Andree Salvo

Southern New Hampshire University

3-2 Activity: Network Assessment Approach

Instructor: Robert Chubbuck

Approach

My approach to assessing the network involves a *layered approach* that integrates people, processes, and technology. According to Fortinet, ***"For cybersecurity to be effective, organizations must also consider how they leverage people and processes. When combined into a single, integrated framework, an overlapping strategy based on security tools, people, and processes will yield the most effective defenses." (Fortinet, 2019)*** For **people**, I would examine how well employees are trained to see how they avoid risks (like phishing or avoiding malicious links). For the **process**, I would implement an incident response plan to ensure that threats are being monitored and that our resources are aligned with protecting high-value information. As for **technology**, I would examine how the controls are integrated, rather than just focusing on individual solutions, and check for network segmentation. I would also see if technologies like deception are being employed to identify intruders.

Account

People: I would evaluate new and regular employees to ensure they follow security practices, such as using strong passwords/password hygiene, avoiding shadow IT, recognizing phishing emails, and refraining from clicking on links or images. This involves access privileges and training awareness.

Process: I'd take a look at organizational policies and procedures related to patch management, incident response, and change control to see if they are being followed and if they effectively reduce any sort of risk.

Technology: I would assess any network devices, servers, applications, and endpoints for vulnerabilities, misconfigurations, or outdated software. I'd also review logs, IDS/IPS rules, and firewall configurations to see if technical defenses align with policy and its best practices.

Tools

To get the full picture, these are the tools I would use:

1. **OpenVAS** – I would use OpenVAS to see what vulnerabilities are vulnerable and also scan and prioritize their weaknesses.
2. **Nmap** – Using Nmap will help with network discovery, port scanning, and service fingerprinting by identifying the application, service, and version running on a particular port using specially crafted probes and analyzing the responses they produce
3. **Wireshark** – Identifying packet analysis and monitoring traffic anomalies
4. **SIEM Tools** – Using Splunk or ELK for log aggregation and anomaly detection
5. **IDS/IPS** – Monitoring and protecting networks and systems from malicious activity
6. **OSINT/ NIST framework techniques** – OSINT I would use to gather public information for intelligence, and conduct the NIST framework by applying five of their functions – Identify, protect, detect, respond, and recover.

Full Picture

These sets of tools that I provide together give me a complete view of what's really going on in a network. **OpenVAS** highlights the obvious weaknesses and helps me identify which vulnerabilities are most critical. **Nmap** takes it further by showing me what ports and services are open, and even what OS versions are running, which can reveal hidden risks. From there, **Wireshark** lets me dig into the actual traffic, so if something suspicious slips by the scanners, I can still catch it in the packet analysis.

On the other hand, SIEM tools like Splunk or ELK pull all the logs together so I can connect the dots instead of looking at events in isolation. In essence, pairing it with IDS/IPS gives me live monitoring and protection against active threats, which means I'm not just finding problems but also stopping them too. Finally, adding OSINT helps me see what an attacker might already know about the organization, and using the NIST framework makes sure I'm not just reacting but following a structured approach: Identify, Protect, Detect, Respond, and Recover.

Putting all this together, and it's not just one tool or one angle, it's a layered assessment that shows the vulnerabilities, the traffic, the logs, and even the human side of risk. That's how I know I'm getting the full picture when conducting a network assessment approach.

References

Tarun, R. (2019, January 17). ***A layered approach to cybersecurity: People, processes, and technology*****. Fortinet.** https://www.fortinet.com/blog/industry-trends/a-layered-approach-to-cybersecurity--people--processes--and-tech