Lab 3: Network and Computer Attacks

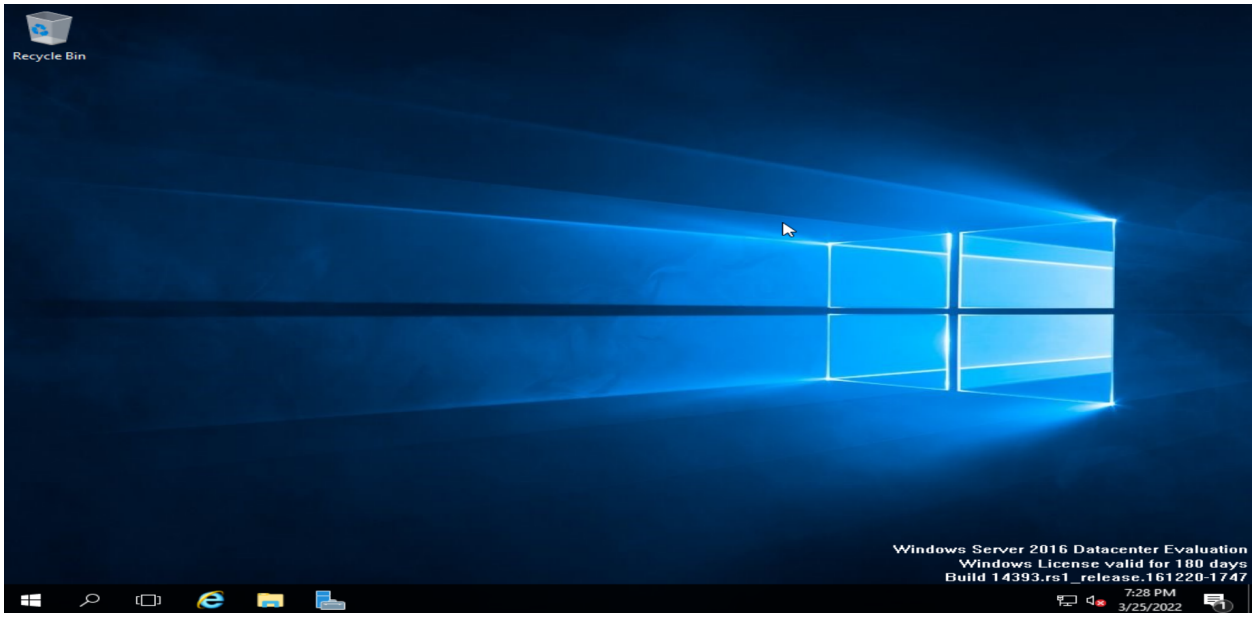
Introduction:

As mentioned in the previous report, the metasploit framework is an incredibly useful testing ground for ethical hackers to hone their craft. The software comes preinstalled on all current versions of Kali, and provides users with a plethora of espionage utilities, exploits, and malware creation tools. The focus of this lab is to use the metasploit framework, and its various functionalities, to gain total control of a target virtual machine via a malicious executable file. Which of course, necessitated the creation of yet another virtual machine.

Part 1: Setting up the Target:

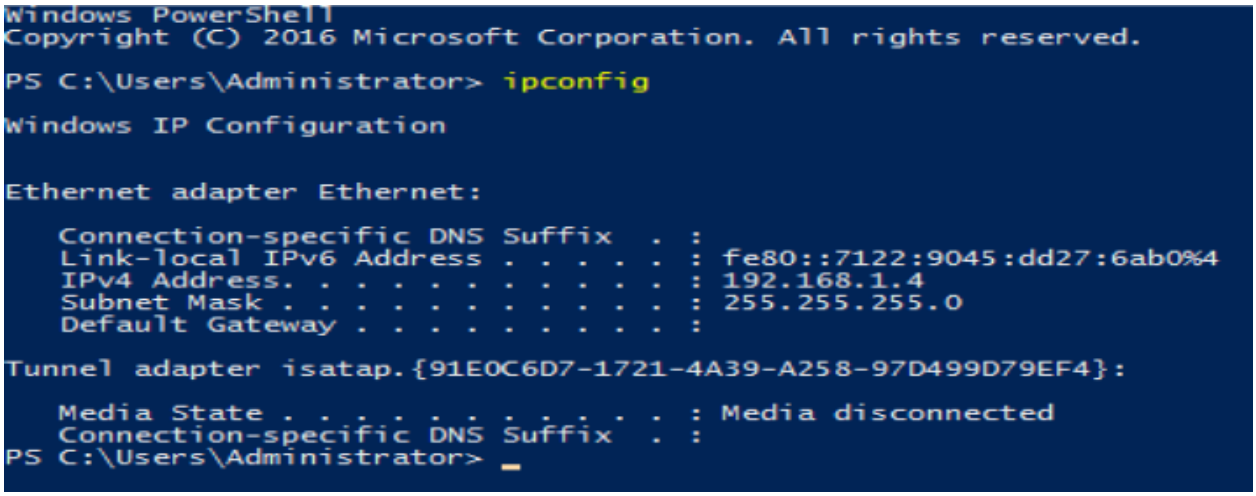
In keeping with the times, the still relatively current Windows Server 2016 was chosen as our target virtual machine's operating system. This time however, we installed from a more traditional ISO image in lieu of a VirtualBox VBI. **Figure 1** shows the desktop of our target VM moments after booting into Windows for the first time.

Figure 1: Windows Server 2016 Target Virtual Machine



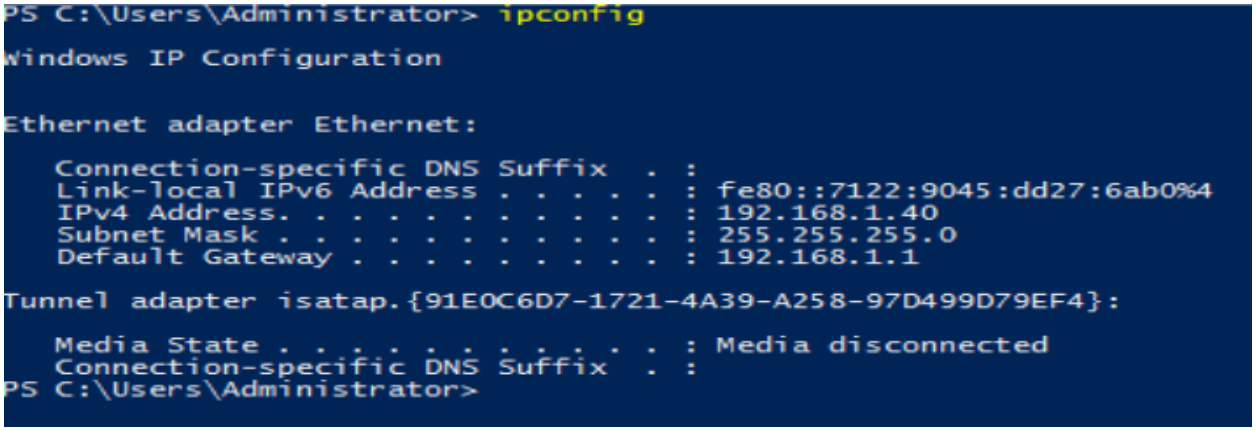
The next steps of the target VM's setup process were the disabling of various Windows security features, the configuration of its networking mode as host only, and the manual assignment of its static IP address. Thereby enabling our two virtual machines to communicate with one another, but not with the host. **Figures 2 and 3** show the target VM's network information before and after configuration.

Figure 2: Target VM's Pre-Configuration Network Information



***** We see the IP address is assigned using DHCP by default

Figure 3: Target VM's Post-Configuration Network Information



***** Manually assigning a static IP address and default gateway

Having now completed the installation and setup processes, the connectivity between our target and Kali virtual machines was verified by pinging one from the other and vice versa. The results are summarized in **Figures 4 and 5**

Figure 4: Target VM Communicating With Kali

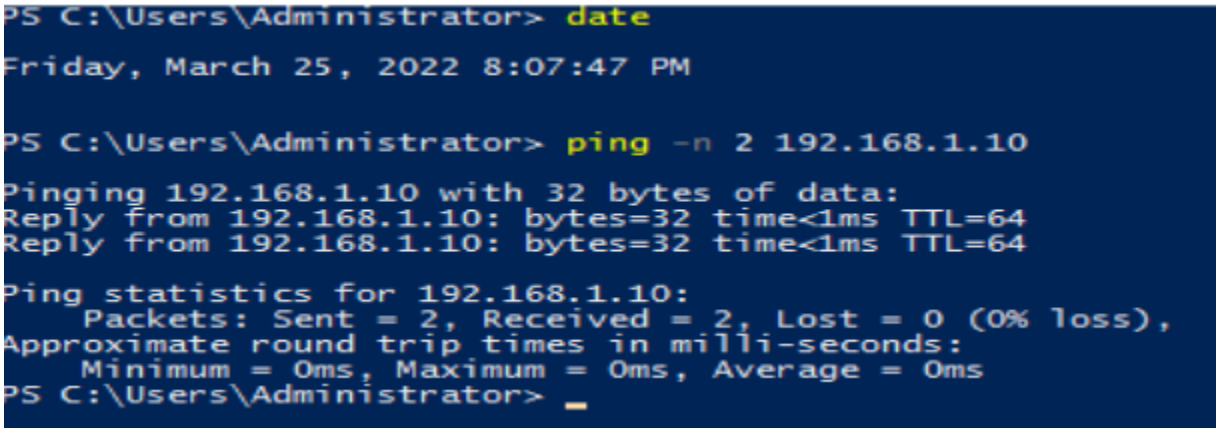
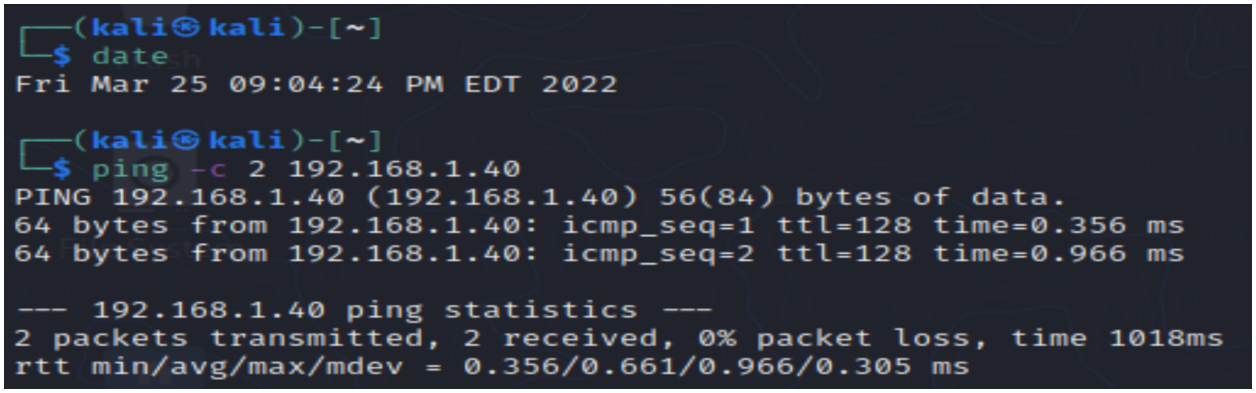


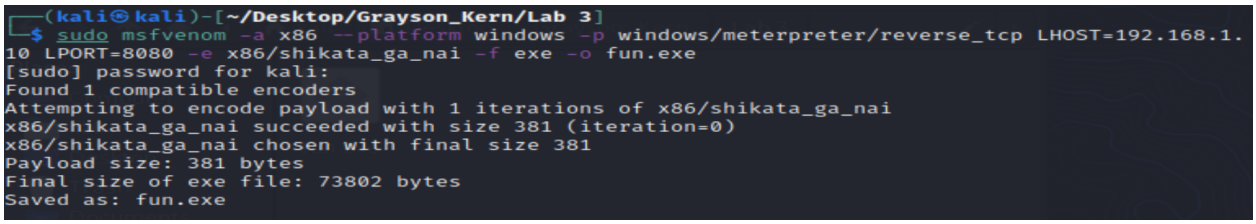
Figure 5: Kali Communicating with Target VM



Part 2: Attacking the Target:

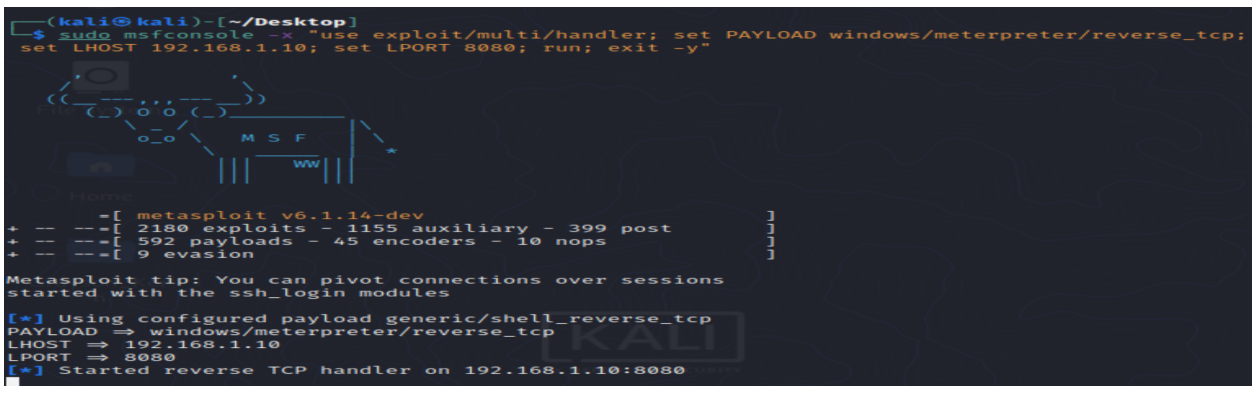
We initiate the first stage of our attack by attaching the Meterpreter revrese_tcp exploit to a seemingly innocuous exe file as a payload. This was accomplished using the msfvenom payload generating utility, as illustrated by **Figure 6.**

Figure 6: Generating Malware“fun.exe”



Upon execution of this file, the meterpreter is loaded into privileged and or occupied address space, allowing it to mimic system level processes and remain relatively undetected. After loading itself into memory, the exploit then establishes a reverse TCP connection with the attacker’s public IP address over the specified port. Thereby affording the attacker code execution privileges provided a meterpreter listener is running over the same port on their machine. **Figure 7** shows such a listener running on the attacking machine, awaiting a connection from the target.

Figure 7: Meterpreter Listener



Upon establishment of a connection, an interactive meterpreter session is launched. Whereby the attacker can assume control over the target machine via shell commands, and or conduct various reconnaissance operations. **Figures 8 through 11** showcase these capabilities and the amount of damage such malware can potentially cause.

Figure 8: Querying the Target Machine's System Information

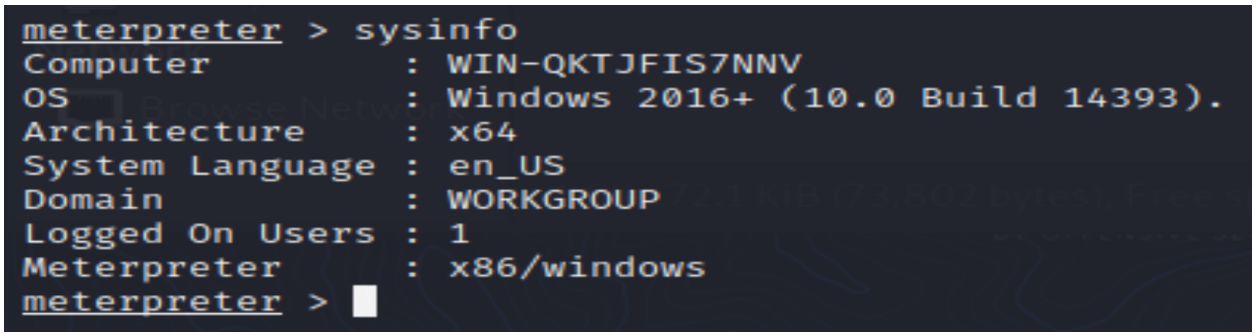


Figure 9: Target Machine Screen Capture

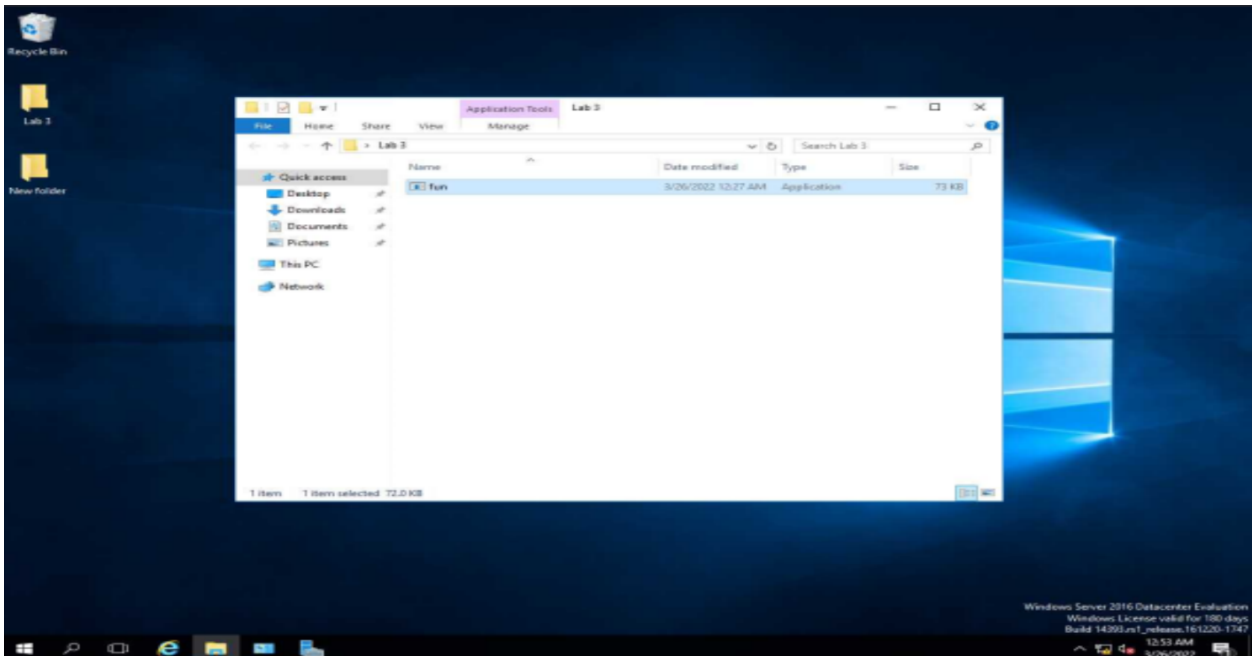
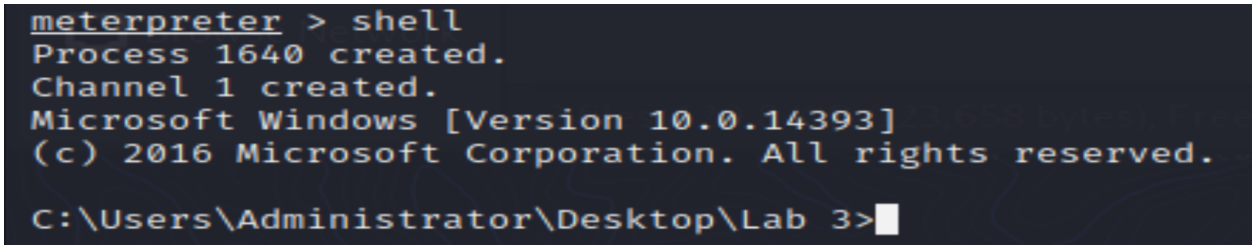
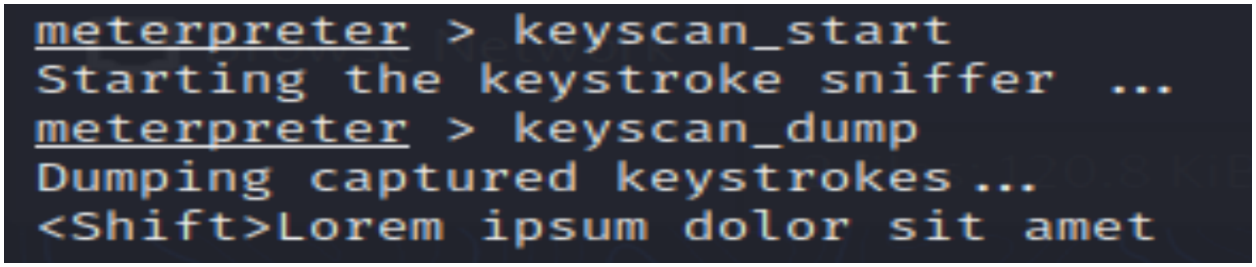


Figure 10: Issuing Shell Commands to the Target Machine



***** From here the attacker can issue any Windows command the infected user account has permission to execute, which as Administrator, is nearly all of them. Thus the attacker may issue the infamous *del C:\\WINDOWS\system32* to effectively brick the target machine if they so choose.

Figure 11: Listening for Keystrokes on the Target Machine



Part 3: Examining Various Malware

CryptoLocker:

As the name suggests, CryptoLocker is a form of ransomware affecting Windows operating systems. Namely XP, Vista, 7, and 8. Primarily transmitted through phishing emails, the program encrypts important files on a target system in an attempt to extort a ransom payment from the victim. Prevention methods include keeping operating systems and anti-virus softwares up to date, conducting routine offline backups of important files, and exercising caution when opening email attachments. If already infected, removal is next to impossible without the attacker's private encryption key, so an ounce of prevention is worth a pound of cure.

Macro Viruses:

Many applications such as those in the *Microsoft Office* suite use specialized macro languages to map instruction sequences to specific user keybinds or programmatic events. Though their primary use case is the automation of complex or repetitive tasks, they can easily be injected with a wide variety of malicious payloads to create what are known as macro viruses. Such viruses are generally much more portable than the likes of worms or trojans, owing to the fact that they exploit application level vulnerabilities in lieu of system level ones. As such, they are capable of running on any operating system for which their underlying software is compatible. Which has made them increasingly popular following the rise of smartphones post 2010.

Modern versions of *Microsoft Office* software require users to manually enable macro execution privileges, which is where social engineering comes into play. Oftentimes hackers will disguise virus bearing Word documents or Excel spreadsheets as something important like a bank statement, invoice, or warranty information. Generally the file will instruct the user to enable macro execution in order to view some "confidential information" which if the user is

gullible enough to do, will compromise their system with whatever payload the macro is loaded with.

Stuxnet Worm:

Worms are a class of malware characterized by their ability to rapidly reproduce and spread across networks in the absence of human intervention. They can be particularly devastating to corporate and organizational networks, where they can quickly and efficiently infect a vast amount of hosts. The Stuxnet worm is perhaps the most infamous in recent history due to its sabotage of Iranian uranium enrichment facilities in January 2010. It accomplished this feat by infecting, and subsequently reprogramming their centrifuge control systems at the programmable logic level. Effectively hating the nation's controversial nuclear program.

Stuxnet was spread using a wide variety of propagation methods, most notably via remote execution vulnerabilities found in the Windows print spooler, and server services. Though eventually detected almost worldwide, the country with the highest concentration of infections was by far Iran. They were also the only country whose nuclear facilities were sabotaged. This implicates the Iranian nuclear program as the intended target of the Stuxnet attack. The rest of the infected countries were simply collateral damage resulting from over propagation. This lack of control is one of the main disadvantages of worms over other classes of malware.

Spyware:

Spyware is a broad subclass of malware whose primary purpose is the collection of information from a target system for use by a third party. Many different types and threat levels of spyware exist depending on the information they collect, ranging from annoying adware toolbars to malicious keyloggers and rootkits. The Alibaba toolbar is a specific example of the former, and does little more than log URLs and serve pop-up ads.

Software Vulnerabilities:

The United States Cybersecurity and Infrastructure Security Agency (CISA) maintains a database of various software vulnerabilities and their mitigation measures on their website https://us-cert.cisa.gov/ CVE-2021-44683 in particular, is a high threat address bar spoofing vulnerability affecting current versions of the *DuckDuckGo* mobile browser. This type of vulnerability allows hackers to spoof malicious web pages as legitimate, and can be exploited to trick users into supplying sensitive information.