CERT Incident Note IN-98.04: Advanced Scanning

The CERT Coordination Center publishes incident notes to provide information about incidents to the Internet community.

Advanced Scanning

Tuesday, September 29, 1998

We have received reports of two scanning techniques being used by intruders to map networks and identify systems:

- "Stealth" scanning
- Scanning to identify system or network architecture

In addition to the reports we have received, the Dahlgren Division of the Naval Surface Warfare Center has published information indicating that multiple intruders may be using these attacks in a coordinated effort. This information is available at

http://www.nswc.navy.mil/ISSEC/CID/co-ordinated_analysis.txt

Stealth Scanning

The "stealth" scans appear to have a common goal: to gather information about target sites while avoiding detection by using techniques that might be overlooked by intrusion detection systems and system administrators. These techniques include

- Inverse Mapping

  In an 'Inverse Mapping' scan, intruders send packets that normally would go unnoticed or cause no unusual behavior to a list of addresses. For hosts that do not exist, however, routers will return an ICMP *host unreachable* message. By determining what hosts *do not* exist, an intruder can infer what hosts *do* exist, and so gain information about the structure of your network.

  Any packet type can be used to generate the ICMP *host unreachable* message, but we have received reports that intruders are actively using RESET packets, SYN-ACK packets, and DNS response packets for which no query was ever made.

- Slow Scans

  In a "slow scan" intruders scan the network at a slow rate that is likely to avoid detection. These types of scans are difficult to detect automatically, because you must maintain a history of all the packets you've received in order to detect new packets that may be related to old traffic.

Scanning to Identify System or Network Architecture

Intruders have also employed scanning techniques to identify the operating system used by a particular host, or to determine information about the structure of the target network. A tool recently released, called *queso*, relies on the variations in response to unexpected packets to determine the operating system of a particular host.

That is, *queso* sends unexpected packets to a host and examines the response. Because the packets are unexpected, there is no standard response, and so each operating system is free to respond in a unique way. By examining the responses to these unexpected packets, *queso* can determine the kinds of operating systems and TCP/IP stacks installed on your network. This information can be used by an intruder to optimize attacks on your network, or to identify sets of machines with particular vulnerabilities.

This is similar in effect to the scans described in

http://www.cert.org/incident_notes/IN-98.01.irix.html

except that *queso* recognizes a variety of operating systems, whereas the scans described in Incident Note 98.01 recognized only IRIX.

The following excerpt from tcpdump shows a queso probe against a machine running Solaris 2.5.1. (Information in boldface type indicates the target system's first response packet.)

```
server.24728 > solaris1.local.10.in-addr.arpa.telnet: S 1119794168:1119794168(0) win 4660
solaris1.local.10.in-addr.arpa.telnet > server.24728: S 442322772:442322772(0) ack 1119794169 win 9112 <mss 536>
(DF)
server.24728 > solaris1.local.10.in-addr.arpa.telnet: R 1119794169:1119794169(0) win 0
server.24729 > solaris1.local.10.in-addr.arpa.telnet: S 1119794168:1119794168(0) ack 0 win 4660
solaris1.local.10.in-addr.arpa.telnet > server.24729: R 0:0(0) win 0 (DF)
server.24730 > solaris1.local.10.in-addr.arpa.telnet: F 1119794168:1119794168(0) win 4660
server.24731 > solaris1.local.10.in-addr.arpa.telnet: F 1119794168:1119794168(0) ack 0 win 4660
solaris1.local.10.in-addr.arpa.telnet > server.24731: R 0:0(0) win 0 (DF)
server.24732 > solaris1.local.10.in-addr.arpa.telnet: SF 1119794168:1119794168(0) win 4660
solaris1.local.10.in-addr.arpa.telnet > server.24732: S 442455494:442455494(0) ack 1119794169 win 9112 <mss 536>
(DF)
server.24732 > solaris1.local.10.in-addr.arpa.telnet: R 1119794169:1119794169(0) win 0
server.24733 > solaris1.local.10.in-addr.arpa.telnet: P win 4660
server.24734 > solaris1.local.10.in-addr.arpa.telnet: S 1119794168:1119794168(0) win 4660
solaris1.local.10.in-addr.arpa.telnet > server.24734: S 442581319:442581319(0) ack 1119794169 win 9112 <mss 536>
(DF)
server.24734 > solaris1.local.10.in-addr.arpa.telnet: R 1119794169:1119794169(0) win 0
```

The following excerpt, also from tcpdump, shows a *queso* probe against a machine running NT Workstation 4.0:

```
server.5856 > ntwork1.nt.local.netbios-ssn: S 1276897729:1276897729(0) win 4660
ntwork1.nt.local.netbios-ssn > server.5856: S 285465669:285465669(0) ack 1276897730 win 8576 <mss 1460> (DF)
server.5856 > ntwork1.nt.local.netbios-ssn: R 1276897730:1276897730(0) win 0
server.5857 > ntwork1.nt.local.netbios-ssn: S 1276897729:1276897729(0) ack 0 win 4660
ntwork1.nt.local.netbios-ssn > server.5857: R 0:0(0) win 0
server.5858 > ntwork1.nt.local.netbios-ssn: F 1276897729:1276897729(0) win 4660
ntwork1.nt.local.netbios-ssn > server.5858: R 0:0(0) ack 1276897730 win 0
server.5859 > ntwork1.nt.local.netbios-ssn: F 1276897729:1276897729(0) ack 0 win 4660
ntwork1.nt.local.netbios-ssn > server.5859: R 0:0(0) win 0
server.5860 > ntwork1.nt.local.netbios-ssn: SF 1276897729:1276897729(0) win 4660
ntwork1.nt.local.netbios-ssn > server.5860: S 285465749:285465749(0) ack 1276897730 win 8576 <mss 1460> (DF)
server.5860 > ntwork1.nt.local.netbios-ssn: R 1276897730:1276897730(0) win 0
server.5861 > ntwork1.nt.local.netbios-ssn: P win 4660
ntwork1.nt.local.netbios-ssn > server.5861: R 0:0(0) ack 1276897729 win 0
server.5862 > ntwork1.nt.local.netbios-ssn: S 1276897729:1276897729(0) win 4660
ntwork1.nt.local.netbios-ssn > server.5862: S 285465789:285465789(0) ack 1276897730 win 8576 <mss 1460> (DF)
server.5862 > ntwork1.nt.local.netbios-ssn: R 1276897730:1276897730(0) win 0
```

Note that the responses of the two operating systems differ as early as the first response packet (highlighted above). By comparing these differences to a dictionary of known response characteristics, *queso* is often able to determine the type of operating system employed by the target machine. Users can also extend *queso* to distinguish other kinds of operating systems, or other devices that will respond to TCP/IP packets.

We have received reports of incidents in which intruders have launched coordinated scans that may have been used to discover information about the structure of the target network. By launching similar scans from two or more distinct networks against a single target network, and then comparing the different responses, intruders may be able to infer information about the structure of the target network. By using two or more networks to launch a scan against a third network, an intruder can

- Discover alternate routes into your network
- Infer aspects of the topology of your network
- Increase the bandwidth available to launch a denial of service attack
- Reduce the likelihood of detection

Conclusion

Intruders are using a variety of techniques to gain information about networks and systems on those networks. Intruders can use this information to tailor their attacks to target networks or to find a set of machines that share a certain vulnerability.

Intruders have recently used a number of very large-scale scans of the Internet looking for certain vulnerabilities, such as those discussed in

http://www.cert.org/incident_notes/IN-98.02.html

The ability to determine the types of operating systems in use helps intruders to focus their attacks on certain types of machines, or to modify their attacks to suit the target.

Do not presume that the topology of your network, the operating systems in use, the products used to connect to the Internet, and other externally visible characteristics are a secret. When you evaluate the security of your network, remember that this information can be discovered by intruders who can use it to their advantage.

Acknowledgements

Our thanks to Stephen Northcutt of the Naval Surface Warfare Center for his assistance.