Document Reference:	VORTU-1	Effective Date:	6 May 2024
Document Name:	Virus Outbreak Red Team Usecase	Expiry Date:	6 May 2025

Virus Outbreak Red Team Usecase

Redback Operations

Document Owner:	Purple Team	Last Modified By:	Liya Thomas
Next Review Date:	17 July 2024	Last Modified on:	5 May 2024

Document Reference:	VORTU-1	Effective Date:	6 May 2024
Document Name:	Virus Outbreak Red Team Usecase	Expiry Date:	6 May 2025

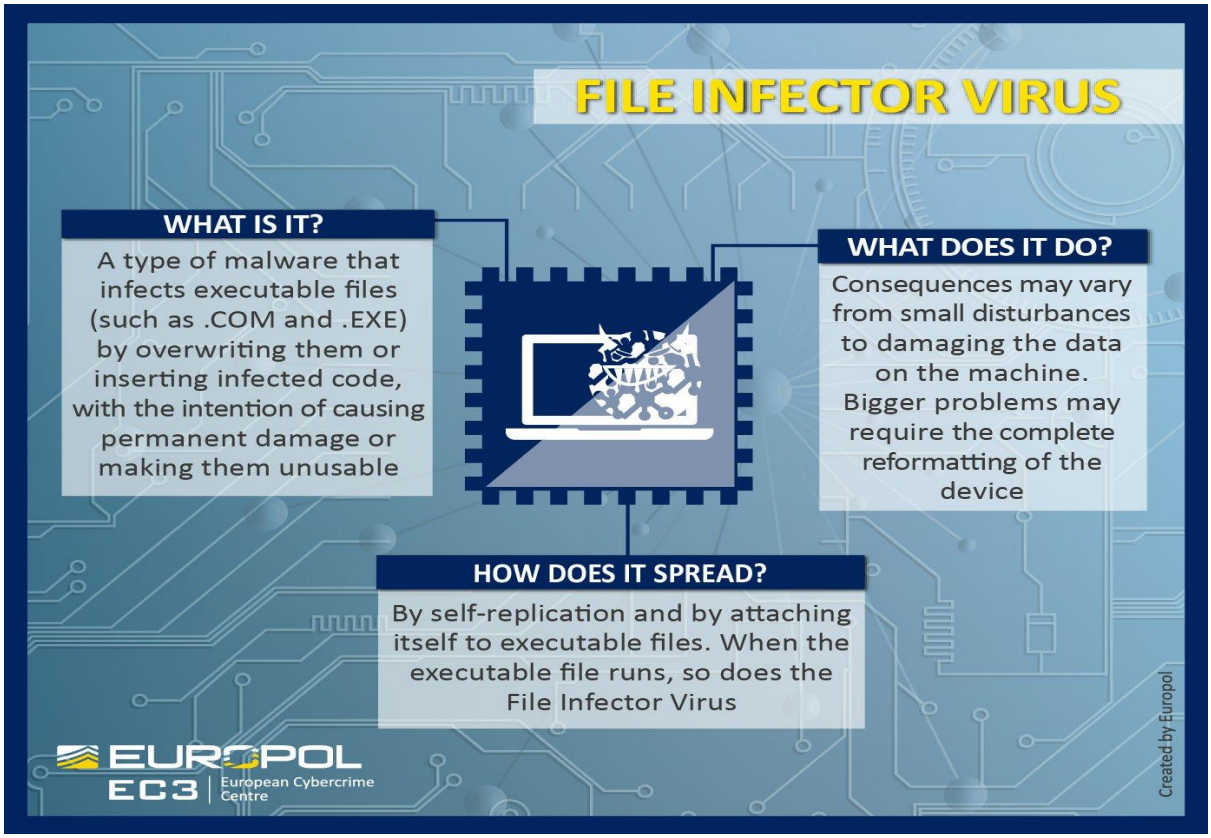
Version	Modified By	Approver	Date	Changes made
0.1	Liya Thomas		5 May 2024	First Draft
0.2	Joel Daniel		6 May 2024	Cosmetic Changes
1.0	Liya Thomas	Joel Daniel	6 May 2024	Approved for Publishing

Table of Contents

1 Introduction:

In the perpetual battle against cyber threats, the specter of virus outbreaks looms large, posing formidable challenges to organizational security. From insidious file infectors to stealthy network viruses, the arsenal of malicious actors continues to evolve, necessitating a comprehensive understanding of these attack vectors. In this red team exercise, we embark on a journey through various virus attack types, each presenting unique complexities and implications. By immersing ourselves in simulated scenarios, we aim to evaluate the resilience of organizational defenses and enhance preparedness to confront these pervasive threats head-on.

2 File Infector Virus :



2.1 Objective:

The primary aim of deploying a file infector virus as part of a red team exercise is to showcase the ease with which such malware can spread within a targeted system and the subsequent impact it can have on compromised systems.

2.2 Steps:

1. Identify Target Systems: Conduct thorough reconnaissance to identify systems with vulnerable software. This involves scanning for outdated applications or operating systems that are susceptible to exploitation.

2. Crafting the Payload: Utilize tools such as Metasploit or custom scripts to craft a file infector virus payload. This payload should be designed to infect executable files commonly used within the target environment.

3. Delivery via Social Engineering: Employ social engineering tactics to deliver the infected file to target users. This could involve crafting convincing phishing emails or utilizing file-sharing platforms where users are likely to download and execute the infected file.

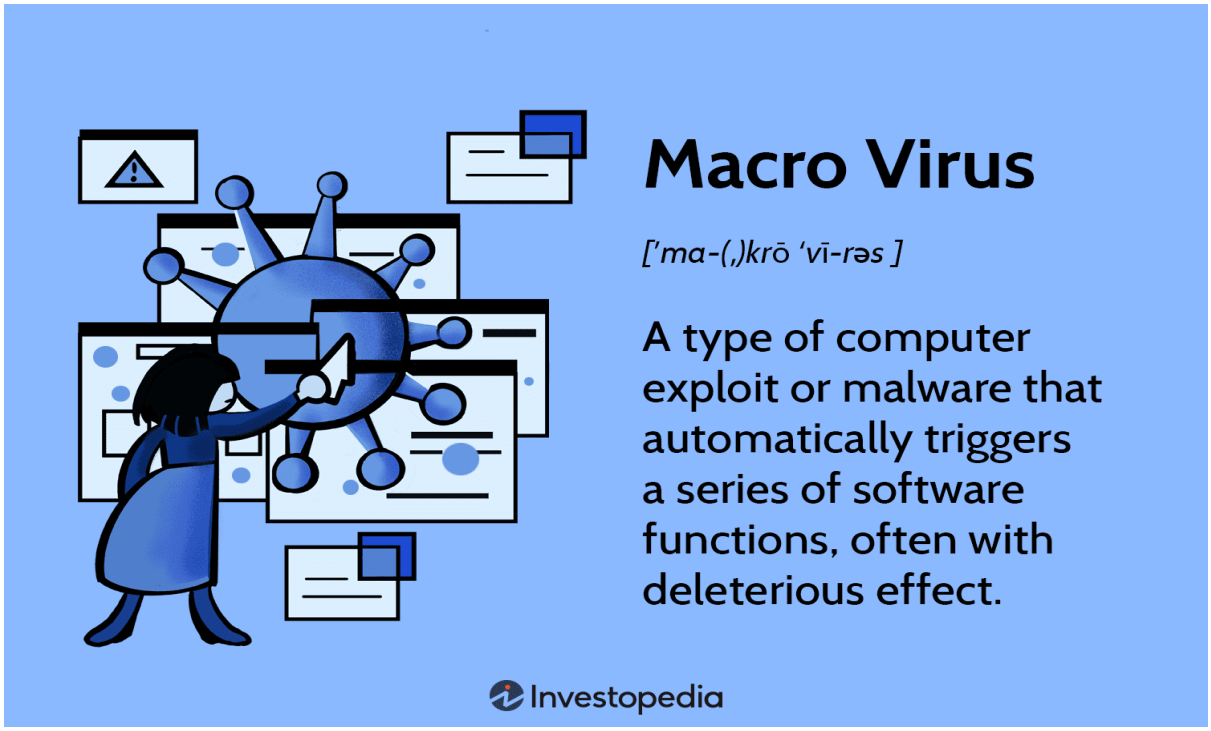
4. Monitoring Antivirus Responses: Continuously monitor antivirus software responses to the infected file. Modify the virus if necessary to evade detection by antivirus programs, ensuring that it maintains its ability to spread and infect files undetected.

5. Tracking Virus Spread: Monitor the spread of the virus within the target network by tracking file modifications and checksum changes. This helps gauge the effectiveness of the virus in infiltrating and spreading within the network.

2.3 Tools and Techniques:

- Metasploit: Utilize Metasploit for crafting and delivering the file infector virus payload. Metasploit provides a comprehensive framework for developing, testing, and executing exploits, making it an ideal tool for red team operations.
- Custom Virus Creation Scripts: Develop custom scripts tailored to the specific requirements of the red team exercise. These scripts can automate various aspects of virus creation and modification, enabling rapid adaptation to changing circumstances.
- Social Engineering Tactics: Employ social engineering techniques to deceive users into executing the infected file. This could include crafting convincing phishing emails or creating enticing file-sharing links that entice users to download and execute the malicious payload.
- Antivirus Evasion Techniques: Employ techniques to evade detection by antivirus software, such as code obfuscation, polymorphism, or encryption. Continuously monitor antivirus responses and modify the virus accordingly to maintain its ability to evade detection.
- Monitoring Tools: Utilize monitoring tools to track the spread of the virus within the target network. These tools can help identify infected files, monitor file modifications, and assess the overall impact of the virus on compromised systems.

3 Macro Virus:



3.1 Objective:

The aim of deploying a macro virus as part of a red team exercise is to demonstrate the effectiveness of such malware in compromising systems through infected documents, thereby highlighting the importance of security measures against macro-based attacks.

3.2 Steps:

1) Crafting Malicious Documents: Utilize Microsoft Office or similar tools to craft malicious documents with embedded macros. These macros can be designed to execute malicious code upon opening the document, exploiting vulnerabilities in the application's macro functionality.

2) Distribution via Phishing: Distribute the malicious documents via phishing emails or file-sharing platforms. Ensure that the emails or files contain enticing subject lines or content to increase the likelihood of users opening them.

3) Encouraging Macro Execution: Employ social engineering tactics or deceptive prompts to encourage users to enable macros when opening the document. This may involve crafting

convincing messages that persuade users to bypass security warnings and enable macros for purportedly legitimate reasons.

4)Monitoring for Infections: Continuously monitor for successful infections across target systems. Track the spread of the macro virus and observe any subsequent system disruptions or data loss resulting from its malicious activities.

3.3 Tools and Techniques:

- Microsoft Office VBA Scripting: Utilize Visual Basic for Applications (VBA) scripting to create the malicious macros embedded within the documents. VBA provides a powerful scripting language that allows for the automation of tasks within Microsoft Office applications, including the execution of malicious code.
- Phishing Email Templates: Develop phishing email templates designed to lure recipients into opening the malicious documents. These templates should be carefully crafted to appear legitimate and persuasive, increasing the likelihood of successful infection.
- Document Encryption: Employ document encryption techniques to evade detection by antivirus software. Encrypting the malicious documents can help bypass static signature-based detection methods used by antivirus programs.

4 Boot Sector Virus

4.1 Objective:

The objective of deploying a boot sector virus as part of a red team exercise is to illustrate the significant impact such malware can have on system boot-up processes and data integrity. By demonstrating the capabilities of a boot sector virus, the red team aims to emphasize the importance of safeguarding against such threats and implementing robust security measures to protect critical system components.

4.2 Steps:

1. Developing the Boot Sector Virus Payload:

To initiate the exercise, the red team must first develop a boot sector virus payload tailored to target specific operating systems or storage devices. This entails thorough research and understanding of the target environment's architecture and boot process. The virus payload should be designed to infect the boot sector of the target system discreetly, ensuring persistence and evasion of detection mechanisms.

2. Injecting the Virus into the Boot Sector:

The next step involves injecting the developed boot sector virus into the boot sector of a target system. This can be achieved using various exploitation techniques, such as

leveraging vulnerabilities in the boot process or through physical access to the system. For remote deployment, exploiting vulnerabilities in network boot protocols or remote management interfaces may be necessary.

3. Monitoring for Anomalies during System Boot-Up:

With the virus injected into the boot sector, the red team must carefully monitor the target system for anomalies during the boot-up process. Anomalies may include errors, delays, or unexpected behavior indicative of the virus's interference with the boot sequence. Monitoring tools specifically designed to track system boot-up processes can aid in detecting such anomalies.

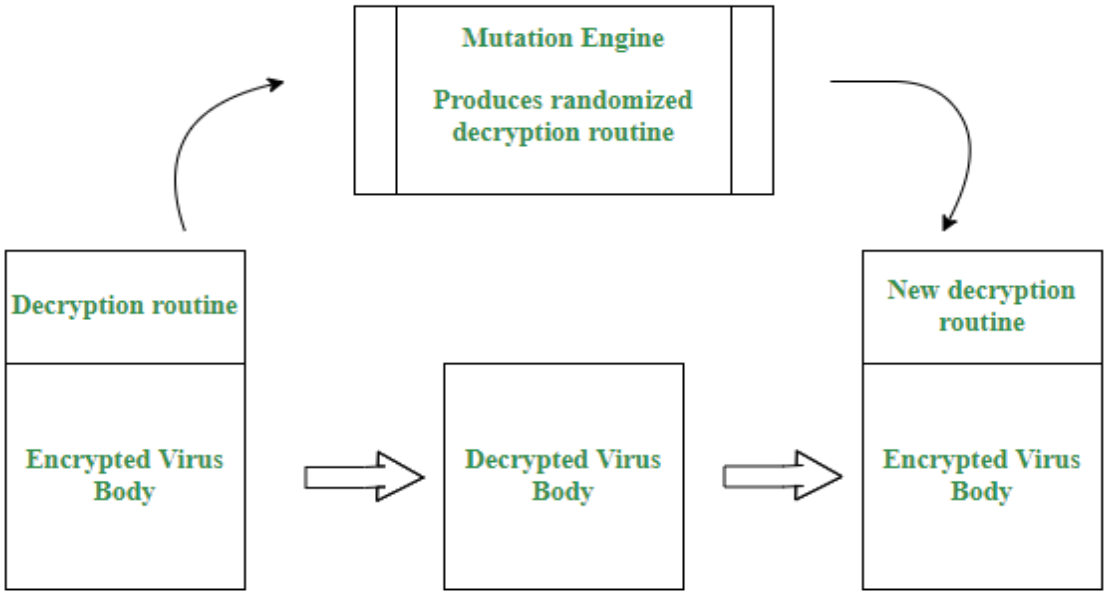
4. Demonstrating Data Loss or Corruption:

Once the virus has successfully infected the boot sector, the red team can demonstrate the consequences of its presence on the target system's data integrity. This may involve showcasing data loss or corruption resulting from the virus's interference with disk partitions or critical system files. By simulating real-world scenarios of data loss or corruption, the red team highlights the severity of the threat posed by boot sector viruses.

4.3 Tools and Techniques:

- Boot Sector Manipulation Tools: Utilize specialized tools designed for manipulating boot sectors to develop and inject the boot sector virus payload into the target system. These tools may include sector editors, boot sector creation utilities, or custom scripts tailored to the specific requirements of the red team exercise.
- Physical Access Exploitation: In scenarios where physical access to the target system is feasible, exploit vulnerabilities in the system's physical security measures to gain access and inject the virus into the boot sector. This may involve techniques such as booting from external media or accessing the system's hardware components directly.
- System Boot-Up Monitoring Tools: Employ monitoring tools capable of tracking system boot-up processes to detect anomalies indicative of boot sector virus activity. These tools can provide real-time alerts and notifications, allowing the red team to promptly respond to any detected threats and assess the impact on the target system.

5 Polymorphic Virus:



5.1 Objective:

The primary objective of deploying a polymorphic virus as part of a red team exercise is to highlight the challenges faced by antivirus software in detecting and mitigating such sophisticated malware. By demonstrating the capabilities of a polymorphic virus, the red team aims to underscore the importance of employing advanced detection and defense mechanisms to combat evolving cyber threats.

5.2 Steps:

1. Creating a Polymorphic Virus:

The initial step involves creating a polymorphic virus capable of altering its code and signatures with each infection. This requires the use of specialized polymorphic virus generation tools and techniques that enable dynamic code obfuscation and mutation. The virus should be designed to generate unique variants with each infection, making it difficult for antivirus software to detect using traditional signature-based methods.

2. Deploying the Virus Across Target Systems:

Once the polymorphic virus is created, the red team deploys it across target systems to assess its effectiveness in evading detection by antivirus software. Care should be taken to ensure varied payloads and infection vectors are used to further obfuscate the virus's presence and evade signature-based detection. This may involve leveraging different delivery mechanisms such as email attachments, malicious websites, or removable media.

3. Monitoring Antivirus Responses and Adapting the Virus Code:

Continuously monitor antivirus responses to the deployed polymorphic virus across target systems. Analyze how antivirus software detects and responds to the virus's presence and adapt the virus code accordingly to bypass detection mechanisms. This may involve modifying the virus's code structure, encryption techniques, or mutation algorithms to evade detection while maintaining its malicious functionality.

4. Demonstrating Impact on Infected Systems:

To showcase the effectiveness of the polymorphic virus, demonstrate its ability to cause random crashes or unusual behavior across infected systems. This can include scenarios where the virus disrupts system processes, corrupts files, or compromises system stability. By highlighting the real-world impact of the virus on infected systems, the red team emphasizes the importance of proactive threat detection and mitigation strategies.

5.3 Tools and Techniques:

- Polymorphic Virus Generation Tools: Utilize specialized polymorphic virus generation tools capable of generating unique variants with each infection. These tools employ advanced code obfuscation techniques and mutation algorithms to evade detection by antivirus software.
- Dynamic Code Obfuscation Techniques: Implement dynamic code obfuscation techniques to continuously modify the virus's code and signatures with each infection. This may include encryption, code permutation, and instruction reordering to obfuscate the virus's behavior and evade static analysis by antivirus software.
- Continuous Monitoring for Antivirus Responses: Employ continuous monitoring tools to track antivirus responses to the deployed polymorphic virus across target systems.

This allows the red team to assess the effectiveness of the virus in evading detection and adapt its code accordingly to bypass detection mechanisms.

6 Resident Virus:

6.1 Objective:

The objective of deploying a resident virus as part of a red team exercise is to showcase the persistence and stealth of such malware within system memory. By demonstrating the capabilities of a resident virus, the red team aims to emphasize the importance of implementing robust security measures to detect and mitigate memory-resident threats effectively.

6.2 Steps:

1. Developing a Resident Virus:

The first step involves developing a resident virus capable of embedding itself in system memory and evading detection by antivirus software. This requires utilizing specialized resident virus creation tools and techniques that enable the virus to inject its code into system processes or system memory regions, ensuring persistence even after system restarts.

2. Infecting Target Systems:

Once the resident virus is developed, the red team infects target systems to demonstrate its sustained activity despite system restarts. Care should be taken to infect multiple systems

across the target environment to assess the virus's impact and propagation capabilities effectively.

3. Monitoring for Unusual Behavior:

Continuously monitor infected systems for performance degradation or unusual behavior indicative of resident virus activity. This may include increased CPU or memory usage, unexpected system crashes, or unauthorized network communication initiated by the virus. Monitoring tools capable of detecting anomalous behavior in real-time should be employed to identify and respond to resident virus activity promptly.

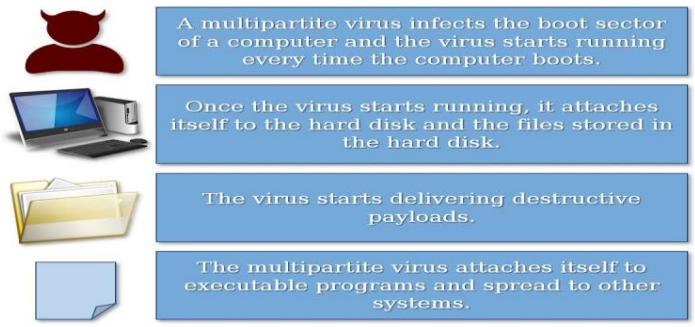
4. Evading Antivirus Scans:

To evade detection by antivirus scans, the resident virus employs memory-scanning evasion techniques that allow it to hide its presence within system memory. This may involve encrypting or obfuscating its code, using stealthy injection techniques, or manipulating system memory structures to evade detection by traditional antivirus software.

6.3 Tools and Techniques:

- Resident Virus Creation Tools: Utilize specialized resident virus creation tools capable of developing malware designed to embed itself in system memory. These tools often provide features for code injection, stealth techniques, and persistence mechanisms necessary for creating effective resident viruses.
- Memory Injection Techniques: Employ memory injection techniques to inject the resident virus's code into system processes or memory regions. This ensures the virus remains active and persistent within system memory, allowing it to evade detection by traditional file-based antivirus scans.
- Memory-Scanning Evasion Strategies: Implement memory-scanning evasion strategies to evade detection by antivirus software. This may include encrypting or obfuscating the virus's code to make it difficult for antivirus scanners to detect, or utilizing stealthy injection techniques that bypass signature-based detection methods.

7 Multipartite Virus :



7.1 Objective:

The objective of deploying a multipartite virus as part of a red team exercise is to showcase the combined effects of boot sector and file infector viruses, maximizing impact and spread within the target environment. By demonstrating the capabilities of a multipartite virus, the red team aims to underscore the importance of implementing comprehensive security measures to defend against complex, multi-vector cyber threats.

7.2 Steps:

1. Developing a Multipartite Virus:

The first step involves developing a multipartite virus capable of infecting both executable files and boot sectors. This requires utilizing specialized multipartite virus creation tools and techniques that enable the virus to spread across multiple infection vectors while maintaining its ability to infect critical boot sectors.

2. Distributing the Virus Payload:

Once the multipartite virus is developed, the red team distributes the virus payload through various vectors, including email attachments, compromised websites, and removable media. Care should be taken to diversify distribution channels to maximize the virus's reach and propagation potential across the target environment.

3. Monitoring for Infections and Tracking Impact:

Continuously monitor for infections across the target environment and track the virus's impact on both files and system boot processes. Utilize network traffic monitoring tools to detect and analyze virus propagation patterns, identifying infected systems and assessing the extent of the virus's spread.

4. Demonstrating Effects of the Multipartite Virus:

To showcase the combined effects of the multipartite virus, demonstrate the resulting data loss, system instability, and network propagation caused by the virus. This may include scenarios where infected files become corrupted, system boot processes are disrupted, and the virus spreads rapidly across interconnected systems within the network.

7.3 Tools and Techniques:

- Multipartite Virus Creation Tools: Utilize specialized multipartite virus creation tools capable of developing malware designed to infect both executable files and boot sectors. These tools often provide features for generating complex infection chains and spreading across multiple vectors.
- Multiple Infection Vector Exploitation: Exploit multiple infection vectors, including email attachments, compromised websites, and removable media, to distribute the multipartite virus payload. This ensures broad coverage and maximizes the virus's propagation potential within the target environment.
- Network Traffic Monitoring Tools: Employ network traffic monitoring tools to detect and analyze virus propagation patterns across the target environment. These tools provide visibility into network communications and can help identify infected systems, track the virus's spread, and assess its impact on network infrastructure.

8 Network Virus :

8.1 Objective:

The primary objective of deploying a network virus as part of a red team exercise is to highlight the risks associated with network-based virus propagation and the exploitation of network vulnerabilities. By demonstrating the capabilities of a network virus, the red team aims to underscore the importance of implementing robust network security measures to defend against such threats effectively.

8.2 Steps:

1. Identifying Target Networks with Vulnerabilities:

The initial step involves identifying target networks with known vulnerabilities in network protocols or services. This requires conducting comprehensive network scans using tools such as Nmap to identify open ports, services running on target systems, and potential vulnerabilities that could be exploited for virus propagation.

2. Developing a Network Virus Payload:

Once vulnerabilities are identified, the red team develops a network virus payload capable of exploiting these vulnerabilities for propagation. This involves leveraging exploit development frameworks such as Metasploit to develop exploits targeting specific vulnerabilities in network protocols or services commonly used within the target environment.

3. Deploying the Virus within the Target Network:

With the network virus payload developed, the red team deploys the virus within the target network using various delivery methods. This may include exploiting network shares, phishing emails containing malicious attachments, or leveraging compromised systems as launch points for further propagation.

4. Monitoring for Virus Spread through Network Connections:

Continuously monitor the target network for signs of virus spread through network connections. This involves analyzing network traffic, monitoring network logs, and identifying anomalous behavior indicative of virus propagation. Network intrusion detection systems (IDS) and intrusion prevention systems (IPS) can aid in detecting and mitigating virus propagation attempts.

5. Demonstrating Increased Network Traffic and Disruptions:

To showcase the impact of the network virus, demonstrate increased network traffic and disruptions caused by its propagation. This may include scenarios where infected systems experience network slowdowns, service disruptions, or unauthorized network connections initiated by the virus. By simulating real-world network-based attacks, the red team highlights the potential risks associated with virus propagation within the target environment.

6. Exploiting Compromised Systems for Further Access or Data Exfiltration:

Exploit compromised systems within the target network for further access or data exfiltration. Once the virus has successfully propagated within the network, leverage compromised systems to escalate privileges, pivot to other network segments, or exfiltrate sensitive data for reconnaissance or malicious purposes.

8.3 Tools and Techniques:

Network Scanning Tools (e.g., Nmap):

Utilize network scanning tools such as Nmap to identify target networks and assess vulnerabilities in network protocols or services.

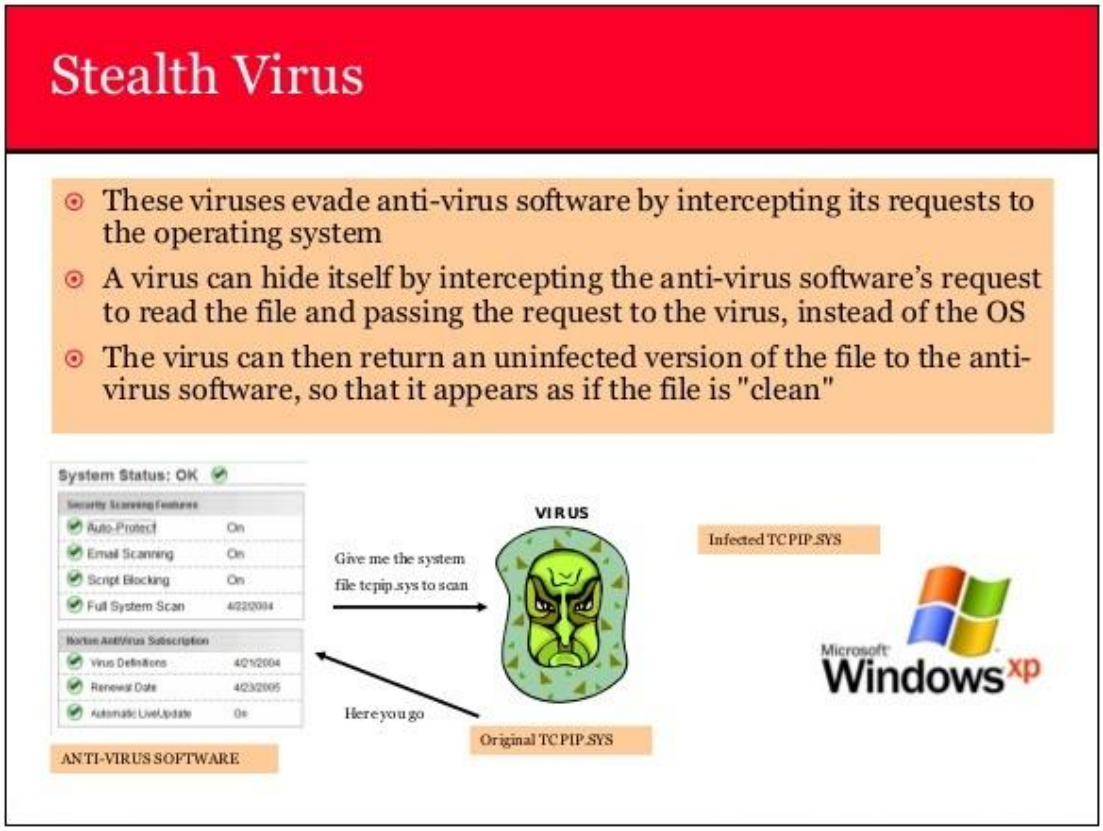
Exploit Development Frameworks (e.g., Metasploit):

Leverage exploit development frameworks like Metasploit to develop exploits targeting identified vulnerabilities for virus propagation within the target network.

Payload Delivery via Network Shares or Phishing Emails:

Deliver the network virus payload via network shares, phishing emails containing malicious attachments, or other vectors to initiate virus propagation within the target network.

9 Stealth Virus :



9.1 Objective:

The primary objective of deploying a stealth virus as part of a red team exercise is to test the effectiveness of such malware in evading detection and carrying out covert operations. By

demonstrating the capabilities of a stealth virus, the red team aims to highlight the challenges faced by traditional security measures in detecting and mitigating advanced threats.

9.2 Steps:

1. Developing a Stealth Virus:

The initial step involves developing a stealth virus capable of hiding its presence and operations from antivirus software and system administrators. This requires utilizing specialized stealth virus development frameworks and techniques that enable the virus to remain undetected by traditional security measures.

2. Deploying the Virus across Target Systems:

Once the stealth virus is developed, the red team deploys it across target systems while ensuring it remains undetected by traditional security measures. This may involve leveraging various infection vectors such as phishing emails, compromised websites, or removable media to initiate virus propagation within the target environment.

3. Monitoring for Anomalies in System Behavior:

Continuously monitor target systems for anomalies in system behavior, network traffic, and file properties indicative of stealth virus activity. This involves analyzing system logs, network traffic patterns, and file attributes to detect any suspicious behavior associated with the stealth virus.

4. Demonstrating Covert Operations:

To showcase the effectiveness of the stealth virus, demonstrate unauthorized access, data manipulation, or exfiltration carried out by the virus without raising suspicion. This may include scenarios where the virus stealthily collects sensitive information, manipulates files or system configurations, or exfiltrates data to external servers without alerting system administrators.

5. Evading Detection and Removal Attempts:

Evade detection and removal attempts by antivirus software through continuous adaptation and evasion techniques. This involves dynamically modifying the virus's code, employing encryption and obfuscation techniques, and evading signature-based detection methods used by antivirus software to detect and remove the stealth virus.

9.3 Tools and Techniques:

- Stealth Virus Development Frameworks: Utilize specialized stealth virus development frameworks capable of generating malware designed to evade detection by traditional security measures. These frameworks provide features for code obfuscation, encryption, and stealthy behavior to hide the virus's presence and operations.
- Encryption and Obfuscation Techniques: Employ encryption and obfuscation techniques to hide the stealth virus's code and evade detection by antivirus software. This may include encrypting the virus's payload, obfuscating code structures, and dynamically modifying the virus's behavior to avoid detection by signature-based detection methods.
- Continuous Monitoring for Suspicious Activities: Continuously monitor target systems for suspicious activities associated with the stealth virus. This involves analyzing system logs, network traffic patterns, and file properties to detect any anomalies indicative of virus activity and respond promptly to mitigate the threat.

Conclusion:

As we conclude our exploration of virus outbreak scenarios, it becomes evident that proactive defense measures are paramount in safeguarding against cyber threats. Through meticulous planning, rigorous testing, and continuous adaptation, organizations can fortify their defenses and mitigate the risks posed by virus outbreaks. By leveraging the insights gained from these red team exercises, we empower organizations to strengthen their cybersecurity posture and navigate the ever-changing threat landscape with confidence and resilience. Together, we can forge a path towards a safer and more secure digital future.

References

File Infector Virus- https://pbs.twimg.com/media/Di81vWzW4AE9iHi.jpg
Macro Virus - https://www.investopedia.com/thmb/TTyRalsRy93aknTdntwRTtjTMx4=/1500x0/filters:no_upscale():max_bytes(150000):strip_icc()/final_macrovirus_definition_0109-fd4ab3ebfe51452bb561f17b691f2f4e.png
Boot Sector Virus - https://www.shutterstock.com/image-photo/network-security-computer-concept-earth-260nw-706266148.jpg
polymorphic virus - https://media.geeksforgeeks.org/wp-content/uploads/20220216151333/polymorphic.png
Resident Virus:- https://media.moddb.com/images/members/4/3019/3018560/profile/resident_virus.jpg
Multipartite Virus- https://i.ytimg.com/vi/pq_B0NrYHvQ/maxresdefault.jpg
Network Virus- https://image.slidesharecdn.com/networkvirus-111211084753-phpapp02/85/network-virus-4-320.jpg
Stealth Virus- https://optimoav.files.wordpress.com/2015/07/stealth-virus.jpg