Assignment 3

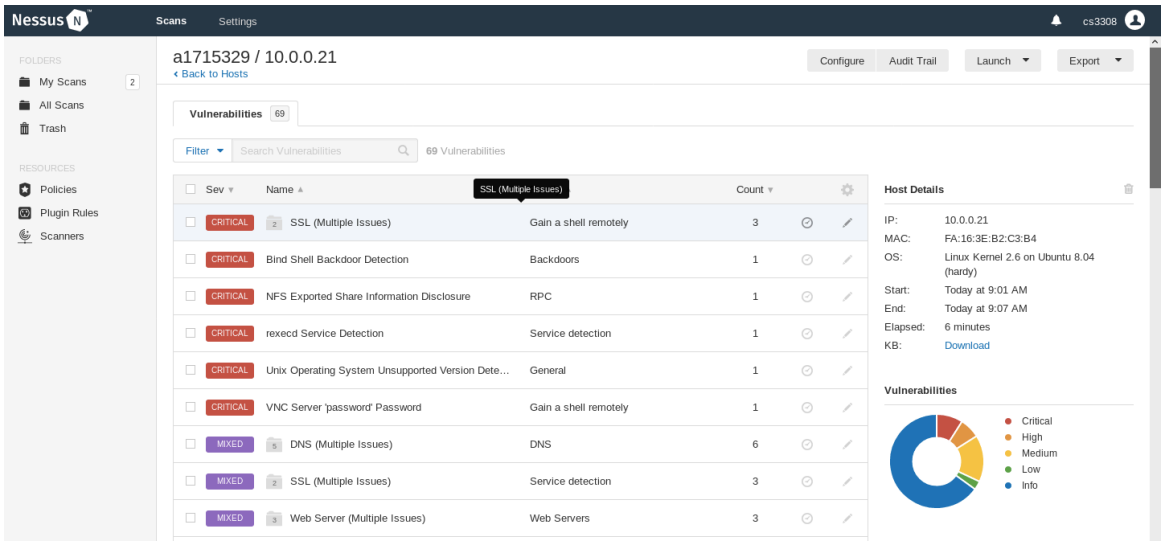
1)

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

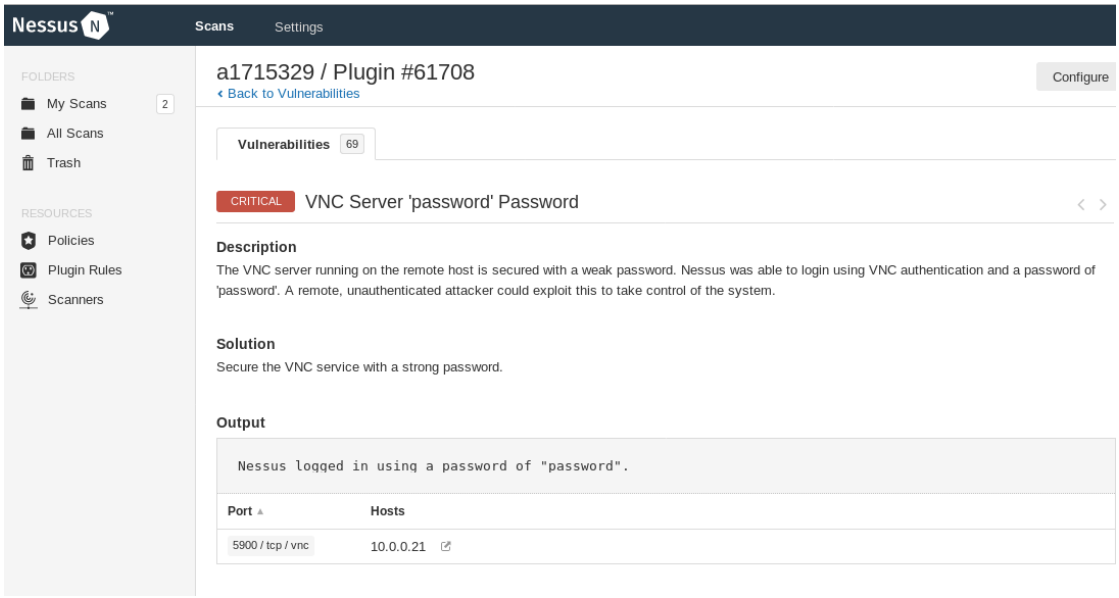
Command: fpdns -D 10.0.0.17
Software version: 9.6.3 -- 9.7.3
Software name: ISC BIND

```
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 :

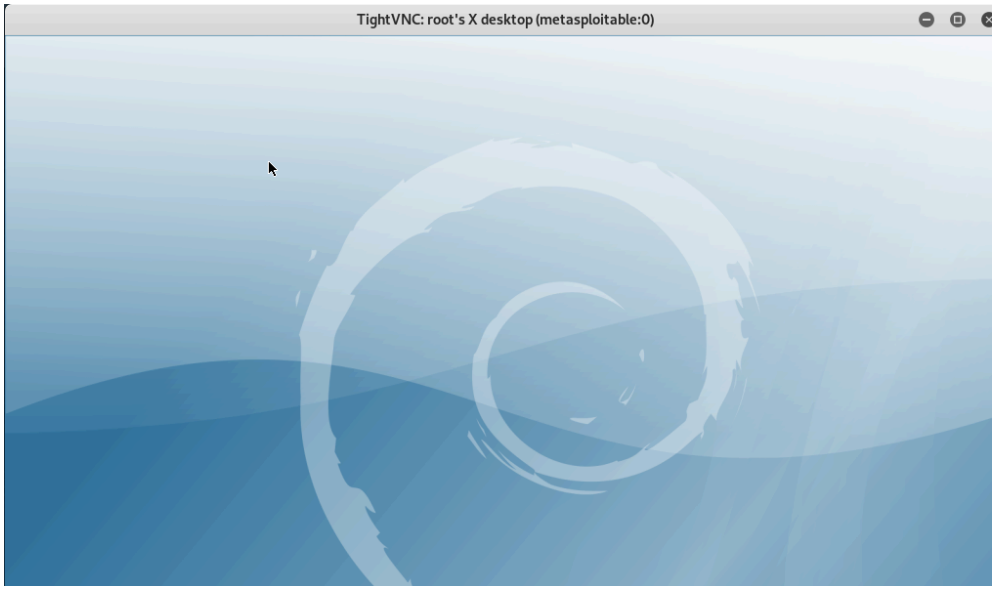


VNC server password:



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

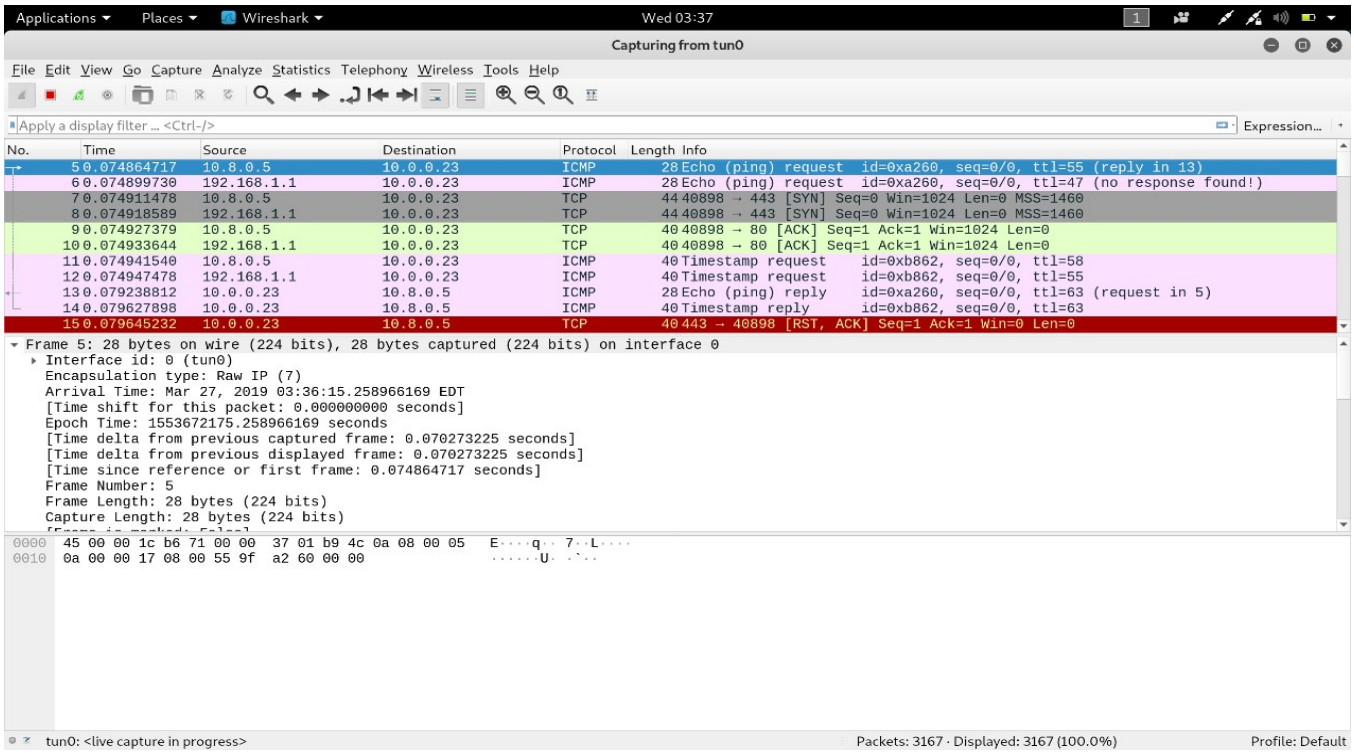
```
root@kali:~# vncviewer 10.0.0.21
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each 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
Spoofed IP address: 192.168.1.1
Real IP address: 10.8.0.2

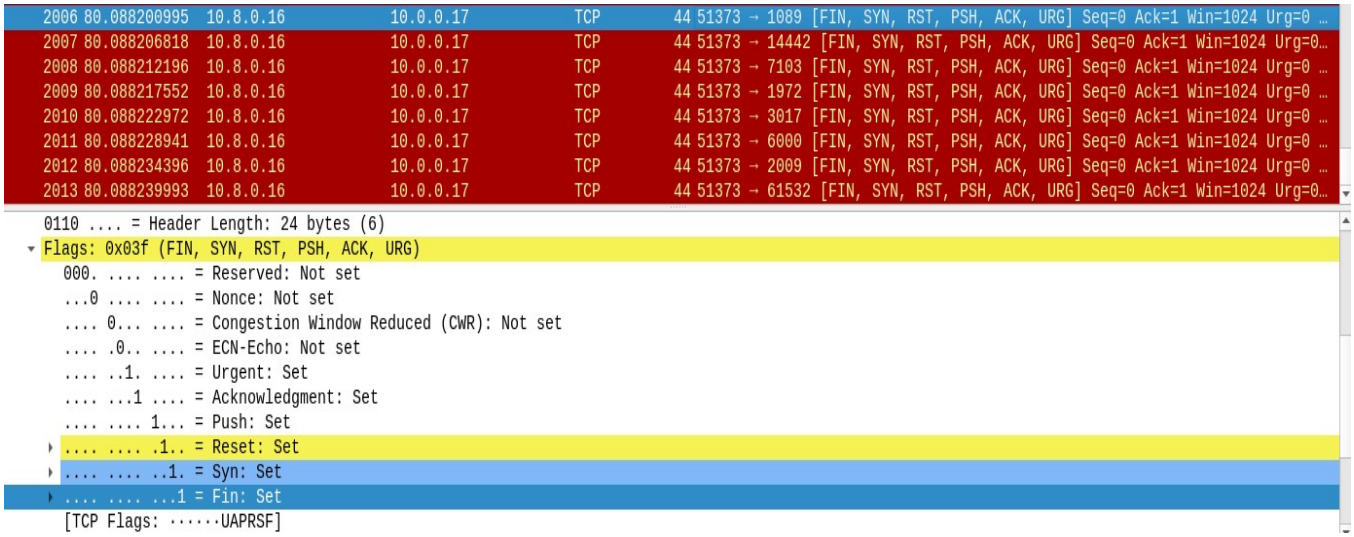
The decoy option can be useful for a black hat hacker as the decoy option in nmap can hide the IP address. This option can confuse the defender that they do not know which IP was scanning them and which were decoys.



4)

Command: nmap --scanflags URGACKPSHRSTSYNFIN 10.0.0.17

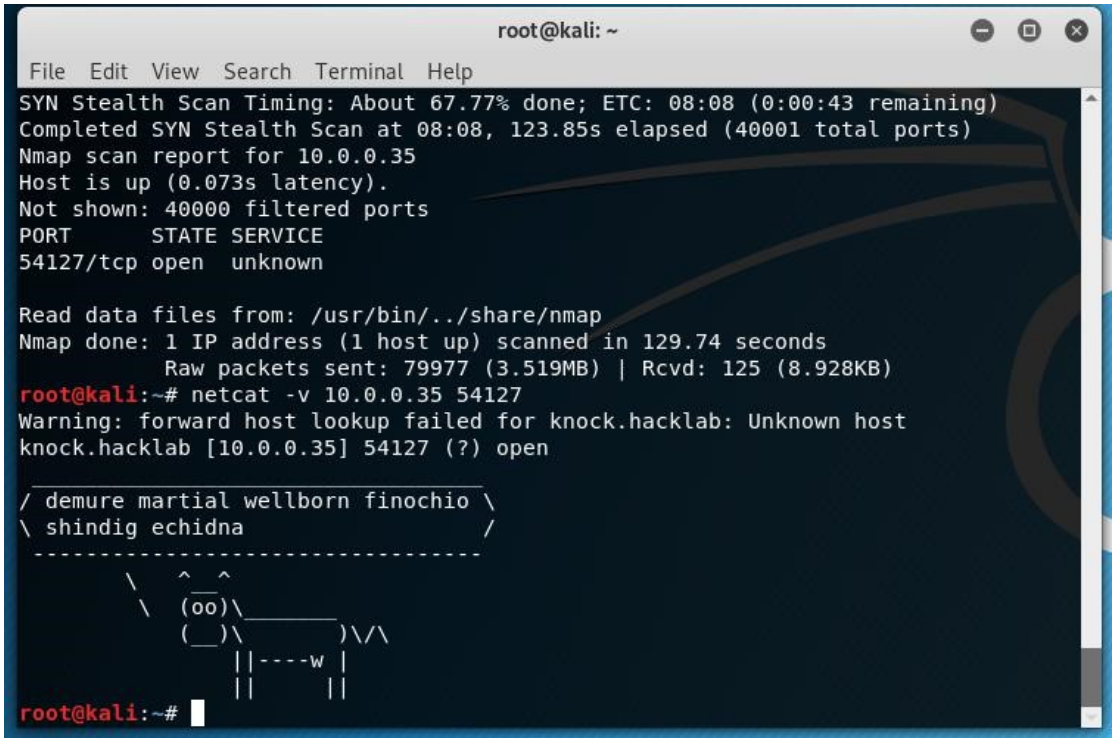
Here this command turns on all the six flags, scan a test host, capture the initial packet using Wireshark



5)

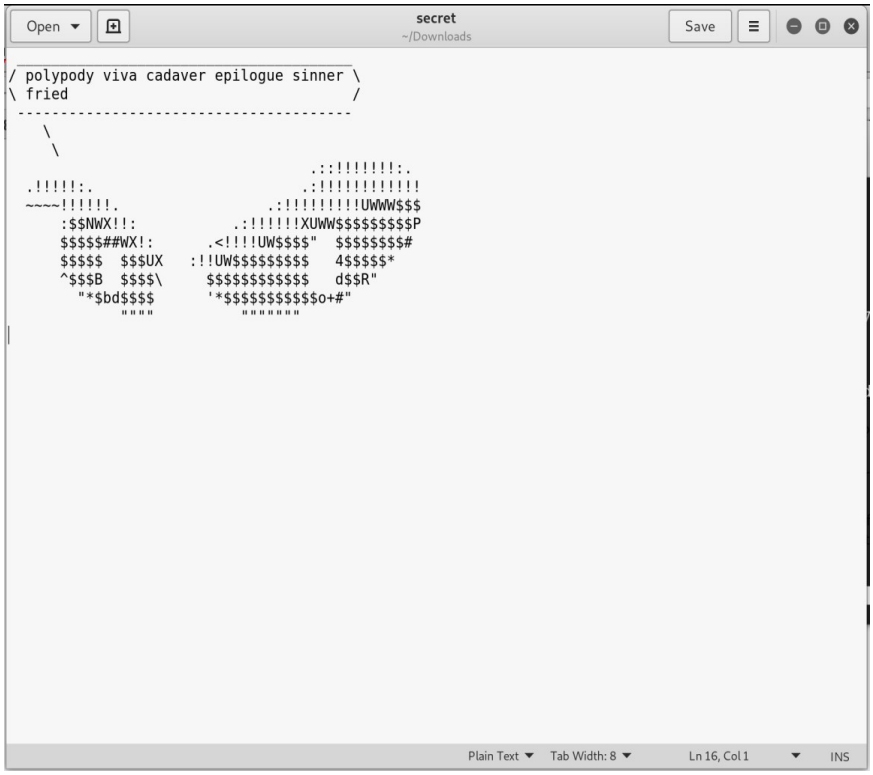
By using nmap -v -p 20000-60000 10.0.0.35 command we find the port number and the we use the command netcat -v 10.0.0.35 54127 will allow to get the secret.

Command: nmap -v -p 20000-60000 10.0.0.35
Port number: 54127
Secret:



6)

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

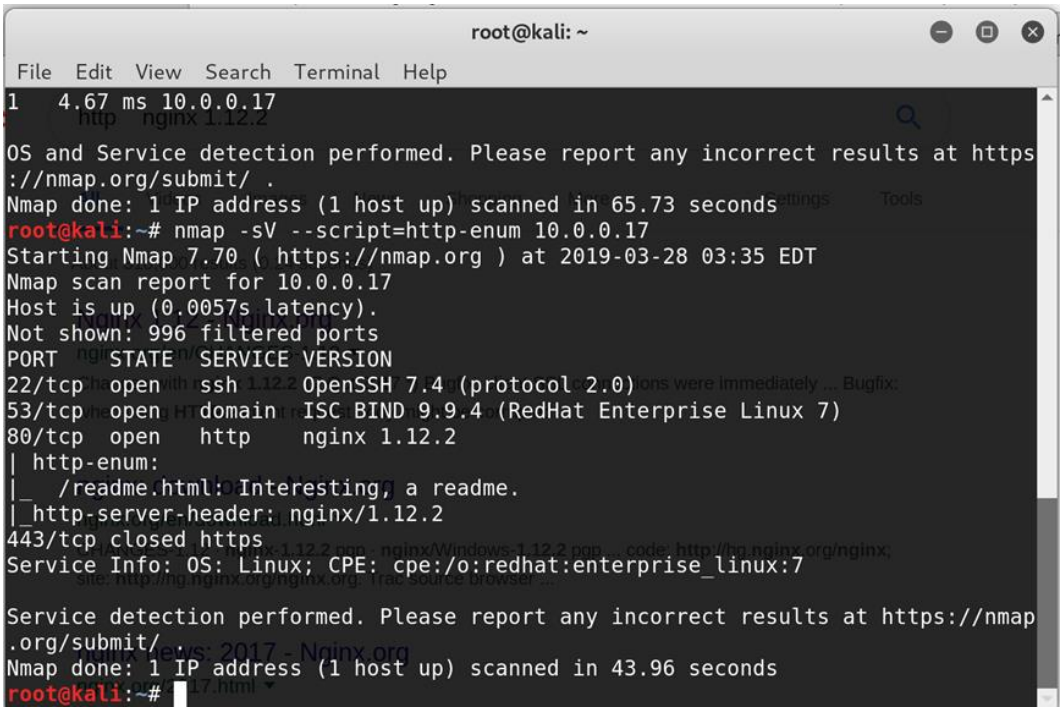


7)

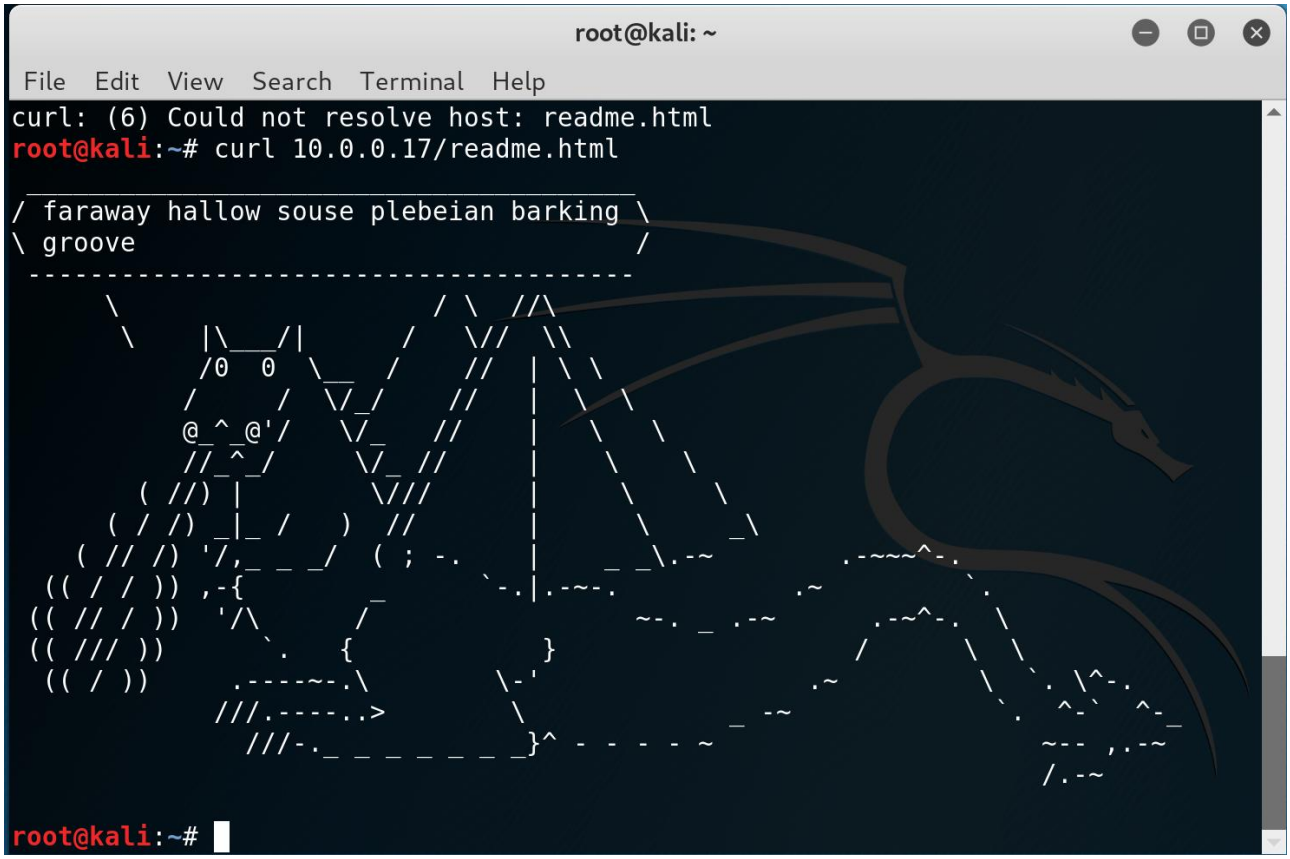
Nmap supports custom scripts (programmed in the Lua language) to extend its scanning capabilities. When you run with the -A switch, Nmap runs all "default" scripts, and you can specify specific scripts using the --script= option in the command line. The pre-installed scripts are located under /usr/share/nmap/scripts/*.nse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

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



Content of file: Dragon



8)

CVE: CVE-2018-7600

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.