6G4Z1104: Computer Forensics and Security Fundamentals

Coursework 1

Rhys Clinch, 18012805

Contents

Task A – Multiple Choice Exam

Task B – System Audit

Computer Misuse Act 1990

The computer misuse act is a set of rules in place to prevent users from causing harm to other users' systems. There are three levels of offences that can lead to a lifetime in prison or a hefty fine depending on the offence committed. The three stages to the computer misuse act are, gaining access to a computer system that is not their own without authorisation and causing small harm to the device; this is the lowest level of offence. The next level is an extended offence of level one and tampering with their system to gain confidential data such as bank details or even placing a keylogger on the system. The third level, part (a) is the deletion of information on a user's device or altering files on the system with the intent of causing harm to the system and rendering their system useless. The last level, part (b) is the production and distribution of a malicious program that is intended to cause harm to a user's system and making their system unusable (Computer Misuse Act 1990, 2018).

Virtualisation can be used to prevent accidental breaches of the act as anything that happens within the virtual machine stays in its virtual state and doesn't physically affect the system. This is because the resources for the virtual machine have been virtualised and virtually created, making it a clone of an actual computer system; this prevents accidental breaches of level 2 in the Computer Misuse Act as it would be tampering with a system otherwise. Using a virtual machine also prevents accidental breaches of level 3 and, attacks such as the denial of service attack can be done without breaching the act itself. This can be done through configuring the network to an internal network type or even using a non-connected network and making it LAN only. The virtual machine can also be configured to a local host only network type to avoid such breaches (Chapter 6. Virtual networking, 2018). When the virtual machine is set up correctly, accidental breaches will be avoided completely unless the user willingly decides to cause malicious intent to the systems/network outside of the virtual machine.

Port Scanning & the TCP Handshake

A port scan is a scan that probes a server for open TCP/UDP ports. It can be used to view what services that server is running and can exploit the security vulnerabilities within those services by providing the potential attacker/admin of the server the current version of the service that is currently running on the server (Whitaker and Newman, 2018). They can then research an exploit within the version of that service through the common vulnerabilities and exposures website.

Port scans use the TCP handshake to establish a connection when it comes to transferring information across a network or from system to system. The first step of a TCP handshake is the SYN segment which initiates the connection between the two parties, and from this a SYN/ACK is sent back which is the acknowledgement segment, or an RST segment is sent back that resets the connection immediately. This would tell the sending machine that the connection has not been made, if the SYN/ACK segment was sent as a response files can be sent back and forth until an RST segment is sent to reset/end the connection (figure 1).

The TCP handshake can be misused when two parties connect to one receiving member, and one of the sending members drops their connection abruptly; this would then stop the other party's connection and an RST segment would be sent which resets the connection between all parties. The result of this is all connections being dropped and the second party member having to re-establish a connection. Meaning, the original party's connection wouldn't be logged (RFC 793, 2018) and they can restrict other online users from transferring files to and from this system/server if they were to repeat this.

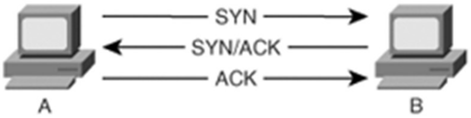
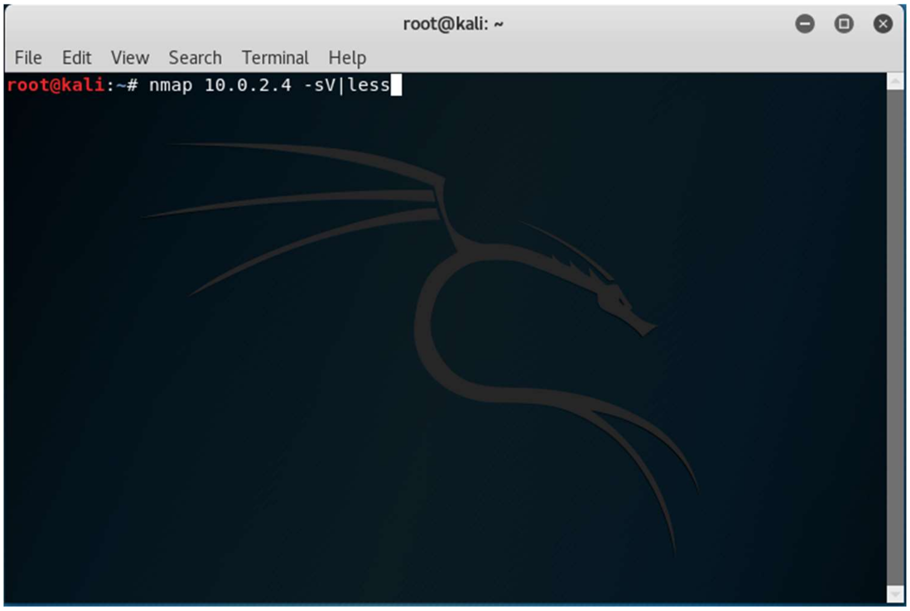


Figure 1: TCP Handshake Diagram (Whitaker and Newman, 2018)

Vulnerability Assessment of Metasploitable Virtual Machine

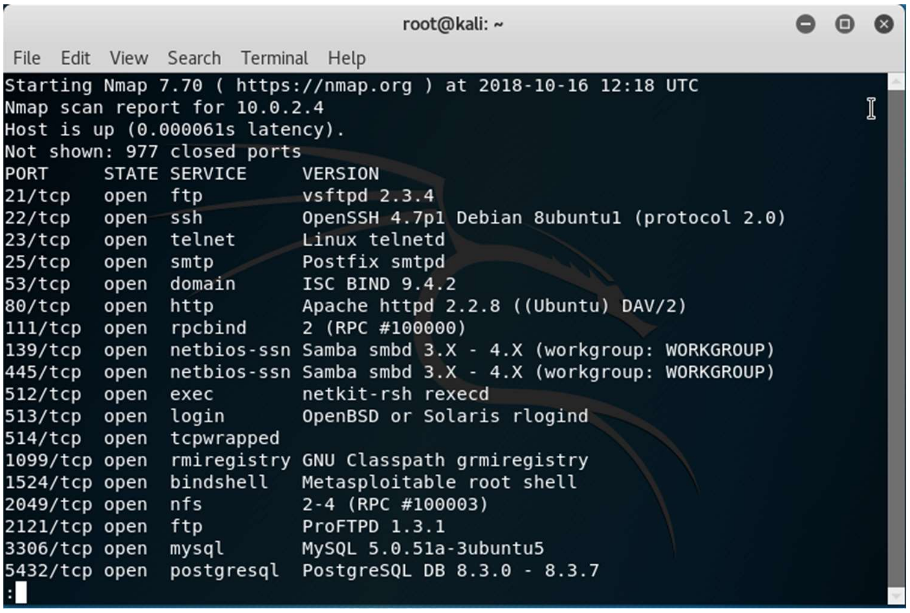
For this task, Nmap was used which is described by (Lyon,2018) as “an open source tool for network exploration and security auditing.” The scan that was decided was the service detection scan (-sV) to find out what ports were open and what services the server was running and the versions of the ones currently in use (Service and Version Detection | Nmap Network Scanning, 2018). For the purposes of not breaching the Computer Misuse Act, the scan was used against another virtual machine that was set up on the local host with the IP address 10.0.2.4.

Once the scan was complete, it displayed eighteen different open ports including the port 80 (http port).



```
root@kali:~# nmap 10.0.2.4 -sV|less
```

Figure 2: Start of port scan

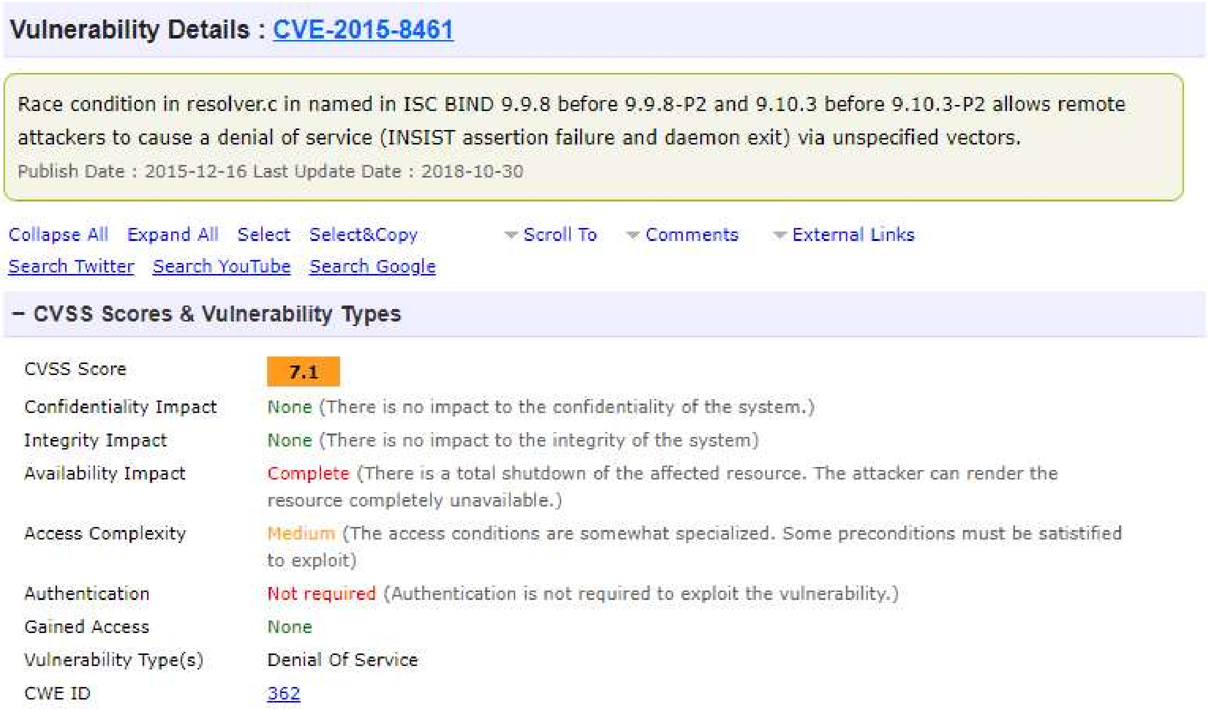


```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-16 12:18 UTC
Nmap scan report for 10.0.2.4
Host is up (0.000061s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
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       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  rmiregistry GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
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
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
:
```

Figure 3: Results of the port scan

Figure 3 displays the results of the port scan from figure 2, showing that there are 18 ports that are currently open and what version of the service that server is running for their current services in use for those ports. E.g. port 2121 is running the ftp service on version 1.3.1. The scan also shows that there are 977 closed ports from this scan.

Common Vulnerabilities and Exploits Identified



Vulnerability Details : CVE-2015-8461

Race condition in resolver.c in named in ISC BIND 9.9.8 before 9.9.8-P2 and 9.10.3 before 9.10.3-P2 allows remote attackers to cause a denial of service (INSIST assertion failure and daemon exit) via unspecified vectors.

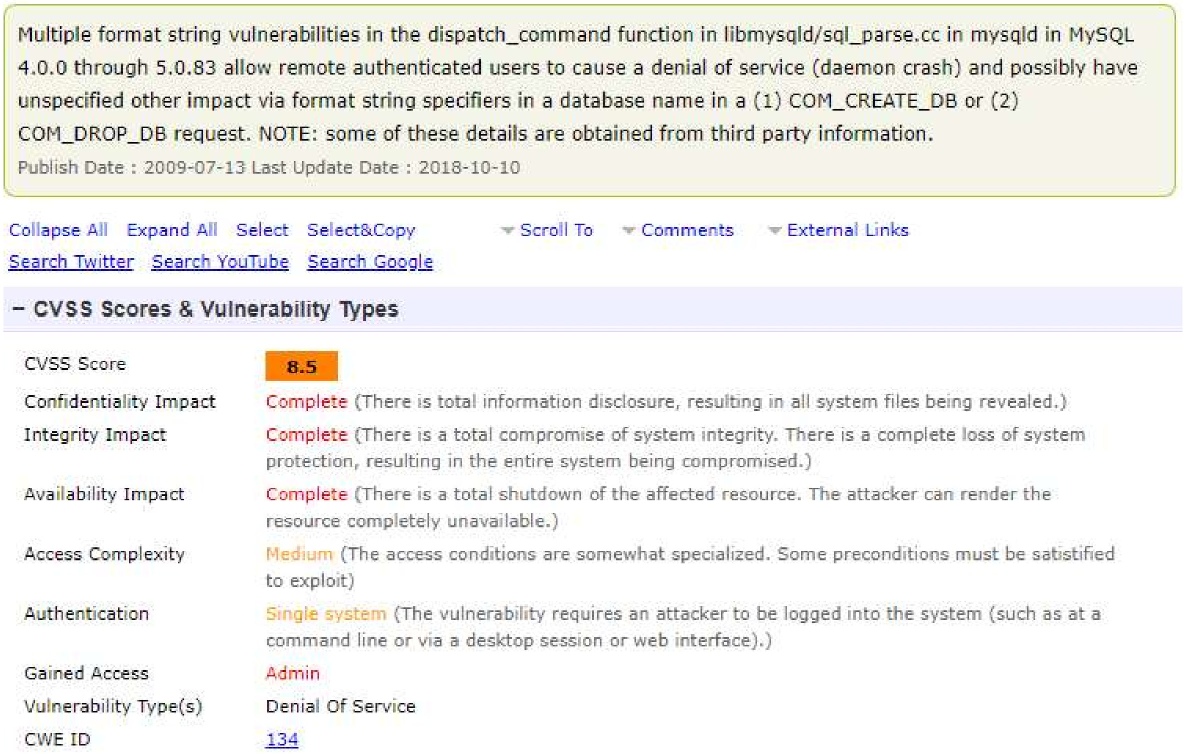
Publish Date : 2015-12-16 Last Update Date : 2018-10-30

− CVSS Scores & Vulnerability Types

CVSS Score	7.1
Confidentiality Impact	None (There is no impact to the confidentiality of the system.)
Integrity Impact	None (There is no impact to the integrity of the system)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satistified to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Denial Of Service
CWE ID	362

Figure 4: Port 53 exploit (CVE-2015-8461, 2018)

Using the common vulnerabilities and exploits website there are many exploits for each service/version of the software that was currently in use which was chosen. Figure 4 displays an exploit within port 53 which is running ISC Bind 9.4.2; this exploit exposes a denial of service attack through a race condition within resolver.c and allows the attacker to remotely deny the service through daemon exit and “unspecified vectors” with no authentication (CVE-2015-8451,2018). This version of the software threatens the availability of the server as it shuts the server down completely, stopping anyone from accessing the site.



Multiple format string vulnerabilities in the dispatch_command function in libmysqld/sql_parse.cc in mysqld in MySQL 4.0.0 through 5.0.83 allow remote authenticated users to cause a denial of service (daemon crash) and possibly have unspecified other impact via format string specifiers in a database name in a (1) COM_CREATE_DB or (2) COM_DROP_DB request. NOTE: some of these details are obtained from third party information.

Publish Date : 2009-07-13 Last Update Date : 2018-10-10

- CVSS Scores & Vulnerability Types

CVSS Score	8.5
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satistified to exploit)
Authentication	Single system (The vulnerability requires an attacker to be logged into the system (such as at a command line or via a desktop session or web interface).)
Gained Access	Admin
Vulnerability Type(s)	Denial Of Service
CWE ID	134

Figure 5: Port 3306 exploit (CVE-2009-2446, 2018)

Figure 5 displays an exploit within port 3306 which is running MYSQL 5.0.51a; this exploit also exposes a denial of service attack using “format strings in the dispatch_command function.” This software exploit requires the attacker to have some authentication and renders the website/server completely offline and threatening the confidentiality, integrity and availability of the server, as the attacker has complete access to all information stored through SQL; this means the integrity and confidentiality of the data stored is now compromised as they have complete roam of all the information (CVE-2009-2446, 2018).

Once the confidentiality, integrity and availability of a server is exposed, there are many implications to a business. These implications could be that the business could lose out on customers if their services are no longer available to their clients, as they cannot access the site if it is encountering a denial of service attack. Another implication is that the information that is meant to be kept secure is now in the hands of the attacker, and they can willingly use that information against both the business and their customers. When all three of these are exposed the business loses potential and current customers that use their site as they see them as unreliable and not secure, especially as they are handling their information.

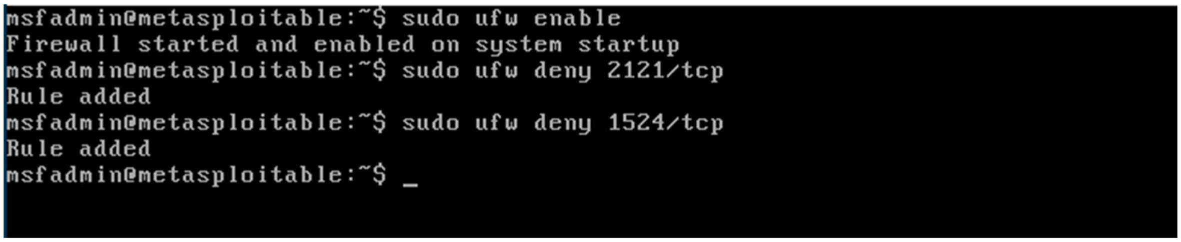
Task C – Mitigation

Firewalls Background

A firewall is part of the computers network security and is located within the computer system/host as a piece of software or hardware. The firewall can monitor what traffic comes in and goes out of the systems network and it has a specific set of rules that can allow certain network traffic packets through, "traffic into or out of a computer filtered through ports" (Firewall – Community Help Wiki, 2018).

For Linux based operating systems the set of rules for an Uncomplicated Firewall are set up by the user through the command prompt, "sudo ufw allow 53/tcp allows incoming tcp packets on port 53" (UFW – Community Help Wiki, 2018). From this, users can set up their own set of rules for their server/host machine and limit the amount of traffic that comes in. The result would be that the user would have achieved their goal of protecting themselves from service exploits that may be running on their server, or even their own system.

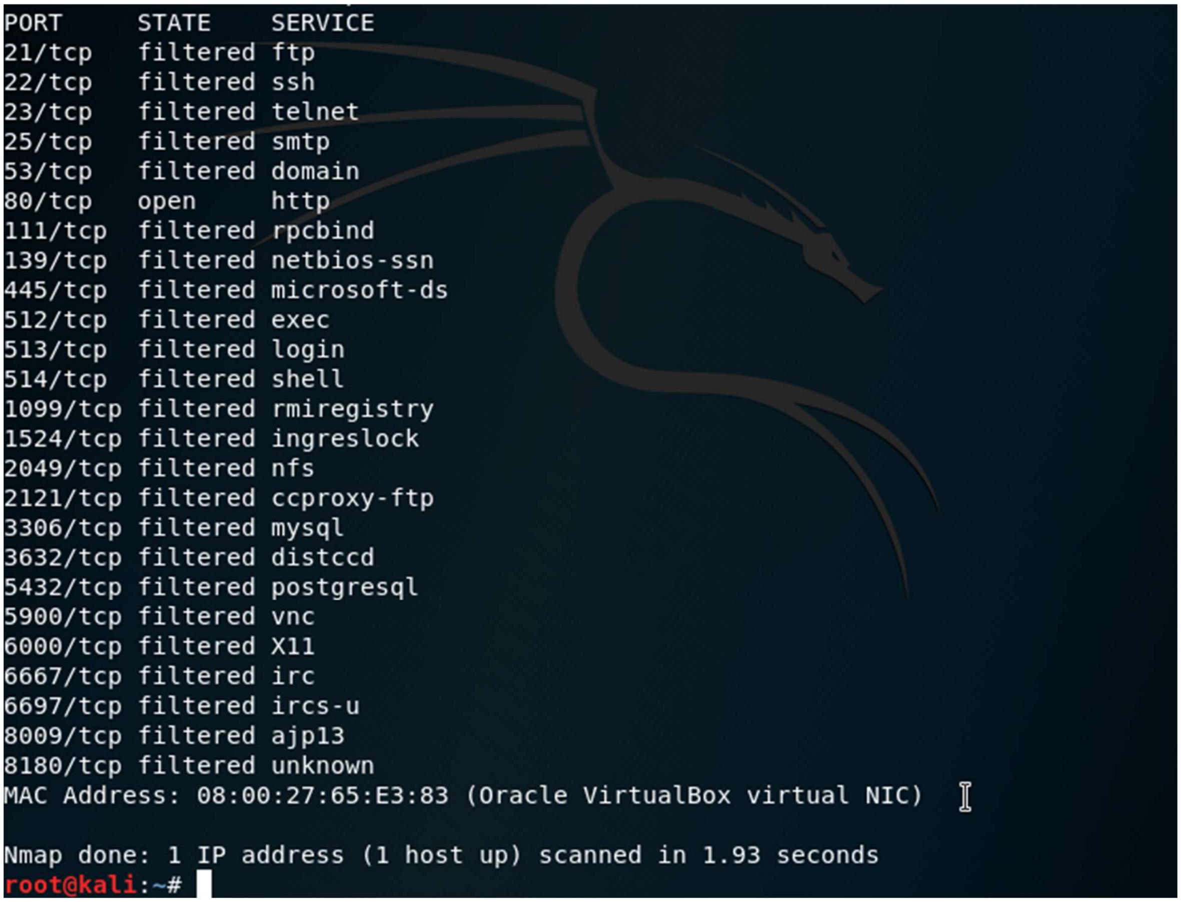
IP Tables Background and Deployment



```
msfadmin@metasploitable:~$ sudo ufw enable
Firewall started and enabled on system startup
msfadmin@metasploitable:~$ sudo ufw deny 2121/tcp
Rule added
msfadmin@metasploitable:~$ sudo ufw deny 1524/tcp
Rule added
msfadmin@metasploitable:~$ _
```

Figure 6: Setting up firewall rules

Figure 6 shows the rules of the firewall being set up, there is a much faster way of blocking all ports but port 80. This can be done by setting the firewall to deny all ports by default and allowing port 80 only (UFW – Community Help Wiki, 2018).



```
PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
53/tcp   filtered domain
80/tcp   open     http
111/tcp  filtered rpcbind
139/tcp  filtered netbios-ssn
445/tcp  filtered microsoft-ds
512/tcp  filtered exec
513/tcp  filtered login
514/tcp  filtered shell
1099/tcp filtered rmiregistry
1524/tcp filtered ingreslock
2049/tcp filtered nfs
2121/tcp filtered ccproxy-ftp
3306/tcp filtered mysql
3632/tcp filtered distccd
5432/tcp filtered postgresql
5900/tcp filtered vnc
6000/tcp filtered X11
6667/tcp filtered irc
6697/tcp filtered ircs-u
8009/tcp filtered ajp13
8180/tcp filtered unknown
MAC Address: 08:00:27:65:E3:83 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.93 seconds
root@kali:~#
```

Figure 7: Filtered ports

For this task another port scan was run with the same command from figure 2 before figure 7. Figure 7 shows the results of that port scan again; every port is now closed/filtered apart from port 80. This was done to reduce the amount of security vulnerabilities that the server had exposed; port 80 is left open because it narrows down all internet traffic to a single port and it is the default port that is used for a HTTP website/web server. Therefore, if this port wasn't open nobody would be able to access the website/server any other way (Berners-Lee and Conolly, 2018).

Additional Mitigation Approaches

The Collins dictionary states that “defence is action that is taken to protect someone or something against attack” (Defence definition and meaning | Collins English Dictionary, 2018). Defence is the process in which a person would set up multiple methods much like a firewall with rules to prevent other users from gaining access so easily, these are known as countermeasures.

When it comes to additional mitigation for a server, the damage done can be reduced with a few of these technical and non-technical methods:

- Creating regular backups of the server, both before and after changes have been made to the server. The backups made should not be fully stored on the same disk/storage drive.

- An uninterrupted power supply should be a must have in case there is a power cut, otherwise the server would lose all data that has not been stored to a recent backup.

- Limiting the amount of access to the server room stops anyone causing physical damage to the server hardware. Making a secure room with biometrics or even a key card to gain access to the room would help monitor who enters and leaves.

- Setting user privileges would limit the permissions and access rights each user has on the network, making them have the right level of access for their role and nothing else.

References

Berners-Lee, T., Fielding, R. and Nielsen, H. (2018). [online] Rfc-editor.org. Available at: https://www.rfc-editor.org/rfc/rfc1945.txt [Accessed 10 Nov. 2018].

Chapter 6. Virtual networking. (2018) Virtualbox.org. [Online] [Accessed on 15 November 2018] https://www.virtualbox.org/manual/ch06.html#network_nat.

Computer Misuse Act 1990. (2018) Legislation.gov.uk. [Online] [Accessed on 10 November 2018] http://www.legislation.gov.uk/ukpga/1990/18/crossheading/computer-misuse-offences.

CVE-2009-2446. (2018) Cvedetails.com. [Online] [Accessed on 12 November 2018] https://www.cvedetails.com/cve/CVE-2009-2446/.

CVE-2015-8461. (2018) Cvedetails.com. [Online] [Accessed on 12 November 2018] https://www.cvedetails.com/cve/CVE-2015-8461/.

Defence definition and meaning | Collins English Dictionary. (2018) Collinsdictionary.com. [Online] [Accessed on 12 December 2018] https://www.collinsdictionary.com/dictionary/english/defence.

Firewall - Community Help Wiki. (2018) Help.ubuntu.com. [Online] [Accessed on 10 December 2018] https://help.ubuntu.com/community/Firewall.

Lyon, G. (2018) *Chapter 15. Nmap Reference Guide | Nmap Network Scanning*. Nmap.org. [Online] [Accessed on 10 November 2018] https://nmap.org/book/man.html#man-description.

RFC 793. (2018) Rfc-editor.org. [Online] [Accessed on 12 December 2018] https://www.rfc-editor.org/rfc/pdfrfc/rfc793.txt.pdf.

Service and Version Detection | Nmap Network Scanning. (2018) Nmap.org. [Online] [Accessed on 10 December 2018] https://nmap.org/book/man-version-detection.html.

UFW - Community Help Wiki. (2018) Help.ubuntu.com. [Online] [Accessed on 10 December 2018] https://help.ubuntu.com/community/UFW.

Whitaker, A. and Newman, D. (2018) *Port Scanning > Penetration Testing and Network Defense: Performing Host Reconnaissance*. Ciscopress.com. [Online] [Accessed on 11 November 2018] http://www.ciscopress.com/articles/article.asp?p=469623&seqNum=3.