

*auxiliary/scanner/smtp/smtp\_enum*

**There are more tool are there through which we can enumerate more and Further things**

Tool name is : enum4linux

With the help of this tool we can enumerate and gather info like username, groups, share network

Command :- enum4linux [ip]

Wappalyzer

**Linux System Enumeration Tool**

* **Enum4linux is a tool for enumerating information from Windows and Samba systems:**
  + enum4linux -u CEH -p Pa55w0rd -U 10.0.2.23
    - -u Username, -p Password, -U users information