How to Use NMAP (3) on a Security Test

When port scanning a Microsoft Windows Server, and some Linux/Unix servers, they can block discovery via techniques such as Ping. They do this via blocking all ICMP traffic at the firewall. Thus, the following will always yield a negative result.

```
$ ping 172.16.2.101
PING 172.16.2.101 (172.16.2.101) 56(84) bytes of data.
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
--- 172.16.2.101 ping statistics ---
5packets transmitted, 0 received, 100% packet loss, time 0ms
rtt min/avg/max/mdev = 1.100/1.100/1.100/0.000 ms
$
```

However, if we scan standard ports then we can identify systems. For example, the following is a standard scan of a Windows Server 2008. Nmap is configured using the **-Pn** option so that it does not perform an Ping Scan prior to performing a port scan

```
$ nmap -Pn -sT -p 0-1000 172.16.2.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-02 08:12 EDT
Nmap scan report for 172.16.2.101
Host is up (0.0014s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
88/tcp  open  kerberos-sec
135/tcp open  msrpc
139/tcp open  netbios-ssn
389/tcp open  ldap
445/tcp open  microsoft-ds
464/tcp open  kpasswd5
593/tcp open  http-rpc-epmap
636/tcp open  ldapssl
$
```

The key point to note is that systems such as servers provide services via TCP/UDP to other computers on the network. Unless these services have strict access control policies that limit access to a specific IP address then we can access the services via accessing the ports. In addition, specific systems such as Microsoft Servers will run specific ports that allow us to identify them. For example, a Typical Microsoft Servers will run the following TCP ports.

• 53/tcp	DNS Domain Name Services
• 80/tcp	HTTP Web Service
• 88/tcp	Kerberos Authentication Service
• 135/tcp	Microsoft RCP Services
• 139/tcp	Microsoft NETBIOS Service
• 389/tcp	LDAP/Active Directory Service
• 445/tcp	Microsoft SMB Service
• 464/tcp	Kerberos Authentication Password Service
• 636/tcp	LDAP/Active Directory Service OVER SSL