SCHOOL OF ENGINEERING AND INFORMATION TECHNOLOGY

ZEIT8020 Cyber Offence - Threats and Opportunities [S1, 2023]

Assignment 4: Practical Project (Theoretical)

MAROSKE, Alexander Tracy George - z5470869

Due Date: 9th June 2023

Abstract

This study presents a comprehensive analysis of offensive security tradecraft and its application in developing a theoretical offensive strategy against a fictious medium-sized Australian financial institution, Bank of Kangaroonies. Leveraging the MITRE ATT&CK framework and the Cyber Kill Chain model, the author identifies vulnerabilities in the target's environment and defences, map them to relevant techniques and stages, and create an integrated Attack Flow. The reconnaissance process refines the Attack Flow, and the author has designed attack scenarios considering resources, capabilities, countermeasures, and challenges. The analysis culminates in an evaluation of the potential impact of the attack on the target's assets and operations, along with suggestions for defensive measures and policy recommendations. This research highlights the importance of understanding offensive security tradecraft and employing established frameworks to enhance an organisation's security posture and mitigate the risk of a successful cyber-attack.

Executive Summary.

In this theoretical exercise, the author analysed the security posture of a medium-sized Australian financial institution, “Bank of Kangaroonies.” The goal of this exercise was to demonstrate offensive cybersecurity tradecraft using a blend of the MITRE ATT&CK framework and the Cyber Kill Chain model. The author identified key assets, such as customer data, financial records, and critical infrastructure components, that could be attractive to threat actors.

The author’s analysis of the target’s environment and defences revealed several vulnerabilities that could be exploited by adversaries. The author used open-source intelligence gathering techniques, such as OSINT (T1597) and network service scanning (T1046), to refine their understanding of the target’s IT infrastructure. To develop a theoretical offensive strategy, the author created an integrated Attack Flow, mapping identified vulnerabilities to relevant MITRE ATT&CK techniques and Cyber Kill Chain stages.

The strategy included steps such as spearphishing (T1566), input capture (T1056), exploiting public-facing applications (T1190), lateral movement (TA0008), and data exfiltration (TA0010). The author determined the resources and capabilities needed to execute the attack scenarios and assessed potential countermeasures and challenges. A key aspect of the author’s strategy was to leverage open-source exploits and known malware, rather than zero-day or custom-developed malware, due to resource constraints.

The potential impact of the author’s attack scenarios on the target’s assets and operations was significant, ranging from unauthorized access to sensitive data to disruption of critical systems. The author identified artifacts and signatures generated by the cyber offensive activities, such as log files and network traffic patterns, which could be used by the target to detect and respond to the attacks.

To strengthen the target’s security posture, the author recommended implementing effective countermeasures, such as enhancing email security, deploying robust intrusion detection systems, and adopting multi-factor authentication for remote access. The author also advised policymakers on strategic issues related to cyber capabilities, doctrine, and partnerships to further enhance the organisation’s resilience against cyber threats.

Overall, this exercise demonstrated the value of blending the MITRE ATT&CK framework and the Cyber Kill Chain model to develop a comprehensive understanding of an organisation’s security posture and potential attack vectors. By doing so, the author was able to identify vulnerabilities, develop theoretical attack scenarios, and recommend defensive measures to protect the target organisation from potential cyber-attacks.

Introduction

In this essay, the author explores the offensive cybersecurity tradecraft and its application to a medium-sized Australian financial institution, which has been fictitiously named “Bank of Kangaroonies.” The primary aim of this exercise is to demonstrate mastery of offensive cybersecurity techniques by developing a theoretical attack scenario using a blend of the MITRE ATT&CK framework and the Cyber Kill Chain model. The author’s focus will be on understanding the target’s environment, identifying vulnerabilities, and devising a comprehensive offensive strategy, while also considering potential defensive measures. It is important to note that the scope of this document is limited to theoretical analysis and does not involve any real-world hacking activities or the use of zero-day or custom-developed malware. The author will focus on leveraging open-source exploits and known malware due to resource constraints. This approach enables the author to delve deeper into the chosen topic while still showcasing the breadth of their understanding of the course material. The essay is structured as follows:

1. Initial target analysis: The author identifies the key assets of the financial institution that may be attractive to threat actors, assesses the target’s environment and defences, and establishes a goal for their theoretical offensive strategy.

2. Conduct theoretical reconnaissance: The author gathers open-source intelligence about the target organisation to gain insights into its network topology, systems, applications, and potential vulnerabilities.

3. Develop a theoretical offensive strategy: The author designs attack scenarios using selected MITRE ATT&CK techniques and Cyber Kill Chain stages, determines the resources and capabilities needed to execute the attack, and assesses potential countermeasures and challenges.

4. Analyse the impact on the target and potential defensive measures: The author evaluates the potential impact of the attack scenarios on the target’s assets and operations, identifies artifacts and signatures generated by the cyber offensive activities, suggests improvements to the target’s security posture, and provides advice to policy makers on strategic issues.

By following this structure, the author will not only demonstrate their understanding of offensive cybersecurity tradecraft but also highlight the importance of integrating different methodologies, such as the MITRE ATT&CK framework and the Cyber Kill Chain model, to develop a comprehensive and effective offensive strategy.

Initial Target Analysis

In this section, the author conducts an initial analysis of the medium-sized Australian financial institution "Bank of Kangaroonies" to identify its key assets that might be attractive to threat actors. The author will assess the target's environment and defences and establish a goal for their theoretical offensive strategy.

1.1 Identify key assets.

Bank of Kangaroonies, as a financial institution, has several key assets that are of interest to potential threat actors. These assets include customer data, such as personal and financial information, transaction records, and account balances; internal systems and applications used for managing customer accounts, processing transactions, and supporting financial products and services; and the bank's IT infrastructure, which includes on-premises and cloud-based systems, network components, and security measures (Chismon & Ruks, 2015).

1.2 Assess the target's environment.

To gain a better understanding of the bank's IT infrastructure, the author studied their on-premises and cloud-based systems, network topology, applications, and protocols in use. The author’s findings revealed that the bank primarily relies on a hybrid cloud architecture, with some critical systems hosted in-house and others hosted on third-party cloud service providers. The bank's network topology consists of multiple layers, including perimeter defences, internal network segments, and endpoint devices. The applications and protocols in use range from standard financial applications to custom-built software solutions (Bertino & Islam, 2014).

1.3 Evaluate the target's defences.

The evaluation of the bank's cybersecurity measures revealed the use of firewalls, intrusion detection systems, and anti-malware software. While these measures provide a basic level of protection, the author identified potential weaknesses that could be exploited by threat actors. For instance, the author found that some systems were using outdated software versions with known vulnerabilities, and the bank's email system appeared to be susceptible to phishing attacks (Kaspersky, 2017).

1.4 Set the goal.

Based on the identified vulnerabilities and potential attack vectors, the author established a goal for their theoretical offensive strategy: to gain unauthorized access to the bank's customer data and exfiltrate sensitive information. To achieve this goal, the author will leverage the MITRE ATT&CK framework and the Cyber Kill Chain model to develop a comprehensive attack scenario that demonstrates their mastery of offensive cybersecurity tradecraft (Hutchins, Cloppert, & Amin, 2011).

Conduct Theoretical Reconnaissance

In this section, the author will gather open-source intelligence (OSINT) about Bank of Kangaroonies to gain insights into its network topology, systems, applications, and potential vulnerabilities. The author will apply techniques like OSINT (T1597) and network service scanning (T1046) to collect information and analyse the techniques and stages in the context of the target's environment and defences.

2.1 Review MITRE ATT&CK techniques and Cyber Kill Chain stages related to the identified vulnerabilities.

The author reviewed the relevant MITRE ATT&CK techniques and Cyber Kill Chain stages that could be applied in exploiting the identified vulnerabilities. For instance, the author considered spearphishing (T1566) and phishing for information (T1598) as potential techniques to target the bank's vulnerable email system.

2.2 Analyse the techniques and stages in the context of the target's environment and defences

Considering the bank's hybrid cloud architecture, the author examined potential vulnerabilities related to cloud security, such as weak access controls (T1586), exploitation of remote services (T1210), and data exfiltration from cloud storage (T1537). Additionally, the author analysed the risks associated with outdated software, which may be exploited using known techniques like exploitation for privilege escalation (T1068) and exploitation for defence evasion (T1211).

2.3 Select appropriate techniques and stages for each part of the integrated Attack Flow

Based on our analysis, we selected the following techniques and stages for our integrated Attack Flow:

- Initial Access: Spearphishing (T1566)

- Execution: User Execution (T1204)

- Persistence: Create Account (T1136)

- Privilege Escalation: Exploitation for Privilege Escalation (T1068)

- Defence Evasion: Exploitation for Defence Evasion (T1211)

- Credential Access: Input Capture (T1056)

- Discovery: System Network Configuration Discovery (T1016)

- Lateral Movement: Remote Services (T1021)

- Collection: Data from Local System (T1005)

- Exfiltration: Exfiltration Over C2 Channel (T1041)

- Command and Control: Web Service (T1102)

By the end of this step, the author refined and improved the integrated Attack Flow, providing a more accurate and comprehensive representation of the adversary's potential actions during a cyber-attack against Bank of Kangaroonies.

3. Develop a Theoretical Offensive Strategy

In this section, the author will develop a theoretical offensive strategy against Bank of Kangaroonies by designing attack scenarios, determining the resources and capabilities needed, assessing potential countermeasures and challenges, and discussing the strengths and weaknesses of both the MITRE ATT&CK and Cyber Kill Chain methodologies.

3.1 Design the attack scenarios by describing how the selected MITRE ATT&CK techniques and Cyber Kill Chain stages can be applied in each part of the integrated Attack Flow

The author's theoretical offensive strategy begins with spearphishing (T1566 - MITRE ATT&CK) to gain initial access (Cyber Kill Chain) to the target's network. Using a crafted email containing a malicious attachment, the author persuades an employee to interact with the email and inadvertently execute the malware. Upon execution, the malware establishes persistence (Cyber Kill Chain) on the compromised system by creating a new account (T1136 - MITRE ATT&CK). It then leverages known vulnerabilities in outdated software for privilege escalation (Cyber Kill Chain) through exploitation (T1068 - MITRE ATT&CK) and defence evasion (Cyber Kill Chain) through techniques such as obfuscated files or information (T1027 - MITRE ATT&CK).

Next, the malware captures user credentials through techniques such as input capture (T1056 - MITRE ATT&CK) to facilitate credential access (Cyber Kill Chain) to other systems on the network. System network configuration discovery (T1016 - MITRE ATT&CK) helps identify valuable targets during the discovery stage (Cyber Kill Chain), and lateral movement (Cyber Kill Chain) through remote services (T1021 - MITRE ATT&CK) allows the malware to compromise multiple systems. Data from local systems (T1005 - MITRE ATT&CK) is collected during the collection stage (Cyber Kill Chain), and the exfiltration process commences over a command and control (C2) channel (T1041 - MITRE ATT&CK) during the exfiltration stage (Cyber Kill Chain). The C2 infrastructure is hidden using a web service (T1102 - MITRE ATT&CK) to avoid detection during the command-and-control stage (Cyber Kill Chain).

3.2 Determine the resources and capabilities needed to execute the attack scenarios.

To execute this attack, the author would require:

- A phishing email template and a list of targeted employees

- A malicious payload, such as a remote access trojan (RAT)

- Vulnerability scanning tools to identify outdated software and potential exploits

- A command-and-control (C2) infrastructure for managing the compromised systems

- Exfiltration techniques to transfer collected data securely and discreetly

3.3 Assess potential countermeasures and challenges in executing the attack scenarios.

Some potential challenges and countermeasures that the author might encounter during this attack include:

- Employee awareness training that could decrease the success rate of spearphishing

- Advanced security measures, such as intrusion detection systems (IDS) and endpoint protection, which could detect and block the malicious activities

- Regular patching of software vulnerabilities that would reduce the available attack surface

- Implementation of multi-factor authentication (MFA) that could hinder unauthorized access to systems

3.4 Discuss the strengths and weaknesses of both methodologies in the context of the attack scenarios.

The MITRE ATT&CK framework provides a granular and technique-focused perspective on the attack, allowing for a detailed analysis of each step. However, it may be less effective in representing the overall progression of an attack. In contrast, the Cyber Kill Chain offers a high-level view of the attack stages, which aids in understanding the attack's general flow. However, it may lack the granularity needed to analyse specific techniques. By combining both methodologies, as demonstrated in section 3.1, we can create a comprehensive and structured representation of a cyber-attack against Bank of Kangaroonies.

4. Analyse the Impact on the Target and Potential Defensive Measures

In this section, the author will evaluate the potential impact of the attack scenarios on Bank of Kangaroonies' assets and operations, identify artifacts and signatures generated by the cyber offensive

activities, suggest improvements to the target's security posture, and provide advice to policy makers on strategic issues regarding cyber capabilities, doctrine, and partnerships.

4.1 Evaluate the potential impact of the attack scenarios on the target's assets and operations.

The attack scenarios outlined in the theoretical offensive strategy could have significant consequences for Bank of Kangaroonies. Compromised assets could include customer data, financial records, internal communications, and intellectual property. Unauthorized access to these assets could lead to financial losses, reputational damage, and regulatory penalties. Additionally, the attack could disrupt the bank's operations, causing service outages and impacting customer trust.

4.2 Identify artifacts and signatures generated by the cyber offensive activities.

The cyber offensive activities in the attack scenarios would generate various artifacts and signatures, including:

- Phishing email patterns and associated indicators of compromise (IoCs)

- Malicious payloads, such as the remote access trojan (RAT) and associated network traffic

- User account creation and manipulation events

- Vulnerability scanning tools and related network traffic

- Command-and-control (C2) infrastructure communication patterns

4.3 Suggest improvements to the target's security posture by addressing vulnerabilities and implementing effective countermeasures.

To strengthen Bank of Kangaroonies' security posture, we recommend the following improvements:

- Conduct regular employee training on phishing awareness and safe computing practices

- Implement multi-factor authentication (MFA) to secure access to critical systems

- Regularly update and patch software to minimize the attack surface

- Employ intrusion detection systems (IDS) and endpoint protection to detect and block malicious activities

- Monitor network traffic for anomalies and signs of compromise

- Conduct periodic security assessments and penetration tests to identify and remediate vulnerabilities

4.4 Provide advice to policy makers on strategic issues regarding cyber capabilities, doctrine, and partnerships.

To effectively address cyber threats and build resilience, policy makers should:

- Develop and maintain a comprehensive cyber doctrine outlining the nation's approach to cyber defence, deterrence, and response

- Foster public-private partnerships to facilitate information sharing and collaboration between government agencies and private sector organisations

- Encourage international cooperation on cyber norms, threat intelligence sharing, and capacity building

- Invest in the development of domestic cyber capabilities, including education, research, and workforce development

- Create and enforce regulations that promote strong cybersecurity practices among organisations operating within the nation's critical infrastructure sectors

Conclusion

In conclusion, the purpose of this essay was to demonstrate offensive security tradecraft and create a theoretical offensive strategy against Bank of Kangaroonies. By analysing the target's environment and defences, identifying vulnerabilities, and mapping them to MITRE ATT&CK techniques and Cyber Kill Chain stages, we developed an integrated Attack Flow. We then refined this Attack Flow with relevant reconnaissance and designed attack scenarios, considering resources, capabilities, countermeasures, and challenges. Finally, we analysed the potential impact of the attack on the target and offered suggestions for defensive measures and policy recommendations.

Throughout this exercise, we have illustrated the importance of understanding offensive security tradecraft and leveraging frameworks like MITRE ATT&CK and the Cyber Kill Chain. These frameworks can be instrumental in guiding security professionals in defending their organisations against cyber threats. By anticipating an attacker's actions, identifying vulnerabilities, and implementing effective countermeasures, organisations like Bank of Kangaroonies can significantly improve their security posture and mitigate the risk of a successful cyber-attack.

References

Bertino, E., & Islam, N. (2014). Botnets and Internet of Things security. Computer, 50(2), 76-79.

Chismon, D., & Ruks, M. (2015). Threat intelligence: Collecting, analysing, evaluating. MWR InfoSecurity.

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defence informed by analysis of adversary campaigns and intrusion kill chains. Leading Issues in Information Warfare & Security Research, 1, 80.

Kaspersky. (2017). Financial cyberthreats in 2016. Kaspersky Lab ZAO.