Section 1.0.7 Computer Networks Fundamentals

Remote Access

Cracking OSCP: Your Roadmap to Ethical Hacking Success

Socials: HackProKP

Github: https://github.com/at0m-b0mb/Cracking-OSCP-Your-Roadmap-to-Ethical-Hacking-Success

Complete Youtube Playlist:
https://www.youtube.com/watch?v=MvkNbn8i2so&list=PLyrv3TPh3ejYNZipa0OIUvkdjHeUTRJ3J&index=1&t=0s

Remote Desktop Protocol (RDP):

- Developed by Microsoft, RDP is widely used for remote access to Windows-based systems.
- It allows users to connect to a remote computer's desktop interface and control it as if they were physically present.
- RDP encrypts data transmission between the client and the server to ensure security.
- It's commonly used for administrative tasks, technical support, and remote collaboration.

Client-Server Architecture

Features

- DESKTOP ACCESS
- REMOTE CONTROL
- AUDIO AND VIDEO STREAMING
- CLIPBOARD REDIRECTION
- PRINTER AND DRIVE REDIRECTION

Security

ENCRYPTION

AUTHENTICATION

NETWORK SECURITY

Use Cases

- Remote Administration
- Remote Work
- Technical Support

Virtual Network Computing (VNC):

VNC is a cross-platform remote desktop protocol that allows you to view and interact with the desktop of a remote computer.

Unlike RDP, VNC is not tied to a specific operating system, making it compatible with Windows, macOS, Linux, and other platforms.

VNC implementations vary, with some offering encryption and authentication features for security.

It's often used for remote administration, troubleshooting, and remote support.

Client-Server Architecture

Features

- Full Desktop Access
- Remote Control
- Screen Sharing
- File Transfer
- Clipboard Sharing

Security

ENCRYPTION

AUTHENTICATION

NETWORK SECURITY

Implementations

- There are several implementations of VNC available!
  - RealVNC
  - TightVNC
  - UltraVNC
  - TigerVNC
  - TurboVNC

Use Cases

REMOTE ADMINISTRATION

TECHNICAL SUPPORT

REMOTE WORK AND COLLABORATION

Secure Shell (SSH):

SSH is a cryptographic network protocol that provides secure access to a remote computer over an unsecured network.

While primarily used for secure command-line access to Unix-like systems (e.g., Linux, macOS), SSH can also provide secure tunneling for other protocols.

SSH provides strong encryption and authentication mechanisms, making it suitable for secure remote access and file transfer.

It's commonly used by system administrators, developers, and network engineers for remote server management and data transfer.

Encryption and Authentication

Client-Server Model

Terminal Access and Command Execution

Secure File Transfer

Tunneling and Port Forwarding

Telnet:

Telnet is an older remote access protocol that provides terminal emulation over a network connection.

Unlike SSH, Telnet does not provide encryption or strong authentication, making it insecure for transmitting sensitive information over public networks.

Telnet is primarily used for accessing legacy systems and network devices that do not support modern encryption protocols.

Due to its security vulnerabilities, Telnet usage is generally discouraged in favor of more secure alternatives like SSH.

Client-Server Architecture

Text-Based Communication

Protocol Operation

Security Considerations

Use Cases

Thank You! 😊 ❤️

- Please Like 👍 and Subscribe 📖 to never miss a video 🎥
- And to help me with the Algorithm 🤖
- And It's completely Free!!! 💵
- Love you guys ❤️