CSCI 530: Security Systems

Lab 7: Intrusion Detection; Submission Due: November 15th 2024

Name: Anne Sai Venkata Naga Saketh
USC Email: annes@usc.edu
USC ID: 3725520208

Question 1:

What was the result of your test to determine the ping threshold size in the "Snort in ids mode" section above? That is, what's the smallest value for ping's "-s <size>" that triggers an alert?

Answer:
Ping’s -s <size> option has a minimum value of 801 that sets off an alert in intrusion detection mode.

Question 2:

In the /var/log/snort directory I find one file named alert and several files whose names begin with snort.log. What is the difference between their contents and purposes?

Answer:
The /var/log/snort directory has the alert file, which logs Snort alerts for suspicious activities detected on the network. These alerts are generated based on Snort’s rules and include details like event type, IP addresses, and timestamps. On the other hand, the snort.log files capture raw packet data and broader network traffic information. These files are great for in-depth analysis and troubleshooting of network events. The alert file focuses on specific security incidents, while the snort.log files provide a comprehensive record of traffic for detailed investigation.

Question 3:

Here is a sample snort alert:

```
[**] [1:1748:8] FTP command overflow attempt [**]
[Classification: Generic Protocol Command Decode] [Priority: 3]
11/24-14:02:32.735830 192.168.1.4:3247 -> 192.168.1.1:21
TCP TTL:128 TOS:0x0 ID:20571 IpLen:20 DgmLen:358 DF
***AP*** Seq: 0x1C5D5B76 Ack: 0x681EACAD Win: 0x4470 TcpLen: 20
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2002-0606][Xref =>
http://www.securityfocus.com/bid/4638]
```

Visit the URLs contained in it. What is the purpose of an "Xref" in a snort alert?

Answer:
The “Xref” feature in a Snort alert provides hyperlinks to external sources that offer comprehensive information about the specific security threat or vulnerability detected. These references assist users in comprehending the nature and impact of the alert by directing them to databases such as CVE or SecurityFocus, where technical details and remediation steps can be obtained. The Xrefs in the provided example pertain to a vulnerability in the 3Cdaemon 2.0 FTP server.

Question 4:

Here is a rule:

alert tcp $HOME_NET 23 -> $EXTERNAL_NET any (msg:"TELNET login incorrect"; content:"Login incorrect";)

Explain it. Under the circumstances the rule represents, who is doing what? where? State precisely to which packets the rule applies, and what is the resulting action when such packets are seen. Explain the difference between the roles played by the two embedded strings "TELNET login incorrect" (what's that? why is it there? what does it do?) versus "Login incorrect" (why is it there? what does it do?).

Answer:
This Snort rule is to detect failed Telnet login attempts from an internal network ($HOME_NET) to any external network ($EXTERNAL_NET) by monitoring TCP traffic on port 23. If the packet’s payload contains the phrase “Login incorrect,” indicating a failed login attempt, Snort raises an alert. The rule includes the string msg:”TELNET login incorrect”, informing users that it pertains to a failed Telnet login. The string content:”Login incorrect” is what Snort searches for within the packet’s data to detect the failed login attempt. Essentially, the first string provides the alert message, while the second string is the specific content Snort checks for in the packet to identify the event, helping to flag potential unauthorized access attempts.