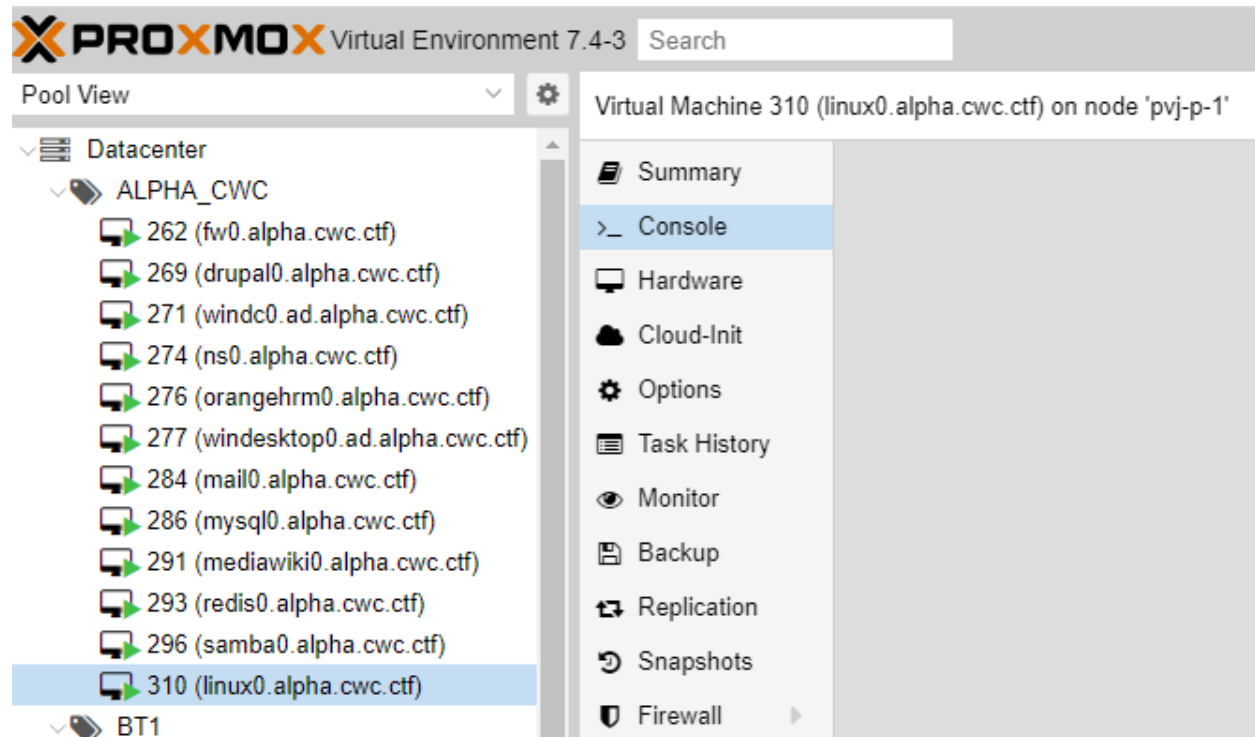


Using windows 10.

1, Connet the OpenVPN

2, Log on PROXMOX, I was assigned to Alpha team.



3, Log on Windows PuTTY, use the #310 Linux machine.

Target Range: 10.24.5.0/24

4, Run command: `nmap -sCV -v -T 4 -Pn 10.24.5.0/24`

icanhasaccess@linux0: ~

```
icanhasaccess@linux0:~$ nmap -sV -Pn -v 10.24.5.0/24
```

```
Starting Nmap 7.01 ( https://nmap.org ) at 2023-05-27 19:28 UTC
NSE: Loaded 35 scripts for scanning.
Initiating Parallel DNS resolution of 256 hosts. at 19:28
Completed Parallel DNS resolution of 256 hosts. at 19:28, 0.01s elapsed
Initiating Connect Scan at 19:28
Scanning 64 hosts [1000 ports/host]
Discovered open port 22/tcp on 10.24.5.8
Discovered open port 22/tcp on 10.24.5.16
Discovered open port 22/tcp on 10.24.5.24
Discovered open port 22/tcp on 10.24.5.32
Discovered open port 80/tcp on 10.24.5.8
Discovered open port 80/tcp on 10.24.5.16
Discovered open port 80/tcp on 10.24.5.32
Completed Connect Scan against 10.24.5.8 in 0.58s (63 hosts left)
Completed Connect Scan against 10.24.5.16 in 0.58s (62 hosts left)
Completed Connect Scan against 10.24.5.24 in 0.58s (61 hosts left)
Completed Connect Scan against 10.24.5.32 in 0.58s (60 hosts left)
Discovered open port 22/tcp on 10.24.5.1
Discovered open port 443/tcp on 10.24.5.1
Discovered open port 53/tcp on 10.24.5.1
Discovered open port 80/tcp on 10.24.5.1
Connect Scan Timing: About 35.11% done; ETC: 19:30 (0:00:57 remaining)
Connect Scan Timing: About 66.55% done; ETC: 19:30 (0:00:31 remaining)
Completed Connect Scan against 10.24.5.48 in 85.47s (59 hosts left)
Completed Connect Scan against 10.24.5.55 in 86.47s (58 hosts left)
Completed Connect Scan against 10.24.5.22 in 86.57s (57 hosts left)
Completed Connect Scan against 10.24.5.58 in 86.67s (56 hosts left)
Completed Connect Scan against 10.24.5.36 in 86.77s (55 hosts left)
```

Need to find other hosts that are up, what services are running on active machines, and the version numbers.

Need to keep an eye on our internal machines to see if there is any red team activity.

Try to do some webapp pen testing seeing as how there probably isn't any brute forcing needed.

The Nmap scan was successful!! Found several suspicious vulnerability hosts.

icanhasaccess@linux0: ~

```
Host is up.
All 1000 scanned ports on 10.24.5.5 are filtered

Nmap scan report for 10.24.5.6
Host is up.
All 1000 scanned ports on 10.24.5.6 are filtered

Nmap scan report for 10.24.5.7
Host is up.
All 1000 scanned ports on 10.24.5.7 are filtered

Nmap scan report for 10.24.5.8
Host is up (0.0047s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 10.24.5.9
Host is up.
All 1000 scanned ports on 10.24.5.9 are filtered

Nmap scan report for 10.24.5.10
Host is up.
All 1000 scanned ports on 10.24.5.10 are filtered

Nmap scan report for 10.24.5.11
Host is up.
All 1000 scanned ports on 10.24.5.11 are filtered

Nmap scan report for 10.24.5.12
Host is up.
All 1000 scanned ports on 10.24.5.12 are filtered

Nmap scan report for 10.24.5.13
Host is up.
All 1000 scanned ports on 10.24.5.13 are filtered

Nmap scan report for 10.24.5.14
Host is up.
All 1000 scanned ports on 10.24.5.14 are filtered

Nmap scan report for 10.24.5.15
Host is up.
All 1000 scanned ports on 10.24.5.15 are filtered

Nmap scan report for 10.24.5.16
Host is up (0.0046s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 10.24.5.17
Host is up.
All 1000 scanned ports on 10.24.5.17 are filtered
```

## Details:


<https://10.24.5.1/>

```
All 1000 scanned ports on 10.24.5.0 are filtered

Nmap scan report for 10.24.5.1
Host is up (0.0034s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9 (protocol 2.0)
53/tcp    open  domain   NLNet Labs Unbound
80/tcp    open  http     nginx
443/tcp   open  ssl/http nginx
```

- pfSense login webpage (**PROMISING!!**)

⚠ Not secure | <https://10.24.5.1>



Your connection is not private


Attackers might be trying to steal your information from **10.24.5.1** (for example, passwords, messages, or credit cards). [Learn more](#)

NET:ERR\_CERT\_AUTHORITY\_INVALID

Advanced

Back to safety

⚠ Not secure | <https://10.24.5.1>



SIGN IN

Username

Password

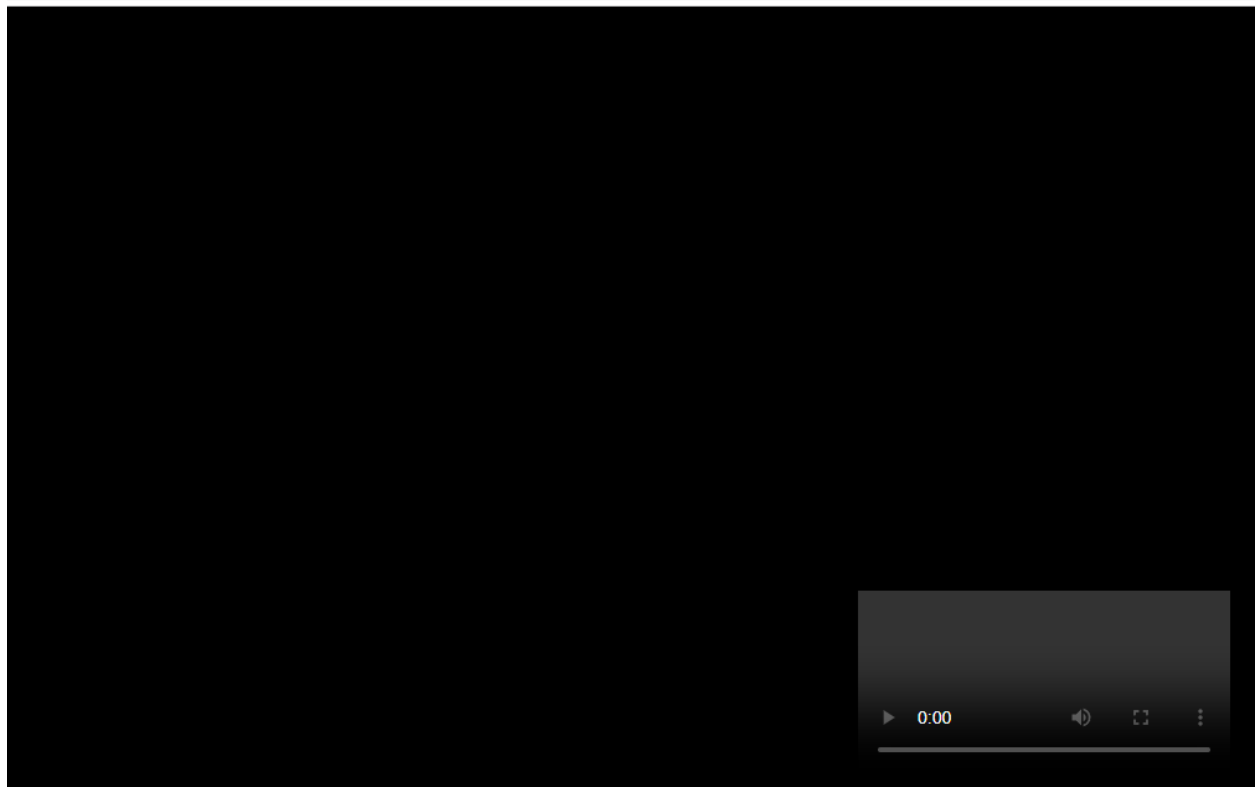
SIGN IN

<http://10.24.5.8>

```
Nmap scan report for 10.24.5.8
Host is up (0.0047s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

- <http://10.24.5.8/audio/Rock%20Me%20Mama.ogg>



















⚠ Not secure | 10.24.5.8/audio/Rock%20Me%20Mama.ogg



<http://10.24.5.16/>

```
Nmap scan report for 10.24.5.16
Host is up (0.0046s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

- a bunch of .png images (next page). The biggest image looks to be decrypted of some sort, and the smaller images under it are in order going from left to right and from top to bottom. Images were lettered from a (the decrypted) and b-q (the smaller images)

 Not secure   10.24.5.16				
<h2>Index of /</h2>				
	<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
<hr/>				
	<a href="#">a.png</a>	2023-03-01 19:27	554K	
	<a href="#">b.png</a>	2023-03-01 19:28	5.0K	
	<a href="#">c.png</a>	2023-03-01 19:28	5.2K	
	<a href="#">d.png</a>	2023-03-01 19:28	5.0K	
	<a href="#">e.png</a>	2023-03-01 19:28	11K	
	<a href="#">f.png</a>	2023-03-01 19:27	4.7K	
	<a href="#">g.png</a>	2023-03-01 19:27	4.7K	
	<a href="#">h.png</a>	2023-03-01 19:27	4.7K	
	<a href="#">i.png</a>	2023-03-01 19:27	4.9K	
	<a href="#">j.png</a>	2023-03-01 19:28	5.0K	
	<a href="#">k.png</a>	2023-03-01 19:28	12K	
	<a href="#">l.png</a>	2023-03-01 19:28	5.0K	
	<a href="#">m.png</a>	2023-03-01 19:28	11K	
	<a href="#">n.png</a>	2023-03-01 19:27	4.7K	
	<a href="#">o.png</a>	2023-03-01 19:27	12K	
	<a href="#">p.png</a>	2023-03-01 19:28	5.0K	
	<a href="#">q.png</a>	2023-03-01 19:28	11K	
<hr/>				
Apache/2.4.18 (Ubuntu) Server at 10.24.5.16 Port 80				

<http://10.24.5.24/>

```
Nmap scan report for 10.24.5.22
Host is up.
All 1000 scanned ports on 10.24.5.22 are filtered

Nmap scan report for 10.24.5.23
Host is up.
All 1000 scanned ports on 10.24.5.23 are filtered

Nmap scan report for 10.24.5.24
Host is up (0.0046s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 10.24.5.25
Host is up.
All 1000 scanned ports on 10.24.5.25 are filtered

Nmap scan report for 10.24.5.26
Host is up.
All 1000 scanned ports on 10.24.5.26 are filtered
```

The Nmap scan report does not explicitly mention any vulnerabilities on the host with the IP address 10.24.5.24. The report primarily provides information about the open port (22/tcp) and the service running on that port (OpenSSH 7.2p2).

While the scan report itself does not indicate vulnerabilities, it's important to note that vulnerability assessment goes beyond just port scanning. Additional security testing, such as vulnerability scanning or penetration testing, would be required to identify any potential vulnerabilities in the system.

① 10.24.5.24



## This site can't be reached

10.24.5.24 refused to connect.

Try:

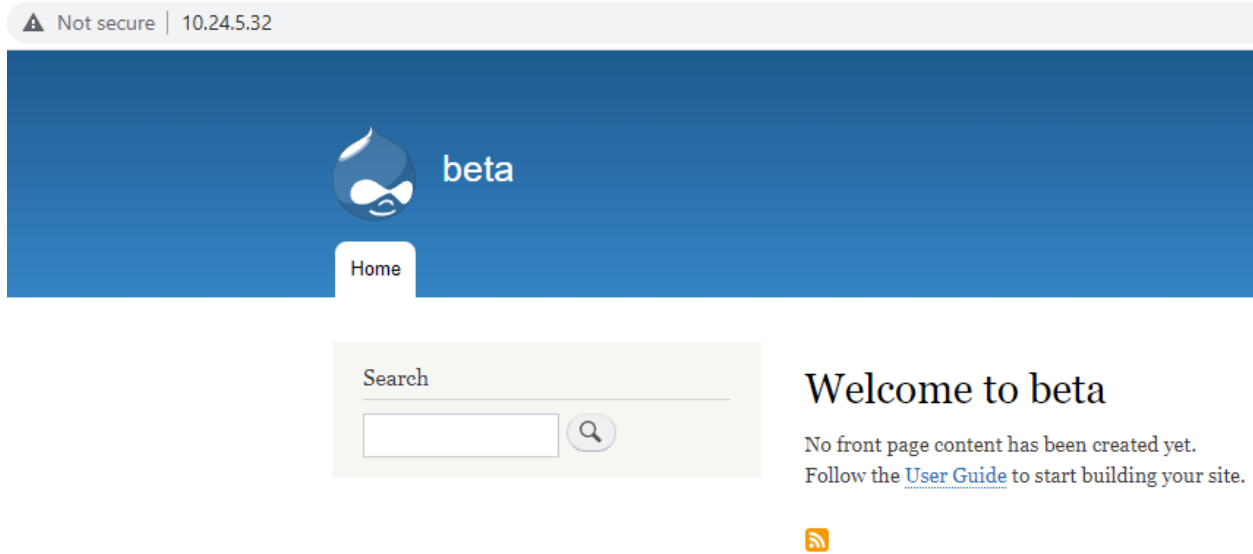
- Checking the connection
- [Checking the proxy and the firewall](#)

ERR\_CONNECTION\_REFUSED

<http://10.24.5.32/>

```
Nmap scan report for 10.24.5.32
Host is up (0.0039s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```


- a webpage with login (**PROMISING!!**)



<http://10.24.5.64/> - ubuntu apache2 webpage

```
Nmap scan report for 10.24.5.64
Host is up (0.0034s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```





## Apache2 Ubuntu Default Page

### ubuntu

#### It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

#### Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```

/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf

```

### 10.24.5.80 - mailing server? Found smtp, pop3, and imap

```

Nmap scan report for 10.24.5.80
Host is up (0.0043s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
110/tcp   open  pop3     Dovecot pop3d
143/tcp   open  imap     Dovecot imapd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

\* The host is up and responsive, with a latency of 0.0043 seconds.

\* There are 997 closed ports that were not shown in the report.

\* Port 22/tcp is open and running an SSH (Secure Shell) service. The SSH service is identified as OpenSSH 7.2p2 running on Ubuntu 4ubuntu2.10.

\* Port 110/tcp is open and running a POP3 (Post Office Protocol version 3) service. The specific software identified is Dovecot pop3d.

\* Port 143/tcp is open and running an IMAP (Internet Message Access Protocol) service. The specific software identified is Dovecot imapd.

\* Additional service information indicates that the host is running a Linux operating system, with the kernel being part of the Ubuntu distribution.

Please note that this scan report provides a snapshot of the open ports and identified services at the time of the Nmap scan. It does not explicitly mention any vulnerabilities on the host.

<http://10.24.5.88/>

```
Nmap scan report for 10.24.5.88
Host is up (0.0032s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

- database error page? Might be mysql

← → ↻ ⚠ Not secure | 10.24.5.88

# Sorry! This site is experiencing technical difficulties.

Try waiting a few minutes and reloading.

(Cannot access the database)

<http://10.24.5.104/> - another ubuntu apache2 webpage

```
Nmap scan report for 10.24.5.104
Host is up (0.0035s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

⚠ Not secure | 10.24.5.104



ubuntu

## Apache2 Ubuntu Default Page

### It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

### Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

## 10.24.5.112 - dns?

```
Nmap scan report for 10.24.5.112
Host is up (0.0035s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
53/tcp    open  domain   ISC BIND 9.8.1-P1
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

The Nmap scan report for the IP address 10.24.5.112 provides the following information about the host:

- The host is up and responsive, with a latency of 0.0035 seconds.
- There are 998 closed ports that were not shown in the report.
- Port 22/tcp is open and running an SSH (Secure Shell) service. The SSH service is identified as OpenSSH 6.6.1p1 running on Ubuntu 2ubuntu2.13.
- Port 53/tcp is open and running a DNS (Domain Name System) service. The specific software identified is ISC BIND 9.8.1-P1.
- Additional service information indicates that the host is running a Linux operating system, with the kernel being part of the Ubuntu distribution.

Please note that this scan report provides a snapshot of the open ports and identified services at the time of the Nmap scan. It does not explicitly mention any vulnerabilities on the host.

## 10.24.5.128 - samba, ook puzzle, GUEST ACCOUNT!!

```
Nmap scan report for 10.24.5.128
Host is up (0.0052s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
139/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: OOK-PUZZLE0)
445/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: OOK-PUZZLE0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

The Nmap scan report for the IP address 10.24.5.128 reveals the following information about the host:


- The host is up and responsive, with a latency of 0.0052 seconds.
- There are 997 closed ports that were not shown in the report.
- Port 22/tcp is open and running an SSH (Secure Shell) service. The SSH service is identified as OpenSSH 7.2p2 running on Ubuntu 4ubuntu2.10.
- Port 139/tcp is open and running a NetBIOS-SSN service. The specific software identified is Samba smbd 3.X, and the workgroup name is "OOK-PUZZLE0".
- Port 445/tcp is open and running a NetBIOS-SSN service. The specific software identified is also Samba smbd 3.X, and the workgroup name is "OOK-PUZZLE0".
- Additional service information indicates that the host is running a Linux operating system, with the kernel being part of the Ubuntu distribution.

Please note that this scan report provides a snapshot of the open ports and identified services at the time of the Nmap scan. It does not explicitly mention any vulnerabilities on the host.

```
Nmap scan report for 10.24.5.136
Host is up (0.0059s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

<http://10.24.5.136/installer/installerUI.php> - orange HRM, Human resources management landing page

← → ↻ ⚠ Not secure | 10.24.5.136/installer/installerUI.php



Welcome License Database Configuration System Check Admin User Creation Confirmation Installing Registration [Help ?]

## Welcome to the OrangeHRM ver 2.6.0.1 Setup Wizard

This installer creates the OrangeHRM database tables and sets the configuration files that you need to start.

Click **[Next]** to Start the Wizard.

**OrangeHRM.com**

OrangeHRM Web Installation Wizard ver 0.2 © OrangeHRM Inc 2005 - 2009 All rights reserved.

[https://www.cvedetails.com/vulnerability-list/vendor\\_id-6180/Orangehrm.html](https://www.cvedetails.com/vulnerability-list/vendor_id-6180/Orangehrm.html) - OrangeHRM CVEs

[CVE-2007-1193](#) looks like promising.

18 <a href="#">CVE-2007-1193</a>	2007-03-02	2011-03-08	9.3	None
Multiple unspecified vulnerabilities in the Login page in OrangeHRM before 20070212 have unknown impact and attack vectors.				
Total number of vulnerabilities : 18 Page : 1 (This Page)				

10.24.5.160 - another samba server, netbios-ssn, also GUEST ACCOUNT

```
Nmap scan report for 10.24.5.160
Host is up (0.0057s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
139/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: SAMBA0)
445/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: SAMBA0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

The Nmap scan report for the IP address 10.24.5.160 provides the following information about the host:

- The host is up and responsive, with a latency of 0.0057 seconds.

- Please note that this scan report provides a snapshot of the open ports and identified services at the time of the Nmap scan. It does not explicitly mention any vulnerabilities on the host.

```

Nmap scan report for 10.24.5.176
Host is up (0.0060s latency).
Not shown: 981 closed ports
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Microsoft DNS
88/tcp    open  kerberos-sec  Windows 2003 Kerberos (server time: 2023-05-27 19:37:48Z)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows 98 netbios-ssn
389/tcp   open  ldap         (primary domain: AD)
445/tcp   open  kpasswd5?
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap
3269/tcp  open  tcpwrapped
3389/tcp  open  ssl/ms-wbt-server?
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
49157/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc        Microsoft Windows RPC
49159/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: WINDC0; OS: Windows, Windows 98; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows server 2003, cpe:/o:microsoft:windows 98

```

- The host is up and responsive, with a latency of 0.0060 seconds.
- There are 981 closed ports that were not shown in the report.
- Port 53/tcp is open and runs a Microsoft DNS service.
- Port 88/tcp is open and running a Kerberos-sec service. The specific version identified is Windows 2003 Kerberos.
- Port 135/tcp is open and runs Microsoft Windows RPC (Remote Procedure Call).
- Port 139/tcp is open and runs a NetBIOS-SSN service, specifically for Microsoft Windows 98.
- Port 389/tcp is open and runs an LDAP (Lightweight Directory Access Protocol) service.
- Port 445/tcp is open and running a Microsoft-DS service, with the primary domain identified as "AD" (Active Directory).
- Port 464/tcp is open, possibly running a service related to Kerberos password change.
- Port 593/tcp is open and running Microsoft Windows RPC over HTTP 1.0.
- Port 636/tcp is open but running a TCP-wrapped service, where the specific service cannot be determined from the scan.
- Ports 3268/tcp, 3269/tcp, 3389/tcp, and various ports in the range 49152-49159/tcp are open and running Microsoft Windows RPC services.

- One service remains unrecognized, and the Nmap scan suggests submitting the fingerprint for further analysis.

The service information indicates that the host is running Windows and Windows 98 operating systems. It's important to note that the presence of open ports does not necessarily indicate vulnerabilities, but further security assessments should be conducted to identify any potential security risks.

10.24.5.184 - another windows machine, windesktop0.ad.beta.cwc.ctf, active directory?

```
Nmap scan report for 10.24.5.184
Host is up (0.0043s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE          VERSION
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn      Microsoft Windows 98 netbios-ssn
445/tcp   open  microsoft-ds     Microsoft Windows 10 microsoft-ds
3389/tcp   open  ssl/ms-wbt-server?
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
Service Info: OSs: Windows, Windows 98, Windows 10; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_98, cpe:/o:microsoft:windows_10
```

The Nmap scan report for the IP address 10.24.5.184 provides the following information about the host:

- The host is up and responsive, with a latency of 0.0043 seconds.
- There are 991 closed ports that were not shown in the report.
- Port 135/tcp is open and running Microsoft Windows RPC (Remote Procedure Call).
- Port 139/tcp is open and running a NetBIOS-SSN service, specifically for Microsoft Windows 98.
- Port 445/tcp is open and running the Microsoft-DS service, which is associated with Microsoft Windows 10.
- Port 3389/tcp is open, and it may be running an SSL-based service, possibly related to the Microsoft Windows Remote Desktop Protocol (RDP).
- Ports 49152/tcp, 49153/tcp, 49154/tcp, 49155/tcp, and 49156/tcp are open, running Microsoft Windows RPC services.
- The service information indicates that the host is running Windows, Windows 98, and Windows 10 operating systems.

It's important to note that the presence of open ports does not necessarily indicate vulnerabilities, but further security assessments should be conducted to identify any potential security risks.

**TO BE CONTINUED...**