

PILL Box Vulnerability Assessment

Jack Husted

IS-6323-002 Security Risk Analysis

Robert Kaufman

3/1/2023

For this lab I will be conducting a vulnerability assessment of UTSA's PILL in the CSL NPB 1.252. The PILL network is located at the IP range 192.168.101.150-205. I will be utilizing tools such as Nmap, Metasploit, and Nikto to perform my assessment. Since this is an exercise, I have been authorized to only scan the 192.168.101.150-205 range. I must be careful in my approach and not scan anything below or above that range, as that would be logged and likely flagged. The goal of this lab is to scan for vulnerabilities and not to exploit them. Using the tools above, I will discuss my findings and determine the risks of each within this report. All screenshots will be attached as figures at the end of this report.

On Sunday 2/26/2023 I used my UTSA ID card to gain access to the CSL NPB 1.252 to perform the technical requirements of this lab. Once I entered, I found the designated range along with the login credentials for the machine. These machines were running Windows but contained Kali virtual machines. As per the lab instructions, I went ahead and booted up the Kali VM. This is where all the tools that I need are located. In the bottom right corner of the monitor and clicked network icon to ensure that I was on the "Enterprise.net" network. After I confirmed I was on the correct network, I was ready to begin using tools for my analysis.

The first tool that I booted up was Metasploit. "The Metasploit framework is a very powerful tool which can be used by cybercriminals as well as ethical hackers to probe systematic vulnerabilities on networks and servers. Because it's an open-source framework, it can be easily customized and used with most operating systems" (Buckbee). Metasploit is an extremely useful tool that even has other tools built into it such as Nmap. I needed to be careful to not exploit anything with Metasploit, as that is not the objective of this lab. Technically I only used Metasploit to run Nmap, and while I would be able to just run Nmap via the terminal, I decided to run it through Metasploit to explore potential vulnerabilities. Metasploit contains modules that have exploits for vulnerabilities on a system. These modules can provide insight on the damage that can be caused by the vulnerabilities on the range. When Metasploit booted up, I used the command "nmap -sS -O -sV -oN /root/output.txt 192.168.101.150-205". This can be viewed in **Figure 1**. The first switch I used on the Nmap command was "-sS". This switch performs a TCP SYN scan. The next switch was "-O", which will enable OS fingerprint detection for the machines. The "-sV" switch will show the ports version information. The "-oN" signifies that I want to output the results to a file and the "/root/output.txt" is where I want the file to output to. It was important to include this switch, as the Kali machine is not internet enabled, and for good reason, which I will touch on in the next paragraph. Finally, the "192.168.101.150-205" is the given range, as per the lab instructions. The results of this scan were very concerning.

In the next part of this lab, I will be reporting on Nmap's results. Since there were several hosts, I will be going into detail on the largest vulnerabilities that I found. Nmap reported that a total of 19 hosts were up, which all can be seen in **Figure 2**. The first scanned machine was .150 machine. This machine had port 53 domain, port 135 msrpc, port 139 netbios-ssn, port 445 microsoft-ds, and port 3389 ms-wbt-server all open. In the last lab, I covered the vulnerabilities associated with the port 135-139 range and port 445. Port 135 is Microsoft's Remote Procedure Call and is used for remote access to a machine. This port can be used as an open vulnerability for denial of service, worms, and remote access. Port 139 NetBios is used for file and print sharing. It is utilized by worms, trojans, and backdoors to gain access to a system. Port 445 Microsoft-ds is used for networking. An interesting exploit that I found could utilize any of these 3 ports. The Microsoft Security Bulletin MS03-026 stated that the exploitation of these

vulnerabilities could allow an attacker to run code of their choice. “To exploit this vulnerability, the attacker would require the ability to send a specially crafted request to port 135, 139, 445 or 593 or any other specifically configured RPC port on the remote machine. For intranet environments, these ports would normally be accessible, but for Internet connected machines, these would normally be blocked by a firewall. In the case where these ports are not blocked, or in an intranet configuration, the attacker would not require any additional privileges” (Microsoft). Port 445 on this machine was also showing the workgroup that it was located on which was “ENTERPRISE” which can be seen in **Figure 3**. The combination of port 135, 139, and 445 were shown on multiple systems on this IP range, most notably combinations of the port 135-139 range, which are all related to print and file sharing. This range has a sleuth of exploits that can be used if the machine is internet facing like remote code execution, remote desktop control, and can be used to plant malware on a machine. Port 3389 is associated with Windows Remote Desktop and is intended for remoting into a system. “Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft, which provides a user with a graphical interface to connect to another computer over a network connection. The user employs RDP client software for this purpose, while the other computer must run RDP server software” (HackTricks). This port is often utilized for rogue access to a user’s desktop by a hacker or by trojans as a backdoor for a system. Using the same port, a separate machine located at IP 192.168.101.154 the service xrdp was listed. “XRDP is a free and open-source implementation of Microsoft RDP (Remote Desktop Protocol) server for operating systems other than Windows, such as Linux. It offers some key advantages” (ITpro). Xrdp is essentially a free, open-source version of rdp that does not require proprietary software to utilize. Xrdp had its own exploits specific to itself. “Buffer overflow in the xrdp_bitmap_invalidate function in xrdp/xrdp_bitmap.c in xrdp 0.4.1 and earlier allows remote attackers to execute arbitrary code via a crafted request” (Mitre CVE database). A number of machines were using the “Aladdin/Safenet HASP license manager 15” version of the HTTP service on port 1947. “The Sentinel License Manager enforces and manages licensing in multi-user environment. It keeps track of all the licenses and handles requests from network users who want to run your application, granting authorization to the requesters to allow them to run the application, and denying requests when all licenses are in use” (Exploit Database). An exploit for this service allows for an attacker to delete or write files to a machine by using a directory reversal attack. Another common service that was being used by these machines was port 22 SSH or Secure Shell. SSH was created with the intention of replacing port 21’s Telnet and port 23’s File Transfer Protocol. Telnet is inherently insecure because it broadcasts texts sent in plaintext with no encryption for anyone to see. Using a man-in-middle attack, you could theoretically intercept transmissions and swipe credentials that are put out over the network. FTP suffered from a similar issue in that files and text sent were, in fact, not encrypted. SSH aimed to address these issues. The creator, Tatu Ylonen, explains SSH perfectly in this quote: “I have written a program to securely log from one machine into another over an insecure network. It provides major improvements in security and functionality over existing telnet and rlogin protocols and implementations. In particular, it prevents IP, DNS and routing spoofing. My plan is to distribute the software freely on the Internet and to get it into as wide use as possible” (SSH Academy). SSH is a widely used service, but it does have vulnerabilities. “sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of

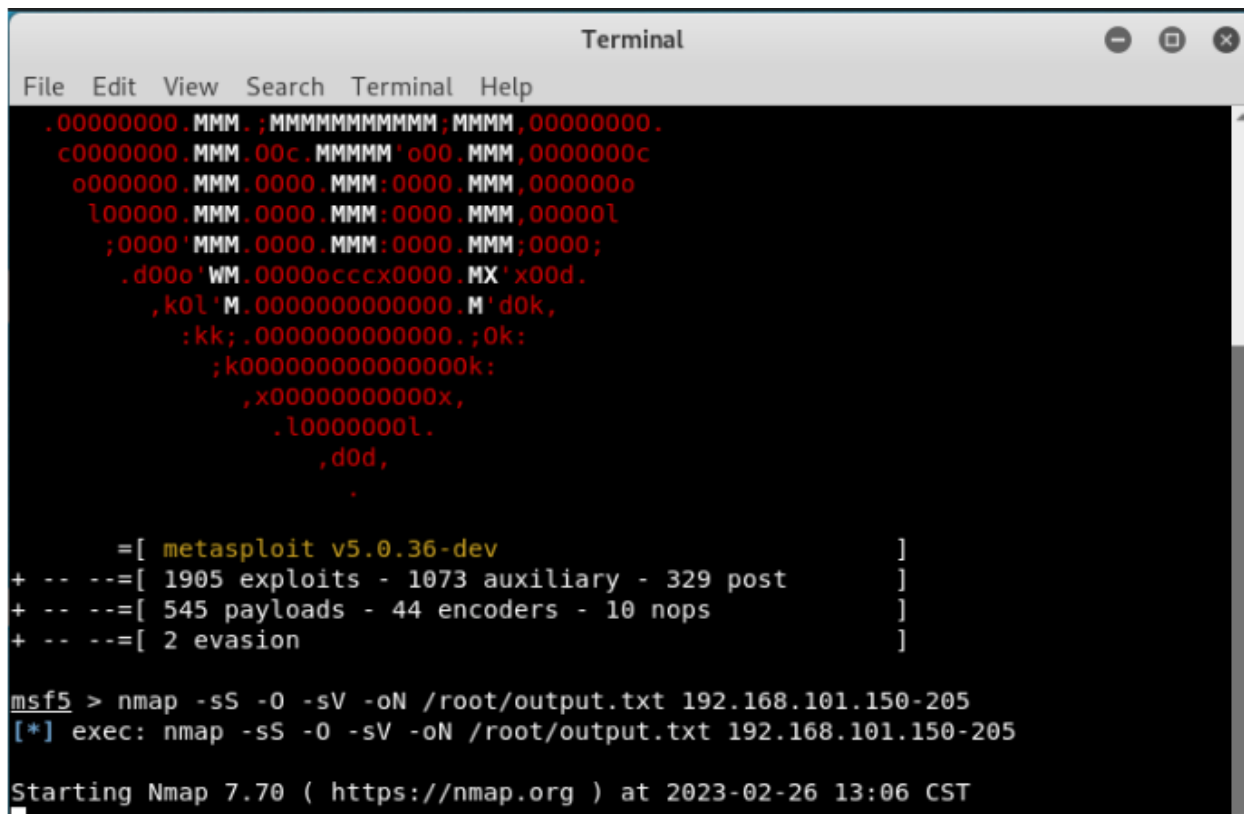
the sshd process, if the configuration specifies running the command as a different user” (NIST). Privilege escalation is one of many tactics a hacker will use to gain access to information. On the machine located at IP 192.168.101.176 a few services caught my eye. On port 427, service location protocol is used to discover services on a local network and is designed in a way that allows it to be used out of the box. This port is associated with denial-of-service attacks from remote users if exploited. “srvloc.sys in Novell Client for Windows before 4.91 SP3 allows remote attackers to cause an unspecified denial of service via a crafted packet to port 427 that triggers an access of pageable or invalid addresses using a higher interrupt request level (IRQL) than necessary” (Mitre CVE database). This machine also had port 80 http, used to send and receive webpages, along with port 8000 which was marked as http-alt. While this alternate port number is used as an alternative to port 80 for http, it has also been used by many trojans and viruses as a means for communication. The port 8300 for the Transport management interface was running on this machine as well. This port had a CVE registered that could cause a denial of service. “Messenger Agents (nmma.exe) in Novell GroupWise 2.0.2 and 1.0.6 allows remote attackers to cause a denial of service (crash) via a crafted HTTP POST request to TCP port 8300 with a modified val parameter, which triggers a null dereference related to “zero-size strings in blowfish routines”” (Mitre CVE database). Located at IP 192.168.101.197 had port 554 real time streaming protocol open. “Real Time Streaming Protocol (RTSP) is an application-level network communication system that transfers real-time data from multimedia to an endpoint device by communicating directly with the server streaming the data” (Posey). The compelling part of this port is that it seems to be used for a camera. Because I used a service scan switch, I was able to see that this port was being used by the Axis 207w camera. I was able to track down 4 CVEs for this camera which ranged from cross-site scripting vulnerabilities to cross-site request forgery. One that I found particularly interesting was a vulnerability that stated that the camera was storing the WPA key in cleartext. “The AXIS 207W camera stores a WEP or WPA key in cleartext in the configuration file, which might allow local users to obtain sensitive information” (CVE Details). Coming into possession to the WPA key of a network would allow a user or hacker to connect to its associated network. If these cameras were set up in a business that contained sensitive information, it could be utilized by a bad actor as a means of gaining access to said information. The last machine on this list was what I considered to be the most concerning of the bunch and had 23 total ports open. Located at IP 192.168.101.203, this machine had some familiar ports like port 21 ftp, port 22 ssh, port 23 telnet, and port 80 http, all of which I have already touched in this report. However, it also had some ports open that were clearly very high risk. Port 111, RPCbind “Provides information between Unix based systems. Port is often probed, it can be used to fingerprint the Nix OS, and to obtain information about available services. Port used with NFS, NIS, or any rpc-based service” (HackTricks). This port has some security concerns such as malware, and sensitive information that you may not want broadcasted. Continuing down the list of many open ports for this machine was port 513 login. I discovered that a worm named the ADM worm commonly uses this port to communicate and replicate. This worm is specific to Linux machines and was first discovered in 1998. “It spreads itself from system to system by using a Linux security breach (so called “buffer overrun” breach) that allows to upload to remote system and run there a short piece of code that then downloads and activates the main worm component” (Kaspersky). It also spreads via the Berkeley Internet Name Domain which was used commonly among UNIX distributions (Kaspersky). The worm is made up of 8 files total and utilizes scripts and executables. The worm first starts by using a buffer overrun attack and using a carefully crafted block of data, then code is ran on the target

machine. “That code opens a connection to infected machine, gets the rest of worm code and activates it. At that moment the machine is infected, and starts to spread worm further” (Kaspersky). The worm will then edit web server start pages with “The ADM Inet w0rm is here !”. Because this port is open, I think it a real possibility that this machine is already infected with this worm and the machine should be quarantined for inspection. Its neighboring port, port 514, is also utilized by the ADM worm and supports my claim that the machine may already be infected. The next port that piqued my interest was port 1524 Bindshell. The service version that was listed on this port was Metasploitable root shell and would allow for remote access to a machine. If a hacker wanted to exploit this vulnerability they could utilize a tool such as NetCat to connect and gain access to a root shell. Once connected to a root shell, a hacker could likely change the properties of the operating system on this machine, therefore gaining any information they set out for. If a port like this was open in a real scenario, I would be led to believe that a hacker more than likely already exploited this computer and planted this bindshell to keep access to a machine. Coincidentally, I did some research into Metasploitable and it is a vulnerable version of Linux. “Metasploitable is an intentionally vulnerable Linux virtual machine that can be used to conduct security training, test security tools, and practice common penetration testing techniques” (Offsec). Furthermore, port 2049 is of risk to the machine and network. “Network File System (NFS) - remote filesystem access [RFC 1813] [RFC5665]. A commonly scanned and exploited attack vector. Normally, port scanning is needed to find which port this service runs on, but since most installations run NFS on this port, hackers/crackers can bypass fingerprinting and try this port directly” (Speed Guide). Port 2121 ccproxy-ftp, which “functions as a relay for the File Transfer Protocol to enable you control connections based upon source and destination addresses and user authentication” (Oracle), had many backdoors such as the “Hupigon.aejq”. Hupigon would allow for a remote attacker to connect to the FTP server using any credentials of their liking and could also remotely execute code. A service running on port 5900 named virtual network computing which is responsible for remote control programs, such as Apple remote desktop, had some malware, denial of service, and unauthorized access vulnerabilities associated with the port. The last port I will be covering will be port 6667 Internet Relay Chat, which is connected to at least 25 different trojans and backdoors, and is a port I have exploited myself in a previous lab of a different course at UTSA. “Internet Relay Chat (IRC) is a network of Internet servers that use a specific protocol through which individuals can hold real-time online conversations via PCs and other devices” (Trend Micro). This is IRC’s intended purpose, Trend Micro continues on this quote to state that “Many of today’s botnets utilize IRC to communicate with bot-infected machines” (Trend Micro). IRC is one of the most popular ways a hacker would utilize command and control as a botnet. “Simply put, once a machine is compromised, it is programmed to connect to a preset IRC channel and wait for further instructions from the server. An attacker can then remotely control the compromised bot to perform actions on his or her behalf, and in the worst case scenario, an attacker can use multiple bots together and perform a catastrophic attack such as a Distributed Denial of Service attack” (O’Reilly). In my limited experience, I do not think that a business, or in this case, a lab would have IRC as an intended service. Most organizations would be smart to have a port like this open as against the rules, and if it were open I would think one of two things. The first would be that someone, either through negligence or on purpose, is possibly going against company policy, which you would likely want to discover anyways. Or the second, that the machine has been compromised. This machines Nmap scan can be found in **Figure 4**.

The second assessment tool that I ran was a program called Nikto. “Nikto is an Open Source software written in Perl language that is used to scan a web-server for the vulnerability that can be exploited and can compromise the server. It can also check for outdated version details of 1200 server and can detect problems with specific version details of over 200 servers” (GeeksForGeeks). Nikto aims to show a user of how to secure their webserver on their network by showing documented vulnerabilities based on your scan. On this network, only three webserver were found, and none of them were completely secure. Some of the common vulnerabilities for all three of these servers was cross-site scripting protection, also known as XSS. “Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it” (OWASP). These sort of attacks can be extremely malicious, even going as far as to editing the HTML code for the webpage. This can lead to a regular user being sent a script to be ran on their machine, because it looks trusted. These web servers were also using Apache, but they were all out of date. I machine that is not patched could suggest that it is vulnerable to a plethora of potential exploits. System information could be extracted via the php information file from these webserver, which again can lead to reconnaissance information that can be utilized to exploit a machine. Some of these results can be viewed in **Figure 5**.

In summation, I was able to scan the network via Nmap and Nikto. The results of the Nmap scan showed some interesting ports that were open. Ports 135, 139, and 445, which I covered in the previous lab were open on multiple machines, and if vulnerable, can prove to be a headache. Port 22 SSH and port 21 FTP were being used on this network, which is not uncommon but running an out of date version does make your network vulnerable. Various RPC ports were found on the machines. Aside from this, the most interesting machine was the last machine, which the Nmap results showed NFS, Bindshell, and IRC, all of which can be very dangerous to a network and run significant risk. I was also able to scan the webserver found on three machines on this network, all of which were vulnerable to XSS. I believe this was a successful lab that will be a useful experience as I move through the incoming security audit project within this class. The knowledge that I obtained through out this lab can be used in future labs, and a future career as a security professional.

Figures



```

Terminal
File Edit View Search Terminal Help
.00000000.MMM.;MMMMMMMMMMMM;MMM,00000000.
c0000000.MMM.00c.MMMMM'o00.MMM,0000000c
o000000.MMM.0000.MMM:0000.MMM,000000o
l00000.MMM.0000.MMM:0000.MMM,00000l
;0000'MMM.0000.MMM:0000.MMM;0000;
.d00o'WM.0000occcx0000.MX'x00d.
,kOl'M.0000000000000.M'dOk,
:kk;.0000000000000.;Ok:
;k000000000000000k:
,x000000000000x,
.l0000000l.
,d0d,
.

=[ metasploit v5.0.36-dev ]
+ -- --=[ 1905 exploits - 1073 auxiliary - 329 post ]
+ -- --=[ 545 payloads - 44 encoders - 10 nops ]
+ -- --=[ 2 evasion ]

msf5 > nmap -sS -O -sV -oN /root/output.txt 192.168.101.150-205
[*] exec: nmap -sS -O -sV -oN /root/output.txt 192.168.101.150-205

Starting Nmap 7.70 ( https://nmap.org ) at 2023-02-26 13:06 CST

```

Figure 1. Running Metasploit which can also run Nmap.

```

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Sun Feb 26 13:11:10 2023 -- 56 IP addresses (19 hosts up) scanned in 268.53
seconds

```

Figure 2. Nmap reporting the total hosts up on the network.

```

445/tcp open  microsoft-ds  Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
(workgroup: ENTERPRISE)

```

Figure 3. Port 445 showing the workgroup information.

Network Distance: 1 hop
 Service Info: OS: Linux; Device: webcam; CPE: cpe:/o:linux:linux_kernel:2.6.20

Nmap scan report for 192.168.101.203
 Host is up (0.00056s latency).
 Not shown: 977 closed ports

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	<u>vsftpd</u> 2.3.4
22/tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp	open	telnet	Linux <u>telnetd</u>
25/tcp	open	<u>smtp?</u>	
53/tcp	open	domain	ISC BIND 9.4.2
80/tcp	open	http	Apache <u>httpd</u> 2.2.8 ((Ubuntu) DAV/2)
111/tcp	open	rpcbind	2 (RPC #100000)
139/tcp	open	netbios-ssn	Samba <u>smbd</u> 3.X - 4.X (workgroup: WORKGROUP)
445/tcp	open	netbios-ssn	Samba <u>smbd</u> 3.X - 4.X (workgroup: WORKGROUP)
512/tcp	open	exec?	
513/tcp	open	login?	
514/tcp	open	shell?	
1099/tcp	open	<u>rmiregistry</u>	GNU Classpath <u>gmiregistry</u>
1524/tcp	open	bindshell	Metasploitable root shell
2049/tcp	open	nfs	2-4 (RPC #100003)
2121/tcp	open	ccproxy-ftp?	
3306/tcp	open	mysql?	
5432/tcp	open	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp	open	vnc	VNC (protocol 3.3)
6000/tcp	open	X11	(access denied)
6667/tcp	open	irc	UnrealIRCd
8009/tcp	open	ajp13?	
8180/tcp	open	unknown	

MAC Address: FE:DF:73:A0:07:70 (Unknown)
 Device type: general purpose
 Running: Linux 2.6.X
 OS CPE: cpe:/o:linux:linux_kernel:2.6
 OS details: Linux 2.6.9 - 2.6.33
 Network Distance: 1 hop
 Service Info: Hosts: localhost, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Figure 4. The last machines open ports.

- + Target Host: 192.168.101.197
- + Target Port: 80
- + GET The anti-clickjacking X-Frame-Options header is not present.
- + GET The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
- + GET The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
- + Target Host: 192.168.101.176
- + Target Port: 80
- + GET The anti-clickjacking X-Frame-Options header is not present.
- + GET The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
- + GET The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
- + Target Host: 192.168.101.203
- + Target Port: 80
- + GET Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
- + GET The anti-clickjacking X-Frame-Options header is not present.
- + GET The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
- + GET The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
- + GET Uncommon header 'tcn' found, with contents: list
- + GET Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See <http://www.wisec.it/sectou.php?id=4698ebdc59d15>. The following alternatives for 'index' were found: index.php
- + GET Multiple index files found: /index.php, /index.shtml

Figure 5. The results of the Nikto scan on the network for some of the machines.

Works Cited

- Allen, J. (2022, February 16). *What is XRDp?* IT PRO. Retrieved March 23, 2023, from <https://www.itpro.com/mobile/remote-access/368057/what-is-xrdp>
- Audit My PC. (2010, March 13). *TCP 8000 - port protocol information and warning!* Audit My PC - Free Internet Security Audit | Firewall Test and web tools to check your security and privacy. Retrieved March 23, 2023, from <https://www.auditmypc.com/tcp-port-8000.asp>
- Buckbee, M. (2022, February 24). *What is Metasploit? the beginner's guide.* Varonis. Retrieved March 23, 2023, from <https://www.varonis.com/blog/what-is-metasploit>
- CVE Details. (2007). *Axis " 207W network camera : Security vulnerabilities.* Axis 207w Network Camera : List of security vulnerabilities. Retrieved March 23, 2023, from https://www.cvedetails.com/vulnerability-list/vendor_id-400/product_id-12118/Axis-207w-Network-Camera.html
- Exploit Database. (2016, June 16). *Gemalto Sentinel License manager 18.0.1.55505 - directory traversal.* Exploit Database. Retrieved March 23, 2023, from <https://www.exploit-db.com/exploits/39968>
- GeeksForGeeks. (2022, September 30). *What is Nikto and it's usages ?* GeeksforGeeks. Retrieved March 23, 2023, from <https://www.geeksforgeeks.org/what-is-nikto-and-its-usages/>
- HackTricks. (2023). *111/TCP/UDP - pentesting portmapper.* HackTricks. Retrieved March 23, 2023, from <https://book.hacktricks.xyz/network-services-pentesting/pentesting-rpcbind>
- HackTricks. (2023). *3389 - Pentesting RDP.* HackTricks. Retrieved March 23, 2023, from <https://book.hacktricks.xyz/network-services-pentesting/pentesting-rdp#basic-information>
- Kaspersky. (2016). *ADM.* Kaspersky Threats. Retrieved March 23, 2023, from <https://threats.kaspersky.com/en/threat/Net-Worm.Linux.Adm/>
- Microsoft. (2003). *Microsoft Security bulletin MS03-026 - critical.* Microsoft Learn. Retrieved March 23, 2023, from <https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2003/ms03-026?redirectedfrom=MSDN>
- Mitre. (2006). *CVE-2006-4511.* CVE. Retrieved March 23, 2023, from <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4511>
- Mitre. (2006). *CVE-2006-6307.* CVE. Retrieved March 23, 2023, from <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6307>
- Mitre. (2008). *CVE-2008-5902.* CVE. Retrieved March 23, 2023, from <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5902>

- NIST. (2021). *CVE-2021-41617 Detail*. NVD. Retrieved March 23, 2023, from <https://nvd.nist.gov/vuln/detail/CVE-2021-41617>
- OffSec. (2020, March 30). *Requirements - Metasploit Unleashed*. OffSec. Retrieved March 23, 2023, from <https://www.offsec.com/metasploit-unleashed/requirements/#:~:text=Metasploitable%20is%20an%20intentionally%20vulnerable,practice%20common%20penetration%20testing%20techniques>.
- Oracle. (2010). *FTP proxy*. Moved. Retrieved March 23, 2023, from <https://docs.oracle.com/cd/E19047-01/sunscreen32/806-6347/6jfa0g88p/index.html>
- Posey, B. (2023, February 22). *What is Real time streaming protocol (RTSP)?*: Definition from TechTarget. Virtual Desktop. Retrieved March 23, 2023, from <https://www.techtarget.com/searchvirtualdesktop/definition/Real-Time-Streaming-Protocol-RTSP>
- S, K. (n.d.). *Cross site scripting (XSS)*. Cross Site Scripting (XSS) | OWASP Foundation. Retrieved March 23, 2023, from <https://owasp.org/www-community/attacks/xss/>
- SpeedGuide. (n.d.). *Port 2049 (TCP/UDP)*. SpeedGuide. Retrieved March 23, 2023, from <https://www.speedguide.net/port.php?port=2049>
- SSH Academy. (2017, March 14). The story of the SSH port is 22. Retrieved March 23, 2023, from <https://www.ssh.com/academy/ssh/port>
- Trend Micro. (2023). *Internet relay chat (IRC)*. Definition. Retrieved March 23, 2023, from <https://www.trendmicro.com/vinfo/us/security/definition/internet-relay-chat-irc>
- Verma, P. (n.d.). *Wireshark Network Security*. O'Reilly Online Learning. Retrieved March 23, 2023, from <https://www.oreilly.com/library/view/wireshark-network-security/9781784393335/ch05s03.html>