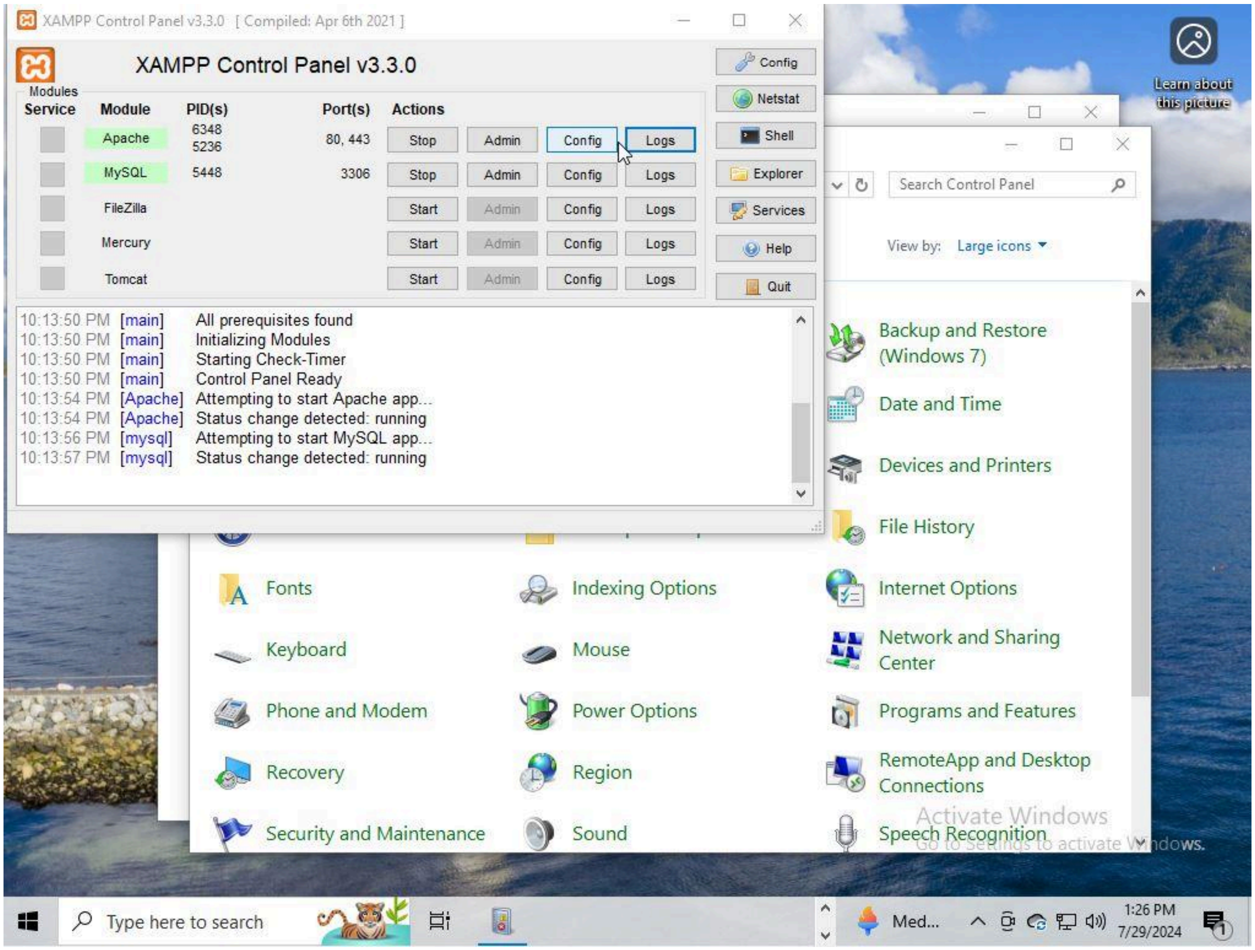
Objective

This phase has the objective of deploying a Kali Linux as an attack machine while deploying a Windows 10 VM as a web server using XAMPP. The goal is to find and exploit vulnerabilities in the web server on the Windows 10 VM.

Deployment and Configuration

Windows 10 VM

- Successful installation of Windows 10 on VMWare.
- Successful installation and implementation of XAMPP.
- Configured XAMPP to run Apache and MySQL.
- Creation of PHP file to test the Web Server's Setup.
- Enable Logging on the Virtual Machine.



XAMPP Control Panel v3.3.0 [Compiled: Apr 6th 2021]

XAMPP Control Panel v3.3.0

Modules

Service	Module	PID(s)	Port(s)	Actions			
	Apache	6348 5236	80, 443	Stop	Admin	Config	Logs
	MySQL	5448	3306	Stop	Admin	Config	Logs
	FileZilla			Start	Admin	Config	Logs
	Mercury			Start	Admin	Config	Logs
	Tomcat			Start	Admin	Config	Logs

```
10:13:50 PM  [main]     All prerequisites found
10:13:50 PM  [main]     Initializing Modules
10:13:50 PM  [main]     Starting Check-Timer
10:13:50 PM  [main]     Control Panel Ready
10:13:54 PM  [Apache]   Attempting to start Apache app...
10:13:54 PM  [Apache]   Status change detected: running
10:13:56 PM  [mysql]    Attempting to start MySQL app...
10:13:57 PM  [mysql]    Status change detected: running
```

Kali Linux VM

- Successful installation of Kali Linux on VMWare.
- Successful update and upgrade of Kali Linux, including Nmap and Metasploit used for the Penetration Test.

- Successful installation of Nessus & Armitage.

Network Configuration

- Successfully set both VMs to use a NAT network, ensuring that they are on the shared network. Used Ping and Nmap as a test from the attacking machine to ensure the connection is active.

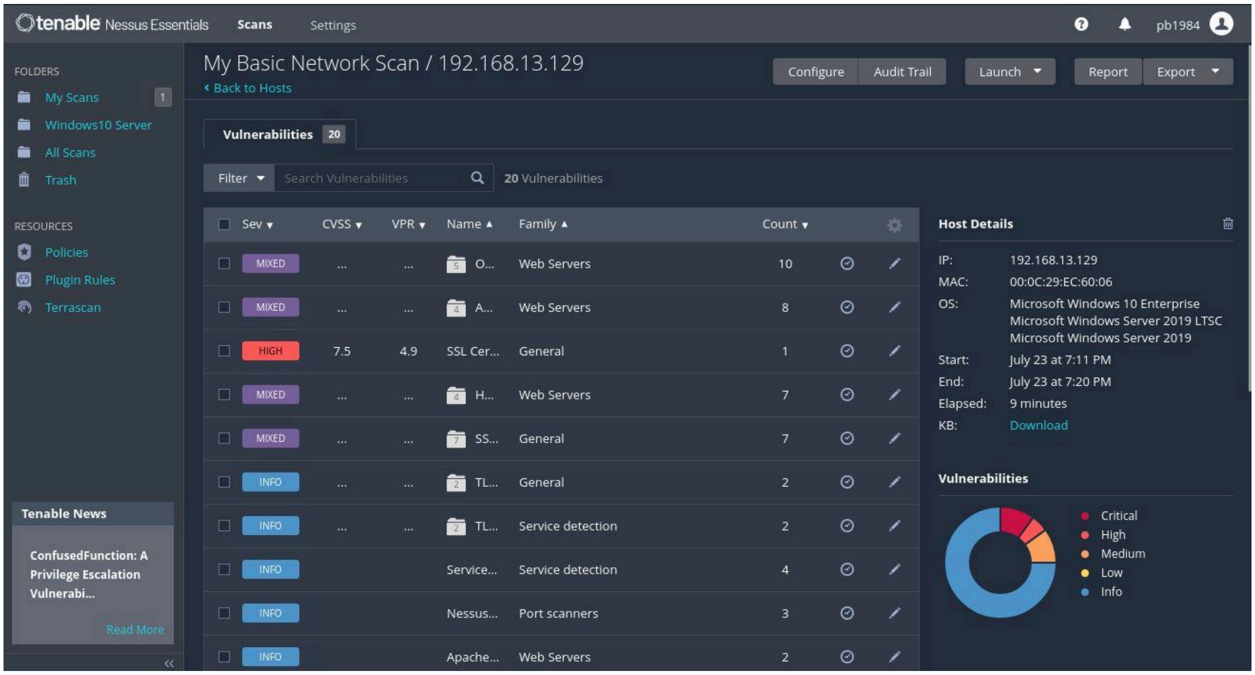
Problem Solving - Initial Test

Reconnaissance

- Ran a ping command to confirm the active connection between VMs.
- Ran an Nmap scan with 'nmap -sS -O 192.168.13.129'.

Vulnerability Scanning

- Ran a Nessus vulnerability scan to 192.168.13.129, resulting in 20 vulnerabilities.
- The scan showed several Critical and High vulnerabilities.



My Basic Network Scan / 192.168.13.129

20 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
MIXED	...	...	5 O...	Web Servers	10
MIXED	...	...	4 A...	Web Servers	8
HIGH	7.5	4.9	SSL Cer...	General	1
MIXED	...	...	4 H...	Web Servers	7
MIXED	...	...	7 SS...	General	7
INFO	...	...	2 TL...	General	2
INFO	...	...	2 TL...	Service detection	2
INFO			Service...	Service detection	4
INFO			Nessus...	Port scanners	3
INFO			Apache...	Web Servers	2

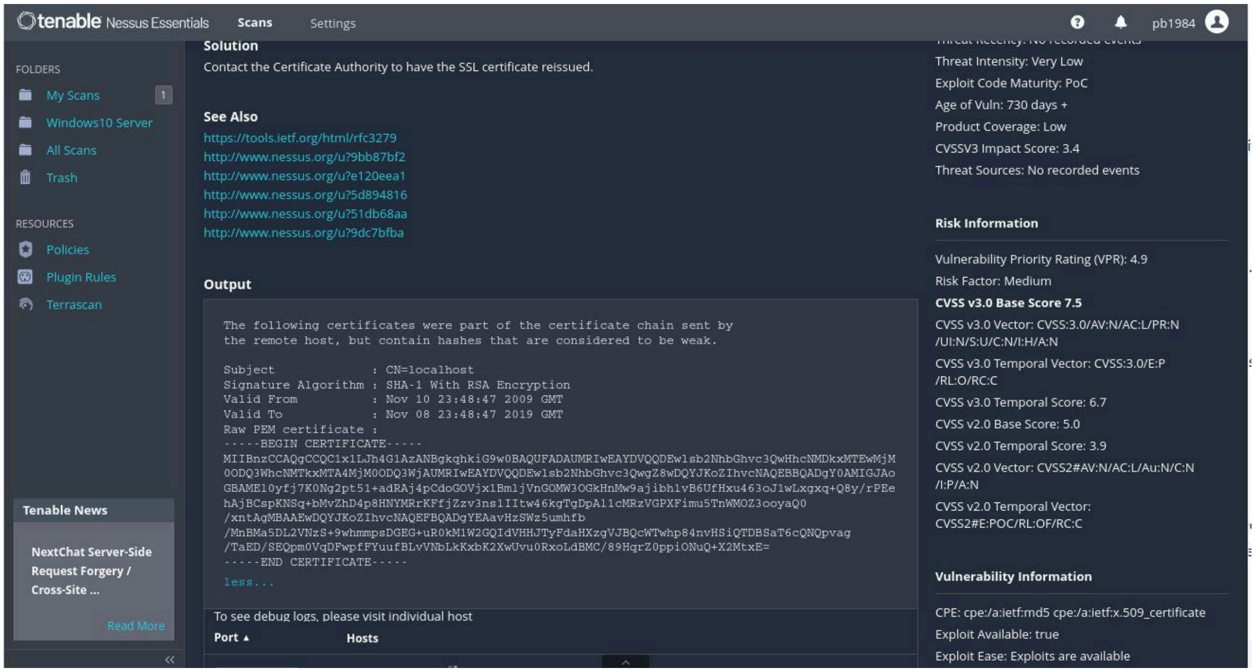
Host Details

IP: 192.168.13.129
MAC: 00:0C:29:EC:60:06
OS: Microsoft Windows 10 Enterprise
Microsoft Windows Server 2019 LTSC
Microsoft Windows Server 2019
Start: July 23 at 7:11 PM
End: July 23 at 7:20 PM
Elapsed: 9 minutes
KB: Download

Vulnerabilities

Tenable News

ConfusedFunction: A Privilege Escalation Vulnerabi...



Solution

Contact the Certificate Authority to have the SSL certificate reissued.

See Also

https://tools.ietf.org/html/rfc3279
http://www.nessus.org/u?9bb87bf2
http://www.nessus.org/u?e120eea1
http://www.nessus.org/u?5d894816
http://www.nessus.org/u?51db68aa
http://www.nessus.org/u?9dc7bfba

Output

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

Subject             : CN=localhost
Signature Algorithm : SHA-1 With RSA Encryption
Valid From          : Nov 10 23:48:47 2009 GMT
Valid To            : Nov 08 23:48:47 2019 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIBnzCCAQgCCQC1x1LJh4G1AzANBgkqhkiG9w0BAQUFADAUMRIwEAYDVQQDEwlsb2NhbGhvc3QwHhcNMDkxMTEwMjM
0ODQ3WhcNMTkxMTA4MjM0ODQ3WjAUMRIwEAYDVQQDEwlsb2NhbGhvc3QwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAo
GBAME10yfj7K0Ng2pt51+adRAj4pCdoGOVjx1BmljVnGOMW3OGkHnMw9ajibh1vB6UfHxu463oJ1wLxgxq+Q8y/rPEe
hAjBCspKNSq+bMvZhD4p8HNYMRrKFfjZzv3ns1IItw46kgTgDpAl1cMRzVGPXFimu5TnWMOZ3ooyaQ0
/xntAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAavHzSWz5umhfb
/MnBMa5DL2VNzS+9whmmpsDGEG+uR0kM1W2GQIdVHHJTyFdaHXzgVJBQcWTwhp84nvHSiQTDBSaT6cQNQpvag
/TaED/SEQpm0VqDFwpfFYuufBLvVNbLkKxbK2XwUvu0RxoLdBMC/89HqrZ0ppiONuQ+X2MtxE=
-----END CERTIFICATE-----
less...
```

To see debug logs, please visit individual host

Port ▲	Hosts

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: PoC
Age of Vuln: 730 days +
Product Coverage: Low
CVSSV3 Impact Score: 3.4
Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 4.9
Risk Factor: Medium
CVSS v3.0 Base Score 7.5
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
CVSS v3.0 Temporal Vector: CVSS:3.0/E:P/RL:O/RC:C
CVSS v3.0 Temporal Score: 6.7
CVSS v2.0 Base Score: 5.0
CVSS v2.0 Temporal Score: 3.9
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N
CVSS v2.0 Temporal Vector: CVSS2#E:POC/RL:OF/RC:C

Vulnerability Information

CPE: cpe:/a:ietf:md5 cpe:/a:ietf:x.509_certificate
Exploit Available: true
Exploit Ease: Exploits are available

Analysis

Vulnerability Assessment

- As noted in the screenshots above, OpenSSL vulnerabilities were a gigantic part of the scanning through Nessus, cross-referenced with the CVE databases.

Exploitation

Metasploit

- Ran Armitage as a GUI to run Metasploit on the Target Machine.

Challenges

Connection Issues

- Difficulty connecting the network initially.
- I changed the network adapter setting to NAT, allowing the network to work properly.

Software Installation

- Did not have Armitage, Zenmap, or Nessus.
- I downloaded and installed all three of the programs after a fair amount of trial and error.

Armitage/Metasploit Issues

- I couldn’t remember how to use some of the attacks needed.
- This is an ongoing issue that will be remedied during the Testing Phase with more practice.