Search …

Top Posts

Download OctoSniff 2.0.3 Full Version - PlayStation and XBox IP Sniffer

Download Spy MAX v1.0 - Android

Metasploitable 2 enumeration – Hacking Tutorials

February 10, 2019 by Ace

In this new Metasploit Hacking Tutorial we will likely be enumerating the Metasploitable 2 digital machine to collect helpful data for a vulnerability evaluation. Enumeration in arithmetic or pc science is known as itemizing quite a lot of components in a set. Enumeration within the hacking context is the method of retrieving usernames, shares, companies, web directories, teams, computer systems on a community. This can be known as community enumeration. During this course of we may even accumulate different helpful community associated data for conducting a penetration check. An necessary a part of the Metasploitable 2 enumeration course of is the port scanning and fingerprinting course of. Port scanning is used to probe a server or host for open TPC and UDP ports. Fingerprinting is the method of figuring out the companies related to these ports. A very fashionable software used for community enumeration, port scanning and fingerprinting is

Remote Administration Tool

Download AndroRat Full Version - Android Remote Administration Tool

Download Spy MAX v2.0 - Android Remote Administration Tool

Download Havij 1.17 Pro - SQL Injection Tool

Top Android Remote Administration Tools (RATs) of 2019 [UPDATED]

Download Droidjack 4.4 Full Version - Remote Administration Tools

Download OmniRAT Full Version - Android Remote Administration Tool

NMap (Network Mapper) which we will likely be utilizing all through this tutorial. We may even use an enumeration software known as enum4linux. Enum4linux is a software used for enumerating data from Windows and Samba hosts.

After we’ve efficiently accomplished enumerating the Metasploitable 2 VM we will likely be doing a vulnerability evaluation on the community facet within the subsequent tutorial. With data retrieved from the enumeration course of, for instance the operating system model and operating companies with model, we will likely be in search of identified vulnerabilities in these companies. We will likely be utilizing the Open Source Vulnerability Database (OSVDB) and the Common Vulnerabilities and Exposures (CVE) for this objective. The final step is to scan the goal host for these vulnerabilities with a vulnerability scanner known as OpenVAS on Kali Linux.

Metasploitable 2 enumeration and port scanning

In this a part of the Metasploitable 2 enumeration tutorial we will likely be enumerating the operating companies, accounts and carry out an open port scan. We will likely be utilizing NMap to scan the digital machine for open ports and we will likely be fingerprinting the related companies. In this tutorial we’ll solely be focussing on enumerating the community facet of the Metasploitable 2 machine. We will cowl the web facet in a special tutorial the place we will likely be enumerating web purposes and directories, performing SQL injection assaults and exploit the susceptible web companies.

I assume you may have already put in the Metasploitable digital machine from the earlier tutorial and if it shouldn't be operating by now it's time to hearth it up now. When you login to the susceptible host with msfadmin as username and password you need to use the ifconfig command to find out its IP handle. You also can use netdiscover on the Kali linux machine to scan a variety of IP addresses for the goal host. Use the next command on the terminal:

> ***netdiscover –r 192.168.111.zero/24***

This command will return all dwell host on the given IP vary, on this instance will probably be the 192.168.111.zero/24 vary which consists of IP 192.168.111.zero to 192.168.111.255. Of course you need to scan the IP vary your Metasploitable 2 VM set up is positioned by yourself community.

> ***The netdiscover -r 192.168.111.zero/24*** *command discovers all IP addresses in the given vary.*

Nmap port scan and repair scan

We will begin the open port scan with scanning the goal host with NMap. We will use a TCP SYN scan for this objective and than we'll scan the goal for open UDP ports. The SYN scan is named a stealthy port scan as a result of it doesn't end the complete TCP handshake. A full TCP connection begins with a 3 means handshake the place a SYN packet is ship by NMap as the primary a part of the handshake. When a port on the goal machine is open, it’s going to reply with a SYN-ACK packet. When there isn’t any response from the goal on the primary SYN packet, than the port is both closed or filtered by a firewall. The third step on this course of is the host machine that ought to reply to the SYN-ACK with an ACK packet to finish the complete TCP handshake. In the case of a SYN scan its by no means does and is subsequently known as stealthy.

When you begin a SYN scan (and another port scan) from NMap with out specifying the port vary then NMap will scan solely the primary 1.000 ports that are thought-about a very powerful ports as a substitute of all 65.535 ports. To scan all ports you must use the -p- flag. The Nmap SYN scan command makes use of the -sS flag as used within the following command to SYN scan port 1 to port 65.535:

> ***nmap -sS -p- [taget IP address]***

A SYN scan doesn’t full the three means TCP handshake as a result of the SYN/ACK packet shouldn’t be responded to with an ACK packet.

> *The Nmap SYN scan is usually known as a stealthy scan which means that it goes unnoticed. This is true for previous firewalls, which solely log full TCP connections, however not for contemporary firewalls which additionally log uncompleted TCP connections.*

Are open ports susceptible?

Just as a result of a port is open doesn’t imply that the underlying software program is susceptible. We have to know the model of the operating system and operating companies. With this data we will decide if there are identified vulnerabilities obtainable to be exploited. The results of the service and OS scan will give us the proper data to analyze additional throughout the vulnerability evaluation. To get this data we’ll run the port scan with the -sV choice for model detection and the –O choice for OS detection to retrieve the variations of the operating companies and the OS. The Nmap OS and Version scan does full the complete TCP handshake and utilizing methods like banner grabbing to get data from the operating companies.

> *You also can use the –A choice as a substitute of –O to allow OS Detection, model detection, script scanning and hint route suddenly. This shouldn't be a stealthy means of scanning.*

Nmap Service scan with OS detection

Password : EHT or BreachSec

Use the next command to start out the Nmap port scan with service and OS detection:

```
Nmap –sS –sV -O [target IP address]
```

After operating this command NMap will return an inventory of open ports and the related companies:

Metasploitable 2 port scan with service and OS scan

The Nmap port and repair scans returns numerous open ports, listening companies and the model of the operating system. The goal host is operating Linux 2.6.9 – 2.6.33 as operating system. We can see that the host is operating an SSH service utilizing OpenSSH, a telnet service, an Apache 2.2.eight webserver, 2 SQL servers and a few extra companies. Let's sum all companies with model and port in an inventory we've be utilizing within the subsequent chapter the place we'll do a vulnerability evaluation and search for widespread vulnerabilities:

- Vsftpd 2.three.four on open port 21
- OpenSSH four.7p1 Debian 8ubuntu 1 (protocol 2.zero) on open port 22
- Linux telnetd service on open port 23
- Postfix smtpd on port 25
- ISC BIND 9.four.2 on open port 53
- Apache httpd 2.2.eight Ubuntu DAV/2 on port 80
- A RPCbind service on port 111
- Samba smbd three.X on port 139 and 445
- three r companies on port 512, 513 and 514
- GNU Classpath grmiregistry on port 1099
- Metasploitable root shell on port 1524
- A NFS service on port 2049
- ProFTPD 1.three.1 on port 2121
- MySQL 5.zero.51a-3ubuntu5 on port 3306

- PostgreSQL DB eight.three.zero – eight.three.7 on port 5432
- VNC protocol v1.three on port 5900
- X11 service on port 6000
- Unreal ircd on port 6667
- Apache Jserv protocol 1.three on port 8009
- Apache Tomcat/Coyote JSP engine 1.1 on port 8180

> *Most of the operating companies scanned by Nmap will most likely be susceptible.*

Of course we all know the Metasploitable 2 digital machine is deliberately susceptible. Therefor one can solely suspect that the majority, if not all, of the companies comprise vulnerabilities, backdoors and so forth. In this hacking tutorial we'll solely cowl enumeration ways, port scanning and a vulnerability evaluation on the community facet. In the Metasploitable tutorials to comply with we will likely be exploiting the vulnerabilities. Let's proceed with person enumeration.

Nmap UDP scan

So far we've solely scanned for open TCP ports, which is the default for Nmap, and never for open UDP ports. Let's use the next command to start out an UDP scan:

> ***nmap -sU 192.168.111.128***

We also can use the -p flag to outline ports to be scanned. The UDP scan will take some extra time to complete than a TCP scan. Nmap return the next details about the open UDP ports it has discovered:

```
PORT     STATE SERVICE
53/udp   open  area
111/udp  open  rpcbind
137/udp  open  netbios-ns
2049/udp open  nfs
```

Please be aware that UDP scans could trigger numerous false positives. The false positives could happen as a result of UDP lacks an equal of a TCP SYN packet. When a scanned UDP port is closed the system will reply with a ICMP port unreachable message. The absence of such package deal signifies that the UDP port is open for a lot of scanning instruments. When a firewall is current on the goal host which blocks the ICMP unreachable message than all UDP ports look like open. When the firewall blocks a single port the scanner may even falsely report that the port is open.

Metasploitable 2 person enumeration

User enumeration is a vital step in each penetration check and must be accomplished very completely. With person enumeration the penetrations tester will get to see what customers have entry to the server and which customers exist on the community. Another objective for person enumeration is for getting access to the machine through the use of brute drive methods. Since the username is already identified to the penetration tester the one factor left to brute drive is the password. There are a number of methods of enumerating customers on a Linux system. We will likely be taking a look at 2 completely different strategies:

1. Enumerating customers utilizing a Nmap script named smb-enum-customers.
2. Enumerating customers by means of a null classes utilizing rpclient.

Let’s begin with enumerating customers utilizing the NMap script.

Enumerating customers with NMap

In order to enumerate the person accounts obtainable on the goal machine we will likely be utilizing the next Nmap script: smb-enum-customers. We can run the NMap script through the use of the next command:

> ***nmap –script smb-enum-customers.nse –p 445 [target host]***

The script output is a protracted record of obtainable customers on the host:

As you may see there are numerous usernames on the Metasploitable 2 machine. Among them are numerous service accounts and the admin account which is called msfadmin. Let’s take a look on the second technique to retrieve an inventory of person accounts from the Metasploitable 2 server through the use of a null session on the Samba server.

Enumerating person accounts by means of null classes with rpcclient

Rpcclient is a Linux software used for executing shopper facet MS-RPC features. A null session is a reference to a samba or SMB server that doesn’t require authentication with a password. No username or password is required to set-up the connection and subsequently it’s known as a null session. The allowance of null classes was enabled by default on legacy techniques however has been disabled from Windows XP SP2 and Windows Server 2003. The connection makes use of port 445 which is an open port on out goal host as we’ve seen within the outcomes of the port scan.

Let’s open up a brand new terminal window and arrange a null session with the Metasploitable 2 samba server utilizing the next command:

> ***rpcclient –U “” [target IP address]***

The –U choice defines a null username adopted by the IP handle of the Metasploitable 2 VM. You will likely be requested for a password, simply press enter to proceed:

Start a null session utilizing rpcclient

The command line will change to the rpcclient context which is indicated by the rcpclient $> on the command line. Now run the next command within the rpcclient context:

> ***rcpclient $> querydominfo***

querydominfo

The querydominfo command returns the area, server, the entire customers on the system and another helpful data. The outcome reveals us there are a complete of 35 person accounts obtainable on the goal system. Now run the next command to retrieve an inventory of those 35 customers:

rcpclient $> enumdomusers

enumdomusers

The result’s an inventory of all person accounts obtainable on the system. Now that we all know which person accounts can be found on the server we will use the rpcclient to question the person information for extra data utilizing the next command:

> ***rcpclient $> queryuser [username]***

Let’s question the person information for the msfadmin account with the next command:

> ***rcpclient $> queryuser msfadmin***

This will return details about the profile path on the server, the house drive, password associated settings and much more. This is nice data which might be queried with out administrator entry! If you wish to study extra about the best way to use the rpcclient simply kind the assistance command for an summary of obtainable choices.

> *Use the netshareenum command on Metasploitable 2 to enumerate its community shares.*

Enumeration with enum4linux

Enum4linux is used to enumerate Windows and Samba hosts and is written in Perl. The software is mainly a wrapper for smbclient, rpcclient, net and nmblookup. Let’s take a look at the best way to use enum4linux and run it on Metasploitable 2. Below are the commonest choices utilized in enum4linux. To get an summary of various choices use the –assist flag.

```
Usage: ./enum4linux.pl [options]ip

-U        get userlist
-M        get machine record*
-S        get sharelist
-P        get password coverage data
-G        get group and member record
-d        be detailed, applies to -U and -S
-u person   specify username to make use of (default “”)
-p cross   specify password to make use of (default “”
-a        Do all easy enumeration (-U -S -G -P -r -o -n -i).
-o        Get OS data
-i        Get printer data
```

Let’s run enum4linux on Metasploitable 2 with all choices utilizing the next command:

```
enum4linux 192.168.111.128
```

After enum4linux has completed it returns us numerous helpful data. We acquired an summary of the shares obtainable on our goal host:

enum4linux shares

And additionally an summary of the obtainable customers:

enum4linux customers

And the next data concerning the operation system:

enum4linux OS data

So far we’ve collected details about the operating system, the person accounts, open ports and the operating companies with model numbers on this Metasploitable 2 enumeration tutorial.

Note: Use Virtual Machine and scan on VirusTotal before downloading any program on Host Machine for your privacy.

Ethical Hacking Tutorials, Kali Linux
Kali Linux, kali linux tutorials, metasploitable 2 enumeration, metasploitable tutorials

‹ Exploiting VSFTPD v2.3.4 on Metasploitable 2
› Metasploit and Metasploitable 2 Installation Guide

Leave a Comment

Name *

Email *

Website

Post Comment

□ Notify me of follow-up comments by email.

□ Notify me of new posts by email.

This site uses Akismet to reduce spam. Learn how your comment data is processed.

Article Categories

Select Category ▾

Recent Posts

- Download REMCOS Professional Full Version
- How to Create SQL Vulnerability Checker using Python?
- Download Spy MAX v2.0 – Android Remote Administration Tool
- Download Loki RAT Full Version – Python Powered RAT
- Tracing IP of Facebook Friends

Links

- About Us
- Contact Us
- Privacy Policy