Assignment-2

Devarakonda Sravani

21BEC7224

ECE

In this let's explore Metasploit tool in kali Linux OS and scan the own computer and find the vulnerabilities and exploits in it.

Step-1

- First we have to get the ipv4 address of the system then we are checking and scan the system using nmap command .

Command : map 192.168.0.109

```
┌──(nature㉿kali)-[~]
└─$ nmap 192.168.0.109
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-26 09:45 IST
Nmap scan report for 192.168.0.109
Host is up (0.0080s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 2.75 seconds
```

Step-2

Command : map 192.168.0.109 -sV

```
┌──(nature㉿kali)-[~]
└─$ nmap 192.168.0.109 -sV
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-26 09:46 IST
Nmap scan report for 192.168.0.109
Host is up (0.00080s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs
: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.96 seconds
```

- We can see port no 139 and 445 resembles SMB. So we have to explore for exploits in smb.
- Now lets open Metasploit in our kali Linux which is exploit on framework that gives access to on resystem.

Step-3

Command : sudo msfconsole

Step-4

Command: grep scanner search smb

- We can enter "search smb" or "grep scanner search smb".

```
msf6 > grep scanner search smb
   5   auxiliary/scanner/http/citrix_dir_traversal                 20
19-12-17       normal     No     Citrix ADC (NetScaler) Directory Traversal S
canner
   6   auxiliary/scanner/smb/impacket/dcomexec                      20
18-03-19       normal     No     DCOM Exec
   7   auxiliary/scanner/smb/impacket/secretsdump
               normal     No     DCOM Exec
   8   auxiliary/scanner/dcerpc/dfscoerce
               normal     No     DFSCoerce
  48   auxiliary/scanner/smb/smb_ms17_010
               normal     No     MS17-010 SMB RCE Detection
  62   auxiliary/scanner/smb/psexec_loggedin_users
               normal     No     Microsoft Windows Authenticated Logged In Us
ers Enumeration
  76   auxiliary/scanner/dcerpc/petitpotam
               normal     No     PetitPotam
  84   auxiliary/scanner/sap/sap_smb_relay
               normal     No     SAP SMB Relay Abuse
  86   auxiliary/scanner/sap/sap_soap_rfc_eps_get_directory_listing
               normal     No     SAP SOAP RFC EPS_GET_DIRECTORY_LISTING Direc
tories Information Disclosure
  87   auxiliary/scanner/sap/sap_soap_rfc_pfl_check_os_file_existence
               normal     No     SAP SOAP RFC PFL_CHECK_OS_FILE_EXISTENCE Fil
e Existence Check
  88   auxiliary/scanner/sap/sap_soap_rfc_rzl_read_dir
               normal     No     SAP SOAP RFC RZL_READ_DIR_LOCAL Directory Co
ntents Listing
  94   auxiliary/scanner/smb/smb_enumusers_domain
               normal     No     SMB Domain User Enumeration
  98   auxiliary/scanner/smb/smb_enum_gpp
               normal     No     SMB Group Policy Preference Saved Passwords
Enumeration
  99   auxiliary/scanner/smb/smb_login
               normal     No     SMB Login Check Scanner
 103  auxiliary/scanner/smb/smb_lookupsid
               normal     No     SMB SID User Enumeration (LookupSid)
 105  auxiliary/scanner/smb/pipe_auditor
               normal     No     SMB Session Pipe Auditor
 106  auxiliary/scanner/smb/pipe_dcerpc_auditor
               normal     No     SMB Session Pipe DCERPC Auditor
 107  auxiliary/scanner/smb/smb_enumshares
               normal     No     SMB Share Enumeration
 110  auxiliary/scanner/smb/smb_enumusers
               normal     No     SMB User Enumeration (SAM EnumUsers)
 111  auxiliary/scanner/smb/smb_version
               normal     No     SMB Version Detection
 115  auxiliary/scanner/snmp/snmp_enumshares
               normal     No     SNMP Windows SMB Share Enumeration
 117  auxiliary/scanner/smb/smb_uninit_cred
               normal     Yes    Samba _netr_ServerPasswordSet Uninitialized
Credential State
 131  auxiliary/scanner/smb/impacket/wmiexec                       20
18-03-19       normal     No     WMI Exec
```

Step-5

Command: use auxiliary/scanner/smb/smb_ms17_010

```
msf6 > use auxiliary/scanner/smb/smb_ms17_010
msf6 auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name          Current Setting        Required  Description
   ----          ---------------        --------  -----------
   CHECK_ARCH    true                   no        Check for architecture on vul
                                                  nerable hosts
   CHECK_DOPU    true                   no        Check for DOUBLEPULSAR on vul
                                                  nerable hosts
   CHECK_PIPE    false                  no        Check for named pipe on vulne
                                                  rable hosts
   NAMED_PIPES   /usr/share/metaspl     yes       List of named pipes to check
                 oit-framework/data
                 /wordlists/named_p
                 ipes.txt
   RHOSTS                               yes       The target host(s), see https
                                                  ://docs.metasploit.com/docs/u
                                                  sing-metasploit/basics/using-
                                                  metasploit.html
   RPORT         445                    yes       The SMB service port (TCP)
   SMBDomain     .                      no        The Windows domain to use for
                                                   authentication
   SMBPass                              no        The password for the specifie
                                                  d username
   SMBUser                              no        The username to authenticate
                                                  as
   THREADS       1                      yes       The number of concurrent thre
                                                  ads (max one per host)


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 192.168.0.109
RHOSTS ⇒ 192.168.0.109
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[-] 192.168.0.109:445     - Host does NOT appear vulnerable.
[*] 192.168.0.109:445     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

- In this way we can run a scan on any system. we can gain the access of the system too if it is we find the vulnerabilities in that auxiliary scan.