Assignment 1

New Attempt

- Due Sep 17, 2024 by 11:59pm
- Points 100
- Submitting a file upload
- File Types pdf

Due: September 17, 2024 (11:59 PM). Please submit your assignment on Canvas as a PDF.

Information Gathering: Understanding the Target

Information gathering is the first step of the penetration testing process. To be able to carry out penetration testing, you need to gather information about the target. The more information you have about your target the more chance of success. In this assignment, you perform passive and active information gathering using open-source intelligence and vulnerability scanning tools such as Dig, Nmap and Nessus. You will scan a network to identify possible targets and then identify their potential vulnerabilities to use in the next phase of penetration testing, vulnerability exploitation.

Setup

For this assignment, you will need the following VMs: Router, Kali, Windows 7. Confirm that Kali & Windows 7 have Internet access.

Tasks

1 Passive Information Gathering

Passive Information Gathering is generally only useful if there is a very clear requirement that the information gathering activities never be detected by the target. Passive information gathering is done using publicly available information. Passive information gathering is usually challenging to perform as we are never sending any traffic to the target organization neither from one of our hosts nor “anonymous” hosts or services across the Internet. This means we can only use and gather archived or stored information. Such information can be out of date or incorrect meaning that we are limited to results gathered from a third party in this process. Passive information-gathering activities include but are not limited to identifying IP addresses and sub-domains, people, technologies, the content of interest, and vulnerabilities of the target organization. To gather this information a PenTester does not use intrusive scanning but only uses public domain applying techniques and tools available to everyone. This is an important step as it will make the later activities more focused.

1.1 OPEN SOURCE INTELLIGENCE [20%]

Passive information gathering is also referred to as open source intelligence (OSINT).

Task 1: Select a technology company that you have never heard of. Perform a thorough passive information gathering on the selected company and present your results in a brief report. Include your methodology and rationale in information gathering. Report the results of using at least two open source intelligence tools such as Maltego, theHarvester, Shodan, Recon-ng, SpiderFoot and Censys in your information-gathering process.

Collect information across multiple categories such as:

- **Corporate Structure:** Ownership, subsidiaries, key personnel
- **Digital Footprint:** Domain information, server details, digital infrastructure
- **Social Media Presence:** Social network analysis, mentions, and engagements
- **Product and Service Offerings:** Detailed descriptions and market positioning
- **Compliance and Legal:** Regulatory filings, compliance issues, legal proceedings

Identify any potential privacy concerns based on the company's digital footprint. Include any data privacy laws or regulations considered to ensure compliance with ethical standards.

1.2 DNS SERVER INTERROGATING [20%]

DNS is a hierarchical tree-structured system. Each time you look for a domain name the query proceeds recursively into the hierarchy starting at the root. DNS servers are entrusted to translate human-readable domain names to IP addresses. It is not uncommon for organizations to use more than one domain for a single IP address. As a result, DNS service potentially can provide valuable information about an organization's public footprint and potentially expose an attack surface.

In the following tasks, you will use the dig tool to explore the DNS servers to gain information about the target organization. dig which stands for domain information groper is a software tool for interrogating DNS name servers. It performs DNS lookups and displays what name server(s) return in response to queries.

Setup: Dig is pre-installed in Kali Linux.

Here is an example of how to use dig:

```
root@kali:~# dig google.com

; <<>> DiG 9.11.3-1ubuntu1.8-Ubuntu <<>> www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38585
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.google.com.                        IN      A

;; ANSWER SECTION:
www.google.com.         284     IN      A       172.217.14.196

;; Query time: 3 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
```

```
;; WHEN: Mon Aug 12 17:05:40 PDT 2019
;; MSG SIZE  rcvd: 59
```

At the bottom, we can see that our query is sent to the server (127.0.0.53), and it took 3 milliseconds to respond. The Answer Section is as follows

```
;; ANSWER SECTION:
www.google.com.         284     IN      A       172.217.14.196
```

This tells us that the result is type A which is an address record, and the IP address of the name “google.com” is 172.217.14.196. The expiry time is "284" indicating that this record is valid for three minutes. The "class" field is usually always IN for the Internet.

1.2.1 BASICS

Task 2: Using dig find the IP address of **www.sfu.com (http://www.sfu.com/)** . What is the IP address?

Task 3: The returned answer from the previous task includes a CNAME part. What does this mean?

1.2.1 UNDERSTANDING HIERARCHY

Run the command:

```
dig -t NS.
```

This command provides information about the nameservers in the root hierarchical level of domain names.

Task 4: Run a query to ask a root server about **mail.sfu.ca** without using recursion (Hint use the @ for directing the query to a specific root server). What command did you use? What is the result of the query?

Task 5: The answer to the previous task will not give you the IP address of **mail.sfu.ca**. Instead, follow the “path” down in the hierarchy of the nameservers to find the address of **mail.sfu.ca** without using recursion. What commands did you use? What is the IP you found?

2 Active Information Gathering

In active information gathering, PenTester engages actively with the target and because of that, the targeted organization may become aware of the process. Active information gathering usually starts with mapping the network and scanning the open services for vulnerabilities.

2.1 NETWORK MAPPING AND PORT SCANNING [40%]

If you know the network you are interested in targeting but not the specific IP addresses you need to scan the target network. In the following tasks, you will learn how to use Nmap for network scanning. Nmap (network mapper) is a software tool to discover hosts and services on a computer network by sending packets and analyzing the responses. Once you know the IP address of the target you can learn more about it through port scanning. Port scanning is the act of remotely testing ports to find out

what state they are in. When a port is open this means that an application is listening and accepting connections on that port.

Setup: Nmap is preinstalled in Kali Linux. To do the following tasks you need to open and run Kali Linux VM, and a Windows 7 VM in the same local network.

Task 6: What is the IP address of the local network in the form of IP/netmask? What command did you use to find this?

Task 7: Perform a **full ping** scan in the local network using Nmap and identify all potential targets. Report the results of the scan and point to the IPs of the potential target machines. What commands did you use to scan the network?

Task 8: Perform a TCP SYN scan on the target using Nmap. Report the result. What command did you use to perform the scan? Perform a **TCP full scan** for TCP SYN scan. Report the result. What command did you use to perform the scan? What is the difference between this method of scanning and the one that you used for the TCP SYN scan?

Task 9: Perform full port scanning on the target. Report the results. Can you infer the operating system from the results? If yes, indicate how. If not explain why.

Task 10: Different ways exist to identify a target's operating system. Using Nmap shows **two** different ways to do that. Report the results and associate the IPs with the operating systems.

Nmap Scripting: Nmap's Scripting Engine (NSE) (https://nmap.org/book/man-nse.html) extends its capabilities by enabling automated tasks such as network discovery, vulnerability detection, and exploitation. Written in Lua programming language, these scripts can perform a range of functions, including version detection, brute-forcing, malware detection, and custom scanning. While Nmap comes with a large collection of pre-built scripts, users can also create or modify scripts to fit specific requirements.

Task 11: Use an Nmap script to check if the target machine is vulnerable to the EternalBlue exploit. Provide the script name, the exact command you used, and report the results of the scan.

2.2 VULNERABILITY SCANNING [20%]

In the following tasks, you will use Nessus to perform an advanced scan on the target. Nessus is capable of scanning a wide range of technologies including operating systems, network devices, hypervisors, databases, web servers, and critical infrastructure to detect vulnerabilities that could allow unauthorized control or access to sensitive data on a system.

Setup: Nessus is usually not distributed with Kali. You can check if it is installed by running

```
service nessusd start
```

If you get an error that means Nessus is not installed. To install Nessus you should:

- Download it from here (https://www.tenable.com/downloads/nessus) and click debian6_amd64.deb
- Right click the downloaded file, select Open with other application, and select Software

- After the installation open a terminal and type `service nessusd start`
- Open Firefox and navigate to **https://localhost:8834 (https://localhost:8834/)**
  - In the case you see a certificate error try to add an exception in your browser
- Go to **this (https://www.tenable.com/products/nessus/activation-code)** link and click Register Now in the Free Plan (Nessus Essentials)
- Select a new username and password for Nessus and when prompted use the activation code you obtained from registering for Nessus
- Wait to download and install the plugins (This can take 20-30 minutes)

Task 12: Perform an advanced scan on the Windows 7 target machine. Report the high/critical vulnerabilities of the system. Which of these could be used directly to exploit and gain access to the target system and which to gain more info or perform a denial of service attack according to your opinion?