Paul Polsinelli

IFT 302 43489

Sum 20

Lab 3

1. **Network Mapping**



1. **Threat Modelling - STRIDE**

**Spoofing Identity**- Identity spoofing attacks are a major threat to any facility, including this one. Attackers can gain access to credentials and passwords using techniques such as social engineering and phishing attacks. (1) Tactics in these methods include dumpster diving, emailing malicious code, researching social media, hacking wi-fi in a public place, obtaining passwords written down, or simple looking over a shoulder while one types in a password.

Many subtypes of spoofing are used either by themselves or in conjunction with social engineering methodologies. Attackers can mimic trusted websites, make it appear that a call is from a specific number that may be trusted, disguising IP addresses, ARP, and DNS’s to both hide the attacker’s identity as well as infiltrate a network. (1)

All Employees and visitors are susceptible to as well as capable of identity spoofing.

**Tampering with Data**- Data tampering is a high threat both within the facility and outside of it in its supply chain. Threats from data tampering directly affecting the substation include counterfeit parts, software, regulatory and compliance requirements, contracts and legal documents, and video and media assets. (2) Counterfeit parts can lead to catastrophic events and losses due to parts failures. Tampered software can allow intrusions and/or run malicious code, equally causing catastrophic events and losses. Regulatory and compliance requirements falsification can lead to equipment failure and catastrophe, as well as legal entanglements and shutdowns. Contract and legal document tampering can also cause legal entanglements and shutdowns. Video and media files can be corrupted and/or altered to cause failure of procedures and/or operations.

**Repudiation, Deniability-** A key element of cyber-security is non-repudiation. With repudiation, an attacker can remainanonymous and emboldened to continue attacks. It is key to the concept of authenticity and therefore authorization. It is also the key ingredient to an attacker successfully avoiding consequences for their attack. Lack of retaliation will assure that attacks will be larger in number and frequency than otherwise. This principle applies at the substation for both cybersecurity and physical security, at least for those who wish to attain access through subterfuge.

**Information Disclosure-** All web applications used by the facility must be stringently secured against attacks. Passwords should never be stored as text within them in case of forceful browsing and directory indexing. (3) Bcrypt or PBKDF2 hashed password encryption must be employed as they are the most vetted encryption algorithms. (4) Disclosure issues to be aware of include banner grabbing/active reconnaissance, source code disclosure, inappropriate handling of sensitive data, and file name & file path disclosure. (5)

**Denial of Service-** In addition to exploiting vulnerabilities thatwould cause the substation computer system to crash, there are other attacks that could interrupt timely access. Three common ones are Buffer overflow attacks, which would send more traffic to the facility’s network address than it could handle; ICMP flood attacks would cause the network to be flooded with pings; and SYN flood, which would request a connection to the server but never complete the handshake on all ports, essentially blocking them all. (6)

**Elevation of Privilege-** EoP or Privilege Escalation occurs when a low-level account is compromised and is either taken over or covertly used to gain access to higher levels of permissions by taking advantage of security flaws. (7) Such a situation in the case of the substation would be disastrous. Equipment being made to malfunction at the substation is only the start of what could go wrong. Gaining higher permissions could expose other passwords and accounts and put the integrity of the software and the entire grid in jeopardy.

1. **Risk Mitigation**

There are many steps that can be taken to mitigate all the concerns stated above. One practice that can be implemented is the principle of least privilege. Anyone with access to either the physical grounds or the network should have the bare minimum amount of privilege necessary to perform their function. Privileges can be severely restricted to anyone not on premises at the time of accessing the system. This will guarantee additional identification and verification that’s necessary to gain physical entrance. This can lessen the effectiveness of social engineering used to stage an attack on the substation.

Further on the threat of social engineering, because of its effectiveness, security must be carried out both during work and non-work hours, at the workplace and outside the workplace. All paperwork that is obsolete should be level P-7 shredded before it is disposed of as well. (8)

Technology will play a heavy role in cybersecurity for the facility, specifically, Endpoint Detection and Response (EDR). EDR will monitor all endpoints of the system to detect intrusions and add encryption to them to prevent intrusions in the first place. An added benefit of the technology are the automated responses when certain conditions are met so that an intrusion can be detected and countered quickly, before much or any damage is done. There are a variety of software platforms to implement the practice and adds a strong layer in the security envelope. (9)

As outlined at the beginning of this paper, Next Generation FireWall (NGFW) technology will provide another level of fortification to the substation network. Each appropriate node will be equipped with either Protocol-based Intrusion Detection System (PIDS), Host-Based Intrusion Detection System (HIDS), or Network Intrusion Detection System (NIDS) where appropriate to add the necessary security redundancy, overlap, and diversity needed.

PIDS will secure the web server by controlling and interpreting the protocol between a user/device and the server. NIDS will examine all traffic from all deices on the network, comparing to known attacks. HIDS will run on the terminal server and thick clients to monitor incoming and outgoing packets, taking system snapshots over time to compare for detection of unauthorized activity. (10) Together, they will provide strength in depth to the network.

References

1. What is Spoofing?, Forcepoint, <https://www.forcepoint.com/cyber-edu/spoofing>, 2020
2. Dirk Kanngiesser, These Are the Seven Deadly Sins of Data Tampering, techradar, <https://www.techradar.com/news/these-are-the-seven-deadly-sins-of-data-tampering>, Jan 25, 2019
3. 6 Most Feared Web Application Attacks and How to Beat Them – Part 6 (Information Disclosure), EC-Council, <https://blog.eccouncil.org/6-most-feared-web-application-attacks-and-how-to-beat-them-part-6-information-disclosure/>
4. Lucaskauffman, About Secure Password Hashing, IT Security Community Blog, StackExchange, <https://security.blogoverflow.com/2013/09/about-secure-password-hashing/#:~:text=Passwords%20should%20be%20hashed%20with,can%20use%20bcrypt%20you%20should.>, Aug 13, 2013
5. Information Disclosure Issues and Attacks in Web Applications, Netsparker, <https://www.netsparker.com/blog/web-security/information-disclosure-issues-attacks/#:~:text=Information%20disclosure%20is%20when%20an,subject%20matter%20in%20normal%20circumstances.>, Jun 19, 2019
6. What is a Denial of Service Attack (DoS), paloalto, <https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos>
7. Jeff Melnick, What is Privilege Escalation?, netwrix, <https://blog.netwrix.com/2018/09/05/what-is-privilege-escalation/>, Mar 25, 2020
8. Lauren Hilinski, What are the Different Shredder Security Levels, Shred Nations, <https://www.shrednations.com/2018/11/what-are-different-shredder-security-levels/>, Aug 28, 2019
9. Paul Shread, Top Endpoint Detection and Response (EDR) Solutions, eSecurity Planet, <https://www.esecurityplanet.com/products/top-endpoint-detection-response-solutions.html#methodology>, Jun 4, 2020
10. Intrusion Detection System (IDS), GeeksforGeeks, <https://www.geeksforgeeks.org/intrusion-detection-system-ids/>