ISEC-615 - Fundamentals of Cybersecurity

Assignment No. 3 - Cybersecurity Attacks and Defense

Due: 07/07/2019

Eric Webb

[ew774@mynsu.nova.edu](mailto:ew774@mynsu.nova.edu)

Dr. Yair Levy

**Table of Contents.**

Bad Actors in cyberspace .………………………………………………………………….…………3.

Types of Cybersecurity Attacks ……………………………………………………….…………....4, 5.

Types of System Attacks …………………………………………………………………................5.

Cyber Defense ………….………………………………………………………………......................5, 6.

Cyber Defense Partners/Structures/Programs ……………………………………………….6, 7.

Conclusion ………………………….………………………………………………………………………….7.

Work Cited .…………………………………………………………………………………………………....8.

Certificate of Authorship ………………….……………………………………………………………..9.

**Bad Actors in Cyberspace.**

There are a multitude of bad actors that threaten the cybersecurity realm. Each of these have their own motivations, resources, and capabilities.

One threat actor is the concept of a nation state. Nation states are highly sophisticated and have extensive resources from government entities. They can use techniques such as Advanced Persistent Threats to maintain a presence unbeknownst to the network. Nation states typically are motivated by politics and militaristic gains rather than for financial. Another Highly sophisticated bad actor is the concept of Organized Crime. Much like nation states Organized Crime will have sophisticated resources to carry out their attacks but un-like nation states they are typically motivated by financial gain. Typically holding Personal information or proprietary data hostage for value using techniques such as a ransomware attack.

This brings us to another bad actor which is the concept of Hacktivists. Hacktivists combine the technical knowledge of a hacker with the personal views of an activists. Similar to a nation state they are motivated by political measures or want to get their message heard. They have less resources then a nation state but are persistent with their determination.

From these we can get an idea of a few of the types of bad actors in cyberspace along with their reasons for carrying out attacks. (Tollefson, n.d.)

**Types of Cyber Security Attacks.**

In cybersecurity there are many different types of attacks designed to do a multitude of nefarious things. Some are designed to disrupt networks while others are used covertly.

To begin one of the more famous types of attacks is the concept of a Denial of Service attack. (Referred to as a DoS attack.) These attacks are meant to disrupt systems from preforming there tasks at hand and effectively denying the service they were once offering. If it causes your system to crash then it is a DoS attack. Second we have the concept of a Man in the Middle attack. (Also referred to as a MITM attack.) These attacks are performed covertly in-between to mediums of communication. A sender will send some data which will get captured by the attacker who then alters that data nefariously to be sent to the receiver still mimicked as if it was from the original sender. The sender has no idea their data was compromised and the receiver still thinks the data came from the sender. Next on the list is social engineering attacks. These attacks take advantage of the incompetence of the human psyche. One of the biggest examples of a social engineering attack is a Spear Phishing were an attacker will craft an attack specifically designed for their target. Such an example would be an email specifically designed in a way to make you more likely to click on it. Another popular attack is a SQL injection attack. In this attack threat agents will take advantage of a form field to manipulate data on the back end by injecting harmful SQL code into form fields to be later compiled by the backend effectively manipulating your data base. Lastly, we have the concept of Cross Site Scripting also called XSS. Similar to SQL injection, XSS uses scripting code instead of SQL to perform scripts in such a manner that’s unintended or detrimental to your web application. Some examples of this are running scripts to enable key logging or for stealing user cookies. (Top 10 Most Common Types of Cyber Attacks. n.d.)

**Types of System Attacks.**

When setting up a good security posture it is important to defend against system attacks. These are attacks specifically targeted at the host’s software and hardware components.

One type of system attack is the exploitation of a backdoor. Backdoors can be used to access your system for legitimate remote access for an authorized user but if left vulnerable can be exploited for an attacker to get access and compromise your system. This can be done by taking advantage of an open logical port or even simply plugging into an open physical port, Because of this strict auditing and access control methodologies should be implemented. Another type of system attack is a software exploitation, this takes advantage of systems software to carry out an attack. One example could be default passwords on a system that have not been updated to the new owner. Another system attack example would be a buffer overflow. This happens when software is not properly designed to handle inputs and the attacker takes advantage of the lack of input validation. This can cause a Denial of Service or leak important data. (Cicnavi , 2015).

**Cyber Defense.**

To mitigate cyberattacks it is good to have a plethora of tools to apply these defenses. To defend against these attacks Lockheed Martin has coined the term the cyber kill chain. This is a step by step process for defending against attacks by visualizing the attack process an attacker uses to manipulate your network.

The kill chain begins with reconnaissance, to block unwanted reconnaissance you can use web analytics to detect who is viewing your content and firewall access control lists to deny unwanted access to classified information. Another tool for cyber defense is different types of intrusion detection systems to detect when unwanted software is being installed, ran, and connected on your network. Besides just detecting nefarious activities, you can use different types of intrusion prevention systems to deny unwanted weaponization and disrupt unwanted commands and controls. Besides using Firewalls, IDS, and IPS you can use DNS redirects and honeypots to Deceive would be attackers as well. (Beal, n.d.)

**Cyber Defense Partners/Structures/Programs.**

To secure our daily lives the government has Federal, state, and local entities and procedures to protect the common good of the public. To begin at a federal level we have the FBI, DoD, and the DHS to help protect our nation’s citizens both domestically and internationally. The FBI has teams such as its cyber division, cyber action threat teams, and computer crimes task force to help protect our national security. (Cyber Crime, 2016). State governments typically publish an IT strategic plan to explain their cybersecurity posture. A state with a good security posture will have its systems monitored and evaluated in real time, making sure its employees are have taken security awareness, and reducing high-risk security findings. Typically states will have independent security task forces to handle these concepts. (Dawson & Desouza 2016). Local municipalities also have the need for cybersecurity, Because of this the State Cyber Resiliency Act was drafted. This lends support to local governments to write guidelines, standards, and educating government employees. Typically local governments work closely with police cyber defense teams to mitigate risk and catch perpetrators. (DeSimone, 2019).

**Conclusion.**

In this article, we have discussed bad actors in cyber space such as nation states, organized crime syndicates, and hacktivists. We also discussed different types of cyber-attacks such as DoS attacks, Man in the middle attacks, Cross site scripting, and SQL injections. System attacks were also a topic of discussion such as Backdoors, software vulnerabilities, and buffer overflow. To defend from these attacks we discussed cyber defense tools such as firewalls, intrusion detection systems, and intrusion prevention systems and what part of the cyber kill chain they can help defend against. From this that brought up the topic of cyber defense initiatives at federal, state, and local levels such as the FBI cyber task force, state security guidelines, and local government co-operation with police task force. In conclusion, it is important to understand threat agents, cyberattacks, system attacks, cyber defenses, and how they relate with government entities.

**Work Cited.**

Beal, V. (n.d.). Cyber Kill Chain. Retrieved June 29, 2019, from <https://www.webopedia.com/TERM/C/cyber-kill-chain.html>

Cicnavi. (2015, December 03). Different Types of System Vulnerabilities and Attacks. Retrieved June 26, 2019, from <https://www.utilizewindows.com/different-types-of-system-vulnerabilities-and-attacks/>

Cyber Crime. (2016, May 03). Retrieved June 29, 2019, from <https://www.fbi.gov/investigate/cyber>

Cyber threat actor. (n.d.). Retrieved June 24, 2019, from <https://itlaw.wikia.org/wiki/Cyber_threat_actor>

Dawson, G., & Desouza, K. C. (2016, July 29). How state governments are addressing cybersecurity. Retrieved June 29, 2019, from <https://www.brookings.edu/blog/techtank/2015/03/05/how-state-governments-are-addressing-cybersecurity/>

DeSimone, J. (2019, June 10). Cybersecurity doesn't stop at the federal level - our states need help. Retrieved June 29, 2019, from <https://thehill.com/opinion/cybersecurity/439112-cybersecurity-doesnt-stop-at-the-federal-level-our-states-need-help>

Top 10 Most Common Types of Cyber Attacks. (n.d.). Retrieved June 26, 2019, from <https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/>

Tollefson, R. (n.d.). How to Explain Threat Actor Types and Attributes. Retrieved June 26, 2019, from <https://resources.infosecinstitute.com/category/certifications-training/securityplus/sec-domains/threats-attacks-and-vulnerabilities-in-security/how-to-explain-threat-actor-types-and-attributes/#gref>

**Certification of Authorship**



Submitted to: Professor Yair Levy.

Student’s Name: Eric Webb

Date of Assignment: 07/07/2019

Title of Assignment: Assignment No. 3 - Cybersecurity Attacks and Defense

Certification of Authorship: I hereby certify that I am the author of this document and that any assistance I received in its preparation is fully acknowledged and disclosed in the document. I have also cited all sources from which I obtained data, ideas, or words that are copied directly or paraphrased in the document. Sources are properly credited according to accepted standards for professional publications. I also certify that this paper was prepared by me for this course.

Student's Signature: ERIC WEBB