SCAN TECHNIQUES

Danilo Vizzarro
info@danilovizzarro.it

29 March 2007

Scan Techniques

The port scanning techniques are used to identify the open ports on a target machine. All the scans can be identified by using an Intrusion Detection System like Snort. The following report will discuss the different kinds of scans.

TCP CONNECT() SCAN

This type of scan, the attacker will send a SYN packet to all the ports of the target machine. If one or more ports are open, the target will reply with a SYN|ACK packet, and the attacker will complete the handshake with an ACK packet. If the ports are closed the target will reset the connection by sending an RST packet. The TCP Connect() Scan can be executed by the following command:

```
[root@localhost ~]# nmap -sT 192.168.1.22
```

SYN SCAN

This is a scan that differs from the TCP Connect() Scan because the handshake never gets completed. The attacker will send a SYN packet to all the ports of the target, and in case one or more ports are open, it will receive a SYN|ACK packet. At this point the attacker will reset the connection by sending an RST packet. If the ports are closed, the target will reset the con-

nection by sending an RST packet. In both cases the handshake will never be completed. The SYN Scan can be executed by the following command:

```
[root@localhost ~]# nmap -sS 192.168.1.22
```

FIN SCAN

This is a different type of scan where the attacker sends packets that have only the FIN flag active to all the ports of the target. For the open ports, the target will ignore the packets, for the closed ports it will reply with RST packets. The FIN Scan can be executed by the following command:

```
[root@localhost ~]# nmap -sF 192.168.1.22
```

XMAS SCAN

This scan is similar to the FIN Scan where instead of sending a FIN packet, is sent a FIN|URG|PSH packet.

The XMAS Scan can be executed by the following command:

```
[root@localhost ~]# nmap -sX 192.168.1.22
```

NULL SCAN

This scan is similar to the FIN Scan and to the XMAS Scan with the difference that the TCP packet has no flag active. The NULL Scan can be executed by the following command:

```
[root@localhost ~]# nmap -sN 192.168.1.22
```

UDP SCAN

This is a kind of scan used to discover the opened UDP ports. The UDP packets are sent to all the ports and if they are opened, the target will not

reply, otherwise it will reply with an ICMP Port Unreachable packet. The UDP Scan can be executed by the following command:

```
[root@localhost ~]# nmap -sU 192.168.1.22
```

DECOY SCAN

The Decoy Scan is a technique that implements the IP Spoofing. Its aim is to hide the real source of the scan. The Decoy Scan can be executed by the following command:

```
[root@localhost ~]# nmap -sS 192.168.1.22 -D 1.1.1.1,2.2.2.2
```

After the option '-D´ there is the possibility to specify different IP addresses. In our example, the target will receive to each port scanned 3 packets, one from the real attacker, one from the IP address 1.1.1.1 and one from the IP address 2.2.2.2. The result is that the target will think that 3 attackers are scanning its machine all together simultaniously. When hundreds of spoofed IP addresses are executing the scan on the same machine, it will be very difficult to identify the real attacker.

IDLE SCAN

The Idle Scan is a complex technique which permit to be quite hidden. This scan require 3 players: an attacker, a zombie and a target. The zombie should not generete other traffic except the one of interest to the attacker.

- The attacker will send a SYN|ACK packet to one port of the zombie that will reply with an RST packet containing the IP ID.
- The attacker will send a spoofed SYN packet to one port of the target using the address of the zombie.

- If the port is closed the target will reply to the zombie with an RST packet and the zombie will not increment the IP ID, if the port is open the target will reply with a SYN|ACK packet and the zombie will increment of 1 the IP ID.
- The attacker will send another SYN|ACK packet to the zombie and check if the IP ID has been incremented or not.

PING SCAN

This scan is used to detected which hosts are online in a network. The Ping Scan can be executed by the following command:

```
[root@localhost ~]# nmap -sP 192.168.1.*
```

OS FINGERPRINTING

The OS Fingerprinting is a technique used to discover the Operating System of the target. It can be executed by the following command:

```
[root@localhost ~]# nmap -sO 192.168.1.22
```