RV College of Engineering®

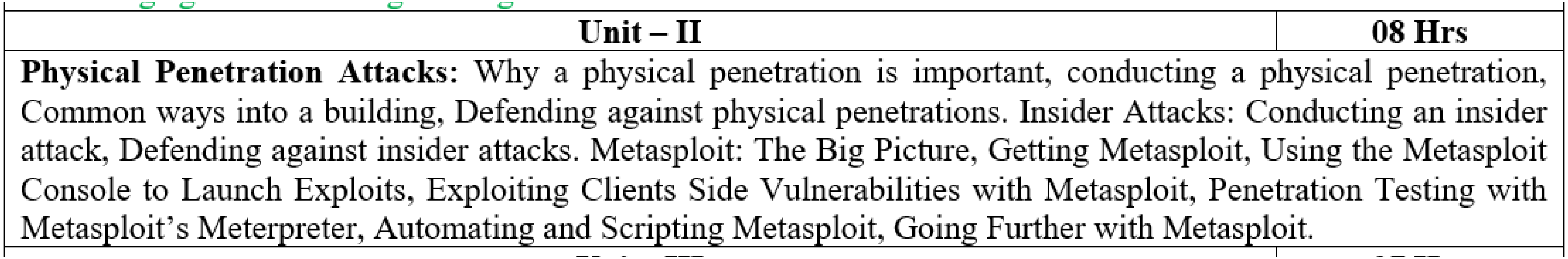
Go, change the world

CYX55TBD-Introduction to Vulnerability Assessment & Penetration Testing

Chapter- 5 Physical Penetration Attacks

Course Incharge: Dr.Mohana
Department of Computer Science & Engineering (Cyber Security)
RV College of Engineering, Bangalore-560059

Unit - II Syllabus

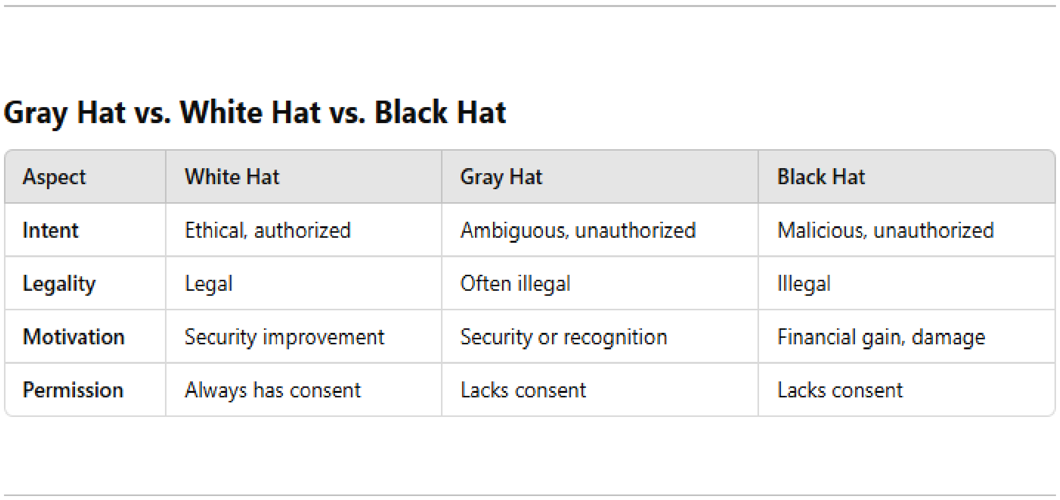


Unit – II	08 Hrs
Physical Penetration Attacks: Why a physical penetration is important, conducting a physical penetration, Common ways into a building, Defending against physical penetrations. Insider Attacks: Conducting an insider attack, Defending against insider attacks. Metasploit: The Big Picture, Getting Metasploit, Using the Metasploit Console to Launch Exploits, Exploiting Clients Side Vulnerabilities with Metasploit, Penetration Testing with Metasploit's Meterpreter, Automating and Scripting Metasploit, Going Further with Metasploit.	

Learning Objectives

- Why a physical penetration is important
- •Conducting a physical penetration
- Common ways into a building
- Defending against physical penetrations

Gray Hat Hackers



Gray Hat vs. White Hat vs. Black Hat

Aspect	White Hat	Gray Hat	Black Hat
Intent	Ethical, authorized	Ambiguous, unauthorized	Malicious, unauthorized
Legality	Legal	Often illegal	Illegal
Motivation	Security improvement	Security or recognition	Financial gain, damage
Permission	Always has consent	Lacks consent	Lacks consent

Physical Penetration Attacks

- Gaining **unauthorized physical access** to hardware systems, facilities, or sensitive areas to compromise security.
- These attacks are often employed by malicious actors, including cybercriminals, competitors, or even state-sponsored groups, to obtain confidential data, disrupt operations, or install malicious components.

Goals:

Data Theft: Accessing sensitive information stored on devices or systems.

System Disruption: Tampering with hardware to cause failure or downtime.

Surveillance or Espionage: Installing spyware or keyloggers.

Planting Malware: Embedding malicious firmware or hardware.

Techniques:

- **Social Engineering**: Exploiting human weaknesses to gain access (e.g., posing as maintenance personnel).
- **Tailgating/Piggybacking**: Following authorized personnel into restricted areas.
- **Bypassing Physical Security**: Using tools to pick locks, disable alarms, or bypass biometric systems.
- **Hardware Manipulation**: Physically tampering with devices, such as:
  - Installing keyloggers or malware-infected USB devices.
  - Intercepting electromagnetic emissions (TEMPEST attacks).
  - Modifying circuits to compromise security features.

Examples:

- An attacker disguises themselves as IT staff to replace a secure computer with a compromised device.
- Inserting a rogue USB device into a computer to install malware.
- Accessing a server room through an unlocked door or weak biometric system.

Defenses Against Physical Penetration Attacks:

- **Physical Security**:
  - Employ locks, security guards, surveillance cameras, and motion sensors.
  - Use biometric or multi-factor authentication for sensitive areas.
- **Awareness Training**:
  - Educate employees on social engineering tactics.
  - Encourage reporting of suspicious activity.
- **Device Security**:
  - Ensure physical ports are disabled or restricted.
  - Implement tamper-evident seals on devices.
- **Access Control**:
  - Limit access to critical systems to authorized personnel only.
  - Regularly audit and update access privileges.
- **Environmental Measures**:
  - Shield sensitive equipment to prevent electromagnetic interception.
  - Secure power and network cables to prevent tapping.

Why a physical penetration is important?

- It evaluates the effectiveness of physical security controls in protecting sensitive data, critical systems, and infrastructure.

1. Identifies Vulnerabilities in Physical Security
2. Protects Critical Assets
3. Mitigates Insider Threats
4. Simulates Real-world Attacks
5. Protects Against Combined Threats
6. Compliance and Regulations
7. Improves Overall Security Posture
8. Prevents Financial and Reputational Damage