OCR@UC Lab

Lab 1 - OSINT Tools (Module 3)

LESSON TITLE:

WARNING:

Warning: Any use of penetration testing techniques on a live network could result in expulsion and/or criminal prosecution. Techniques are to be used in lab environments, for educational use only or on networks for which you have explicit permission to test its defenses.

Level:

☐ Beginner
☒ Intermediate
☐ Advanced

Audience: ☒ Instructor-led
☐ Self-taught

Lesson Learning Outcomes: Upon completion of this lesson, students will be able to:

- Demonstrate the use of public internet resources for passive recon
- Demonstrate the use of port scanning for active recon

Materials List:

- Internet connection
- Browsers: Firefox (preferred), Google Chrome, or Internet Explorer
- Intro to Ethical Hacking lab environment

Introduction

In this lab we will explore using some of the various tools used in open source intelligence gathering. Follow the steps below and answer all questions in your own words with as much detail as possible. Paste screen shots where requested. Turn in the entire document to your instructor. Include your username in the filename.

Systems/tools used:

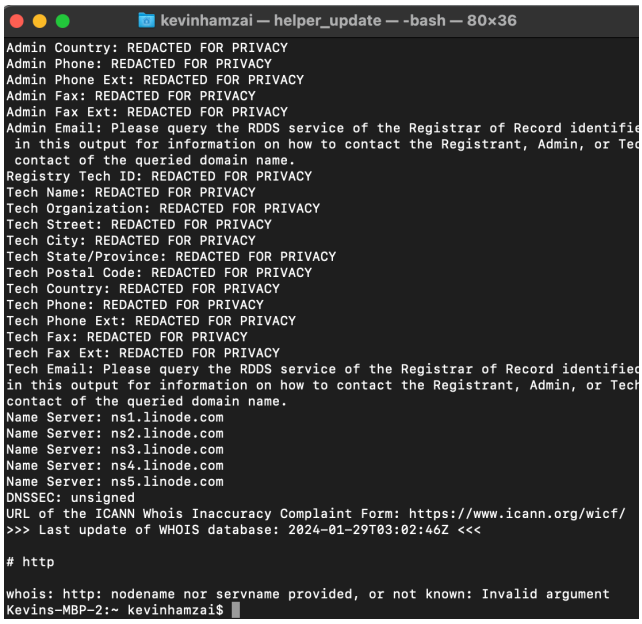
- Kali Linux *(u: root, p: toor)*
- Web browser

Module Activity Description:

Part One: Passive Recon (does not require range access)

Run a whois command on nmap.org.

1. **Paste a screen shot of the information returned.**



2. **What specific information from these results might be useful for a penetration tester?**

   DNS info, domains ip address admin name, domain information and personal contact information.

   Domain name nmap.org

   Registrar WHOIS Server: http://whois.dynadot.com

   Registrar : Dynadot, LLC

   Email : abuse@dynadot.com

   Phone : +16502620100

   Country : US

3. **What other tools/services could you use to find similar information?**

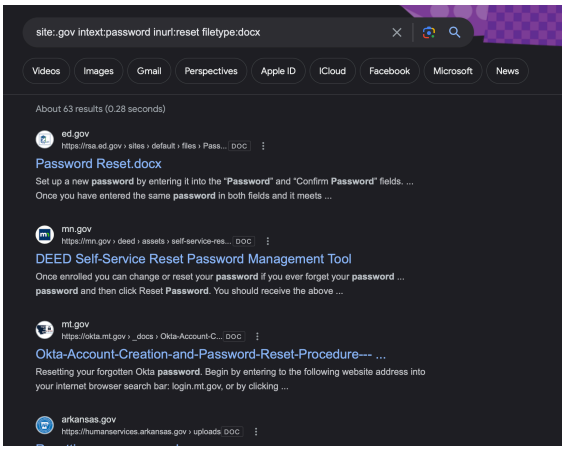
Dig : DNS lookup tool that provides domain info, Nslookup, WHOIS lookup services, Domaintools

Using Google Dorks, run a search and narrow the results to only include: all .gov TLDs, the term "password" inside the body of the page, the term "reset" in the URL, and only return .docx files.

1. **What was the search query that you used?**

Site: gov intext:password inure:reset filetype:docx

2. **Past a screen shot of the results of the Google Dorks search results.**

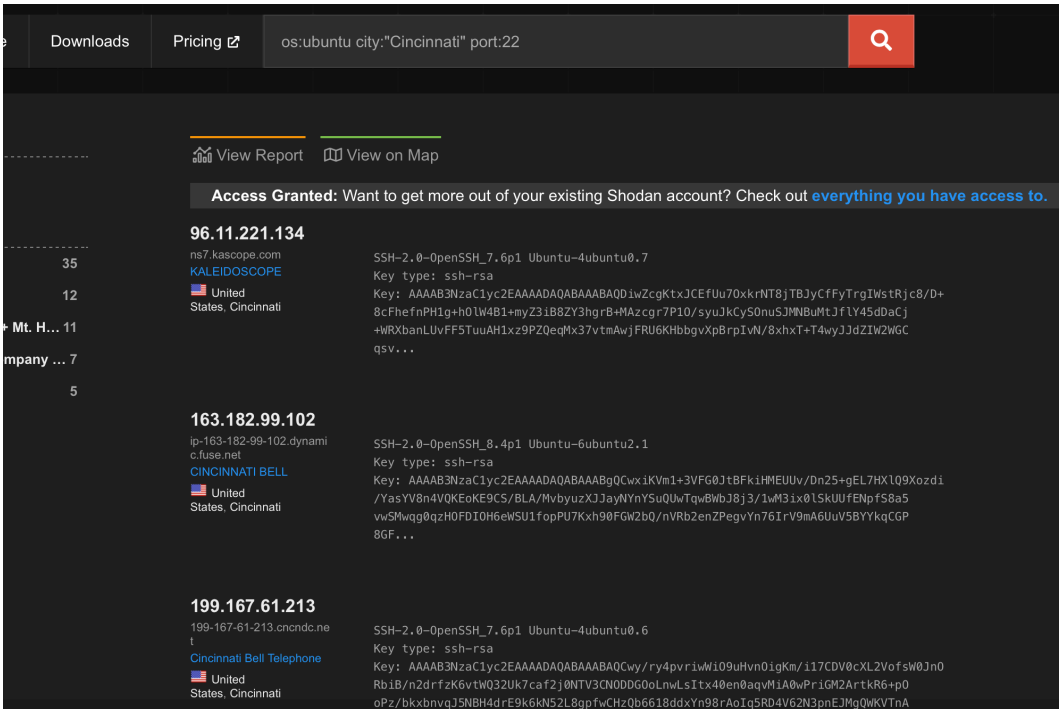


3. **Open a few files. Why might this information be useful to a penetration tester?**

They can use email addresses on the website and use them to attack the users. theHarvester can be used and a tool called jigsaw. A pen tester can use LinkedIn to find employees of the target organization and after that they can get their email addresses just by guessing based on their company. Phishing can also take place. There is entry points for spear phishing attacks and also password spraying if the users have weak passwords.

Register for a free Shodan account (www.shodan.io). Research how to use search operators in Shodan and run a search to return results that have an Ubuntu server running with port 22 open and based in Cincinnati, OH.

1. **Past a screen shot of your results.**



Caption

2. **What version of SSH is running on the first returned result?**

SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7

3. **Click though the first link. Are there any interesting vulnerabilities?**

There are three open ports, which are 22, 80 and 443

Version information and operating system

Hackers can exploit these ports and having the version information can be helpful to the hacker so they new which update the system is on and can reveal vulnerabilities to specific software versions, and having the operating system can help tailor attack strategies to target weaknesses.

Module Activity Description:

Part Two: Active Recon (Requires range access)

Run an nmap scan against scanme.nmap.org

1. **Paste a screen shot of the results.**

```
┌──(root㉿kali)-[~]
└─# nmap scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2023-09-10 20:30 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.012s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 9.27 seconds
```

2. **Explain what information from this scan may be useful to a penetration tester.**

IP address and the host name, knowing the host name and the IP can help a pen tester in other attacks. It shows the latency which can show the response time and see if the network gives them a quicker feedback time. Open ports can be exploited for vulnerabilities

Run another nmap scan against scanme.nmap.org. This time include the options to include version detection, the top 13 ports, and operating system detection

3. **Paste a screen shot of the results.**

```
┌──(root㉿kali)-[~]
└─# nmap -sV -f  --top-ports 13 -O scanme.nmap.org

Starting Nmap 7.92 ( https://nmap.org ) at 2023-09-10 20:41 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.030s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f

PORT     STATE    SERVICE       VERSION
21/tcp   filtered ftp
22/tcp   open     ssh           OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
23/tcp   filtered telnet
25/tcp   filtered smtp
53/tcp   filtered domain
80/tcp   open     http          Apache httpd 2.4.7 ((Ubuntu))
110/tcp  filtered pop3
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
143/tcp  filtered imap
443/tcp  filtered https
445/tcp  filtered microsoft-ds
3389/tcp filtered ms-wbt-server
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP
Running: Actiontec embedded, Linux
OS CPE: cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel
OS details: Actiontec MI424WR-GEN3I WAP
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.40 seconds
```

4. **What OS is this system running (Best guess)?**

Ubuntu Linux

5. **What version of Apache is this system running?**

Apache https 2.4.7 ((Ubuntu))

6. **If nmap cannot determine if a host is alive or not, what is the most likely explanation?**

It assumes the host is up and continues with the requested scanning functions

7. **How could you bypass the above?**

Use -Pn option which tells map to skip the host discovery phase

8. **Explain the difference between a –sS and –sT scan? Which is faster and why?**

   -sS is a SYN scan and it initiates the start of a TCP handshake but does not complete it. -sT scan is a TCP connect scan and completes the full TCP handshake. -sS is faster but it doesn't make a full connection, -sS is less likely to be logged, while -sT scans are more detectable since they create complete connections