

Real-World Scenarios 13-2: Deciphering Log Files

Scenario: The same organization used in Real-World Scenario 13-1 has concerns about its firewall. The IT director thinks that an attacker on the Internet is attempting to (and possibly succeeding in) bypassing the firewall, but doesn't know how it is potentially being done or what port is being used to do it.

What application/protocol can you use to easily analyze the firewall logs from your workstation?

How would you configure this on the firewall and at your workstation?

Describe a typical log message with attempted communication and the two main components of it.

If you see a message such as the one listed below, what does it tell you?

```
Tues Apr 21 12:36:01 2014 Cisco Firewall System Log: Blocked incoming TCP packet
```

```
From 64.58.137.211:23475 65.82.117.241:23 as SYN:ACK received but there is no active connection.
```

Real-World Scenarios 13-2 Solution

Use the Syslog protocol. Many Syslog programs are available, such as SolarWinds Kiwi Syslog Server. This can pull the logs from a firewall and other network devices so that you can watch them in real time from your workstation.

The firewall would need to have Syslogging enabled and configured to stream log messages to the IP address of your workstation. The firewall will generate a typical log message when someone on the Internet attempts to connect to it. It will have the source IP address and port as well as the destination IP address and port; for example:

S=207.50.135.54:23 – D=10.1.1.80:1

In the Case Study's Syslog message listed, you are told a lot of information, including the potential attacker's IP address and the port used, as well as the IP address of your firewall and the port that was attempted for access; in this case, port 23 Telnet. The important part here is that the TCP packet was *blocked*. So the firewall succeeded in blocking the potential attack and remained secure. However, devices will fail sometimes. The key is to fail securely. An example of a secure failure would be if a firewall let a packet through (which *will* happen) but the result was that the firewall was shut off immediately afterward by an automated mechanism. Another example would be if an IPS blocked a packet that was legitimate. This is a failure, but a secure one, albeit an inefficient one. Another example is if a WAP let a potential attacker through but redirected the person to a honeypot, or if the WAP shut down altogether.

If you believe that an attacker is possibly getting through the firewall, some active scanning will be appropriate. Connect to the firewall from the public side and use a port scanner such as Nmap or a vulnerability scanner such as Nessus (or both) to find out what (if any) open ports there are and if any of them are substantial vulnerabilities.

Video Solution: Watch the video solution "13-2: Deciphering Log Files."

Simulation: Complete the simulation "13-2: Deciphering Log Files."