Ethical Hacking

Team Member : Shraddha Shendge

Team Member : Sakshi Kedari

Team Member : Priyanka Gaikwad

Team Member : Pritul Raut

Types of Ethical Hacking

1. Penetration Testing: Simulated security breaches where ethical hackers imitate malicious hackers to identify vulnerabilities. This process includes three stages: reconnaissance, staging the attack, and reporting

2. Vulnerability Assessments: Similar to penetration testing but focuses on identifying and categorizing vulnerabilities without exploiting them

3. Malware Analysis: Specialized in analyzing ransomware and malware strains to understand their mechanisms and share findings with companies and the broader security community

4. Risk Management: Assisting with strategic risk management by identifying new threats and helping develop countermeasures

Key Concepts and Protocols

1. Stay Legal: Obtain proper approval before accessing and performing a security assessment.

2. Define the Scope: Determine the scope of the assessment to ensure it remains legal and within the organization's approved boundaries.

3. Disclose the Findings: Notify the organization of all vulnerabilities discovered and provide remediation advice.

4. Respect Data Sensitivity: Adhere to nondisclosure agreements and other terms required by the assessed organization

Types of Hackers

1. Authorized Hackers (White-Hat Hackers): Work legally and ethically to improve security.

2. Unauthorized Hackers (Black-Hat Hackers): Engage in illegal activities for malicious purposes.

3.Grey-Hat Hackers: A blend of both, often revealing vulnerabilities publicly to spread awareness

Benefits of Ethical Hacking

- Identifying Weak Points: Using an attacker’s point of view to discover weak points to fix.
- Real-World Assessments: Conducting assessments to protect networks.
- Data Protection: Safeguarding the security of investors' and customers' data.
- Implementing Security Measures: Strengthening networks and actively preventing breaches

Thank You