Penetration Testing Report

Tony Acosta Hernandez

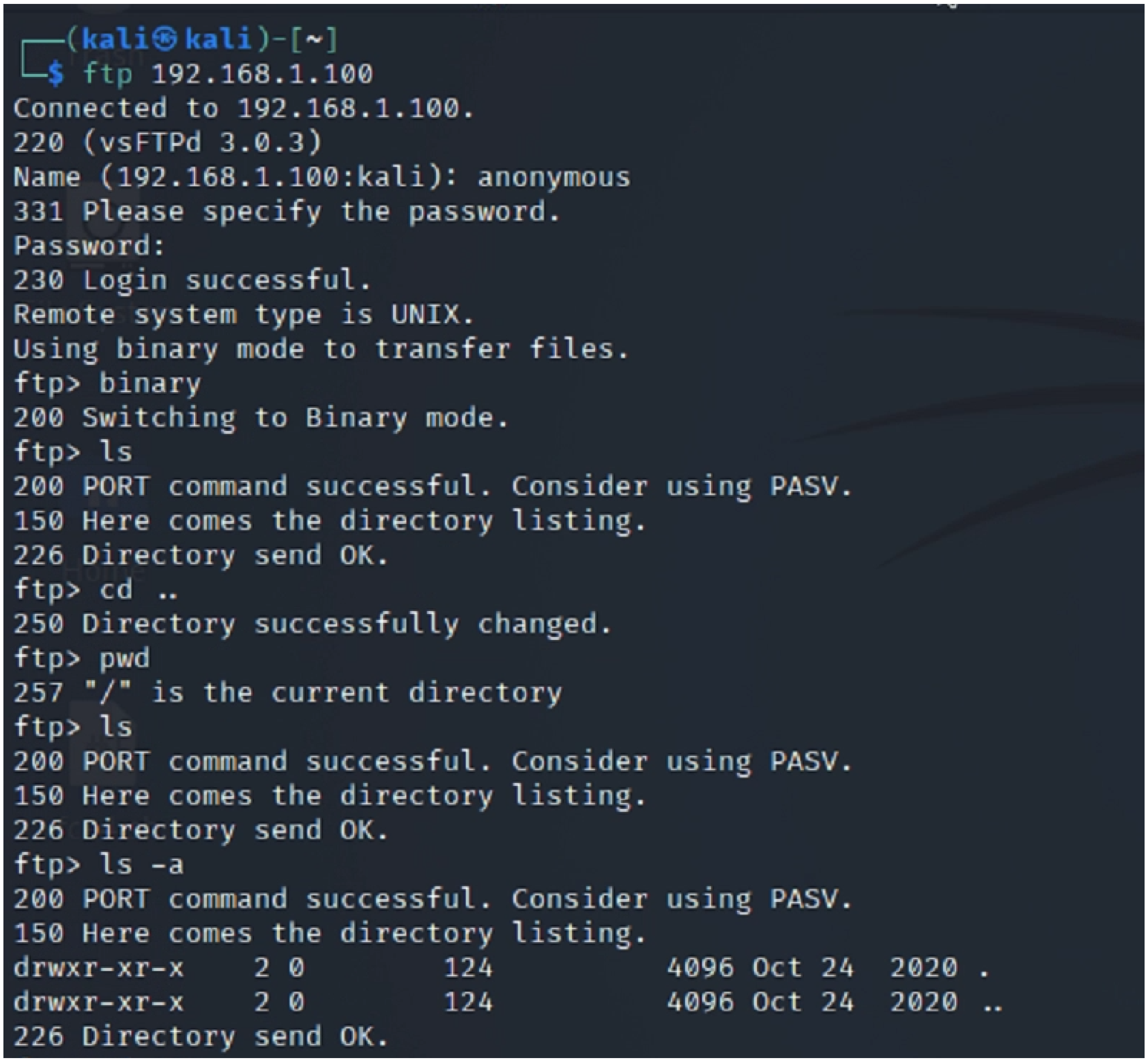
Executive Summary

A penetration test was performed on the machine “acme”, with IP address 192.168.1.100. After the penetration test was conducted, a myriad of issues and vulnerabilities with the machine was revealed. As such, the host machine 192.168.1.100 should be considered a security liability and any information that is on that machine is liable to be compromised. The following report details the vulnerabilities that were found, the ways in which these vulnerabilities were exploited to gain access to the system, and the remediations that are necessary to repair these vulnerabilities.

Summary of Vulnerabilities

The target machine, 192.168.1.100, has several vulnerabilities that can be exploited by malicious attackers. Most of these vulnerabilities stem from several ports that remain open and unfiltered. Some of these ports include:

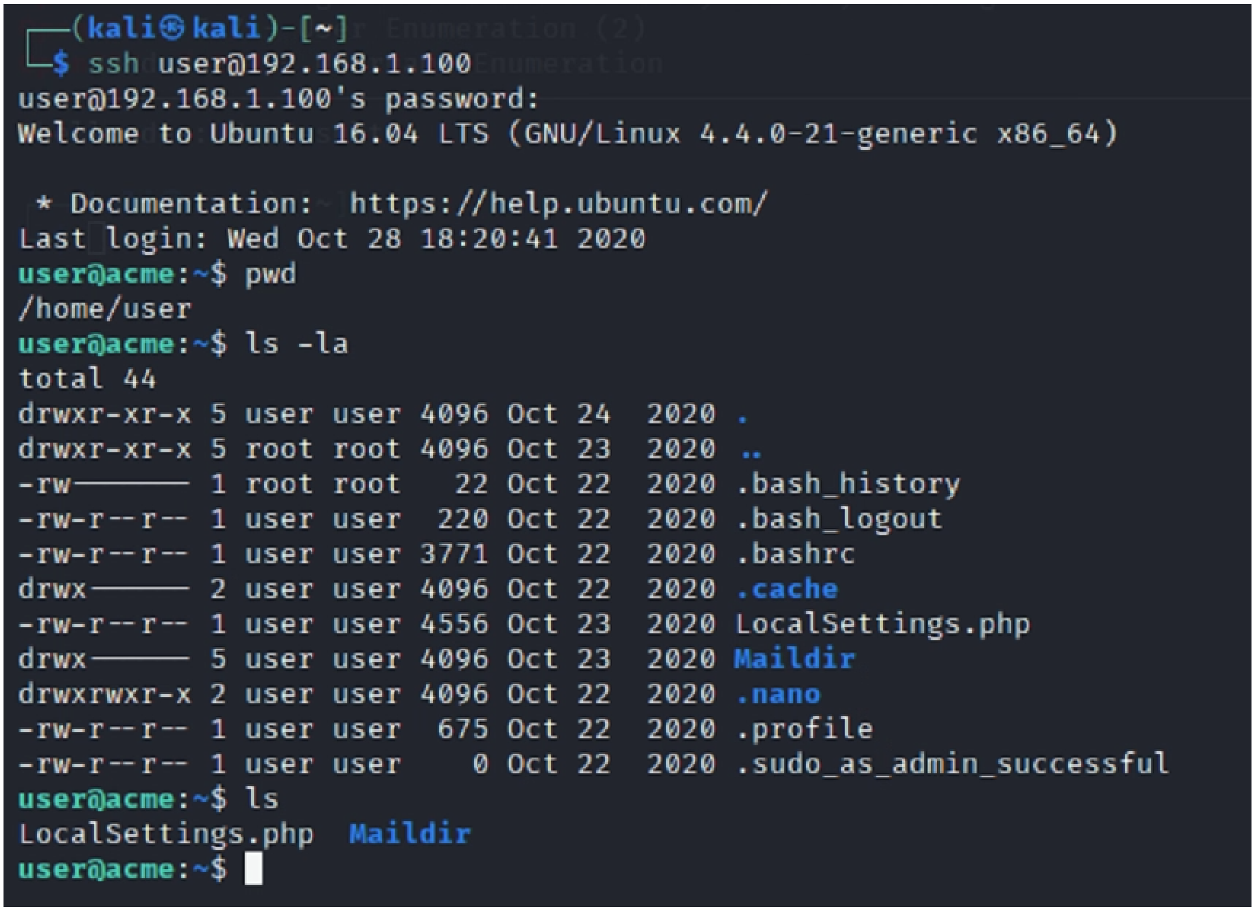
- Port 21/tcp - FTP service
  - The unfiltered FTP port can be exploited to gain access to the remote system. This can be done in two ways: Anonymous login and a credential login. After gaining access, an attacker can view the directories and files.



```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.1.100
Connected to 192.168.1.100.
220 (vsFTPd 3.0.3)
Name (192.168.1.100:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> binary
200 Switching to Binary mode.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> cd ..
250 Directory successfully changed.
ftp> pwd
257 "/" is the current directory
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> ls -a
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        124          4096 Oct 24  2020 .
drwxr-xr-x    2 0        124          4096 Oct 24  2020 ..
226 Directory send OK.
```

- Remediation: Disabling anonymous login as well as filtering the port is a quick and simple way to remediate this vulnerability. FTP connections should only be allowed from verified accounts and locations

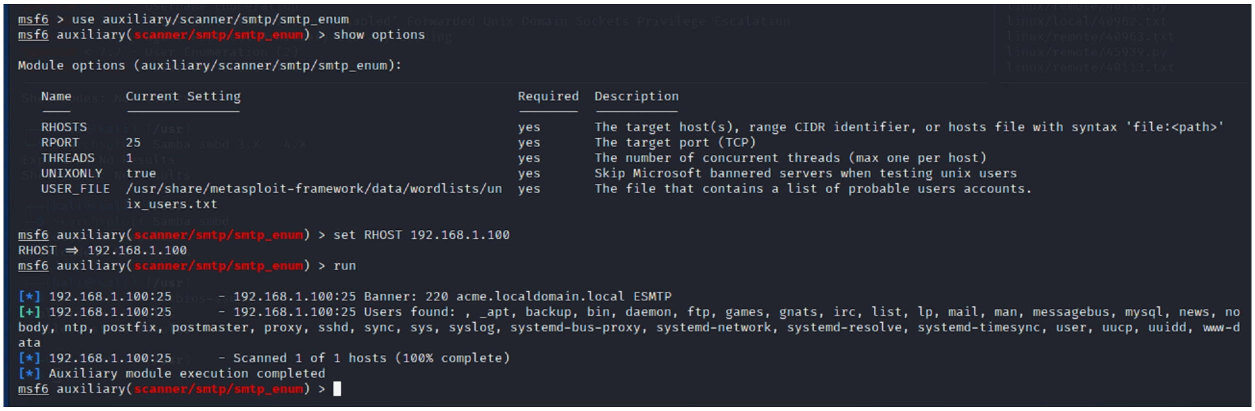
- Port 22/tcp - SSH service
  - The unfiltered SSH port can be exploited to gain access to the remote system. If a list of users on the system is known, an attacker can brute force the password to gain access to the directories and files that are available.



```
┌──(kali㉿kali)-[~]
└─$ ssh user@192.168.1.100
user@192.168.1.100's password:
Welcome to Ubuntu 16.04 LTS (GNU/Linux 4.4.0-21-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
Last login: Wed Oct 28 18:20:41 2020
user@acme:~$ pwd
/home/user
user@acme:~$ ls -la
total 44
drwxr-xr-x 5 user user 4096 Oct 24  2020 .
drwxr-xr-x 5 root root 4096 Oct 23  2020 ..
-rw------- 1 root root   22 Oct 22  2020 .bash_history
-rw-r--r-- 1 user user  220 Oct 22  2020 .bash_logout
-rw-r--r-- 1 user user 3771 Oct 22  2020 .bashrc
drwx------ 2 user user 4096 Oct 22  2020 .cache
-rw-r--r-- 1 user user 4556 Oct 23  2020 LocalSettings.php
drwx------ 5 user user 4096 Oct 23  2020 Maildir
drwxrwxr-x 2 user user 4096 Oct 22  2020 .nano
-rw-r--r-- 1 user user  675 Oct 22  2020 .profile
-rw-r--r-- 1 user user    0 Oct 22  2020 .sudo_as_admin_successful
user@acme:~$ ls
LocalSettings.php  Maildir
user@acme:~$ █
```

- Remediation - Filtering the SSH port so only verified users can access the remote system using SSH would fix this vulnerability. Similarly, using a stronger username and password combination would significantly reduce the ease of brute forcing account logins.

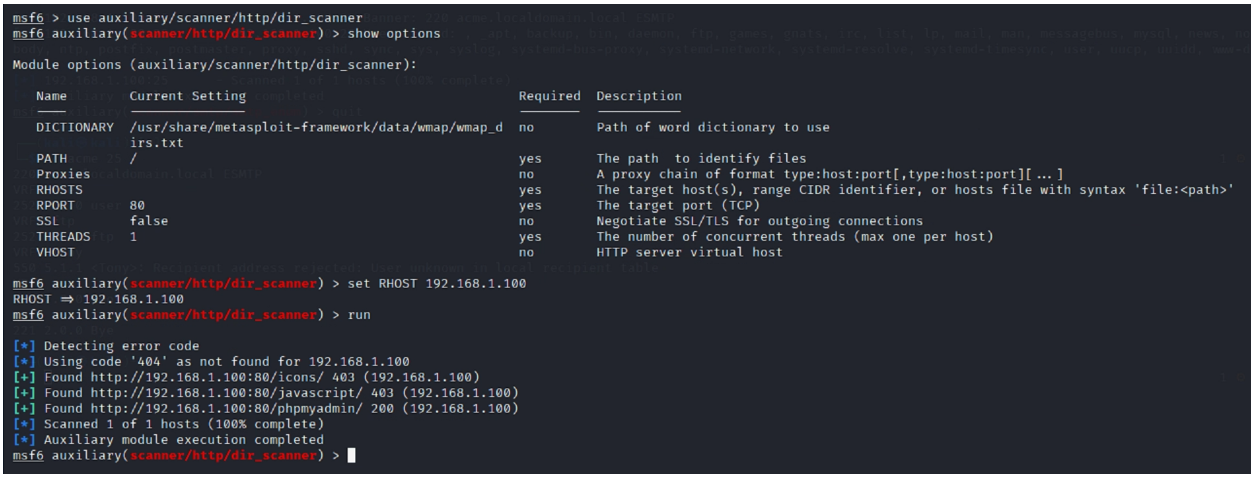
- Port 25/tcp - SMTP service
  - The unfiltered SMTP port can be exploited to gain information that can be used in further attacks, such as user enumeration that can give the different users that are online in the remote system.
  - The version of the SMTP server can also be exploited and used to make attacks on the system more accurate.



```
msf6 > use auxiliary/scanner/smtp/smtp_enum
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting                                    Required  Description
   ----       ---------------                                    --------  -----------
   RHOSTS                                                        yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      25                                                 yes       The target port (TCP)
   THREADS    1                                                  yes       The number of concurrent threads (max one per host)
   UNIXONLY   true                                               yes       Skip Microsoft bannered servers when testing unix users
   USER_FILE  /usr/share/metasploit-framework/data/wordlists/un  yes       The file that contains a list of probable users accounts.
              ix_users.txt

msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOST 192.168.1.100
RHOST ⇒ 192.168.1.100
msf6 auxiliary(scanner/smtp/smtp_enum) > run

[*] 192.168.1.100:25      - 192.168.1.100:25 Banner: 220 acme.localdomain.local ESMTP
[+] 192.168.1.100:25      - 192.168.1.100:25 Users found: , _apt, backup, bin, daemon, ftp, games, gnats, irc, list, lp, mail, man, messagebus, mysql, news, no
body, ntp, postfix, postmaster, proxy, sshd, sync, sys, syslog, systemd-bus-proxy, systemd-network, systemd-resolve, systemd-timesync, user, uucp, uuidd, www-d
ata
[*] 192.168.1.100:25      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) > █
```

- Remediation - The best method to protect against user enumeration would be to correctly configure the mail servers to prevent commands that can be run on it using metasploit that allow user enumeration attacks to happen.

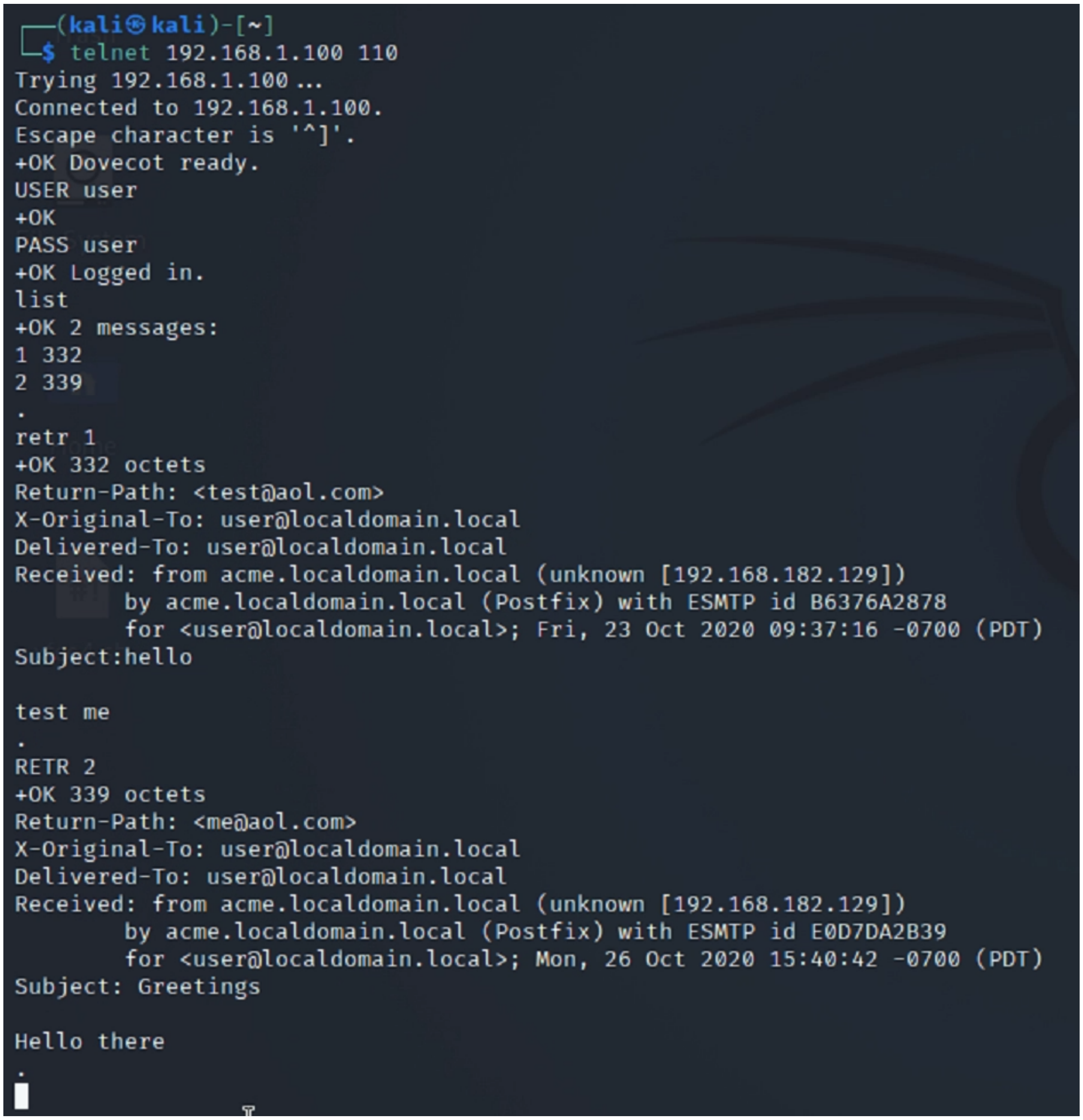
- Port 80/tcp - HTTP service
  - The unfiltered HTTP port can be exploited by attackers and used to gain information about the web server that is on the target machine.



```
msf6 > use auxiliary/scanner/http/dir_scanner
msf6 auxiliary(scanner/http/dir_scanner) > show options

Module options (auxiliary/scanner/http/dir_scanner):

   Name        Current Setting                                  Required  Description
   ----        ---------------                                  --------  -----------
   DICTIONARY  /usr/share/metasploit-framework/data/wmap/wmap_d  no        Path of word dictionary to use
               irs.txt
   PATH        /                                                yes       The path  to identify files
   Proxies                                                      no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                                                       yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT       80                                               yes       The target port (TCP)
   SSL         false                                            no        Negotiate SSL/TLS for outgoing connections
   THREADS     1                                                yes       The number of concurrent threads (max one per host)
   VHOST                                                        no        HTTP server virtual host

msf6 auxiliary(scanner/http/dir_scanner) > set RHOST 192.168.1.100
RHOST ⇒ 192.168.1.100
msf6 auxiliary(scanner/http/dir_scanner) > run

[*] Detecting error code
[*] Using code '404' as not found for 192.168.1.100
[+] Found http://192.168.1.100:80/icons/ 403 (192.168.1.100)
[+] Found http://192.168.1.100:80/javascript/ 403 (192.168.1.100)
[+] Found http://192.168.1.100:80/phpmyadmin/ 200 (192.168.1.100)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/dir_scanner) > █
```

- Remediation - To remediate this vulnerability, one should ensure that the web server protects against the ability for attackers to learn information about the site that shouldn't be accessed, such as information about the databases being used or what's in them. It should also defend against cross site scripting attacks.

- Port 110/tcp - POP3 service
    - The unfiltered POP3 port can be exploited to gain access to the mail server running on port 110. A connection can be made where a malicious hacker can login with credentials, retrieve, send and delete messages.



```
┌──(kali㉿kali)-[~]
└─$ telnet 192.168.1.100 110
Trying 192.168.1.100...
Connected to 192.168.1.100.
Escape character is '^]'.
+OK Dovecot ready.
USER user
+OK
PASS user
+OK Logged in.
list
+OK 2 messages:
1 332
2 339
.
retr 1
+OK 332 octets
Return-Path: <test@aol.com>
X-Original-To: user@localdomain.local
Delivered-To: user@localdomain.local
Received: from acme.localdomain.local (unknown [192.168.182.129])
        by acme.localdomain.local (Postfix) with ESMTP id B6376A2878
        for <user@localdomain.local>; Fri, 23 Oct 2020 09:37:16 -0700 (PDT)
Subject:hello

test me
.
RETR 2
+OK 339 octets
Return-Path: <me@aol.com>
X-Original-To: user@localdomain.local
Delivered-To: user@localdomain.local
Received: from acme.localdomain.local (unknown [192.168.182.129])
        by acme.localdomain.local (Postfix) with ESMTP id E0D7DA2B39
        for <user@localdomain.local>; Mon, 26 Oct 2020 15:40:42 -0700 (PDT)
Subject: Greetings

Hello there
.
```

Remediation - The POP3 port should be filtered and allow access from only verified users and systems. Similarly, the credentials for logging in should be more secure to prevent unauthorized access, and certain commands should be disabled so further information cannot be accessed by an attacker.

List of Tools Used

- Testing Platform: Linux 5.10.0.0-kali7-amd64
- Metasploit: Penetration Testing Framework
- Nmap: Network Scanner
- FTP: Communication Protocol for Transfer of Files
- SSH: Cryptographic Network Protocol
- Telnet: Application Protocol

Sources

https://resources.infosecinstitute.com/topic/writing-penetration-testing-reports/

https://www.offensive-security.com/

Course lectures and notes