Zenmap Intense Scan Results

This document is required to complete part of the course-wide project. The following are results of an Intense Scan performed in Zenmap.

```
Starting Nmap 6.40 ( http://nmap.org ) at 2018-08-04 09:20 Pacific Daylight
Time

NSE: Loaded 110 scripts for scanning.
NSE: Script Pre-scanning.
Initiating ARP Ping Scan at 09:20
Scanning 172.30.0.30 [1 port]
Completed ARP Ping Scan at 09:20, 0.23s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 09:20
Scanning 172.30.0.30 [1000 ports]
Discovered open port 139/tcp on 172.30.0.30
Discovered open port 53/tcp on 172.30.0.30
Discovered open port 23/tcp on 172.30.0.30
Discovered open port 5900/tcp on 172.30.0.30
Discovered open port 3306/tcp on 172.30.0.30
Discovered open port 445/tcp on 172.30.0.30
Discovered open port 80/tcp on 172.30.0.30
Discovered open port 21/tcp on 172.30.0.30
Discovered open port 111/tcp on 172.30.0.30
Discovered open port 22/tcp on 172.30.0.30
Discovered open port 25/tcp on 172.30.0.30
Discovered open port 8180/tcp on 172.30.0.30
Discovered open port 1524/tcp on 172.30.0.30
Discovered open port 8009/tcp on 172.30.0.30
Discovered open port 6667/tcp on 172.30.0.30
Discovered open port 5432/tcp on 172.30.0.30
Discovered open port 514/tcp on 172.30.0.30
Discovered open port 1099/tcp on 172.30.0.30
Discovered open port 6000/tcp on 172.30.0.30
Discovered open port 2121/tcp on 172.30.0.30
Discovered open port 2049/tcp on 172.30.0.30
Discovered open port 513/tcp on 172.30.0.30
Discovered open port 512/tcp on 172.30.0.30
Completed SYN Stealth Scan at 09:20, 0.41s elapsed (1000 total ports)
Initiating Service scan at 09:20
Scanning 23 services on 172.30.0.30
Completed Service scan at 09:20, 11.16s elapsed (23 services on 1 host)
Initiating OS detection (try #1) against 172.30.0.30
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is
disabled. Try using --system-dns or specify valid servers with --dns-servers
NSE: Script scanning 172.30.0.30.
Initiating NSE at 09:21
Completed NSE at 09:21, 31.80s elapsed
Nmap scan report for 172.30.0.30
```

Zenmap Intense Scan Results

```
Host is up (0.0022s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey: 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY,
ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
| ssl-cert: Subject: commonName=ubuntu804-
base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such
thing outside US/countryName=XX
| Issuer: commonName=ubuntu804-
base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such
thing outside US/countryName=XX
| Public Key type: rsa
| Public Key bits: 1024
| Not valid before: 2010-03-17T13:07:45+00:00
| Not valid after:  2010-04-16T13:07:45+00:00
| MD5:   dcd9 ad90 6c8f 2f73 74af 383b 2540 8828
|_SHA-1: ed09 3088 7066 03bf d5dc 2373 99b4 98da 2d4d 31c6
|_ssl-date: 2018-08-04T16:20:12+00:00; -50s from local time.
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-methods: No Allow or Public header in OPTIONS response (status code
200)
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2            111/tcp  rpcbind
|   100000  2            111/udp  rpcbind
|   100003  2,3,4       2049/tcp  nfs
|   100003  2,3,4       2049/udp  nfs
|   100005  1,2,3      46502/udp  mountd
|   100005  1,2,3      59389/tcp  mountd
|   100021  1,3,4      42125/tcp  nlockmgr
|   100021  1,3,4      58483/udp  nlockmgr
|   100024  1          37968/tcp  status
|_  100024  1          53793/udp  status
139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
```

```
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell?
1099/tcp open  java-rmi    Java RMI Registry
1524/tcp open  shell       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
| mysql-info: Protocol: 10
| Version: 5.0.51a-3ubuntu5
| Thread ID: 12
| Some Capabilities: Connect with DB, Compress, SSL, Transactions, Secure
Connection
| Status: Autocommit
|_Salt: !J1V>q@,XX0(v<hu5E>E
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    Unknown security type (33554432)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         Unreal ircd
| irc-info:
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   servers: 1
|   users: 1
|   lservers: 0
|   lusers: 1
|   uptime: 0 days, 0:57:59
|   source host: A46BC482.A40F3517.714E1E9C.IP
|_  source ident: nmap
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-methods: No Allow or Public header in OPTIONS response (status code
200)
|_http-title: Apache Tomcat/5.5
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port514-TCP:V=6.40%I=7%D=8/13%Time=53EB9060%P=i686-pc-windows-windows%r
SF:(NULL,33,"\x01getnameinfo:\x20Temporary\x20failure\x20in\x20name\x20res
SF:olution\n");
MAC Address: 62:BA:80:38:19:87 (Unknown)
```

Zenmap Intense Scan Results

```
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Uptime guess: 0.037 days (since Aug 4 08:27:52 2018)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=201 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Hosts:  metasploitable.localdomain, localhost,
irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| nbstat:
|   NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC:
<unknown>
|   Names
|     METASPLOITABLE<00>   Flags: <unique><active>
|     METASPLOITABLE<03>   Flags: <unique><active>
|     METASPLOITABLE<20>   Flags: <unique><active>
|     \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|     WORKGROUP<00>        Flags: <group><active>
|     WORKGROUP<1d>        Flags: <unique><active>
|_    WORKGROUP<1e>        Flags: <group><active>
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   NetBIOS computer name:
|   Workgroup: WORKGROUP
|_  System time: 2018-08-04T12:20:12-04:00

TRACEROUTE
HOP RTT     ADDRESS
1   2.16 ms 172.30.0.30

NSE: Script Post-scanning.
Initiating NSE at 09:21
Completed NSE at 09:21, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 55.81 seconds
           Raw packets sent: 1020 (45.626KB) | Rcvd: 1016 (41.430KB)
```