CYBER SECURITY LONG-TERM INTERNSHIP

Technology Stack: Cyber security with IBM QRadar

Project Title: Leveraging real-time security intelligence for enhanced defence.

Team ID : LTVIP2024TMID14828

Team Size : 4

Team Leader : Mahalakshmi Talabakthula

Team member : Palepu Divya

Register number : SBAP0014840

MY TASK

INTRODUCTION TO REAL-TIME SECURITY INTELLIGENCE

Security intelligence refers to the practice of collecting, standardizing and analysing data that is generated by networks, applications, and other IT infrastructure in real-time, and the use of that information to assess and improve an organization's security posture. Real-time security monitoring is continuously overseeing and analysing the data traffic and activities in an organization's network to detect, alert, and respond to potential security threats as they happen.

With Security Intelligence solutions, organizations can identify and mitigate those inside threats and many more, by detecting the following: Unauthorized application access or usage. Data loss such as sensitive data being transmitted to unauthorized destinations.

There are a few key principles that define security intelligence:

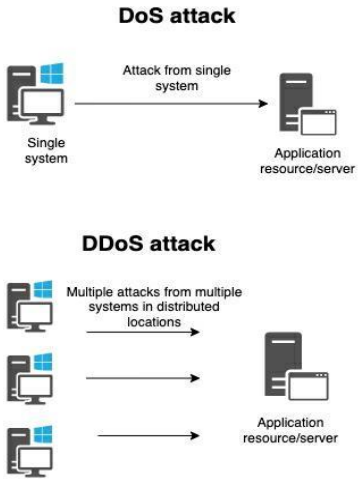
- Real-Time Analysis
- Pre-Exploit Analysis
- Collection, Normalization, And Analysis
- Actionable Insight
- Scalable
- Adjustable Size And Cost

Real Time attacks

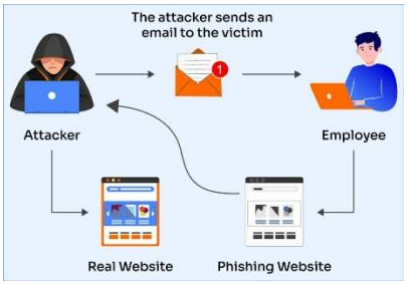
Email spoofing is a type of cyberattack that targets businesses by using emails with forged sender addresses. Because the recipient trusts the alleged sender, they are more likely to open the email and interact with its contents, such as a malicious link or attachment.

- DoS and DDoS attacks.
- Phishing attacks.
- Ransomware.
- SQL injection attacks.
- Brute force attacks.
- Trojan horses
- Spoofing
- Backdoor Trojan
- Password attacks.
- Malware.
- Man-in-the-middle.

- A DoS attack is characterized by using a single computer to launch the attack. A distributed denial-of-service (DDoS) attack is a type of



  DoS attack that comes from many distributed sources, such as a botnet DDoS attack.
- Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through email. The goal is to steal sensitive data like credit card and login information, or to install malware on the victim's machine.

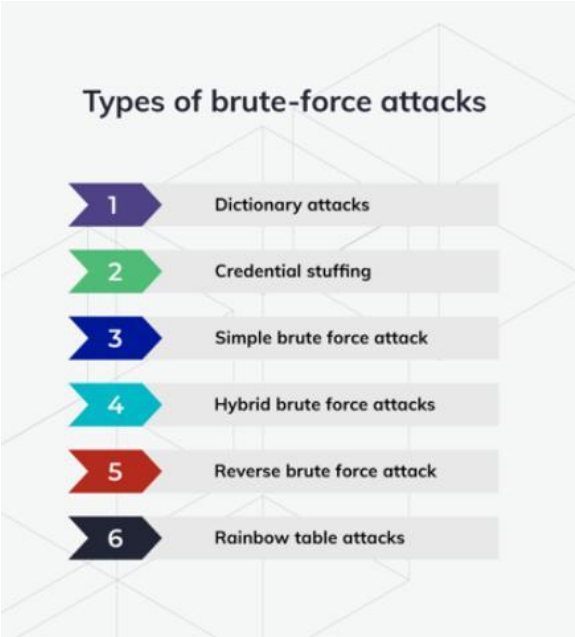


- Ransomware is a type of malware which prevents you from accessing your device and the data stored on it, usually by encrypting your files. A criminal group will then demand a ransom in exchange for decryption. The computer itself may become locked, or the data on it might be encrypted, stolen or deleted.

- SQL injection, also known as SQLI, is a common attack vector that Quses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. This

information may include any number of items, including sensitive company data, user lists or private customer details.

- A brute force attack is a hacking method that uses trial and error to



crack passwords, login credentials, and encryption keys. It is a simple yet reliable tactic for gaining unauthorized access to individual accounts and organizations' systems and networks.

- A Trojan Horse Virus is a type of malware that downloads onto a computer disguised as a legitimate program. The delivery method typically sees an attacker use social engineering to hide malicious code within legitimate software to try and gain users' system access with their software.
- A password attack is any attempt to exploit a vulnerability in user authorization within a digital system.

Conclusion

Real-time intelligence is a rapidly growing field with significant potential for various industries and applications. Organizations can analyze vast amounts of data in real-time and make informed decisions by leveraging technologies such as machine learning, AI, IoT, edge computing, and predictive analytics.Cyber security is one of the most important aspects of the fast-paced growing digital world. The threats of it are hard to deny, so it is crucial to learn how to defend from them and teach others how to do it too.