SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING-IOT Including CS&BCT

COURSE NAME : 19SB402 NETWORKING AND CYBERSECURITY

II YEAR / IV SEMESTER

Unit III- Network Threats

Topic : Impersonation

Impersonation

- A **user impersonation attack** is a type of **fraud** where an attacker poses as a trusted person to steal money or sensitive information from a company.

- Usually, these types of attacks come from **individuals targeting** high-level executives.

- The goal of these bad actors is to **transfer money into a fraudulent account, share sensitive data, or reveal login information to hack a company's network.**

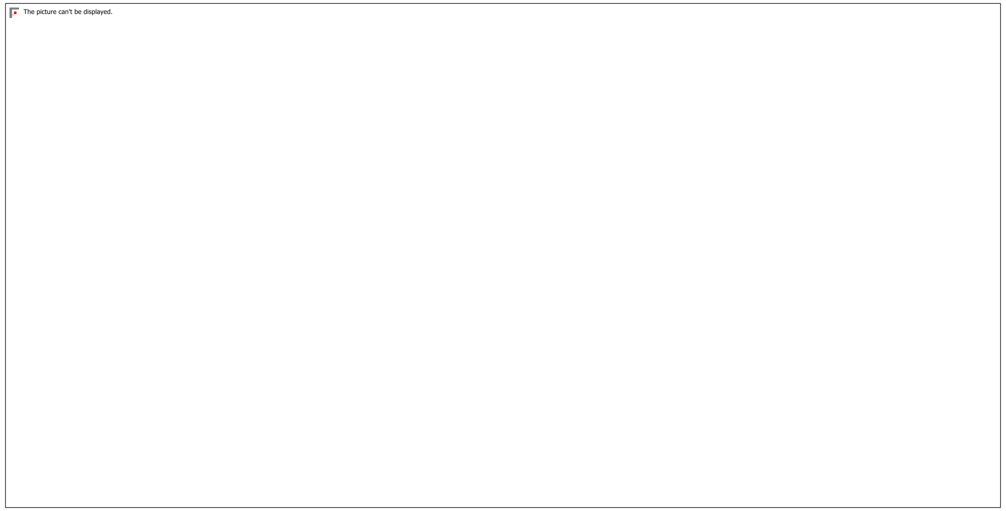
How Does an Impersonation Attack Work?

- **Impersonation attacks** don’t involve malware and often **happen through email.**
- Hackers use **social engineering to gather information** about a targeted employee.
- In addition, they conduct extensive research on their target through social media and other sources.
- This information helps give the attacker credibility and makes their message seem authentic.

- Usually, the targeted person is an employee who can transfer funds or has access to proprietary information.

- The attackers then use this data to create fake emails that appear to originate from high-level executives.

- They’re designed to trick the victim into transferring money or sensitive information.



Examples of Impersonation Attacks

Impersonation is a key strategy used in a **variety of cyberattacks**. Some common examples of impersonation attacks include:

CEO fraud

- Its also known as executive impersonation or whaling, CEO fraud occurs when attackers impersonate an executive–typically a CEO.
- They then reach out to unsuspecting employees to request sensitive data or invoice payment.

Supply chain compromise:

- Attackers specifically target an organization’s supply chain with phishing campaigns.
- If successful, they’ll impersonate the vendor with their legitimate account to request invoice payment.

Account takeover:

- Attackers compromise an employee's account to launch impersonation attacks against coworkers.
- Like other impersonations, account takeover attacks come with similar requests for invoice payment and data sharing.

How we can Stop Impersonation Attacks

Email security that can stop impersonation attacks must:

Analyze the sender and recipient relationship.

- If a trusted colleague sends an email at an odd hour from a new geographic location with an unusual request, contextual analysis flags the anomalies.

Understand an email's tone and language.

- These emails require additional security measures.

Identify compromised vendor accounts.

- Advanced email security can detect unusual behavior from vendors, including irregular invoice timing and new routing numbers.

Any Query????

Thank you……