How to Use NMAP (2) on a Security Test

The standard TCP/UDP port scanning tool that we use when performing a penetration test is **nmap**. It allows us to identify open and closed ports on a target system. The following is the standard nmap command that will scan all UDP on a target IP address. The problem with such a scan is that it can take a very long time to complete. This is due to the way that **nmap** perform UDP scans. Remember that to perform a UDP scan you will need have either **root** or **administrator** level privileges.

```
$ sudo nmap -sU -p 0-65535 192.168.2.12
```

So, the best way to perform a UDP scan using nmap is specify the UDP ports that we wish to scan. The standard UDP ports are listed below.

UDP Port	Port Description
20	FTP Default Data (FTP)
21	FTP Default Control (FTP)
22	Secure Shell (SSH)
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name System (DNS)
69	Trivial Transfer Protocol (TFTP)
79	Finger
92	Network Printing Protocol (NNP)
109	Post Office protocol version 2 (POP2)
110	Post Office protocol version 2 (POP3)
135	PROFILE Naming System
137	NETBIOS Name Service
138	NETBIOS Datagram Service
139	NETBIOS Session Service
161	Simple Network Management protocol (SNMP)
389	Light Data Access Protocol (LDAP)
443	HTTPS over TLS/SSL
541	UUCP-rlogin
3268	Microsoft Global Catalog
3269	Microsoft Global Catalog with LDAP/SSL

We can start to perform UDP scanning my targets specific ports. The following we will perform a UDP scan against TFTP (USP/69) and SNMP (UDP/161).

```
$ sudo nmap -sU -p 69,161 192.168.2.12
Password:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-04 15:00 BST
Nmap scan report for 192.168.2.13
Host is up (0.00056s latency).

PORT    STATE         SERVICE
69/udp open|filtered tftp
161/udp closed        snmp
MAC Address: 00:0C:29:71:F5:CD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
$
```