CSCE 5399 – Network and System Security

Take Home Midterm Exam

Name: Naveen Ajay Karasu EUID# Nk0741

Please put your name on all pages if you print and scan this back in.

Be succinct in your answers… I’m not looking for wordy answers, just brief and complete. **Any copying and pasting of answers from any source will result in 0 points for the entire question**. You are welcome to use any resources except other people/classmates, but make sure your answers are relevant to the material we have covered in class.

1. Information Gathering

a. Describe the difference between active and passive information gathering.

Ans: Active: In this we try to gather information by directly connecting to the target. Like using nmap, telnet, burpsuite in case of webpage to inspect get and post requests.  
 Passive: In this we don’t touch the target directly, we try to gather info from other sources like google, news channel, social media etc..,

b. What are some passive information gathering techniques (not tools)?

Ans:

* We can google about the target.
* We can check social media pages of the target.
* We can connect with people from target to get more information about inside using a excuse that you’re looking for a job.

c. What are some active information gathering techniques?

Ans:

* Basic one will be using nmap scan on the target network for getting all the list of open ports
* Burpsuite to intercept the request sent to the server and modify it create an injection attack to get information on type of database and version of it used.
* We can introduce our self as news article writer and wanted interview people working in so and so field. This might give you access to the office perimeter which then you implant transmitters, spy cam which can be used to gather more information.

d. When would one use active?

Ans:

* When the target has large traffic and we can be invisible or hide in the traffice
* Trying get more information on the type of software or hardware used by the target.
* What type of services the target uses along with the version of the service from hitting the target with wrong information to get error message, which can be used to get above details.

e. When would one use passive?

Ans:

* When the target is very sensitive or have strict control over the traffic
* Don’t want to leave any footprint in their system

2. What is the benefit of learning to think like a hacker? Answer from a business perspective. Use examples that relate to the PROTECTION of the systems being analyzed.

Ans:

Learning to think like hacker give us the perspective how a hacker sees the system and what part he thinks is has value, which may not be important to the target.

From business perspective, we can plan accordingly to protect and keep the running in case attack by having business continuity and Disaster recovery plans and having hacker mind can help in creating a better Risk analysis report and provide the rough estimate for the loss can occur to the target in terms of business.

3. You have port scanned an Internet-facing web server. The following ports are open. 23, 80, 443, 8080 and 63524. What can you tell me about this server from a security perspective? Think like an attacker… how does she see this server? What steps would you take next to plan your attack?

Ans

Port 23: Telnet, 80: HTTP, 443: HTTPS, 8080: HTTP alternative, 63524: No well known source for this port

From Attacker perspective, I can make a phisping email and create a redirecting link which used http instead of https exclusively using port 80 or 8080 instead of 443, and then view the trafice to collect sensitive information like usernames and passwords.

As it uses port 23 instead of port 22, we can perform MITM attack and read the traffic to get login details and files or commands sent to the server.

As for port 63524, we can try to access the website using that port and see what type of message or error we get which can help us understand what type of service is using that port.

After gathering some information, we can try to login into the telnet server and make changes or insert malicious code and backdoor and then earse our steps to have not trace of our attack and legitimate access to the target from the backdoor created earliar.

5. You are asked to set up a vulnerability management system (ongoing vulnerability scanning and remediation) for an Extranet containing approximately 1200 devices (aka nodes). The machines are spread across an entire class B network which has been divided into subnets using the mask 255.255.255.0. All subnets are not being used. The customer has given you a list of assets and IPs, but many domains are dynamic or virtual or contain laptops and other nomadic/mobile devices.

1. The customer has given you an asset list and feels that this is good enough for you to work off of, what do you tell them? What are the challenges with discovery on this network and how do you overcome them?

Ans: List of assest is might not be enough because that it doesn’t tell the status of the device in the network, type of device given above etc.,

The challenge we might face is with the devices whose ip changes each time it gets connected and disconnected, we might be able to get the browser version but some times not knowing underlying os might make our less effective due to platform compatibility of the attack.

So, to overcome this challenge, we might request more informationon the target or we can save the mac addresses to map the devices in the network more accurately.

1. Not having much detail about their network architecture, but knowing there are firewalls, proxies and load balancers in place, what issues should you be aware of, and what general principles would you strive to obey.

Ans:

Knowing about the firewalls , procies in the system can make the attacker think ahead of time used ports which are open and been used more, this helps in understanding how they filter the data via network. So, we can craft the packet in a way It remains authentic that the firewall doesn’t stop the request.

c. Further, what questions would you ask before deciding on a solution and architecture?

Ans:

* Type of data the company deals with.
* Sensitivity of the data
* How the resource are allocated and what ports are they running
* What’s budget allocated for this company.
* Know more about, how they setup the firewall and proxy and their there rules.

6. Describe the underlying security issues described by Dan Kaminsky with the DNS protocol and give a basic explanation how an attacker could take advantage of it.

Ans:

Dan Kaminsky discovered an security issue with the DNS protocol known as DNS cache poisoning in 90’s. Which resulted in a attack in 2008. This vulnerability resulted in allowing attackers to manipulate DNS records in a way that redirects users to malicious websites instead of legitimate ones using DNS caching CDN.

In detail, The attacker exploits by injecting false DNS information into a DNS cache, tricking users into visiting malicious sites when they intended to visit safe ones. This could result in various malicious activities, such as phishing attacks, data theft, or spreading malware.

“According to Dan, they didn’t actually repair DNS, they just took a 16-bit transaction identifier and used UDP source ports as a hack to get a 32-bit transaction identifier.” Didn’t understand what it actually means, What I got from it is instead of resolving the threat they are just trying to overwrite the malicious one.

Ref: T.T. (2016). The great dns vulnerability of 2008 by dan kaminsky. <https://duo.com/blog/the-great-dns-vulnerability-of-2008-by-dan-kaminsky>

7. Port scanning is often one of the first security testing mechanisms used in a penetration test. However, it’s not necessarily a technique often used by real threats today (i.e. – those starting as attacks of opportunity). Justify the use of port scanning in a pentest.

Ans: Pentesting doesn’t only mean attacking the websites, networks and servers. So, When we are try to hack the hardware like motherboard, it might not necessary deal with ports. But knowning what ports are used can play a important role as we will know which part of the motherboard is used for different type of operation. Which can help us understand underlying working of the system indetail, So the attacker might use this information by sending fake signal or request to cpu and access the it resources to perform malicious activity.

Like if we know how the communication between processor is done for regulating the temperature around the processor, we can create a fake process to invoke and shutdown the cpu.

8. The command “nmap 10.1.1.2” would perform a default scan against the specified target. Why do you need to know anything else about nmap? Think about what this exact command may or may not include. (Note: “In order to avoid being a scan monkey” is a good answer, but I need more than that.)

Ans:

Nmap [ipaddress] is the basic command. We have many different variations of it and different types of flags available to us to use like syn flag, xmas flag, flag for getting udp ports, flag for getting tcp ports. The basic scan only checks for top 1000 most used port and gives the result, We can also give the range to check if there are any ports open and running in the given range. We also have different type of level or speed for nmap pining the target, from T1 to T5, T5 being the most noise one. This can help us prevent being discovered by the target firewall. As the average pings allowed by a ip is aroung 15-20 per second for public facing website and it may vary depending on the level, regional the target is operated.