

Assignment 3

1)

When I used the `fpdns -D` on the host IP I was able to get DNS server software/product name and version running on the host 10.0.0.17

Command: `fpdns -D 10.0.0.17`

Software version: 9.6.3 -- 9.7.3

Software name: ISC BIND

```
root@kali:~# fpdns -D 10.0.0.17
fingerprint (10.0.0.17, 10.0.0.17): ISC BIND 9.6.3 -- 9.7.3 [New Rules]
root@kali:~#
```

2) The Nessus scan results for the server on 10.0.0.21 and the graphical desktop screenshot of the server is :

The screenshot shows the Nessus web interface for a scan of host `a1715329 / 10.0.0.21`. The left sidebar contains navigation options like Folders, My Scans, All Scans, Trash, Resources, Policies, Plugin Rules, and Scanners. The main content area shows a table of vulnerabilities with columns for Severity, Name, Description, and Count. The table lists several critical vulnerabilities, including SSL (Multiple Issues), Bind Shell Backdoor Detection, NFS Exported Share Information Disclosure, rexecd Service Detection, Unix Operating System Unsupported Version Detection, and VNC Server 'password' Password. A 'Host Details' panel on the right shows information about the host, including IP, MAC, OS, Start/End times, and Elapsed time. A 'Vulnerabilities' chart at the bottom right shows a distribution of vulnerability severity levels: Critical, High, Medium, Low, and Info.

Sev	Name	Description	Count
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3
CRITICAL	Bind Shell Backdoor Detection	Backdoors	1
CRITICAL	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	rexecd Service Detection	Service detection	1
CRITICAL	Unix Operating System Unsupported Version Detection	General	1
CRITICAL	VNC Server 'password' Password	Gain a shell remotely	1
MIXED	DNS (Multiple Issues)	DNS	6
MIXED	SSL (Multiple Issues)	Service detection	3
MIXED	Web Server (Multiple Issues)	Web Servers	3

Host Details

- IP: 10.0.0.21
- MAC: FA:16:3E:B2:C3:84
- OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- Start: Today at 9:01 AM
- End: Today at 9:07 AM
- Elapsed: 6 minutes
- KB: [Download](#)

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

VNC server password:

Nessus Scans Settings

FOLDERS

- My Scans 2
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Scanners

a1715329 / Plugin #61708 [Back to Vulnerabilities](#) [Configure](#)

Vulnerabilities 69

CRITICAL VNC Server 'password' Password < >

Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution

Secure the VNC service with a strong password.

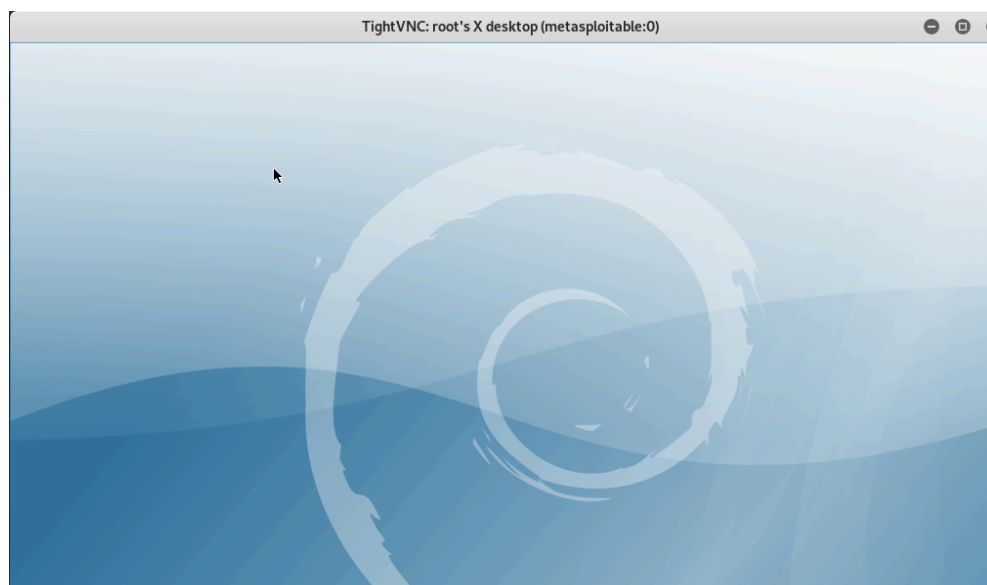
Output

Nessus logged in using a password of "password".

Port	Hosts
5900 / tcp / vnc	10.0.0.21

The command `vncviewer 10.0.0.21` will show the graphical desktop after entering the password got from Nessus scan.

```
root@kali:~# vncviewer 10.0.0.21
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
 32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
 32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using shared memory PutImage
```



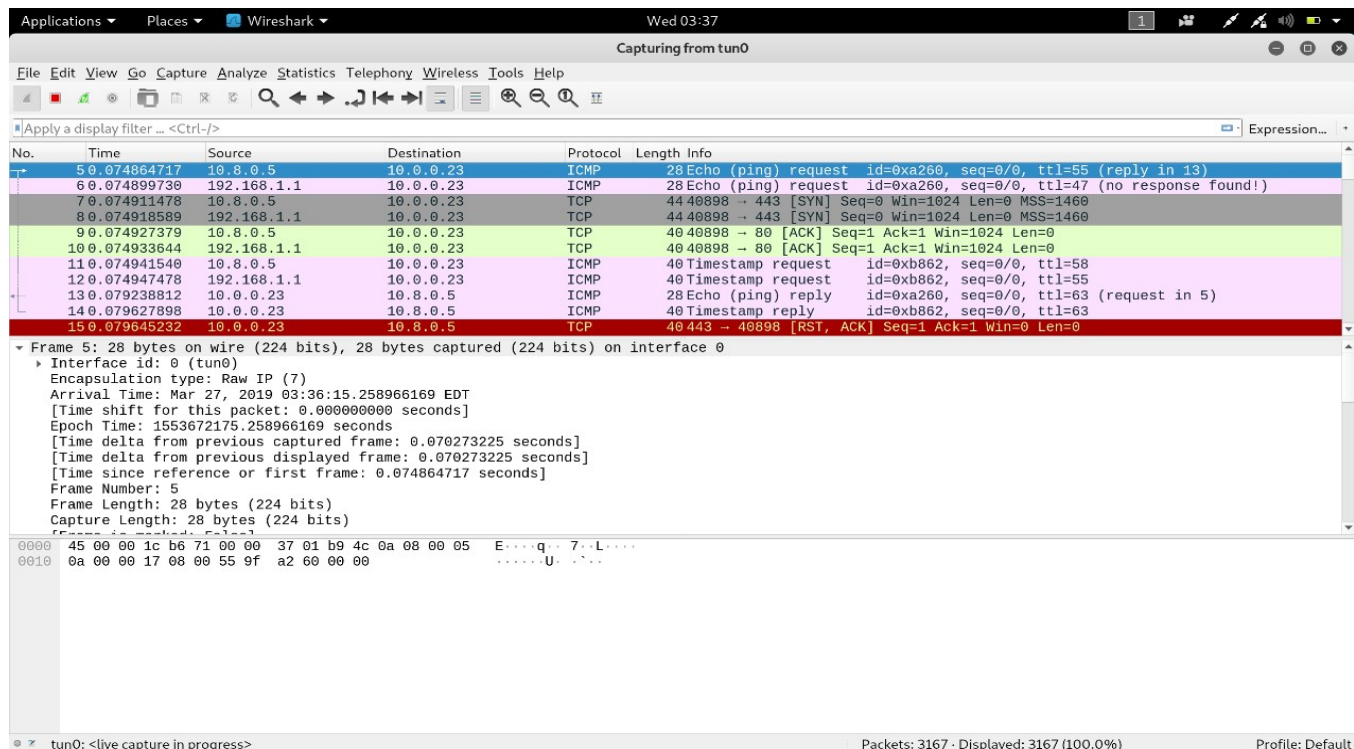
3)

Command: `nmap nessus.hacklab -n -D 192.168.1.1`

Spoofted IP address: 192.168.1.1

Real IP address: 10.8.0.2

The decoy option can be useful for a black hat hacker as the decoy option in nmap can hide the IP address. This option can confuse the defender that they do not know which IP was scanning them and which were decoys.



4)

Command: `nmap --scanflags URGACKPSHRSTSYNFIN 10.0.0.17`

Here this command turns on all the six flags, scan a test host, capture the initial packet using Wireshark

2006	80.088200995	10.8.0.16	10.0.0.17	TCP	44 51373 → 1089 [FIN, SYN, RST, PSH, ACK, URG] Seq=0 Ack=1 Win=1024 Urg=0 ...
2007	80.088206818	10.8.0.16	10.0.0.17	TCP	44 51373 → 14442 [FIN, SYN, RST, PSH, ACK, URG] Seq=0 Ack=1 Win=1024 Urg=0 ...
2008	80.088212196	10.8.0.16	10.0.0.17	TCP	44 51373 → 7103 [FIN, SYN, RST, PSH, ACK, URG] Seq=0 Ack=1 Win=1024 Urg=0 ...
2009	80.088217552	10.8.0.16	10.0.0.17	TCP	44 51373 → 1972 [FIN, SYN, RST, PSH, ACK, URG] Seq=0 Ack=1 Win=1024 Urg=0 ...
2010	80.088222972	10.8.0.16	10.0.0.17	TCP	44 51373 → 3017 [FIN, SYN, RST, PSH, ACK, URG] Seq=0 Ack=1 Win=1024 Urg=0 ...
2011	80.088228941	10.8.0.16	10.0.0.17	TCP	44 51373 → 6000 [FIN, SYN, RST, PSH, ACK, URG] Seq=0 Ack=1 Win=1024 Urg=0 ...
2012	80.088234396	10.8.0.16	10.0.0.17	TCP	44 51373 → 2009 [FIN, SYN, RST, PSH, ACK, URG] Seq=0 Ack=1 Win=1024 Urg=0 ...
2013	80.088239993	10.8.0.16	10.0.0.17	TCP	44 51373 → 61532 [FIN, SYN, RST, PSH, ACK, URG] Seq=0 Ack=1 Win=1024 Urg=0 ...

0110	= Header Length: 24 bytes (6)
▼	Flags: 0x03f (FIN, SYN, RST, PSH, ACK, URG)	
000.	= Reserved: Not set
...0	= Nonce: Not set
....0...	= Congestion Window Reduced (CWR): Not set
....0...	= ECN-Echo: Not set
....1.	= Urgent: Set
....1	= Acknowledgment: Set
....1	= Push: Set
....1.	= Reset: Set
....1.	= Syn: Set
....1	= Fin: Set
[TCP Flags:UAPRSF]		

5)

By using `nmap -v -p 20000-60000 10.0.0.35` command we find the port number and the we use the command `netcat -v 10.0.0.35 54127` will allow to get the secret.

Command: `nmap -v -p 20000-60000 10.0.0.35`

Port number: 54127

Secret:

```

root@kali: ~
File Edit View Search Terminal Help
SYN Stealth Scan Timing: About 67.77% done; ETC: 08:08 (0:00:43 remaining)
Completed SYN Stealth Scan at 08:08, 123.85s elapsed (40001 total ports)
Nmap scan report for 10.0.0.35
Host is up (0.073s latency).
Not shown: 40000 filtered ports
PORT      STATE SERVICE
54127/tcp  open  unknown

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 129.74 seconds
Raw packets sent: 79977 (3.519MB) | Rcvd: 125 (8.928KB)
root@kali:~# netcat -v 10.0.0.35 54127
Warning: forward host lookup failed for knock.hacklab: Unknown host
knock.hacklab [10.0.0.35] 54127 (?) open

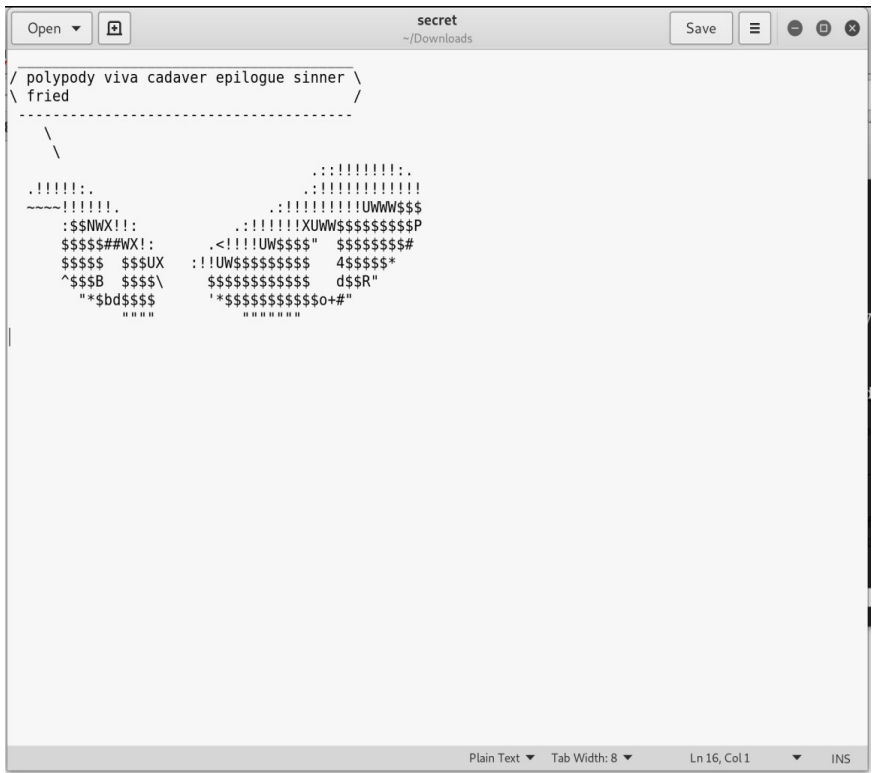
/ demure martial wellborn finochio \
\ shindig echidna /
-----
  \      ^__^
   (oo)\_____)
    (__)\       )\/\
       ||----w |
       ||     ||

root@kali:~#

```

6)

Command: `knock 10.0.0.35 2222:udp 3333:tcp 4444:udp Secret:`



7)

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/> ([Links to an external site.](https://nmap.org/nsedoc/))[Links to an external site.](https://nmap.org/nsedoc/)

There is a standard script called **http-enum**(<https://nmap.org/nsedoc/scripts/http-enum.html> ([Links to an external site.](https://nmap.org/nsedoc/scripts/http-enum.html))[Links to an external site.](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.

Command: `nmap -sV --script=http-enum 10.0.0.17`
`curl 10.0.0.17/readme.html`
Interesting file: `readme.html`

Vector string: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H (V3 legend)

Base score: 9.8 CRITICAL

The vulnerability is present on all Drupal versions 7.x before 7.58, 8.3.x versions before 8.3.9, 8.4.x versions before 8.4.6, and 8.5.x before 8.5.1.

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

Technical Details

Vulnerability Type [\(View All\)](#)

- Input Validation (CWE-20)

Vulnerable software and versions [Switch to CPE 2.2](#)

Configuration 1

OR

- * [cpe:2.3:a:drupal:drupal:*:*:*:*:*](#) [+ versions up to \(including\) 7.57](#)
- * [cpe:2.3:a:drupal:drupal:*:*:*:*:*](#) [+ versions from \(including\) 8.0.0 up to \(excluding\) 8.3.9](#)
- * [cpe:2.3:a:drupal:drupal:*:*:*:*:*](#) [+ versions from \(including\) 8.4.0 up to \(excluding\) 8.4.6](#)
- * [cpe:2.3:a:drupal:drupal:*:*:*:*:*](#) [+ versions from \(including\) 8.5.0 up to \(excluding\) 8.5.1](#)

Configuration 2

OR

- * [cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*](#)
- * [cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*](#)
- * [cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*](#)

* Denotes Vulnerable Software

[Are we missing a CPE here? Please let us know.](#)