

16 Network Security Fundamentals

16.1 Security Threats and Vulnerabilities

- Types of Threats
 - Information theft
 - Data loss and manipulation
 - Identity theft
 - Disruption of service
- Types of Vulnerabilities
 - Technological Vulnerabilities
 - Configuration Vulnerabilities
 - Configuration Vulnerabilities
- Physical Security
 - Hardware threats
 - Environmental threats
 - Electrical threats
 - Maintenance threats

16.2 Network Attacks

- Types of Malware
 - Viruses (needs host)
 - Worms (standalone)
 - Trojan Horses
- Reconnaissance Attacks
 - Internet Queries
 - Ping Sweeps
 - Port Scans
- Access Attacks
 - Password Attacks
 - Trust Exploitation
 - Port Redirection
 - Man-in-the-Middle
- Denial of Service Attacks
 - DoS Attack
 - DDoS Attack

16.3 Network Attack Mitigation

- The Defense-in-Depth Approach
 - VPN
 - ASA Firewall
 - IPS
 - ESA (E-Mail Security appliance) / WSA (Web Security Appliance)
 - AAA Server
- Keep Backups
 - Frequency
 - Validation
 - Storage
 - Security
- Upgrade, Update, and Patch
- Authentication, Authorization, and Accounting
- Firewalls
 - DMZ
- Types of Firewalls
 - Packet filtering
 - Application filtering
 - URL filtering
 - Stateful packet inspection (SPI)
- Endpoint Security

16.4 Device Security

- Cisco AutoSecure: Router# auto secure
- Passwords
- Additional Password Security

```
R1(config)# service password-encryption
R1(config)# security passwords min-length 8
R1(config)# login block-for 120 attempts 3 within 60
R1(config)# line vty 0 4
R1(config-line)# password cisco123
R1(config-line)# exec-timeout 5 30
R1(config-line)# transport input ssh
R1(config-line)# end
```

- Enable SSH

```
Router(config)# hostname R1
R1(config)# ip domain name span.com
R1(config)# crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.span.com % The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Dec 13 16:19:12.079: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#
R1(config)# username Bob secret cisco
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
```

- Disable Unused Services

```
Router# show ip ports all
Router# show control-plane host open-ports
```