Approaches in Modern Cybersecurity

Divaco Colbert
University of Advancing Technology

Author Note

This paper was prepared for NTS350, taught by Karina Stippick, Title Approaches in Modern Cybersecurity.

Approaches in Modern Cybersecurity

Social Engineering: Create a simulated phishing campaign and develop a persuasive email template.

Subject: Urgent Account Security Update Required - Action Needed

Dear [Recipient's Name],

We hope this email finds you well. Our IT team has recently identified a critical security vulnerability that affects all the accounts with [Company/Organization Name]. As part of our commitment to safeguarding your personal information, we require your immediate attention and cooperation to resolve this matter.

To protect your account from unauthorized access and potential data breaches, we have implemented a new security feature that requires you to verify your account information. This standard procedure is designed to maintain the utmost security and prevent unauthorized activity.

To complete the verification process, please follow the steps outlined below:

Click on the provided link: [Insert Link Here and QR code]

You will be redirected to a secure webpage where you will log into your account.

Once logged in, you will be prompted to update your account details, including your password, security questions, and contact information.

After updating your information, please click "Submit" to save the changes.

Please note that failure to verify your account within the next 48 hours may result in a temporary disable of your account until the verification process is completed. We kindly request your immediate attention to avoid any inconvenience.

We understand that your time is valuable, and we apologize for any inconvenience this may cause. However, we need to maintain a secure environment for all our employees.

If you encounter any difficulties or have any questions, please do not hesitate to contact our support team at [Support Email/Phone Number]. Our IT team is available to assist you with the verification process or address any concerns.

Thank you. We greatly appreciate your cooperation in ensuring the security of your account and our company.

Sincerely,

[Fake name or someone that works there] [Your Position/ head of department]
[Company/Organization Name]

Setting up and executing a simulated phishing campaign involves Identifying the target audience and gathering information about the target organization (e.g., company structure, key personnel, and common practices) and determining the objective of the campaign (e.g., gathering credentials, spreading malware). By creating a persuasive email template using social engineering techniques an attacker can grab attention and create a sense of urgency and include a call-to-action that directs recipients to a malicious website or encourages them to download an

attachment or put in their credentials. Creating a Phishing Website is simple using tools like HTTrack or Burp Suite to clone a legitimate website. All the attacker needs to do is modify the cloned website to capture credentials or other sensitive information. The only way to stop this from happening is to train employees to click on any emails that have not been authorized. Also communicating with other people could help to see if it came from them or not.

Insider Threat Simulation: Develop a role-playing exercise where students can act as both attackers and defenders. Simulate an insider threat scenario, such as unauthorized access or data exfiltration, and analyze the effectiveness of security measures.

Role-Playing Exercise: Insider Threat Simulation

Scenario: Unauthorized Data Access and Exfiltration

Objective: To simulate an insider threat scenario and evaluate the effectiveness of security measures in place.

As an attacker with malicious intent, your role is to act as an employee and attempt to gain unauthorized access to sensitive data and exfiltrate it. Your first step is to conduct thorough research on the target system(s) to identify potential vulnerabilities. This may involve gathering information about the organization's infrastructure, software, employees, and security measures.

Based on your research, you need to determine the most effective method to launch your attack. This could involve exploiting weak passwords, leveraging social engineering techniques, or targeting system vulnerabilities. Social engineering can be a particularly effective strategy, as it takes advantage of human psychology, trust, and persuasion to deceive and manipulate your targets.

With your attack plan in place, you will attempt to bypass or overcome the security measures in place. This could involve executing phishing campaigns to trick employees into revealing their login credentials, exploiting software vulnerabilities to gain unauthorized access, or using social engineering techniques to convince individuals to grant you access to restricted areas or sensitive information.

During the attack, you must be cautious and adaptable, adjusting your tactics as needed to overcome any obstacles or unexpected challenges. Remember to document each step of the attack process, including the tools and techniques used, to facilitate analysis and evaluation later.

As a Defender, it is your job to Identify any potential threats within your company. Your role represents the company's security team responsible for preventing and detecting insider threats. You must identify the target systems or data repositories that contain sensitive information. As a defender, you need to plan an attack. Research common insider threat scenarios and techniques. Choose an insider threat scenario to simulate, such as unauthorized access or data exfiltration. Develop a plan for executing the simulated attack. Next, execute the attack, document the steps taken during the attack, and include any tools and techniques utilized. The next step is to monitor the network, system logs, and security alerts to detect the simulated attack. Document all

findings even if they seem like nothing because that nothing can be the reason that compromised the system. You should always strive to mitigate and improve securities strategies. Develop and perform training programs to educate employees about the risks of insider threats and best practices for preventing them. Regularly review and update security measures, considering emerging insider threat techniques and evolving risks. Conduct periodic insider threat simulations to assess the effectiveness of security measures and ensure preparedness.

Insider Threat Setting up and executing Identifying the target audience and gathering information about the target organization (e.g., company structure, key personnel, and common practices) and determining the objective of the campaign (e.g., gathering credentials, spreading malware). By using social engineering techniques or any other method needed an attacker can grab ahold of sensitive information. The only way to stop this from happening is to train employees and regularly monitor employees and networks.

References

Antipov, A. (2021, November 29). *How to write Phishing templates that work | Infosec Resources*. Infosec Resources. https://resources.infosecinstitute.com/topic/how-to-write-phishing-templates-that-work/

Borky, J. M., & Bradley, T. H. (2018). Protecting Information with Cybersecurity. In *Springer eBooks* (pp. 345–404). https://doi.org/10.1007/978-3-319-95669-5_10

Defining Insider Threats | CISA. (n.d.). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats

Mba, J. F. (2023). Red Team VS Blue Team: What's The Difference? *PurpleSec*. https://purplesec.us/red-team-vs-blue-team-cyber-security/