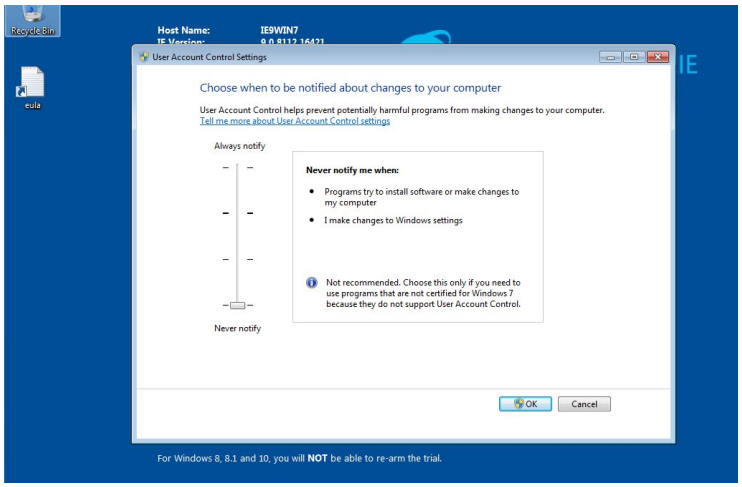
Dom Moore
Kali-Metasploit Lab

Objective: to obtain the target system's Administrator password by delivering a payload-based exploit crafted in Kali Linux.

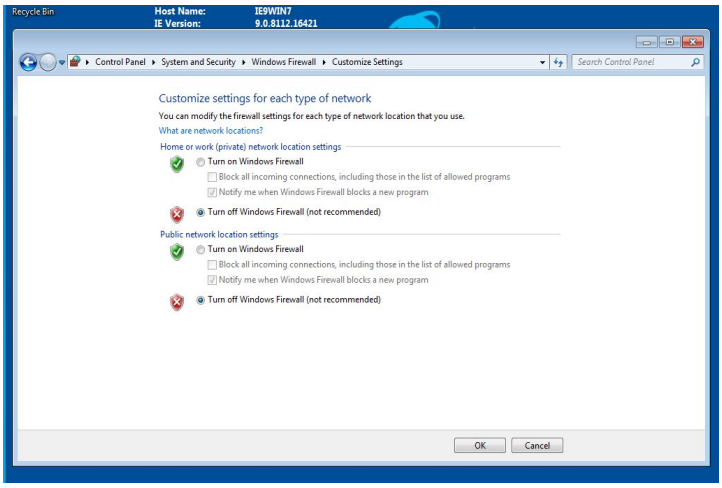
Part 1: My First Cyber Range

- Step1- Deploy Kali Linux and Windows
- Step2- Update Metasploit in Kali Linux to the latest version.
- Step3- Disable Windows Update in your Windows 7 Edge VM.
- Step-4 Disable User Account Controls (UAC) on your Windows 7 Edge VM.
- Step-5 Verify the devices can ping each other. Each device should have internet access.
- Step-6 Establish a means of file sharing between the two devices

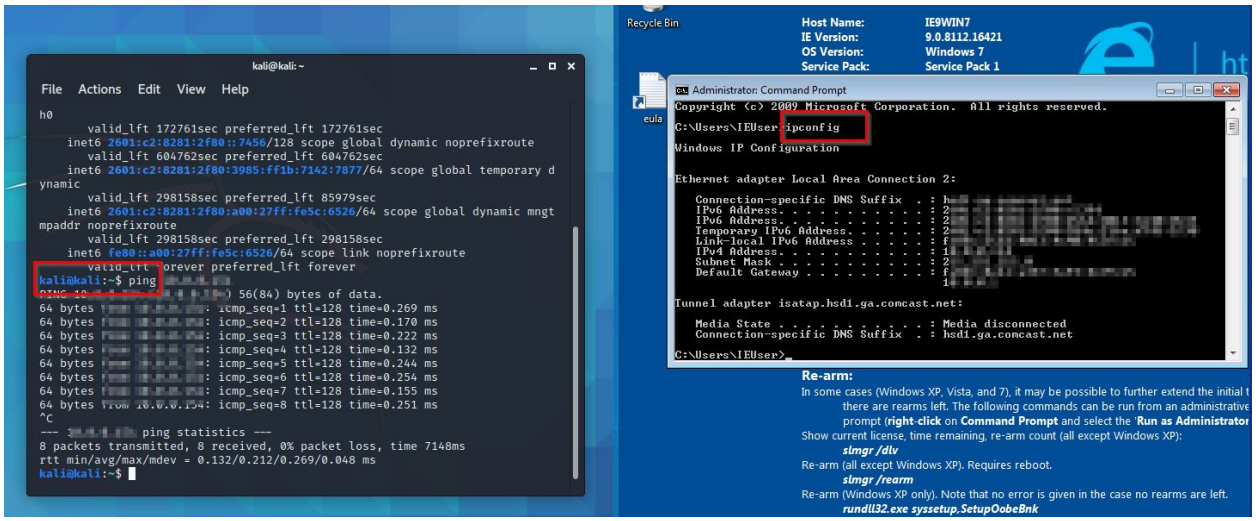
Disable UAC



Disable Firewall



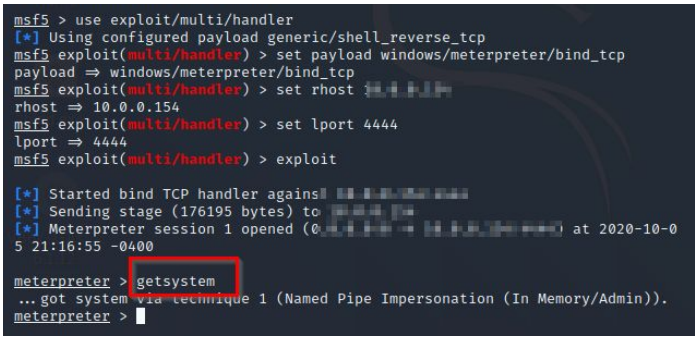
Ping Test



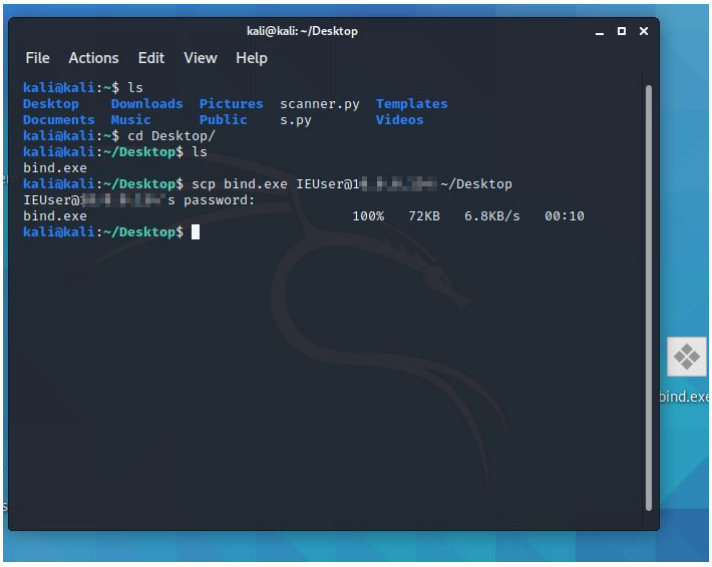
Part 2: My First Exploit

- Step1- On Kali Linux, craft a payload that will create a Meterpreter shell on Windows 7
- Step2- For today's task, assume the payload has been downloaded and executed by the Windows
- Step3- Open a Meterpreter shell in Metasploit.
- Step4- Privilege escalates to systems administrators.
- Step5- Dump the SAM hashes of the Windows 7 PC's user accounts.
- Step6- Crack the password hash to reveal the administrator password

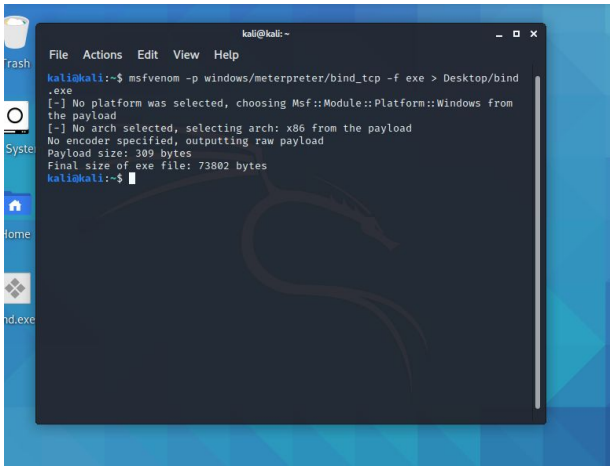
Payload created (bind.exe for windows)



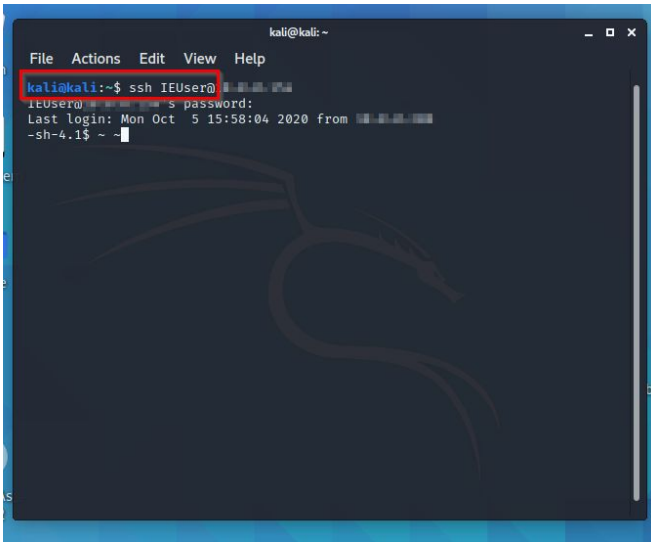
Bind.exe file transfer to remote(scp cmd)



Exploit started/ privilege escalation



SAM files(system passwords)



Hash cracked (crackstation.net)

Enter up to 20 non-salted hashes, one per line:

fc525c9683e8fe067095ba2ddc971889

I'm not a robot

reCAPTCHA
Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
fc525c9683e8fe067095ba2ddc971889	NTLM	Passw0rd!

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Part 3: Report

Discuss what key vulnerabilities were present on the Windows 7 VM that allowed this attack to succeed.

- Outdated windows 7 system, no longer supported for security updates
- (Self-imposed- disabling the firewall/UAC) allowed for easy access to a network
- No entry sign-in or password need to gain access to OS

What policies or procedures could have been implemented to avoid this?

- I would upgrade to an OS that is supported
- I would add role-based users/password for sign-in
- Enable firewall and UAC
- Limit network and file sharing
- Create a policy around downloading unknown files
- Test frequently on adherence to security protocols with staff

What are some reasons this attack might not work in a mature enterprise environment?

- System maybe updates with security features enables
- Added security using router blocking file share or ports
- Role-based privileges assigned to employees
- No repeat passwords for administrators

What tools did you stumble across in your research/lab time that piqued your interest?

- Some tools that I came across was EMPIRE a post-exploitation tool that can be used with python and PowerShell to escalate privilege in windows using PowerShell commands
- SCP command allowed me to copy a file from my local PC to a remote PC through secure ssh.
- There are other features within meterpreter that are interesting (download, audio, and android)

What aspects of today's lab were difficult or felt foreign that you'd like to learn more about in class?

- The most challenging part was working within the windows 7 VM, in the beginning, the VM crashed constantly and would not allow me to share files, later in the process when I wanted to escalate privilege I received errors of denied access. After logging out of both windows VM and kali I deleted the .exe file and began the entire process from the beginning and was able to successfully escalate privilege into the remote desktop.