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

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

Types of Cybersecurity Attacks……………………………………………………….…4

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

Cyber Defense………….………………………………………………………………....6

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

Conclusion………………………………………………………………………….8

Work Cited……………………………………………………………………….....9

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 your 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 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 from 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 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 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 legitimately remotely 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 example would be a buffer overflow. This happens when software is not properly designed to handle inputs. This can cause a Denial of Service or leak important data. (Cicnavi ,2015).

**Cyber Defense:** In your own words (no quotes, but use references to support your claims) describe three different cyber defense tools, methods, and components, as well as how to apply cyber defense methods to prepare a system to mitigate attacks(kill chain).

When hardening a system it is good to

 **Cyber Defense Partners/Structures/Programs:** In your own words (no quotes, but use references to support your claims), describe the Federal, State, and Local Cyber Defense partners/structures/programs by outlining at least three examples

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

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 of Assignment



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