Old Dominion University

CYSE 450 Ethical Hacking and Penetration Testing

Common Social Engineering Techniques, Attacks, and Potential Solutions

Professor: Dr. Rashid Khan

Brian Delos Santos

UIN: 01180618

March 2, 2022

Abstract

Social Engineering has become a serious problem to the security of information systems and especially large multiuser networks. The normalization of the internet and collaborative tools such as email, LinkedIn, Teams, and other digital communication creates an expanding landscape for social engineering attacks. The purpose of social engineering is to manipulate people to gain valuable information, access, or financial gain. With a myriad of social engineering techniques and attacks to look out for, it can be hard to identify and prevent social engineering attacks from compromising the security of a computer network. From what I can tell, protecting computer networks from social engineering will require a multifaceted approach that utilizes every security aspect of a computer network.

Keywords: Social Engineering, Phishing, Impersonation, Typo squatting, Pharming, Tailgating, waterhole attack.

Introduction

Social engineering is one of the largest growing threats to a secure network. It is an all-encompassing term for the wide variety of techniques used by hackers to manipulate users into providing information or system access to computers otherwise secure. The reason social engineering is becoming an increasing issue for modern networks is that these attacks manipulate the user. These are not threats that can be fully mitigated through system configurations. These types of attacks prey on the good nature of human psychology and manipulate unsuspecting victims. The solution is created through a multi layered defense strategy. This strategy can vary, but commonly involves user awareness, policy, procedures that govern use of network resources, and continuous monitoring of network resources. (David).

In Michael Workman's "Gaining Access with Social Engineering: an Empirical Study of the Threat," he mentions the use of mandatory access controls and system level security alone cannot protect information systems from social engineering attacks. This is because social engineering attacks can bypass secure configurations and mandatory access controls by manipulating an authorized user. (Michael). Social engineering is an effective means to hacking a secure computer or network, according to Purplesec's article on cybersecurity statistics, "98% of cyber-attacks rely on social engineering." Widespread use of large multi-user networks and remote work has created a perfect environment for social engineering attacks like phishing, impersonation, pharming and more. This does not mean that the workplace is safe either. Social engineering attacks like dumpster diving, shoulder surfing, tailgating, and reconnaissance are prevalent attacks at physical work locations (2021).

Social Engineering Techniques

Social Engineering attacks are effective because they utilize techniques that mimic social interactions like authority, intimidation, scarcity, familiarity, trust, or urgency to manipulate their targets to willingly divulge information. A hacker utilizing a sense of authority could impersonate a higher up in the target company and use that power to request information from a new employee. Intimidation is when a hacker threatens the target with negative actions unless the target provides the hackers demands. Scarcity is when a hacker manipulates the target to think that they can provide something in short supply. Familiarity is a social engineering technique where a hacker discovers something their target does often and utilizes that to gain

access or information. An example of a social engineering attack that uses familiarity could be as simple as taking advantage of their target commonly opening the door for strangers or constantly calling the IT team for a password reset. Trust is a social engineering tactic where a hacker manipulates the target to believe they aren't doing anything wrong by providing information or access for the hacker. Urgency is a social engineering technique where a hacker manipulates their target to thinking that a fabricated situation is time sensitive, and the target needs to act now. These different types of social engineering techniques can be used in a plethora of dynamic attacks and often times multiple techniques are combined in one attack (Comptia).

Phishing

Given that "98% of cyber-attacks rely on social engineering," cybersecurity professionals cannot turn a blind eye to these vulnerabilities. Phishing is one of the most common social engineering attacks that plague modern networks. A phishing attack is when a malicious actor sends some form of communication to users on a network in an attempt to manipulate the user to provide private information. They are simple, cost effective, highly customizable and easy to distribute. The worst part is that it only takes one successful phishing attack to provide a malicious actor access to a private computer or network. Due to the simplicity, low risk, and high reward nature of this type of attack, phishing has become an increasingly popular method of hacking (2021).

The reason phishing attacks are so dangerous is because they test user awareness and not the system security. This is why I believe the implementation of mandatory cybersecurity awareness training is imperative for the security of large multi-user networks. The trainings should be tailored towards identification of phishing attacks and the different variations to look out for. These trainings should be disseminated to all applicable users on a network and the results should be tracked. This is one way to hold users accountable for their actions and is a foundation to a layered defense approach that includes the user in the security scheme (CompTIA).

Impersonation

Impersonation is a type of social engineering where a hacker pretends to be someone they are not in an attempt to manipulate their target to providing private information, physical or

system access. Impersonation can be achieved through any digital communication or even face to face. The reason impersonation works is because it takes advantage of peoples knee-jerk reaction that someone is who they say they are. Malicious actors attempt to impersonate people of authority or someone their target would not think twice about. For example, a previous employee just stopping by to grab some items he forgot, or even a third-party maintenance worker who has a job in your building. On the surface, these are not suspicious events, but that "employee" could be a malicious actor and may not have even worked there. If users aren't actively watching out for suspicious activity, then your network could be at risk of social engineering attacks like impersonation (What).

Defending secure networks from impersonation attacks are less about strengthening system security configurations and more focused on following an identification and authentication policy. This type of policy will guide authorized personnel on how to properly identify and gain authorization to access systems or a system area. Identification and authentication techniques should be implemented for physical and system access. Physical access can be protected by electronic lock and access badges can be provided to authorized users. The badges will be a form of identification and the electronic lock will authenticate that the badge is valid and grant access. System level identification and authentication methods include the creation of user accounts with unique username that identifies and a password that authenticates the user (What).

Web Based Social Engineering

Users of secure computer networks need to watch out for social engineering attacks in person and on the world wide web. Typo squatting is a social engineering attack where a malicious actor hosts a domain name that is nearly identical to a different website. Pharming is a social engineering attack where a hacker redirects their target to a fraudulent website set up to look as the original. A watering hole attack is when an attacker embeds malware into a site that the target frequently visits and waits for the target to access the website (Comptia). These are more complex social engineering attacks in that the hacker has to invest more time and effort into the initial attack, but they still use the same techniques. For example, a hacker using pharming to gain personal information is using the familiarity technique where the user searches

for a known website but is redirected to a website set up to look similar and function the same manner to obtain sensitive information.

Web based social engineering attacks are complex, but they can be mitigated through a combination of user awareness, access control lists, and policy that governs acceptable use of internet access through network resources. User awareness has been a staple in social engineering mitigation strategies. The user awareness for web based social engineering should focus on taking one's time when traversing the internet over a secure network and identifying potential web based attacks. An access control list is a firewall capability that can deny access to and from the target network. Cybersecurity professionals can configure a firewall to control the websites they can access and prevent negligence like misspelling a website or being redirected to an unapproved website (Comptia).

Insider Social Engineering

The physical workplace is not safe from hacking and especially not social engineering. According to Peter Stephenson, "30 percent of all hacking comes from outsiders; that is, people who are not working for the attacked organization." This statement implies that over half of all hacking starts from within the target organization (Thomas). Social engineering attacks can take advantage of systems environment and users' awareness of their surroundings. Tailgating, shoulder surfing, and dumpster diving are common social engineering attacks that happen on site or in the system environment. Tailgating is when a malicious actor follows behind an authorized person to gain physical access to an area that is locked or off limits. The hacker could do this by acting like it is a coincidence or that they forgot their badge or key by accident. Shoulder surfing is when a malicious actor looks over a user's shoulder to observe login credentials or other sensitive information. Dumpster diving is when a malicious actor sifts through a targets trash in hopes to find sensitive information (Comptia).

As is with most social engineering attacks, the solution to insider social engineering is keeping network users aware of the threat, being able to identify, and report potential social engineering attacks. Organizational cognizance of social engineering with continuous monitoring of network resources will help mitigate insider social engineering attacks, but you can not eliminate this vulnerability. Each day there is a chance that a network user can be compromised by an attacker and choose to perform reconnaissance or aid in a cyber-attack. As a cybersecurity

professional, you cannot prevent this outright. Professionals need to catch an insider in the act, and this is what continuous monitoring of network resources accomplishes. With continuous monitoring of network resources, the target organization has a much better chance at identifying wrongdoing by the insider.

Conclusion

A network can only be as secure as the weakest link and social engineering attacks take advantage of the weakest link. Social engineering is one of the largest growing threats to modern computer networks. It has become more popular over the years because it is easier to manipulate the user than a secure system (Thomas). A common theme from different social engineering attacks is that the solution relies heavily on the user's ability to identify potential attacks. This is why I believe user education is one of the most powerful tools to help defend against social engineering attacks. User education is one way to invest in the user and hold them responsible for the systems they use. Unfortunately, a computer network can never be completely secure from social engineering attacks, but you can be prepared through a layered defense that educates the user, supports system function with policy, and security configurations (Comptia).

References:

2021 Cyber Security Statistics Trends & Data. PurpleSec. (2021, August 6). Retrieved March 14, 2022, from https://purplesec.us/resources/cyber-security-statistics/#:~:text=98%25%20of%20cyber%20attacks%20rely,as%20being%20at%20high%20ri sk.

CompTIA Security+ Certification All-in-One Exam Guide, Seventh Edition (Exam SYO-601). 6th ed., McGraw-Hill Education, 2021.

David, Gragg, “A Multi-Level Defense Against Social Engineering” in the Information Security reading room, Vol. 1.4b, December 2002. http://taupe.free.fr/book/psycho/social%20engineering/Social%20Engineering%20-%20Sans%20Institute%20-%20Multi%20Level%20Defense%20Against%20Social%20Engineering.pdf

Michael Workman Ph.D. (2007) Gaining Access with Social Engineering: An Empirical Study of the Threat, Information Systems Security, 16:6, 315-331, DOI: 10.1080/10658980701788165

Thomas R. Peltier, “Social Engineering: Concepts and Solutions” in information security and risk management, Vol 15, Iss. 5, pp. 13-21, November 2006. https://www.proquest.com/openview/6535856a33b27389b0f070f8a841c1bd/1?pq-origsite=gscholar&cbl=52433

What is impersonation in social engineering? My Security Awareness. (n.d.). Retrieved March 14, 2022, from https://mysecurityawareness.com/article.php?article=384&title=what-is-impersonation-in-social-engineering