Cybersecurity Fundamentals (CS3308/7308) Assignment 3 Example Answers

Question 1 (1point)

What is the DNS server software/product name and version running on the host 10.0.0.17 (ns1.hacklab)?

Use nmap with "-A" option to fingerprint the service(s) running on 10.0.0.17.

Answer: Bind 9.9.4 (RedHat)

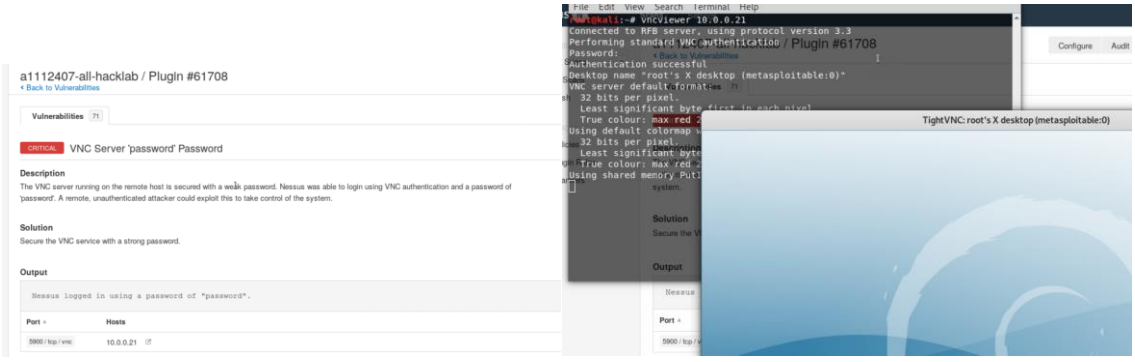
```
root@kali:~# nmap -sU -A 10.0.0.17 -p 53
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-29 21:47 EDT
Nmap scan report for 10.0.0.17
Host is up (0.061s latency).

PORT   STATE SERVICE VERSION
53/udp open  domain  ISC BIND 9.9.4 (RedHat Enterprise Linux 7)
| dns-nsid:
|_  bind.version: 9.9.4-RedHat-9.9.4-73.el7_6
| dns-recursion: Recursion appears to be enabled
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:redhat:enterprise_linux:7

TRACEROUTE (using port 53/udp)
HOP RTT      ADDRESS
1   62.58 ms 10.0.0.17

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 16.26 seconds
```

Question 2 (1 point)

Based on (i.e., taking advantage of the vulnerability) the Nessus scan results for the server on 10.0.0.21 (or 10.0.0.32), obtain a screenshot of the (graphical) desktop of this server.

Nessus scan discovered a VNC server with password of "password".

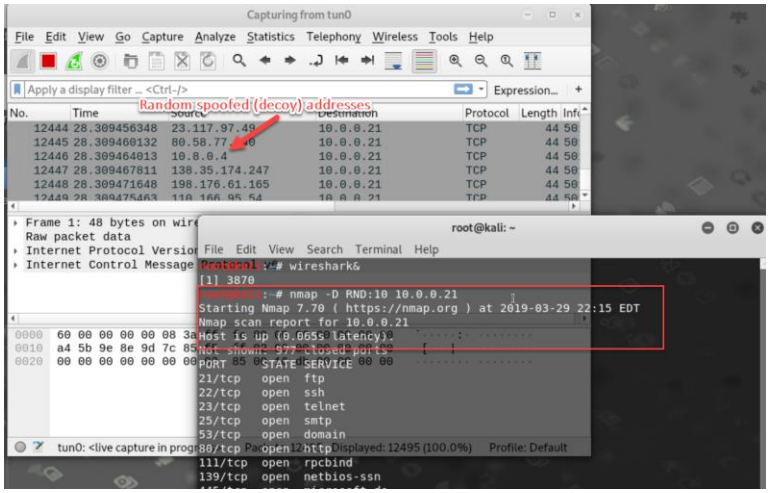
Connect to it using vncviewer.



Question 3 (1 points)

Use the Nmap decoy option (-D please read the Nmap manual for how to use this option) against any single host in the UofA Hacklab, and capture some packets using Wireshark during the scanning. Paste a screenshot showing packets coming from a spoofed source IP address, along with your real IP address. How could the decoy option be useful for a black hat hacker?

You can specify specific spoofed (decoy) IP addresses, or let nmap choose random IP addresses as follows.

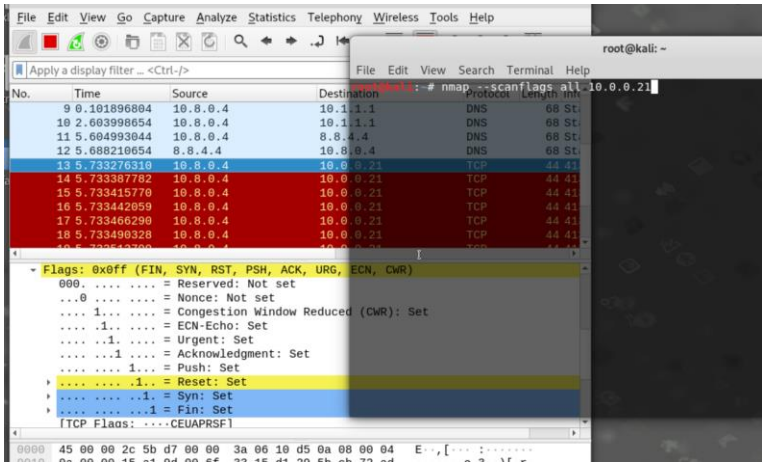


Question 4 (1 point)

Nmap allows you to turn TCP flags on and off individually. Come up with a command that turns on ALL six flags on, scan a test host, capture the initial packet using Wireshark. Paste (a) the command and (b) a screen shot from Wireshark showing all the flag bits set to 1 (similar to this but with all flags set to 1).

You can use one of the following options

- --scanflags ACKFINURGPSHRST SYN
- --scanflags all



Note that the question mentioned 6 flags, but there are actually now **8 flags**, including CWR and ECN (new flags used for congestion control).

Question 5 (1 point)

There is a network service running on 10.0.0.35 (knock.hacklab) behind a port somewhere between 20000 and 60000. Identify the port number and connect to it using netcat ("nc" or "netcat" command. Use --help to find usage) to retrieve the secret.

- Simply scan with option “-p 20000-60000” to specify port range then use nc (or telnet) to connect to the port

```
root@kali:~# nmap -sS -n -p 20000-60000 10.0.0.35
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-29 22:37 EDT
Nmap scan report for 10.0.0.35
Host is up (0.064s latency).
Not shown: 40000 filtered ports
PORT      STATE SERVICE
54127/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 107.45 seconds
root@kali:~# netcat 10.0.0.35 54127
 _____________________________________
/ demure martial wellborn finochio \
\ shindig echidna                   /
 -------------------------------------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||
root@kali:~#
```

Question 6 (2 point)

The host 10.0.0.35 (knock.hacklab) is running what's known as a "port knocking" with the following configuration: The host 10.0.0.35 (knock.hacklab) is running what's known as a "port knocking" with the following configuration:

/etc/knockd.conf

```
[options]
        UseSyslog

[opencloseWWW]
        sequence      = 2222:udp,3333:tcp,4444:udp
        seq_timeout   = 15
        tcpflags      = syn
        start_command = /bin/firewall-cmd --zone=public --add-rich-rule="rule family="ipv4" source address="%IP%" service name="http" accept"
        cmd_timeout   = 3
        stop_command = /bin/firewall-cmd --zone=public --remove-rich-rule="rule family="ipv4" source address="%IP%" service name="http" accept"
```

As you can see, it is configured to open HTTP (port 80) for 3 seconds after the predefined knock sequence. Write a script (or use some tool) to execute the sequence and grab the secret at http://10.0.0.35/secret.

You could either use nmap script or install the knock client that comes with knockd (apt install knockd). Make sure to switch between UDP and TCP.

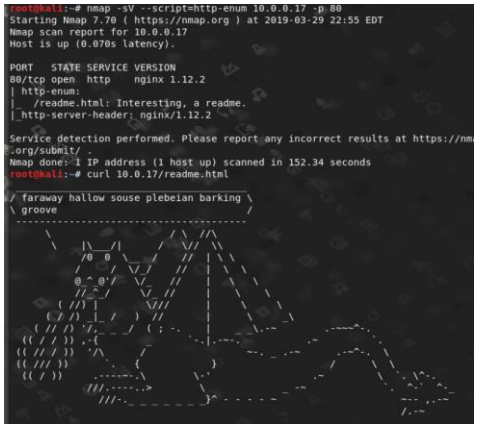
```
root@kali:~# cat knock.sh
#!/bin/bash
nmap -Pn -sU -n 10.0.0.35 -p 2222
nmap -Pn -sS -n 10.0.0.35 -p 3333
nmap -Pn -sU -n 10.0.0.35 -p 4444
sleep 1
curl http://10.0.0.35/secret
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-29 22:48 EDT
Nmap scan report for 10.0.0.35
Host is up (0.060s latency).

PORT     STATE    SERVICE
3333/tcp filtered dec-notes

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-29 22:48 EDT
Nmap scan report for 10.0.0.35
Host is up (0.060s latency).

PORT     STATE    SERVICE
4444/udp filtered krb524

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
 _____________________________________
/ polypody viva cadaver epilogue sinner \
\ fried                                 /
 -------------------------------------
    \
     \                          I
                                  .::!!!!!!!:.
  .!!!!!:.                       .:!!!!!!!!!!
  ~~~~!!!!!.                 .:!!!!!!!!UWWW$$$
      :$$NWX!!:           .:!!!!!!XUWW$$$$$$$$P
      $$$$$##WX!:      .<!!!!UW$$$$"  $$$$$$$#
      $$$$$  $$$UX   :!!UW$$$$$$$$   4$$$$$*
      ^$$$B  $$$$\     $$$$$$$$$$   d$$R"
        "*$bd$$$$      '*$$$$$$$$$$o+#"
             """"          """""""
```

Question 7 (2 points)

Nmap supports custom scripts (programmed in the Lua language) to extend its scanning capabilities. When you run with the -A switch, Nmap runs all "default" scripts, and you can specify specific scripts using the --script= option in the command line. The pre-installed scripts are located under /usr/share/nmap/scripts/*.nse and documentation is available at https://nmap.org/nsedoc/.

There is a standard script called **http-enum** (https://nmap.org/nsedoc/scripts/http-enum.html) that enumerates (does a dictionary attack) against an HTTP web server using a default "fingerprint" file (see /usr/share/nmap/nselib/data/http-fingerprints.lua for the content) to find interesting files and directories. Run this script against 10.0.0.17 (ns1.hacklab) to find an interesting file. Get the content of that file.



Question 8 (1 point)

Look up the CVE for a vulnerability known as "drupalgeddon2" and find out the CVSS 3.0 Vector String and Base Score. What software and version does this vulnerability affect?

CVE-2018-7600 Detail

Current Description

Drupal before 7.58, 8.x before 8.3.9, 8.4.x before 8.4.6, and 8.5.x before 8.5.1 allows remote attackers to execute arbitrary code because of an issue affecting multiple subsystems with default or common module configurations.

Source: MITRE
Description Last Modified: 03/29/2018
View Analysis Description

Impact

CVSS v3.0 Severity and Metrics:
Base Score: 9.8 CRITICAL
Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H (V3 legend)
Impact Score: 5.9
Exploitability Score: 3.9

Attack Vector (AV): Network
Attack Complexity (AC): Low
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Unchanged
Confidentiality (C): High
Integrity (I): High
Availability (A): High

CVSS v2.0 Severity and Metrics:
Base Score: 7.5 HIGH
Vector: (AV:N/AC:L/Au:N/C:P/I:P/A:P) (V2 legend)
Impact Subscore: 6.4
Exploitability Subscore: 10.0

Access Vector (AV): Network
Access Complexity (AC): Low
Authentication (AU): None
Confidentiality (C): Partial
Integrity (I): Partial
Availability (A): Partial
Additional Information:
Allows unauthorized disclosure of information
Allows unauthorized modification
Allows disruption of service