Practical no: 1

Name: Saloni Vishwakarma
Batch-Roll no: C1-13
Subject: Computer Security Lab
Date of execution: 2 September 2023

Aim: Introduction to Computer Security Foundations

Task 1: History of Computer Crimes and Information System Security
- Research and present notable historical computer security breaches and incidents.
- Discuss the evolution of security measures in response to these incidents.

1) Mydoom Malware(2004) : Mydoom malware is a computer worm that was first released in 2004. The worm is spread by email attachments and infected websites. Once a computer is infected, the worm will automatically send itself to all the contacts in the victim's address book. Mydoom is also capable of launching denial-of-service attacks against websites. It is typically spread through email attachments or by downloading infected files from the Internet. It is also known by its file name, W32.Mydoom@mm, and is classified as a mass-mailing worm. This type of malware is designed to spread itself by sending emails with infected attachments to addresses found in the address book of an infected computer. When the attachment is opened, the Mydoom malware infects the computer and begins to replicate itself. Mydoom can cause a number of problems on an infected computer, including deleting files, stealing information, and causing the system to crash. Mydoom is considered to be one of the most destructive computer viruses ever created. The worm has caused billions of dollars in damage and is considered to be one of the most destructive computer viruses ever released.

Impact:
Once inside a system, MyDoom initiates its damaging processes. It seeks to exploit vulnerabilities and establish a backdoor, providing cybercriminals unauthorized access to the infected machine. This unauthorized access enables various nefarious activities, including data exfiltration, remote control, and participation in botnets. As part of a botnet, compromised devices can be harnessed to launch coordinated and powerful DDoS attacks, overwhelming targeted websites or services with an avalanche of traffic, rendering them inaccessible.

Moreover, MyDoom possesses the ability to target specific domains, potentially crippling an organization's online presence and communications. Its payload includes mechanisms to thwart attempts to remove or disinfect the worm, making its eradication a challenging endeavor. This persistence, coupled with its rapid propagation, exacerbates the overall impact.

The damage inflicted by MyDoom is multifaceted. It can disrupt business operations, compromise sensitive data, and lead to financial losses due to service interruptions and remediation efforts. In addition, the compromised systems can be enlisted for further cybercriminal activities, amplifying the worm's destructive potential. The propagation rate and wide-ranging capabilities of MyDoom emphasize the importance of robust email security, continuous software updates, and proactive cybersecurity practices.

Security Measures:
In response to the Mydoom malware attack in 2004, various security measures were taken by organizations, individuals, and the cybersecurity community to mitigate the impact of the attack and prevent future incidents. Here are some of the key security measures implemented in response to the Mydoom malware attack:

-Antivirus and Anti-Malware Updates
-Email Filtering and Attachment Scanning
-Operating System and Software Patching
-Firewall Configuration
-User Education and Awareness
-Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)

These security measures, both technical and educational, helped mitigate the impact of the Mydoom malware attack and contributed to a better overall security posture. They also served as important lessons for the ongoing fight against evolving cyber threats.

2) Code Red(2001) : Code Red was a computer worm observed on the Internet on July 15, 2001. It attacked computers running Microsoft's IIS web server. It was the first large-scale, mixed-threat attack to successfully target enterprise networks.
The Code Red worm was first discovered and researched by eEye Digital Security employees Marc Maiffret and Ryan Permeh when it exploited a vulnerability discovered

by Riley Hassell. They named it "Code Red" because they were drinking the Mountain Dew flavor of the same name at the time of discovery.
Although the worm had been released on July 13, the largest group of infected computers was seen on July 19, 2001. On that day, the number of infected hosts reached 359,000.[3] It spread worldwide, becoming particularly prevalent in North America, Europe and Asia (including China and India).

Impact:
Code Red had a significant impact on the internet during its outbreak. It spread quickly due to the large number of vulnerable IIS servers.
The defacement of websites caused embarrassment and financial losses for affected organizations.
The DDoS attacks on the White House's website resulted in temporary slowdowns and outages.

Security Measures:
In response to the Code Red worm outbreak in 2001, various security measures and countermeasures were taken by organizations, system administrators, and the cybersecurity community to mitigate the impact of the worm and prevent further infections. Here are some of the key security measures and actions that were taken:

-Patch Application
-Network Traffic Filtering
-Intrusion Detection Systems (IDS)
-Quarantine and Isolation
-Security Software Updates
-Log Analysis
-Web Server Security Enhancements
-Security Awareness and Education
-Coordination with Law Enforcement

In some cases, organizations and authorities coordinated with law enforcement agencies to investigate and track down the authors or operators behind the Code Red worm.
The Code Red incident underscored the importance of timely patching, network security, and proactive cybersecurity measures. It also highlighted the need for organizations to have robust incident response plans in place to address and contain such threats quickly.

3) SQL Slammer(2003) : SQL Slammer, also known as SQL Server 2003, is a notable computer worm that emerged in January 2003. It is famous for its rapid propagation and significant impact on the internet.

Impact:
It generates a lot of network packets, which leads to the overloading of servers and slowing down network traffic.
It goes to computer memory without saving itself in the memory and without creating or modifying, any files in the system.
It infects a large percentage of victims' computers within ten minutes.
Microsoft SQL Server 2000 is mostly impacted by the SQL Slammer virus.
SQL slammer Virus can make the email service Fail.
SQL slammer Virus is able to block the network.

Security Measures:
Microsoft had previously released a security patch (MS02-039) to address the SQL Server vulnerability. In response to SQL Slammer, system administrators were urged to immediately apply this patch to protect their systems.
Network administrators implemented firewall rules and filtering to block SQL traffic at port 1434/UDP, which was commonly used by SQL Slammer. This helped prevent the worm from entering or spreading within networks.

SQL Slammer served as a wakeup call for the importance of proactive cybersecurity measures, rapid patching, and network security. It demonstrated the potential for worms to spread rapidly and cause widespread disruption on the internet. In response to the incident, organizations and the cybersecurity community focused on improving security practices to mitigate future threats.

4)Sasser(2004) : The Sasser worm, which emerged in April 2004, is a computer worm that targeted Microsoft Windows operating systems. Here is an overview of the Sasser worm, including its payload, impact, and security measures taken in response:

Impact:
System Reboots: Sasser was designed to cause infected systems to reboot continuously. This behavior resulted in system instability and disruption as computers restarted repeatedly.

Network Congestion: The worm's scanning and propagation activity generated a significant amount of network traffic, causing network congestion in affected environments.
Financial Costs: Sasser caused financial losses due to system downtime, technical support, and cleanup efforts.

Security Measures:
-Patch Deployment
-Isolation of Infected Systems
-Cleanup and Remediation
-Firewall Rules
-Enhanced Intrusion Detection and Prevention
-User Education
-Law Enforcement Action

Sasser served as a reminder of the importance of timely patching and the potential for worms to exploit vulnerabilities in unpatched systems. It also highlighted the need for robust incident response plans and enhanced network security measures to detect and mitigate such threats effectively.

5) Blaster worm: Blaster Worm was a virus program that mainly targeted Microsoft platforms in 2003. The worm attacked computers by exploiting a security flaw with Microsoft remote procedure call (RPC) process using Transmission Control Protocol (TCP) port number 135. The virus propagated itself automatically to other machines by transmitting itself through email and other methods.

Impact:
When infection occurs, the buffer overflow causes the RPC service to crash, leading Windows to display the following message and then automatically reboot, usually after 60 seconds. Message: Windows must now restart because the Remote Procedure Call (RPC) Service terminated unexpectedly.

Security Measures:
- The most crucial security measure in response to the Blaster worm was the immediate deployment of Microsoft's security patch (MS03-026) to address the DCOM RPC vulnerability.

- Network administrators implemented firewall rules and network filtering to block or restrict traffic on the vulnerable RPC (Remote Procedure Call) ports, such as TCP/UDP port 135. Blocking these ports helped prevent the worm's propagation.
-Infected systems were isolated from the network to prevent the worm from further spreading within organizations. This helped contain the outbreak and reduce the impact on other systems.
-Security software vendors updated their antivirus and anti-malware tools to detect and remove the Blaster worm.

Conclusion: Throughout this history, the field of information system security has grown in response to the escalating threat landscape. Concepts such as encryption, firewalls, intrusion detection systems, and incident response plans have become integral to protecting digital assets. Additionally, legislation and regulations, such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), have been enacted to enforce data protection and privacy rights, making cybersecurity a priority for organizations worldwide.

References:

https://www.kaspersky.com/blog/history-lessons-code-red/45082/
https://www.geeksforgeeks.org/what-is-mydoom/
https://www.xenonstack.com/insights/sasser-virus/#:~:text=Sasser%20worm%20was%20discovered%20in,by%20using%20a%20network%20port.
https://www.techopedia.com/definition/27295/blaster-worm