Advanced Infrastructure Hacking

Question Paper

NotSoSecure Training

Module 1: Networking & Discovery

Exercise 1.1: Network Scanning

Challenge

- Perform an ARP scan on the following two networks and identify the live hosts:
  - 192.168.3.0/24
  - 192.168.X.0/24
- For the list of hosts identified above, identify the following details:
  - Open ports (Both TCP and UDP)
  - Host operating system details as well as version details of the listening services

Exercise 1.2: IPv6

Challenge

- Identify various devices listening on an IPv6 address
- Perform a port scan on all IPv6 devices and identify open ports
- Connect to an identified SNMP Server running on IPv6 and extract sysContact information
- Determine if an IPv4 address is also associated with the SNMP Server and, if so, identify it

Exercise 1.3: OSINT Data Gathering

Challenge

- Enumerate the online presence for the domain identified in Exercise 1.2
- Identify various employees of the company
- Identify leaked credentials
- Identify remote access keys

Module 2: Web Technologies

Exercise 2.1: Exploiting git and CI

Challenge

- Identify a weak configuration on the CI Server
- Obtain access to the git repository
- Upload a webshell and execute OS commands on the server

Exercise 2.2: Websphere Java Exploits

Challenge

- Identify a vulnerability in the web application running on 192.168.3.150
- Obtain a reverse shell by exploiting the identified vulnerability

LAB Challenge 2.3: HeartBleed and ShellShock

Challenge

- Identify a way to access the administrative interface on 192.168.3.180
- Gain a shell on the system by exploiting functionality of the administrative interface

Module 3: Databases

LAB Challenge 3.1: MySQL, SSH and PostgreSQL

Challenge

By exploiting vulnerabilities present in services on 192.168.3.100:

- Identify an account with a weak password and login to the MySQL database
  - Read the file '/etc/passwd' and identify the username corresponding to uid 1001
  - Extract and crack hashes from the MySQL database (mysql.user table) and tables within 'other' databases
- Identify the SSH service running on the host
  - Using an online attack, obtain the password for user identified during the MySQL challenge
  - Obtain the output of the command uname –a
- Identify an account with a weak password and login to the PostgreSQL database
  - Execute OS code and obtain the output of ifconfig on the remote host

Exercise 3.2: Oracle

Challenge

- Identify a default account within the Oracle database and connect
- Identify the privileges this user has
- Escalate privileges and obtain DBA access
- Using this privileged access, execute OS code and obtain interactive 'shell' access as the Oracle user

Exercise 3.3: Postgresql

Challenge

- Connect to the database with the credentials, acquired in Exercise 2.1
- Search for sensitive information, e.g.: user details.

Bonus:

- Identify the privileges this user has
- Escalate privileges and obtain DBA access
- Using this privileged access, execute OS code and obtain interactive ‘shell’ access as the postgres user.

Module: Windows

Exercise 4.1: Domain and User Enumeration

Challenge

- There is a Windows domain within the 192.168.3.0/24 network, what is the name?
- Using data gathered during earlier OSINT activities, find valid user accounts on the identified domain.
- Gain RDP access to a workstation within the range 192.168.X.0/24 using one of the identified accounts.

Exercise 4.2: AppLocker / GPO Restriction Bypass

Challenge

- You have an RDP session as Bob on 192.168.X.17. Attempt to execute the following commands on the host:
  - whoami
  - ipconfig /all
  - net user

Exercise 4.3: Privilege Escalation

Challenge

- You have low privileged access as plum\bob to 192.168.X.17. Attempt to gain local administrative rights on the host.

Exercise 4.4: Post Exploitation (LSASS Dump, AMSI Bypass & LSASecrets)

Challenge

- On 192.168.X.17 gain access to the NTLM hash of plum\kevin
- On 192.168.X.17 gain access to the cleartext password of plum\backupsvc

Exercise 4.5: Active Directory Delegation Issues #1

Challenge

- Identify an account that has delegation rights within the plum.local domain.
- Gain access to this account (hint: we already have the necessary data)
- Using our newly inherited rights, add a new user named pwnedX to the domain.

Warning: Please don't attempt to modify existing accounts (bob/kevin)

Exercise 4.6: Active Directory Delegation Issues #2

Challenge

- Gain access to the share \\DC01\ITSupport$\Server Management and obtain the trophy.

Warning: Please don't attempt to modify existing accounts (bob/kevin)

Exercise 4.7: AV Evasion, WOW64, Pivoting and WinRM #1

Challenge

- Write a custom shellcode loader to evade Windows Defender AV.
- Use Kali to gain a Meterpreter session on the Windows 10 host 192.168.**X**.17
- Use this session to identify a host on the 10.0.2.0/24 network (hint it's not .215)
- Find the hostname and operating system version of the identified host.
- Using Nmap, determine which ports are open on the host.

Exercise 4.8: ADCS

Challenge

- Access the kali machine on 192.168.X.206 and use the certipy tool via proxychains to extract the certificate details which is hosted within 10.0.2.0/24 network.
- Use the Certipy tool to extract the certificate details and NTLM hash of user who is domain admin.

Exercise 4.9: Lateral Movement Using WMIC

Challenge

- Using the privileged account 'godmode', gain a Meterpreter shell on the Domain Controller (192.168.3.215) without using SMB
- Extract user hashes from the Domain Controller

Exercise 4.10: Persistence (Golden Ticket and DCSync)

Challenge

- Create a Golden Ticket on the plum.local domain
- Impersonate a Domain Controller and gain access to domain password hashes.
- Perform a DCSync for **krbtgt** and extract aes key.
- Attempt a diamond ticket, attack.

Exercise 4.11: Cross-Forest Trust Abuse Issues #1 Kerberoasting

Challenge:

- Perform Cross-Forest Enumeration.
- Exploit Cross-Forest Trust to perform Kerberoasting and gain local admin on a host in the new forest.

Warning: Please don't attempt to modify existing accounts

Exercise 4.12: Cross Forest Trust Abuse Issues #2 Foreign Security Principal

Challenge:

- Identify a Foreign security principal (FSP) i.e., any resource in the plum.local having some privilege in other forest partner.local.
- Using this FSP, gain access to partner.local

Note: Please don't attempt to modify existing accounts (plum/jenny)

Exercise 4.13: C2 Framework: Sliver

Challenge:

- Use Sliver C2 framework to perform the exercise 4.11 (‘Cross-Forest Trust Abuse Issues #1 Kerberoasting’)

Exercise 4.14: Logging and Monitoring: Windows Logs and Event Viewer

Challenge:

- Get familiarised with Windows logs, Event Viewer and practice reading various events.
- Locate log event generated for disabling real time monitoring in Windows Defender.
- Increase PowerShell logging to improve Windows logging.

Exercise 4.15: Monitoring and Detections: Wazuh

Challenge:

- Observe and correlate various attacks and malicious activities performed in earlier exercises in Wazuh.

Module 5: Hacking *nix

Exercise 5.1: Enumeration

Challenge

- What services are listening on host 192.168.X.209?
- Identify supported SSH authentication methods.
- Confirm the existence of a computer account with (UBUNTU-X)

Exercise 5.2: Kerberos SSH

Challenge

- Perform credential stuffing attack
- Gain ssh access to the host 192.168.**X**.209

Exercise 5.3: Shell Breakout

Challenge

- Break out of restricted SSH shell as tpv_user user.
- Execute *ip addr* as user tpv_user and store the output.

Bonus

- Identify Alternative breakout scenarios.

Exercise 5.4: Lateral Escalation

Challenge

- Find suid enabled binary with Env variable injection vulnerability.
- Exploit the vulnerability and elevate your privileges to dave.
- Perform a Shell Breakout and obtain full shell access.
- Obtain output of /etc/pwn1.txt as user dave using the SSH Shell.

Exercise 5.5: Apache

Challenge

- Read the file /home/dave/secret.txt on the host 192.168.X.209
- Obtain Reverse shell via webserver (id=www-data)

Bonus

- List at least 2 attack vectors for reading the aforementioned file

Exercise 5.6: X11

Challenge

- On what port is the X11 service running?
- Identify a vector from which you should be able to interact with the X11 service and obtain a screenshot of the desktop on remote host 192.168.X.209
- Obtain a reverse shell by exploiting this vulnerability.

Exercise 5.7: NoSQL Database Hacking + SSH Tunneling

Challenge

- Read the databases and identify the value of flag from mongoDB

Bonus

- Access mongoDB from your 192.168.X.209 kali machine / base (delegate machine)

Exercise 5.8: Privilege Escalation | Docker Breakout

Challenge

As limited user foo or tpv_user on 192.168.X.209:

- Identify ways to run Docker containers
- Identify containers and images available in the system
- Obtain root ssh access using docker and read /etc/pwn.txt on the host

Exercise 5.9: Post Exploitation

Challenge

- Obtain the clear text password for user foo

Lab Challenge 5.10: Persistence with Linux Capabilities

Challenge

- Using Linux capabilities, ensure
- Privileged read / write.
- Privileged execution.

Module 6: VPN Hacking

Exercise 6.1: VPN

Challenge

- Identify a VPN running on 192.168.3.211
- Identify a misconfiguration with the host
- Obtain the ID/group name
- Crack the PSK
- Use ~/Tools/VPN_Config/brute-xauth.sh to identify weak XAUTH credentials
- Connect to the internal network

Bonus

- On the VPN host, obtain access to the julie account
- On the VPN host, obtain access to the root account

Module 7: VLAN Hacking

Exercise 7.1: VLAN #1

Challenge

- Identify the protocols being broadcasted by the switch/routing device on the network
- Observe the traffic, and then answer the following questions:
    - Device name
    - IP address
    - Platform details
    - Software version
- Discover all the VLAN IDs on the network
- Find all the live hosts in the VLANs lower than ID 100

Info: The 3rd octet in the IP address relates to VLAN ID. For example, 10.10.100.210 means it's a host in the VLAN 100. This is a common naming notation for tagged traffic in the real world.

Exercise 7.2: VLAN #2

Challenge

You will have already identified an IP address of a device on VLAN ID 100. Continuing with this attack, perform the following tasks:

- Find the IP address of another device on VLAN 100 (hint - ARP!)
- Gain Telnet access to the second device (If you are connecting to the right device, you will be able to ping the IP and read it's custom telnet banner. Another hint is it's IP address is greater than 10.10.100.200)
- Gain 'enable' access to the device. You'll need to gain access to the Telnet interface (a common/default password value) and then learn to crack Cisco 'secret'/type 5 and type 7 passwords

Exercise 7.3: VLAN Double Tagging

Challenge

- The interface eth2 is connected to a switch in access mode.
- There is another machine sitting at 10.0.20.201 in vlan 20
- This machine has a vulnerable service “Log4j” running on UDP port 4712
- Exploit the machine and gain a reverse shell on kali using double tagging

Module 8: Cloud Pentesting

Exercise 8.1: FaaS / Lamda

Challenge

Access the web application hosted at **https://testlambda.notsofruity.com/pyshell?name=NSS**

- Determine (prove) what service the application is running on
- Identify a vulnerability in the application
- Exploit the vulnerability to expose sensitive internal information

Exercise 8.2: Metadata API #1, Token Enumeration

Challenge

- Use the information gained in the previous exercise to discover further accessible services

Exercise 8.3: AWS CLI and PaaS / S3

Challenge

- Configure the AWS CLI tool on your local machine to gain access to the AWS API
- Find and retrieve sensitive file(s) that might gain you additional further access

Exercise 8.4: IaaS / EC2, Metadata API #2 and Secrets Manager

Challenge

- Connect via SSH to an instance running in the cloud
- Find a way to explore the Metadata API
- Elevate your privileges within the AWS account
- Gain access to a hidden secret file and decode the hash