Cybersecurity Autumn 2023
Exercises Compendium

Magnus Christian Larsen

October 8, 2023

GitHub Username: Autowinto
Student Mail: magla21@student.sdu.dk
Project: https://github.com/Autowinto/JHotDraw
Date: mm/dd/yyyy

Contents

Info

Questions marked in bold are the important questions for report.
Currently in doubt about format of final report. Layout will change.

Exercise 02: Starting the Journey

Thinking About Threats

Answers based on the following relevant articles:

- Microsoft mitigates China-based threat actor Storm-0558 targeting of customer email
- Mitigation for China-based threat actor activity
- Results of Major Technical Investigations for Storm-0558 Key Acquisition

How did they separate access and infrastructure according to data relevance and impact?

They perform background checks, have dedicated identifiable accounts, secure access workstations and MFA using hardware token devices. They prevent the use of email and other communication tools which can compromise machines with malware or keylogs. They use Just in Time and Just Enough Access policies. They added the helper APIs, but failed to update relevant endpoint validation. Developers in other teams assumed that this validation was always performed and thus the disconnect happened.

How do roles and personnel fit into this, and which role could policies and training play?

Lack of evidence because of log retention policies. Because of a disconnect between team roles and personnel, validation was not performed.

Pentesting Intro

Which advantages for penetration testing would you see in the different approaches? What is the best option?

- NAT
- NAT Networks
- Bridged Networking
- Host Only

How does inspecting the ip configuration of a system help you with penetration testing? What is the security relevant aspect?

It does so by giving you info about all internet adapters, their protocols, their addresses, metrics, etc. etc.

How do you get the targeted user to execute our malicious payload?

Social Engineering, Disguising the file, exploiting vulnerabilities that allow for automatic code execution.

Is Metasploitable3 vulnerable to this exploit?

Testing the vulnerability is simple as connecting to the metasploitable vm and accessing sysinfo, verifying if it's correct. The vulnerability in this case, is an open nginx 8080 port, allowing us to connect. Metasploitable3 is very vulnerable to this exploit as it's designed to be so. It should close unused open ports, regularly update kernel and application versions, shut down unnecessary services and require validation before connection. It's quite easy to trick someone to download malicious files through torrenting, limewire, linkin-park-in-the-end.exe etc.

What is the practical use of this exercise? And why is the payload working in the way it is? How does this exercise relate to remote and reverse shells?

The practical use of this exercise is to see how easy it is to gain access to a vulnerable systems shell. The payload works how it does because

Which folder are you in when you get the meterpreter prompt? And whatis the system-information?

I am in the folder that the payload.efi was run at

As user and the owner of this system – how would you mitigate this attack?

By not chmodding and running payloads which I don't know what are smh.

How does knowing usernames help an attacker/penentration tester?

It's a significant advantage as it allows you to brute-force passwords much faster and ensuring that you are actually on a user with specific permissions.

Now that you have access to the Metasploitable machine what else can wedo? Get the list of users on this server, using a shell prompt by typing"shell" into the Meterpreter shell.

TODO

How does knowing usernames help an attacker/penentration tester?

It's a significant advantage as it allows you to brute-force passwords much faster and ensuring that you are actually on a user with specific permissions.

Using the meterpreter shell, check the output of the "arp" command. What do you find? Why could this information be relevant?

It displays internet-to-adapter address tables and when you're connected to a target machine, it shows the tables for that machine, which is very useful information when trying to penetrate.

Now lets be on the other side of the fence and investigate suspicious connections to our metasploitable server. Which command can you use to see network status and connections? Is there an anomaly or suspicious connection to our server? What makes it suspicious?

Unexpected source ip addresses, data transfers when you aren't expecting any, HTTP traffic on an unexpected port etc.

Exercise 03: General Assessment

Finding information with whois

Listing 1: Output of whois command

```
# Hello 185.136.116.160. Your session has been logged.
#
# Copyright (c) 2002 - 2023 by DK Hostmaster A/S
#
# Version: 5.1.0
#
# The data in the DK Whois database is provided by DK Hostmaster A/S
# for information purposes only, and to assist persons in obtaining
# information about or related to a domain name registration record.
# We do not guarantee its accuracy. We will reserve the right to remove
# access for entities abusing the data, without notice.
#
# Any use of this material to target advertising or similar activities
# are explicitly forbidden and will be prosecuted. DK Hostmaster A/S
# requests to be notified of any such activities or suspicions thereof.

Domain:                 sdu.dk
DNS:                    sdu.dk
Registered:             1997-10-09
Expires:                2023-12-31
Registration period:    5 years
VID:                    no
DNSSEC:                 Signed delegation
Status:                 Active

Registrant
Handle:                 ***N/A***
Name:                   Syddansk Universitet (University of Southern Denmark)
Address:                Campusvej 55
Postalcode:             5230
City:                   Odense M
Country:                DK

Nameservers
Hostname:               ns1.sdu.dk
Hostname:               ns2.sdu.dk
Hostname:               ns3.sdu.dk
```

What do you learn about SDU's network? In the protocol, note the IP range.

We learn a whole lot about the network such as the date registered, the expiration date, address of registrant and hostnames.

Are there other Networking-Services @SDU which you could try?

TODO

What is the whois information for nextcloud.sdu.dk? What do you observe in comparison to the whois-information you gathered for www.sdu.dk

TODO

Question: nmap

Nmap scans can be set up to evade firewalls. Which tags would you use for sending packets with specified ip options?

Nmap scans can be set up to evade firewalls. Which tags would you use for spoofing your MAC address?

Scanning the Metasploitable VMs

TODO

Scanning with Legion

TODO

Scanning with Nessus

TODO

Scanning with the Greenbone Vulnerability Manager (GVM)

TODO

Comparing the Tools

†Compare your results from each of the previous activities in each question (e.g., sparta vs nessus vs openvas). Take notes and discuss overlaps and differences in results, pros and cons, ease of use for each tool.
TODO

Collecting the Assessment Information

Find possible vulnerabilities with metasploitable3 (both Windows and Ubuntu). State tools and resources used and then select 4 vulnerable services for each of the metasploitable VMs for which you document the following:

†Service, port number and version number, e.g., FTP 21 vxxxx TODO

†Describe or explain at least one vulnerability that you found for that service, i.e., what is the underlying issue and what can be achieved? How severe is that issue? (You do not have to state how to exploit the vulnerability or go into technical details. We will look into this later btw. The intricate technicalities are mostly outside the scope of the

course.) But make sure you describe what possible outcomes of the exploit are, what the impact for a real system were and how criticial you would assess the issue due to the effects, i.e., argue for your assessment
TODO

†For each of the vulnerabilities in the previous point, note the CVE and/or Source of information about the vulnerability for that version. Using metasploit's info command might help you here, if you want to go to the command line.
TODO

Completing the Assessment

†Create a final report, extending the collected information with an overall review of the security concerns in both the Metasploitable-3 Windows and Ubuntu systems, e.g., different criticality levels of the services (an overview of how bad the situation is) and which ones to to be prioritized when addressing security issues (a selection of the most relevant issues for prioritisation). For this use a combination of the results from the tools that you used or one of the tools.

Note, that you shouldn't just copy and paste the severity of the tools you use, but read through the CVE you selected and try to determine how critical it is. I.e., what is the possible impact? Is the service inoperable, or is intellectual property at risk?
TODO

Exercise 04: SQL Injection

Nessus does say it was unable to get version number for the MySQL serverbecause it is restricted.
†Does it mean the MySQL server is protected against cyber attacks?

try command mysql -h ¡METAPLOITABLE IP¿ -P 3306
†How could that protection look like?
†And what exactly would it protect against?

Spying with SQL Injections

†And what exactly would it protect against?

Exercise 05: Drupal