Activity Guide 1 : Part 3

Ryan Coon

CST-407

Professor Ty Howard

December 10, 2023

**Ransomware**

1. What types of software does the person in "Anatomy of Attack: Cybersecurity Update" use to perform their attack? Research the names and techniques shown and explain what they are.

StartPage

Facebook

Mallware r us

Ransom32

1. What is the primary vulnerability in the company that the hacker relies on to succeed? Give an example of a real-world company that experienced this type of attack.

Reliability that the target is trusting. Using the research of social media to employ a “relationship” and then masking as a high level employee and mimicking their email address to drop the ransomware packet.

Colonial pipeline is one that comes to mind.

1. What extent of damage was done to the victim? Give an example of a real-world company that experienced similar damages due to this type of attack.

All information is held at “ransom”. If payment is not made for the amount requested, the information is then sold to the highest bidder.

1. What type of cybersecurity expert would likely be properly trained to prevent this type of attack, and what type of interventions would they employ?

A cybersecurity analyst/engineer would be best suited to tackle ransomware attacks/prevention. Interventions to employ to best prevent these types of attacks would be prioritizing HTTPS connections, avoid public/unsecured Wi-Fi, practice network segmentation, encrypt your emails, use a certificate management system, and lastly utilize privileged access management.

**SQL Injection**

1. What types of application programs are vulnerable to a SQL injection attack?

Any type of web application or website that use SQL databases like Oracle, SQL Server or MySQL are susceptible to an SQL Injection attack.

1. What type of damage could be done to the victim with this attack? Give an example of a real-world company that experienced this type of attack.

It is not just financial loss to the company that is affected, loss of customer trust, along with personal data such as names, addresses phone numbers and credit cards. An attacker can also delete information in an injection attack.

The most recent company that suffered from an SQL injection attack is the popular game Fortnite. The vulnerability was found that would let the attackers have access to over 350 million user accounts. This was quickly patched.

1. What type of cybersecurity expert would likely be properly trained to prevent this type of attack, and what type of interventions would they employ?

An expert trained in secure coding or web application security would be who you would look to hire. They could employ input validation on forms, parameterized queries, least privilege principle, web application firewalls, patch management and security audits could help prevent these types of attacks.

**Credit Card Skimmers**

1. What types of systems are vulnerable to this attack?

Systems that are vulnerable to this type of attack are any that use the magnetic strip on an a credit or debit card. This would include Point of sale systems such as gas pumps, ATMs and transit ticket dispensers.

1. What type of damage could be done to the victim with this attack? Give an example of a real-world company that experienced this type of attack.

Credit card information can be taken quickly and then card can be used.

Many individuals are the target of this attack and it is quick and easy.

1. What type of cybersecurity expert would likely be properly trained to prevent this type of attack, and what type of interventions would they employ?

A Cybersecurity expert specializing specifically in areas like information security specifically in payment security or fraud prevention would be best for this situation.

Interventions used by these experts would be regular security audits, use of encryption, installing anti-skimming devices, employee training, monitoring and anomaly detection, physical security measures, software updates, and implementing chip technology.

**Man in the Middle**

1. What types of systems are vulnerable to a MITM attack?

Once the hacker has the information they can target multiple banking, online retailers, and SaaS platform customers.

1. What type of damage could be done to the victim with this attack? Give an example of a real-world company that experienced this type of attack.

Attackers can spoof any html based website login pages and intercept sensitive login information.

A recent company that was affected is Equifax.

1. What type of cybersecurity expert would likely be properly trained to prevent this type of attack, and what type of interventions would they employ?

One would want to employ a few different types of experts like network security specialists, security engineers and penetration testers. Some of the methods that could be used would be use of encryption, network segmentation, firewall configuration monitoring tools, key management, certificate implementation, read-teaming, logging, and risk assessments.

**Ethical Dilemmas**

1. In addition, write a 250-word description on what keeps white hat hackers on the right side. A white hat hacker is one who uses computer security skills in service of "good." From a Christian worldview, discuss how people should apply their skills for the common good. Also provide examples by researching the ethical dilemmas behind creating and using white hat hackers. Provide support for your answers by including actual cybersecurity events that have taken place in which white-hat hackers were used to mitigate the criminal attempts of cyber criminals who may have been trying to steal, manipulate, or destroy pertinent information.

Ethical hacking, also known as "white hat" hacking, is the practice of using hacking techniques for defensive or protective purposes. One would want to employ an individual whose morals are sound as they would be searching for vulnerabilities within a company’s infrastructure. You would want someone with a good Christian worldview as they would be helping to secure thousands if not millions of user’s sensitive data. One dilemma that I could see would be the level of disclosure and consequences on revealing these vulnerabilities to the public. For me I wouldn’t reveal anything unless a breach has been made, or that any possible breach points or vulnerabilities have been patched. There is a fine line between hacking and ethical hacking for good, and we must as a good Christian person know that line and not cross it.

References:

“Hacking for Good or Evil: The Ethical Debate Surrounding White Hat Hacking.” Www.linkedin.com, www.linkedin.com/pulse/hacking-good-evil-ethical-debate-surrounding-white-hat-warburton/. Accessed 17 Dec. 2023.

“Man-In-The-Middle (MITM) Attack: Definition, Examples & More | StrongDM.” Discover.strongdm.com, www.strongdm.com/blog/man-in-the-middle-attack#:~:text=Once%20a%20criminal%20has%20this.

“Man-In-The-Middle Attacks: Understanding the Dangers and Protecting Your Information.” Kiteworks | Your Private Content Network, www.kiteworks.com/risk-compliance-glossary/man-in-the-middle-attacks-understanding-the-dangers-and-protecting-your-information/#:~:text=If%20a%20MITM%20attack%20is.

PortSwigger. “What Is SQL Injection? Tutorial & Examples.” Portswigger.net, PortSwigger, 2019, portswigger.net/web-security/sql-injection.

“Recent Ransomware Payments and Settlements.” Fortinet, www.fortinet.com/resources/cyberglossary/recent-ransomware-settlements.

“The Ethics of Hacking.” SecurityScorecard, securityscorecard.com/blog/the-ethics-of-hacking/#:~:text=White%20hat%20hackers%20must%20balance. Accessed 17 Dec. 2023.

“What Is Skimming in Cybersecurity?” B2b.mastercard.com, b2b.mastercard.com/news-and-insights/blog/what-is-skimming-in-cybersecurity/.