**Log Analysis**

**Name:- Kundan Keshav Gawande**

**ID:- 28806**

1. **Firewall Logs**

**Allowed Traffic (Legitimate/Internal or Common Services)**

|  |  |  |
| --- | --- | --- |
| Log Entry | Details | Notes |
| [Allowed] TCP 192.168.1.10:5678 -> 8.8.8.8:53 | Internal to public DNS (Google DNS) over TCP | **DNS request**; uncommon over TCP but legitimate |
| [Allowed] UDP 192.168.1.15:12345 -> 10.0.0.1:161 | Internal to internal SNMP port | **SNMP query**, potentially network monitoring |
| [Allowed] TCP 192.168.1.5:22 -> 10.0.0.2:22 | Internal to internal SSH | Legitimate **SSH** communication |
| [Allowed] TCP 192.168.1.25:443 -> 172.217.0.14:443 | Internal to external HTTPS (Google IP) | Normal **web browsing** traffic |
| [Allowed] TCP 192.168.1.8:80 -> 192.168.1.1:3128 | Internal HTTP to local proxy (Squid) | Common for **proxy** usage |

**Denied Traffic (Potential Threats / Misconfigurations / Suspicious Behavior)**

|  |  |  |
| --- | --- | --- |
| Log Entry | Details | Analysis |
| [Denied] TCP 192.168.100.25:5555 -> 198.51.100.10:443 | Internal to external HTTPS from **uncommon port 5555** | **Suspicious**; could be malware/exfiltration |
| [Denied] ICMP 192.168.1.12 -> 203.0.113.1 | Ping attempt blocked | **Ping blocked** to external address; possibly scanning |
| [Denied] TCP 10.0.0.5:4444 -> 192.0.2.55:80 | Internal to external HTTP via **port 4444** | **Very suspicious**; port 4444 often used in backdoors |
| [Denied] TCP 192.168.1.19:7000 -> 185.199.108.153:8080 | High port to external **GitHub IP (port 8080)** | **Potential exfiltration or C2** communication attempt |
| [Denied] TCP 192.168.1.7:135 -> 198.18.0.1:135 | RPC traffic to external IP | **Risky**; port 135 should be internal only |

### ****Highlights & Recommendations****

#### 🚩 ****Abnormal Port Usage****

* **TCP 5555**, **4444**, and **7000** are high-risk ports often used by malware or unauthorized apps.
* **TCP 135** should be restricted to local network zones only.

#### 🌐 ****External Communication Attempts (Denied)****

* Several attempts to contact **external IPs** over **non-standard or high ports**, like:
  + 198.51.100.10:443 from port 5555
  + 185.199.108.153:8080
  + 192.0.2.55:80 from port 4444

These could indicate **attempts to bypass security measures or C2 communication**.

**2) IDS and IPS Logs**

**Log Analysis Breakdown**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Alert Type | Description | Indicators / Details | Severity | Action Recommended |
| Trojan | ET TROJAN ZLoader Checkin | Indicates **ZLoader malware** communication attempt | 🚨 **Critical** | Immediate endpoint scan; isolate if active |
| CVE Exploit | ET WEB\_SERVER Possible CVE-2021-41773 Apache Path Traversal | Apache vuln. allowing file read or RCE | 🚨 **High** | Patch Apache, check access logs |
| Policy | ET POLICY PE EXE or DLL Windows file download HTTP | File download of .exe or .dll over HTTP | ⚠️ **Medium** | May indicate malware delivery or unsafe practice |
| Reconnaissance | ET SCAN Suspicious inbound scan from 203.0.113.12 | External scan detected | ⚠️ **Medium** | Block source IP, monitor for follow-up attempts |
| Exploit | ET EXPLOIT Shellshock attempt in HTTP User-Agent | Legacy bash vuln. attempt | 🚨 **High** | Review logs, patch if still using vulnerable systems |
| Trojan | ET TROJAN Emotet Checkin | Known **Emotet malware** C2 communication | 🚨 **Critical** | Quarantine host, begin threat hunting |
| Malware | ET MALWARE TrickBot Beacon | TrickBot malware beaconing activity | 🚨 **Critical** | Investigate host, reset credentials |
| DDoS | ET DOS Possible NTP DDoS Amplification Response | NTP DDoS reflection | ⚠️ **Medium** | Check if local NTP is exposed; apply ACLs |
| P2P | ET P2P BitTorrent Handshake Detected | BitTorrent traffic | ⚠️ **Low-Medium** | May be policy violation, check user/system |
| Web Attack | ET WEB\_SERVER Suspicious .php upload attempt | Attempted upload of PHP file (webshell) | 🚨 **High** | Check for webshells, tighten upload rules |

### ****Critical / High-Priority Alerts****

1. **ZLoader, Emotet, TrickBot – Confirmed malware indicators, likely system compromise**
2. **CVE-2021-41773 – Vulnerable Apache system being targeted**
3. **Shellshock attempt – Old but still dangerous if system is unpatched**
4. **Suspicious PHP upload – Could lead to webshell/backdoor access**

### ****Moderate Issues to Investigate****

* **PE file downloads** – Check if it’s legit or unauthorized
* **NTP amplification** – Misuse of local NTP services
* **Inbound scanning** – Could be recon before an attack

### ****Low-Priority or Policy Violation****

* **BitTorrent handshake** – Likely a user violating acceptable use policy; low security risk unless paired with malware

**3) Proxy Logs**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IP Address | URL | Description | Severity | Reason |
| 192.168.1.10 | http://safe-site.com/page1.html | Legitimate webpage | ✅ Low | Normal site, standard content |
| 192.168.1.15 | http://malicious-site.ru/malware.exe | 🚩 Downloaded EXE from **Russian domain** | 🛑 **Critical** | High-risk malware download from foreign source |
| 192.168.1.20 | http://ads-trackers.net/track.js | Tracker script | ⚠️ Medium | Could indicate tracking/adware |
| 192.168.1.25 | http://cdn-images.com/img.png | Image from CDN | ✅ Low | Likely safe |
| 192.168.1.30 | http://suspiciousdomain.org/shell.txt | Text file with potential shell code | 🛑 **High** | File name suggests **web shell or script payload** |
| 192.168.1.40 | http://safe-site.com/index.html | Legit webpage | ✅ Low | No concern |
| 192.168.1.50 | http://download.com/tool.zip | Archive download | ⚠️ Medium | Might be legitimate, but needs inspection |
| 192.168.1.60 | http://malicious.com/virus.bin | Binary file from malicious domain | 🛑 **Critical** | Name and domain both indicate malware |
| 192.168.1.70 | http://trusted-site.com/style.css | CSS file | ✅ Low | Standard static content |
| 192.168.1.80 | http://unknown-source.net/download.exe | EXE from unknown site | 🛑 **High** | Suspicious executable from untrusted domain |

### ****Key Threat Indicators****

* **Executable downloads:**
  + .exe: malware.exe, download.exe
  + .bin: virus.bin
  + .zip: tool.zip (potential malware bundling)
* **Malicious / suspicious domains:**
  + malicious-site.ru, malicious.com, unknown-source.net, suspiciousdomain.org

**Recommendations**

|  |  |
| --- | --- |
| Action | Items |
| 🛑 Block access to: | malicious-site.ru, malicious.com, unknown-source.net, suspiciousdomain.org |
| 🔍 Scan hosts: | 192.168.1.15, 192.168.1.30, 192.168.1.60, 192.168.1.80 — for potential infections |
| 🧪 Sandbox/examine: | Files like malware.exe, virus.bin, download.exe, shell.txt |
| ⚠️ Educate users: | Avoid running unverified downloads or accessing unknown sources |

**Summary Table**

|  |  |  |
| --- | --- | --- |
| Status | Count | Description |
| 🛑 Critical | 4 | EXE/BIN downloads from shady domains |
| ⚠️ Moderate | 2 | Suspicious archives, trackers |
| ✅ Safe | 4 | Legitimate web traffic |