Netscreen Firewall Log: Critical Message Report

```
Jun 2 11:24:16 fire00 sav00: NetScreen device_id=sav00 [Root]system-critical-00436:
Large ICMP packet! From 1.2.3.4 to 2.3.4.5, proto 1 (zone Untrust, int ethernet1/2).
Occurred 1 times. (2006-06-02 11:24:16)
[00001] 2007-04-01 15:32:00 [Root]system-critical-00031: arp req detected an IP
conflict (IP 10.1.1.1, MAC 0027f2424c8c) on interface ethernet1
[00001] 2007-03-12 12:47:36 [Root]system-critical-00001(second traffic alarm): Policy
ID=14 Rate=180 bytes/sec exceeds threshold
[00008] 2006-06-30 13:10:09 [Root]system-critical-00041: VPN 'zzz-primary-vpn' from
a.b.c.d is down.
[00002] 2006-06-30 13:11:41 [Root]system-critical-00040: VPN 'zzz-primary-vpn' from
a.b.c.d is up.
[00001] 2005-05-16 12:55:10 [Root]system-critical-00042: Replay packet detected on
IPSec tunnel on ethernet3 with tunnel ID 0x1c! From z.y.x.w to a.b.c.d/336, ESP, SPI
0xf63af637, SEQ 0xe337.
[00001] 2006-05-25 13:34:33 [Root]system-alert-00008: IP spoofing! From 10.1.1.238:80
to a.b.c.d:49807, proto TCP (zone Untrust, int ethernet3). Occurred 1 times.
```

Questions:

1. **What is the significance of the 'system-critical' and 'system-alert' tags in these logs?**

   A **system-critical** tag indicates that the alert is of high importance as it could impact the security of the network and thus requires immediate attention.

   A **system-alert** is a notification of any suspicious activity or issues, but are not necessarily as urgent.

2. **What is the importance of monitoring 'Large ICMP packets' and why they might be flagged in a firewall log?**

   Large ICMP packets can be indicative of certain types of attacks, such as a **Ping of Death** or **ICMP flood attacks**, which aim to disrupt network service by overwhelming a target with large or numerous ICMP packets. Firewalls flag these to prevent **potential denial of service (DoS)** attacks or to detect unusual activity that could indicate a network probe or reconnaissance.

3. **What could cause an "`arp req detected an IP conflict`" message, and what are the implications of such a conflict on a network?**

   An ARP request detecting an IP conflict occurs when two devices on the same network are configured with the same IP address. This can lead to **network disruptions** such as packet loss, communication delays, or one device being unable to access the network. It can also be a sign of **malicious activity**, like an ARP spoofing attack.

4. **The log mentions a policy ID 14 with a traffic rate exceeding a threshold. Why might exceeding a byte/second rate be of concern?**

   Exceeding a byte/second rate could indicate **malicious activity**, such as a flood attack or an unexpected surge in data transmission, which could overwhelm the network or indicate data exfiltration.

5. **What does it mean when a log entry states that a VPN `'zzz-primary-vpn'` is down and later back up? What impact could this have on network security and availability?**

   When a VPN is down, it means that the secure tunnel for transmitting data between networks is temporarily unavailable, which can interrupt secure communication and potentially expose data if it needs to be sent unencrypted. This can impact business operations that rely on the VPN for secure data transfer, as normal secure communications will need to be halted until the VPN is restored.

6. **The log reports a 'Replay packet detected on IPSec tunnel.' What is a replay attack, and why is it critical to detect these packets?**

   A replay attack occurs when an attacker captures network packets and re-sends them to the network to trick the system into performing unauthorized actions, such as re-authorizing a transaction. Detecting replay packets is critical because it prevents unauthorized access or transactions

Web Scan

```
OSSEC HIDS Notification.
 2006 Sep 12 09:45:56
 Received From: (spongebob) 1.2.3.4->/usr/pages/xx/logs/access_log
 Rule: 31106 fired (level 12) -> "A web attack returned code 200 (success)."
 Portion of the log(s):
 200.96.104.241 - - [12/Sep/2006:09:44:28 -0300] "GET
/modules.php?name=Downloads&d_op=modifydownloadrequest&%20lid=-1%20UNION%20SELECT%200
,username,user_id,user_password,name,%20user_email,user_level,0,0%20FROM%20nuke_users
HTTP/1.1" 200 9918 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET
CLR 1.1.4322)"
```

Questions:

1. **What type of attack is indicated by the log entry in the OSSEC notification and what information was the attacker trying to gain?**

   A SQL Injection attack, indicated by the presence of SQL syntax in the URL (UNION SELECT), which is a common method used by attackers to manipulate database queries and extract

unauthorized information. The attacker was attempting to acquire a list of stored usernames, passwords, ids, and emails.

2. **What does the HTTP status code ‘200’ indicate in the log entry?**

   It indicates that the request was successful and the server returned the requested resource.

3. **What relevant information does the log entry provide about the attacker and how might it be utilized to prevent future attacks?**

   The log entry provides the attacker's IP address (200.96.104.241) and the User-Agent string, which can be used to identify and block the attacker.

Anti Virus Application Log

```
8:55:30 AM | D:\Downloads\ChangeLog-5.0.4.scr | Quarantine Success
9:22:54 AM | C:\Program Files\Photo Viewer\ViewerBase.dll | Quarantine Failure
9:44:05 AM | C:\Sales\Sample32.dat | Quarantine Success
```

1. **What is being quarantined and how can you tell?**

   The log entries show file paths and indicate that the quarantining process is being used to isolate these files from the system. The presence of file paths along with status messages like "Quarantine Success" or "Quarantine Failure" confirms which files are affected and whether they were successfully isolated.

2. **What does the “Quarantine Success” and “Quarantine Failure” status indicate?**

   The **"Quarantine Success"** status indicates that the antivirus or anti-malware software successfully isolated the file from the system, preventing it from causing any harm.

   The **"Quarantine Failure"** status indicates that the file was unsuccessfully isolated.

3. **Why might a quarantine fail?**

   A quarantine could fail for a variety of reasons, such as the library already being in use by the operating system or having insufficient permissions to modify or move the file.

Resources:

https://www.ossec.net/docs/log_samples/

Professor Messer