ISC

(BTech III Jan-April 2024)
Week#7 – Feb 16, 2024

Dhiren Patel

Cyber Threat Hunting

- Cyber threat hunting is a proactive security strategy that seeks to identify and eliminate cybersecurity threats on the network before they cause any obvious signs of a breach.
- Traditional security methodologies and solutions reactively detect threats, often by comparing threat indicators (like the execution of unknown code or an unauthorized registry change) to a signature database of known threats.

Cyber Threat Hunting

- Examples of threat hunting techniques include:
- Searching for insider threats, such as employees, contractors or vendors.
- Proactively identifying and patching vulnerabilities on the network.
- Hunting for known threats, such as high-profile advanced persistent threats (APTs).
- Establishing and executing incident response plans to neutralize cyber threats.

Why?

- Traditional, reactive cybersecurity strategies focus primarily on creating a perimeter of automated threat detection tools, assuming that anything that makes it through these defenses is safe.
- If an attacker slips through this perimeter unnoticed, perhaps by stealing authorized user credentials through social engineering, they could spend months moving around the network and exfiltrating data.
- Unless their activity matches a known threat signature, reactive threat detection tools like antivirus software and firewalls won't detect them.

Discussion on Virus

- Virus family (pattern and style of programming)
- Virus – from whom?
- Virus from Anti-Virus companies!!
- How Anti-Virus software (scanner) works?
- Notion of Black list (E.g. Criminal List at Police station)
- Signature detection
- Zero day attacks
- Behavioural detection

Discussion on JoSAA

- JoSAA – joint seat allocation authority – came into existence in 2015
- Candidate (student) optimal algorithm provides a fair seat based on his/her preferences and availability
- Without JoSAA, JEE topper can grab a seat at NIT Trichi, IIT Bombay, BITS Pilani, NTU Singapore, NIFD/SPA, and hold each one till he/she gets confirmation from MIT !!!
- Stability of Marriage algorithm
- In mathematics, economics, and computer science, the stable marriage problem is the problem of finding a stable matching between two equally sized sets of elements given an ordering of preferences for each element.

Stable marriage problem

- Gale–Shapley algorithm to find a stable matching: The idea is to iterate through all free men while there is any free man available.
- Every free man goes to all women in his preference list according to the order.
- For every woman he goes to, he checks if the woman is free, if yes, they both become engaged!!!
- Given n men and n women, where each person has ranked all members of the opposite sex in order of preference, marry the men and women together such that there are no two people of opposite sex who would both rather have each other than their current partners.

Cyber Threat Hunting

- Proactive threat hunting attempts to identify and patch vulnerabilities before they're exploited by cyber criminals, reducing the number of successful breaches.
- It also carefully analyzes all the data generated by applications, systems, devices and users to spot anomalies that indicate a breach is taking place, limiting the duration of – and damage caused by – successful attacks.
- Plus, cyber threat hunting techniques typically involve unifying security monitoring, detection and response with a centralized platform, providing greater visibility and improving efficiency.

Threat hunting tools and how they work

- **Security monitoring**
- Security monitoring tools include antivirus scanners, endpoint security software and firewalls. These solutions monitor users, devices and traffic on the network to detect signs of compromise or breach.
- **Advanced analytical input and output**
- Security analytics solutions use machine learning and artificial intelligence (AI) to analyze data collected from monitoring tools, devices and applications on the network.

Threat hunting tools and how they work

- **Integrated security information and event management (SIEM)**
- A security information and event management solution collects, monitors and analyzes security data in real-time to aid in threat detection, investigation and response.
- **Extended detection and response (XDR) solutions**
- XDR extends the capabilities of traditional endpoint detection and response (EDR) solutions by integrating other threat detection tools like identity and access management (IAM), email security, patch management and cloud application security.

Threat hunting tools and how they work

- **Managed detection and response (MDR) systems**
- MDR combines automatic threat detection software with human-managed proactive threat hunting.
- **Security orchestration, automation and response (SOAR) systems**
- SOAR solutions unify security monitoring, detection and response integrations and automate many of the tasks involved with each. SOAR systems allow teams to orchestrate security management processes and automation workflows from a single platform for efficient, full-coverage threat hunting and remediation capabilities.

Threat hunting tools and how they work

- **Penetration testing**
- Penetration testing (pen testing) is essentially a simulated cyber attack. Security experts use specialized software and tools to probe an organization's network, applications, security architecture and users to identify vulnerabilities that cybercriminals could exploit. Pen testing proactively finds weak points, such as unpatched software or negligent password protection practices, in the hope that companies can fix these security holes before real attackers find them.

Original New

New Monalisa contains the msg

- “Hello Zelenski, Take delivery of 100 Cruize Missles at Gdańsk port Poland on 26 Jan 2024 0200. –Biden”
- Image is a good candidate as container where small msg can fit in using least affecting bit of the pixel!
- Welcome to the world of Steganography !!
- Steganography techniques involve hiding sensitive information within an ordinary, non-secret file or message, so that it will not be detected.