11- Implementing Secure Network Protocols

Ahmed Sultan
Senior Technical Instructor
ahmedsultan.me/about

Outlines

11.1- Implement Secure Network Operations

11.2- Implement Secure Application Protocols

11.3- Implement Secure Remote Access Protocols

Labs

Lab 16: Implementing Secure Network Addressing Services

Lab 17: Implementing a Virtual Private Network

Lab 18: Implementing a Secure SSH Server

© netriders.academy

11.1- Implement Secure Network Operations

11.2- Implement Secure Application Protocols

11.3- Implement Secure Remote Access Protocols

© netriders.academy

NETWORK ADDRESS ALLOCATION

- Most networks use a mixture of static and dynamic address allocation.
- Interface addresses for routers, firewalls, and some types of servers are best assigned and managed manually.
- Other server services and client workstations can be assigned dynamic IP configurations and accessed using name resolution.
- The Dynamic Host Configuration Protocol (DHCP) provides an automatic method for network address allocation.
- The key point about DHCP is that only one server should be offering addresses to any one group of hosts.

© netriders.academy

NETWORK ADDRESS ALLOCATION (cont.)

- If a **rogue DHCP** server is set up, it can perform DoS (as client machines will obtain an incorrect TCP/IP configuration) or be used to snoop network information.
- DHCP starvation is a type of DoS attack where a rogue client repeatedly requests new IP addresses using spoofed MAC addresses, with the aim of exhausting the IP address pool.
- This makes it more likely that clients seeking an address lease will use the rogue DHCP server.

© netriders.academy

NETWORK ADDRESS ALLOCATION (cont.)

- Enabling the DHCP snooping port security feature on a switch can mitigate rogue DHCP attacks.
- Windows DHCP servers in an AD environment automatically log any traffic detected from unauthorized DHCP servers.
- More generally, administration of the DHCP server itself must be carefully controlled and the settings checked regularly.
- If an attacker compromises the DHCP server, he or she could point network clients to rogue DNS servers and use that as a means to direct users to spoofed websites.
- Another attack is to redirect traffic through the attacker's machine by changing the default gateway, enabling the attacker to snoop on all network traffic.

© netriders.academy

DOMAIN NAME RESOLUTION

- The Domain Name System (DNS) resolves fully qualified domain names (FQDNs) to IP addresses.
- It uses a distributed database system that contains information on domains and hosts within those domains.
- The information is distributed among many name servers, each of which holds part of the database.
- The name servers work over port 53.
- Domain name resolution is a security-critical service and the target of many attacks on both local network and the Internet.

© netriders.academy

DOMAIN NAME RESOLUTION (cont.)

- DNS POISONING
  - ✓ DNS poisoning is an attack that compromises the process by which clients query name servers to locate the IP address for a FQDN.
- There are several ways that a DNS poisoning attack can be perpetrated.

1. Man in the Middle

- ✓ If the threat actor has access to the same local network as the victim, the attacker can use ARP poisoning to impersonate a legitimate DNS server and respond to DNS queries from the victim with spoofed replies.
- ✓ This might be combined with a denial of service attack on the victim's legitimate DNS server.
- ✓ A rogue DHCP could be used to configure clients with the address of a rogue DNS resolver.

DOMAIN NAME RESOLUTION (cont.)

2. DNS Client Cache Poisoning

- ✓ Before DNS was developed in the 1980s, name resolution took place using a text file named HOSTS.
- ✓ Each **name:IP** address mapping was recorded in this file and system administrators had to download the latest copy and install it on each Internet client or server manually.
- ✓ Even though all name resolution now functions through DNS, the HOSTS file is still present and most operating systems check the file before using DNS.
- ✓ Its contents are loaded into a cache of known **name:IP** mappings and the client only contacts a DNS server if the name is not cached.
- ✓ Therefore, if an attacker is able to place a false **name:IP** address mapping in the HOSTS file and effectively poison the DNS cache, he or she will be able to redirect traffic.
- ✓ The HOSTS file requires administrator access to modify.
- ✓ In UNIX and Linux systems it is stored as **/etc/hosts**, while in Windows it is placed in **%SystemRoot%\System32\Drivers\etc\hosts**.

© netriders.academy

DOMAIN NAME RESOLUTION (cont.)

3. DNS Server Cache Poisoning

- ✓ DNS server cache poisoning aims to corrupt the records held by the DNS server itself.
- ✓ This can be accomplished by performing DoS against the server that holds the authorized records for the domain, and then spoofing replies to requests from other name servers.

DNS SECURITY

- DNS Security Extensions (DNSSEC)
  - ✓ Help to mitigate against spoofing and poisoning attacks by providing a validation process for DNS responses.
  - ✓ With DNSSEC enabled, the authoritative server for the zone creates a "package" of resource records signed with a private key (the Zone Signing Key).
  - ✓ When another server requests a secure record exchange, the authoritative server returns the package along with its public key, which can be used to verify the signature.
  - ✓ The public zone signing key is itself signed with a separate Key Signing Key.
  - ✓ Separate keys are used so that if there is some sort of compromise of the zone signing key, the domain can continue to operate securely by revoking the compromised key and issuing a new one.

© netriders.academy

Lab

Lab 16: Implementing Secure Network Addressing Services

© netriders.academy

11.1- Implement Secure Network Operations

11.2- Implement Secure Application Protocols

11.3- Implement Secure Remote Access Protocols

HYPERTEXT TRANSFER PROTOCOL (HTTP)

- The foundation of web technology is the Hyper Text Transfer Protocol (HTTP).
- HTTP enables clients (typically web browsers) to request resources from an HTTP server.
- A client connects to the HTTP server using an appropriate TCP port (the default is port 80) and submits a request for a resource, using a uniform resource locator (URL).
- The server acknowledges the request and responds with the data (or an error message).
- The response and request payload formats are defined in an HTTP header.
- The HTTP payload is usually used to serve HTML web pages, which are plaintext files with coded tags (Hyper Text Markup Language) describing how the page should be formatted.
- A web browser can interpret the tags and display the text and other resources associated with the page, such as binary picture or sound files linked to the HTML page.

© netriders.academy

TRANSPORT LAYER SECURITY

- As with other early TCP/IP application protocols, HTTP communications are not secured.
- Secure Sockets Layer (SSL) was developed by Netscape in the 1990s to address the lack of security in HTTP.
- SSL proved very popular with the industry, and it was quickly adopted as a standard named Transport Layer Security (TLS).
- It is typically used with HTTP (referred to as HTTPS or HTTP Secure) but can also be used to secure other application protocols and as a virtual private networking (VPN) solution.

TRANSPORT LAYER SECURITY (cont.)

- To implement TLS, a server is assigned a digital certificate signed by some trusted **certificate authority (CA)**.
- The certificate proves the identity of the server (assuming that the client trusts the CA) and validates the server's public/private key pair.
- The server uses its key pair and the TLS protocol to agree mutually supported ciphers with the client and negotiate an encrypted communications session.

- *HTTPS operates over port 443 by default.*
- *HTTPS operation is indicated by using https:// for the URL and by a padlock icon shown in the browser.*

© netriders.academy

FILE TRANSFER SERVICES

- A File Transfer Protocol (FTP) server is typically configured with several public directories, hosting files, and user accounts.
- Most HTTP servers also function as FTP servers, and FTP services, accounts, and directories may be installed and enabled by default when you install a web server.
- FTP is more efficient compared to file attachments or HTTP file transfer, but has no security mechanisms.
- All authentication and data transfer are communicated as **plaintext**, meaning that credentials can easily be picked out of any intercepted FTP traffic.

© netriders.academy

FILE TRANSFER SERVICES (cont.)

- SSH FTP (SFTP) addresses the privacy and integrity issues of FTP by encrypting the authentication and data transfer between client and server.
- In SFTP, a secure link is created between the client and server using **Secure Shell (SSH)** over TCP port 22.
- Ordinary FTP commands and data transfer can then be sent over the secure link without risk of eavesdropping or man-in-the-middle attacks.
- This solution requires an SSH server that supports SFTP and SFTP client software.

© netriders.academy

11.1- Implement Secure Network Operations

11.2- Implement Secure Application Protocols

11.3- Implement Secure Remote Access Protocols

REMOTE ACCESS ARCHITECTURE

- Remote access means that the user's device does not make a direct cabled or wireless connection to the network.
- The connection occurs over or through an intermediate network.
- Historically, remote access might have used analog modems connecting over the telephone system or possibly a private link (a leased line).
- These days, most remote access is implemented as a virtual private network (VPN), running over the Internet.
- Administering remote access involves essentially the same tasks as administering the local network.

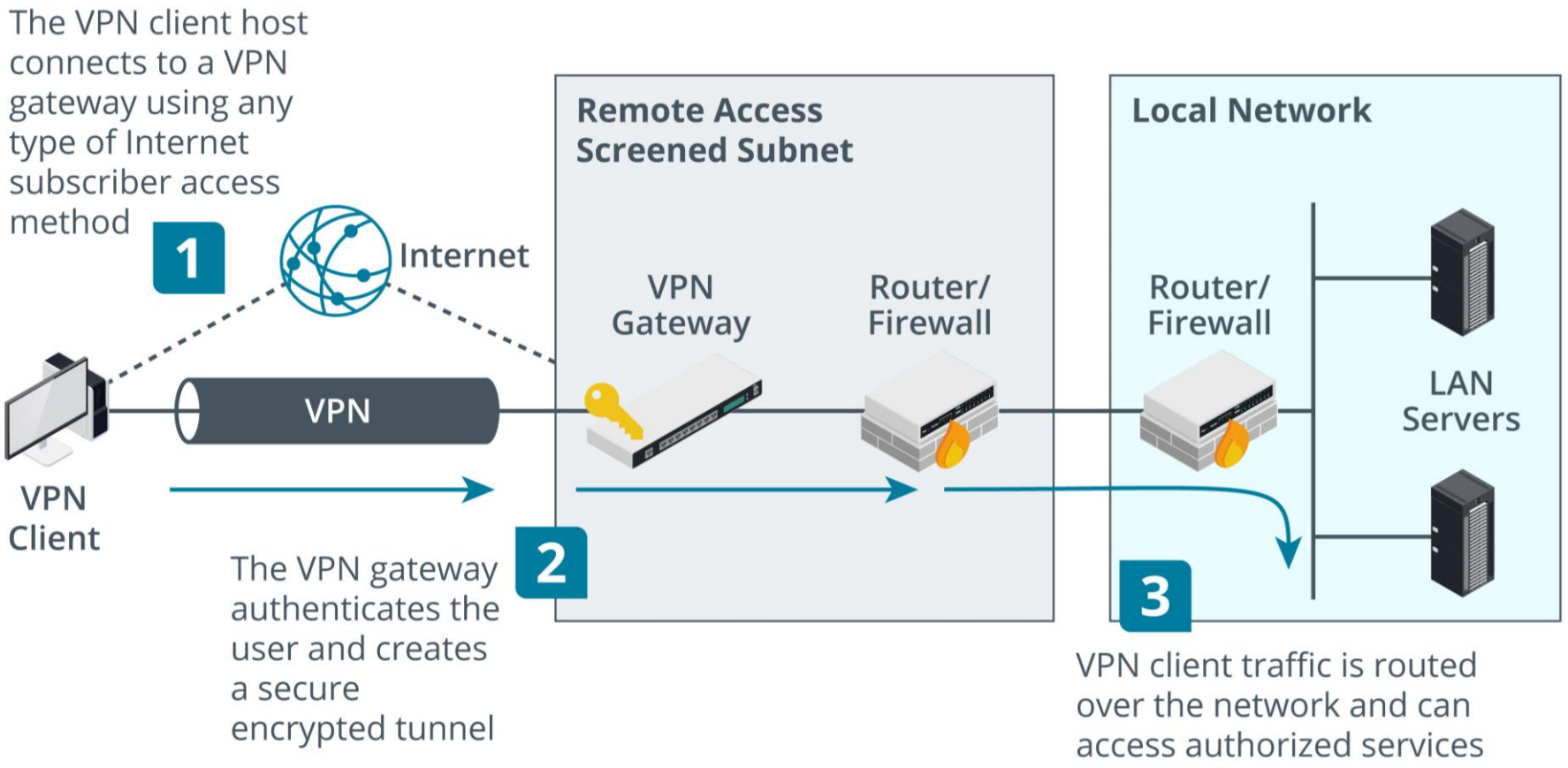
© netriders.academy

REMOTE ACCESS ARCHITECTURE (cont.)

- Only authorized users should be allowed access to local network resources and communication channels.
- Additional complexity comes about because it can be more difficult to ensure the security of remote workstations and servers and there is greater opportunity for remote logins to be exploited.
- With a remote access VPN, clients connect to a VPN gateway on the edge of the private network.

© netriders.academy

REMOTE ACCESS ARCHITECTURE (cont.)

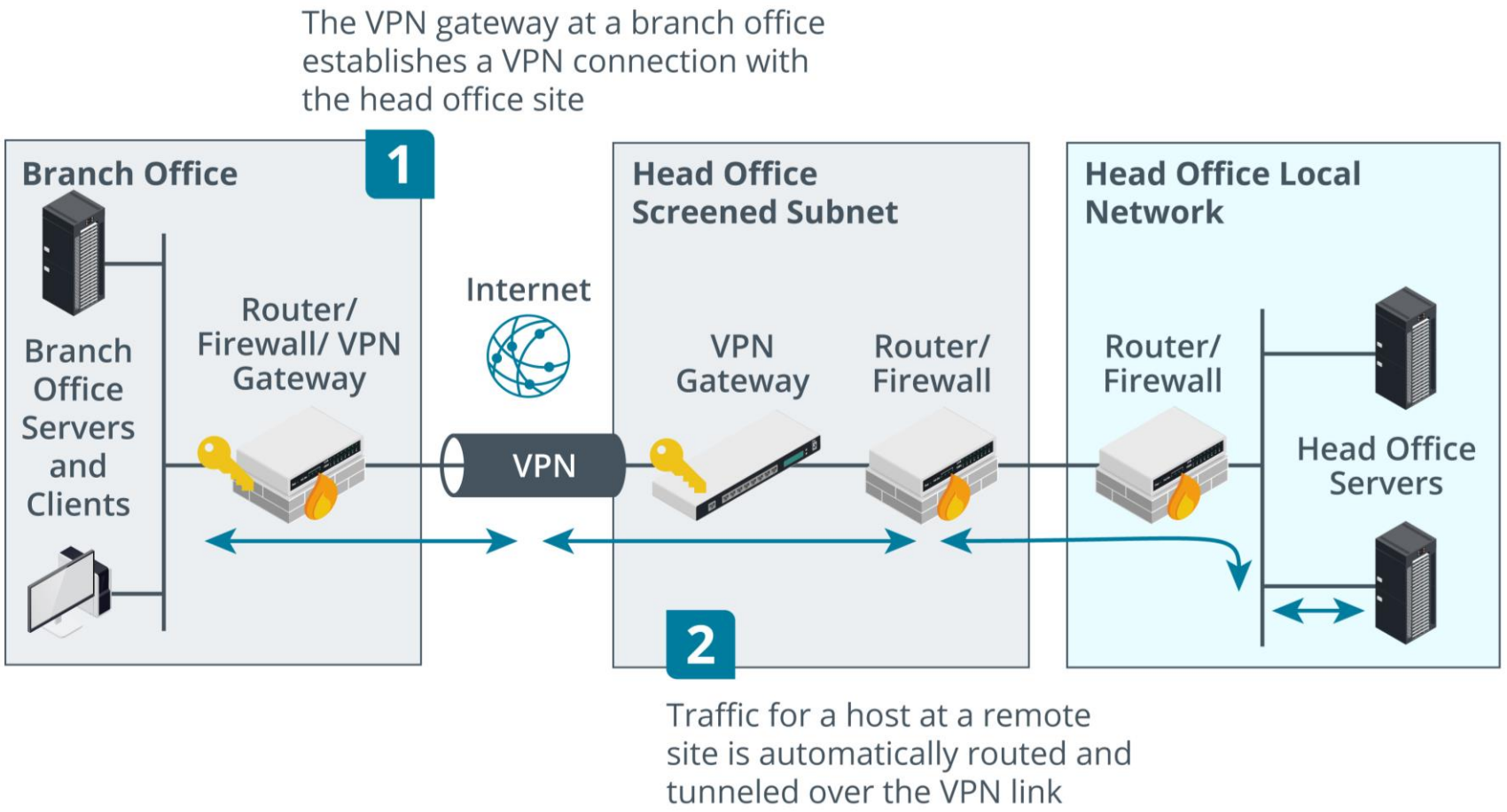


© netriders.academy

REMOTE ACCESS ARCHITECTURE (cont.)

- A VPN can also be deployed in a **site-to-site** model to connect two or more private networks.
- Where remote access VPN connections are typically initiated by the client, a site-to-site VPN is configured to operate automatically.
- The gateways exchange security information using whichever protocol the VPN is based on.
- This establishes a trust relationship between the gateways and sets up a secure connection through which to tunnel data.
- Hosts at each site do not need to be configured with any information about the VPN.
- The routing infrastructure at each site determines whether to deliver traffic locally or send it over the VPN tunnel.

REMOTE ACCESS ARCHITECTURE (cont.)



© netriders.academy

REMOTE DESKTOP

- Another model for remote networking involves connecting to a host within the local network over a remote administration protocol.
- A protocol such as Secure Shell (SSH) traditionally provides terminal access, and there are many tools that can connect to a graphical desktop.
- A GUI remote administration tool sends screen and audio data from the remote host to the client and transfers mouse and keyboard input from the client to the remote host.
- Microsoft's Remote Desktop Protocol (RDP) can be used to access a physical machine on a one-to-one basis.

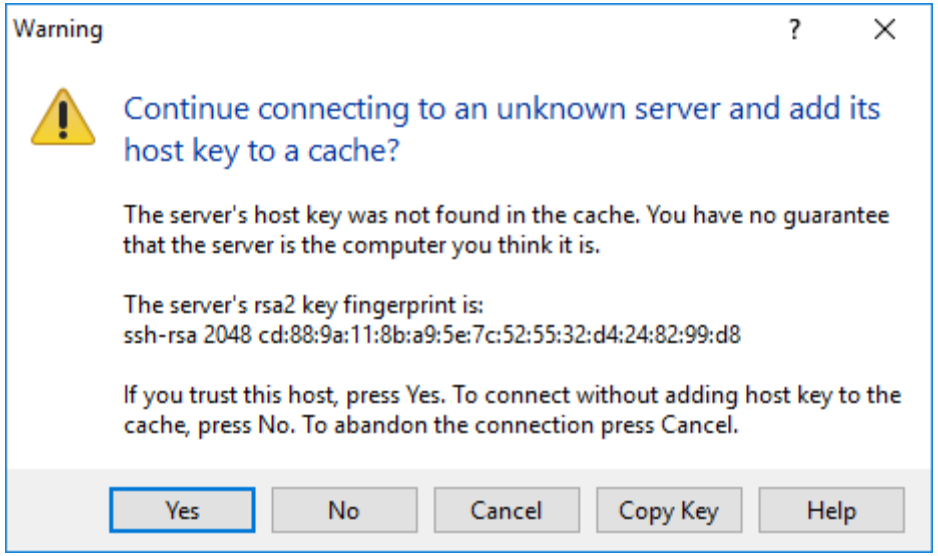
© netriders.academy

SECURE SHELL

- Secure Shell (SSH) is the principal means of obtaining secure remote access to a command line terminal.
- The main uses of SSH are for remote administration and secure file transfer (SFTP).
- There are numerous commercial and open source SSH products available for all the major network operating system (NOS) platforms.
- The most widely used is OpenSSH (openssh.com).
- SSH servers are identified by a public/private key pair (the host key).
- A mapping of host names to public keys can be kept manually by each SSH client or there are various enterprise software products designed for SSH host key management.

© netriders.academy

SECURE SHELL



Lab

Lab 17: Implementing a Virtual Private Network

Lab 18: Implementing a Secure SSH Server