Instructor Materials Chapter 7: Protecting a Cybersecurity Domain

Cybersecurity Essentials v1.1

Cisco | Networking Academy®
Mind Wide Open™

Chapter 7: Protecting a Cybersecurity Domain

Cybersecurity Essentials v1.1

Cisco | Networking Academy®
Mind Wide Open™

Chapter 7 - Sections & Objectives

7.1 Defending Systems and Devices

Describe how cybersecurity domains are used within the CIA triad.

Explain how technologies, processes and procedures protect systems.

7.2 Server Hardening

Explain how to protect servers on a network.

7.3 Network Hardening

Explain how to implement security measures to protect network devices.

7.4 Physical Security

Explain how physical security measures are implemented to protect network equipment.

7.1 Defending Systems and Devices

Cisco | Networking Academy®
Mind Wide Open™

Defending Systems and Devices

Host Hardening

Operating System Security - The operating system plays a critical role in the operation of a computer system and is the target of many attacks.

- An administrator hardens an operating system by modifying the default configuration to make it more secure to outside threats.
- This process includes the removal of unnecessary programs and services.
- Another critical requirement of hardening operating systems is the application of security patches and updates.

Antimalware - Malware includes viruses, worms, Trojan horses, keyloggers, spyware, and adware.

- They all invade privacy, steal information, damage the system, or delete and corrupt data.
- It is important to protect computers and mobile devices using reputable antimalware software.

Defending Systems and Devices

Host Hardening (Cont.)

Patch Management - Patches are code updates that manufacturers provide to prevent a newly discovered virus or worm from making a successful attack. Manufacturers combine patches and upgrades into a comprehensive update application called a service pack.

Host-based Firewalls - A software firewall is a program that runs on a computer to allow or deny traffic between the computer and other connected computers. The software firewall applies a set of rules to data transmissions through inspection and filtering of data packets.

Host Intrusion Detection Systems - A host intrusion detection system (HIDS) is software that runs on a host computer that monitors suspicious activity.

Secure Communications (VPNs) - When connecting to the local network and sharing files, the communication between computers remains within that network. To communicate and share resources over a network that is not secure, users employ a Virtual Private Network (VPN). A VPN is a private network that connects remote sites or users together over a public network, like the Internet.

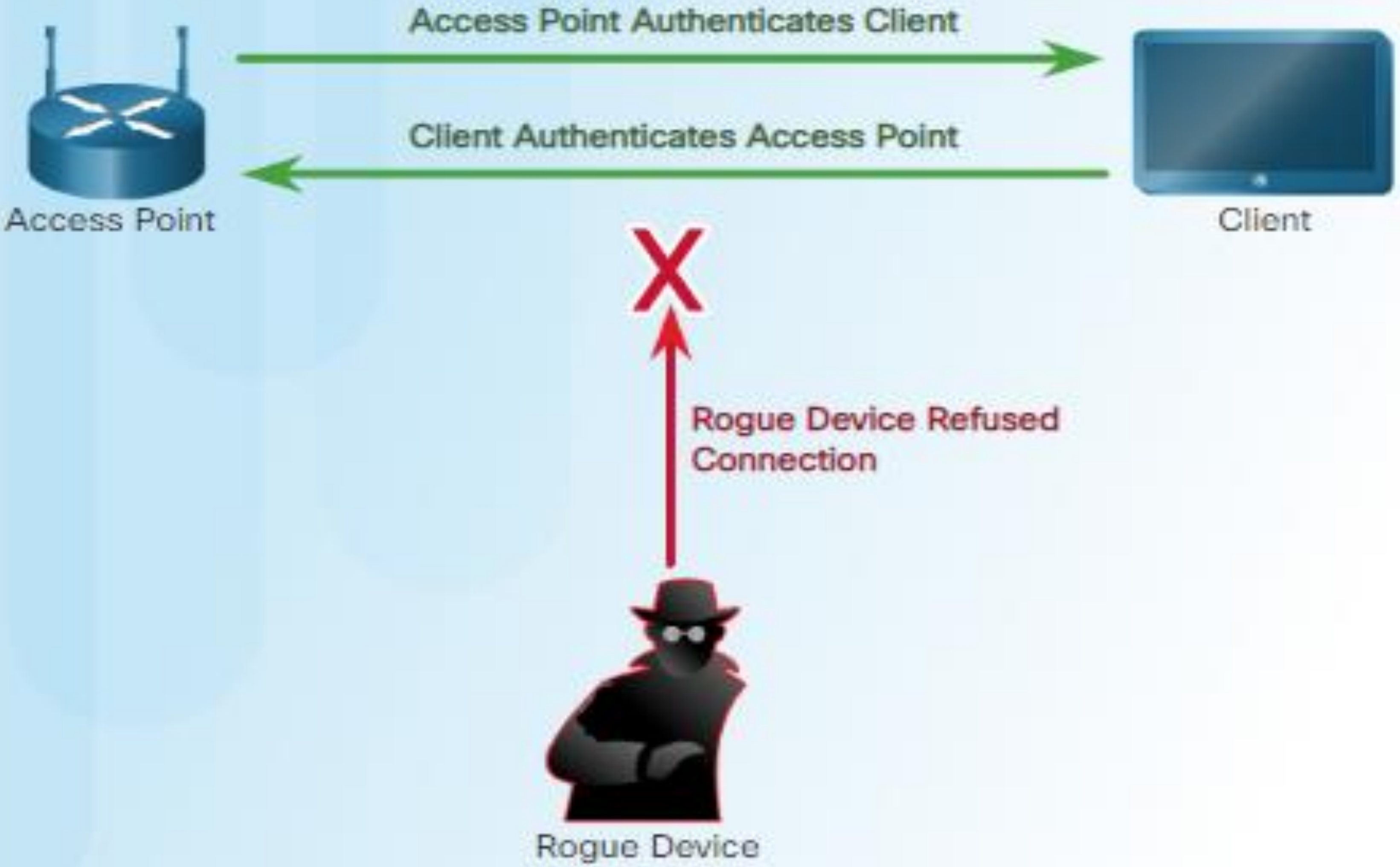
Defending Systems and Devices

Hardening Wireless and Mobile Devices

Wired Equivalent Privacy (WEP) - One of the most important components of modern computing are mobile devices. The majority of devices found on today’s networks are laptops, tablets, smart phones and other wireless devices. WEP is one of the first widely used Wi-Fi security standards. The WEP standard provides authentication and encryption protections.

WPA/WPA2 - The next major improvement to wireless security was the introduction of WPA and WPA2. Wi-Fi Protected Access (WPA) was the computer industry’s response to the weakness of the WEP standard. The WPA standard provided several security improvements.

Mutual Authentication - The imposter can launch a man-in-the-middle attack which is very difficult to detect and can result in stolen login credentials and transmitted data. To prevent rogue access points, the computer industry developed mutual authentication. Mutual authentication, also called two-way authentication, is a process or technology in which both entities in a communications link authenticate to each other.


Access Point Authenticates Client
Client Authenticates Access Point
Access Point
Client
Rogue Device Refused Connection
Rogue Device

Defending Systems and Devices

Host Data Protection

File Access Control – This consists of permissions that limit folder or file access for an individual or for a group of users.

File Encryption – File encryption is a tool used to protect data stored in the form of files. Encryption transforms data using a complicated algorithm to make it unreadable. Software programs can encrypt files, folders, and even entire drives.

System and Data Backups - A data backup stores a copy of the information from a computer to removable backup media. Backing up data is one of the most effective ways of protecting against data loss. If the computer hardware fails, the user can restore the data from the backup after the system is again functional.

Defending Systems and Devices

Images and Content Control

Content Screening and Blocking

Content control software restricts the content that a user can access with a web browser over the Internet.

Content control software can block sites that contain certain types of material such as pornography or controversial religious or political content.

Disk Cloning and Deep Freeze

- Many third-party applications are available to restore a system back to a default state. This allows the administrator to protect the operating system and configuration files for a system.
- Disk cloning copies the contents of the computer’s hard disk to an image file.
- Deep Freeze “freezes” the hard drive partition. When a user restarts the system, the system reverts to its frozen configuration. The system does not save any changes that the user makes, so any applications installed or files saved are lost when the system restarts.

Defending Systems and Devices

Physical Protection and Workstations

Security Cables and Locks - There are several methods of physically protecting computer equipment:

- Use cable locks
- Keep telecommunication rooms locked.
- Use security cages around equipment.

Logout Timers - An employee gets up and leaves his computer to take a break. If the employee does not take any action to secure his workstation, any information on that system is vulnerable to an unauthorized user.

Idle Timeout and Screen Lock - Employees may or may not log out of their computer when they leave the workplace. Therefore, it is a security best practice to configure an idle timer that will automatically log the user out and lock the screen.

Login Times - In some situations, an organization may want employees to log in during specific hours, such as 7 a.m. to 6 p.m. The system blocks logins during the hours that fall outside of the allowed login hours.

Defending Systems and Devices

Physical Protection and Workstations

GPS Tracking – uses satellites and computers to determine the location of a device. GPS technology is a standard feature on smartphones that provides real-time position tracking. GPS tracking can pinpoint a location within 100 meters.

Inventory and RFID Tags - Radio frequency identification (RFID) uses radio waves to identify and track objects. RFID inventory systems use tags attached to all items that an organization wants to track.

7.2 Server Hardening

Cisco | Networking Academy®
Mind Wide Open™

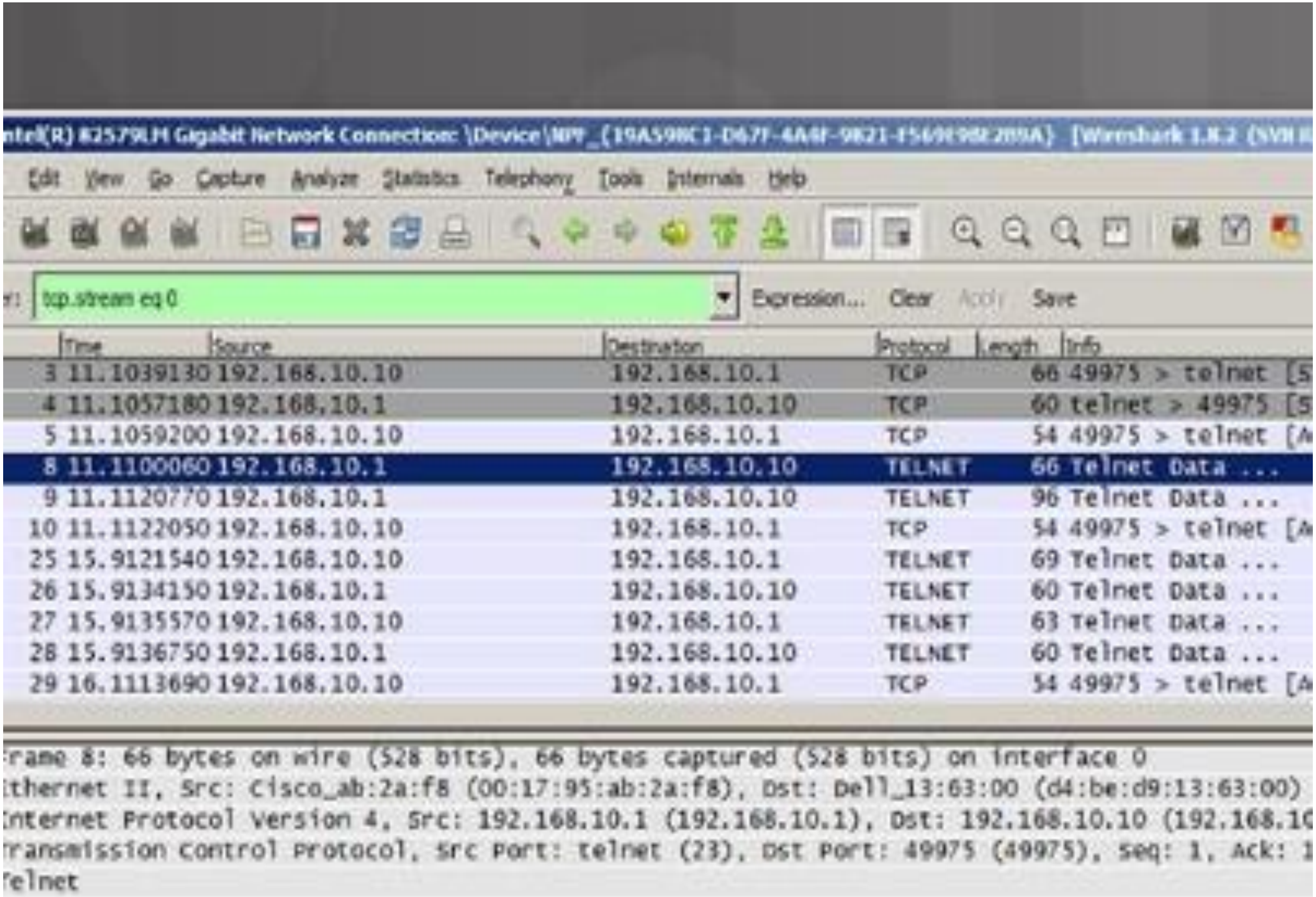
Server Hardening

Secure Remote Access

Managing Remote Access - Remote access refers to any combination of hardware and software that enables users to access a local internal network remotely.

Telnet, SSH, and SCP - Secure Shell (SSH) is a protocol that provides a secure (encrypted) management connection to a remote device.

- **SSH** should replace Telnet for management connections.
- **Telnet** is an older protocol that uses unsecure plaintext transmission of both the login authentication (username and password) and the data transmitted between the communicating devices.
- **Secure copy (SCP)** securely transfers computer files between two remote systems. SCP uses SSH for data transfer (including the authentication element), so SCP ensures the authenticity and confidentiality of the data in transit.



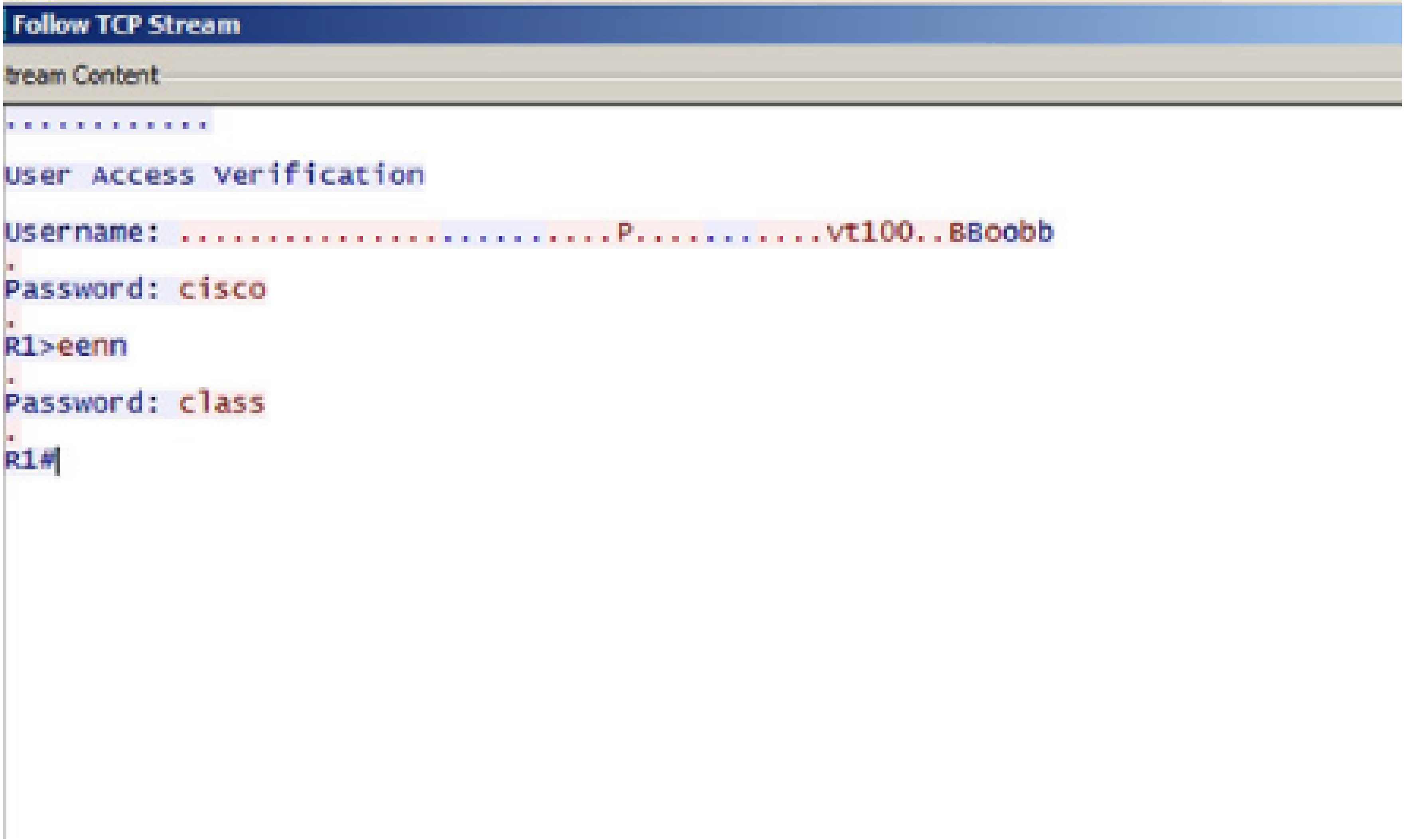
ntel(R) 82579LM Gigabit Network Connection: \Device\NPF_{19A598C1-D67F-4A4F-9821-F569E98E2B9A} [Wireshark 1.8.2 (SVN R

tcp.stream eq 0

```
    Time       Source          Destination     Protocol Length Info
  3 11.1039130 192.168.10.10   192.168.10.1    TCP        66 49975 > telnet [S
  4 11.1057180 192.168.10.1    192.168.10.10   TCP        60 telnet > 49975 [S
  5 11.1059200 192.168.10.10   192.168.10.1    TCP        54 49975 > telnet [A
  8 11.1100060 192.168.10.1    192.168.10.10   TELNET     66 Telnet Data ...
  9 11.1120770 192.168.10.1    192.168.10.10   TELNET     96 Telnet Data ...
 10 11.1122050 192.168.10.10   192.168.10.1    TCP        54 49975 > telnet [A
 25 15.9121540 192.168.10.10   192.168.10.1    TELNET     69 Telnet Data ...
 26 15.9134150 192.168.10.1    192.168.10.10   TELNET     60 Telnet Data ...
 27 15.9135570 192.168.10.10   192.168.10.1    TELNET     63 Telnet Data ...
 28 15.9136750 192.168.10.1    192.168.10.10   TELNET     60 Telnet Data ...
 29 16.1113690 192.168.10.10   192.168.10.1    TCP        54 49975 > telnet [A
```

```
rame 8: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
thernet II, Src: Cisco_ab:2a:f8 (00:17:95:ab:2a:f8), Dst: Dell_13:63:00 (d4:be:d9:13:63:00)
nternet Protocol Version 4, Src: 192.168.10.1 (192.168.10.1), Dst: 192.168.10.10 (192.168.10
ransmission Control Protocol, Src Port: telnet (23), Dst Port: 49975 (49975), Seq: 1, Ack: 1
elnet
```

Plaintext Username and Password Captured

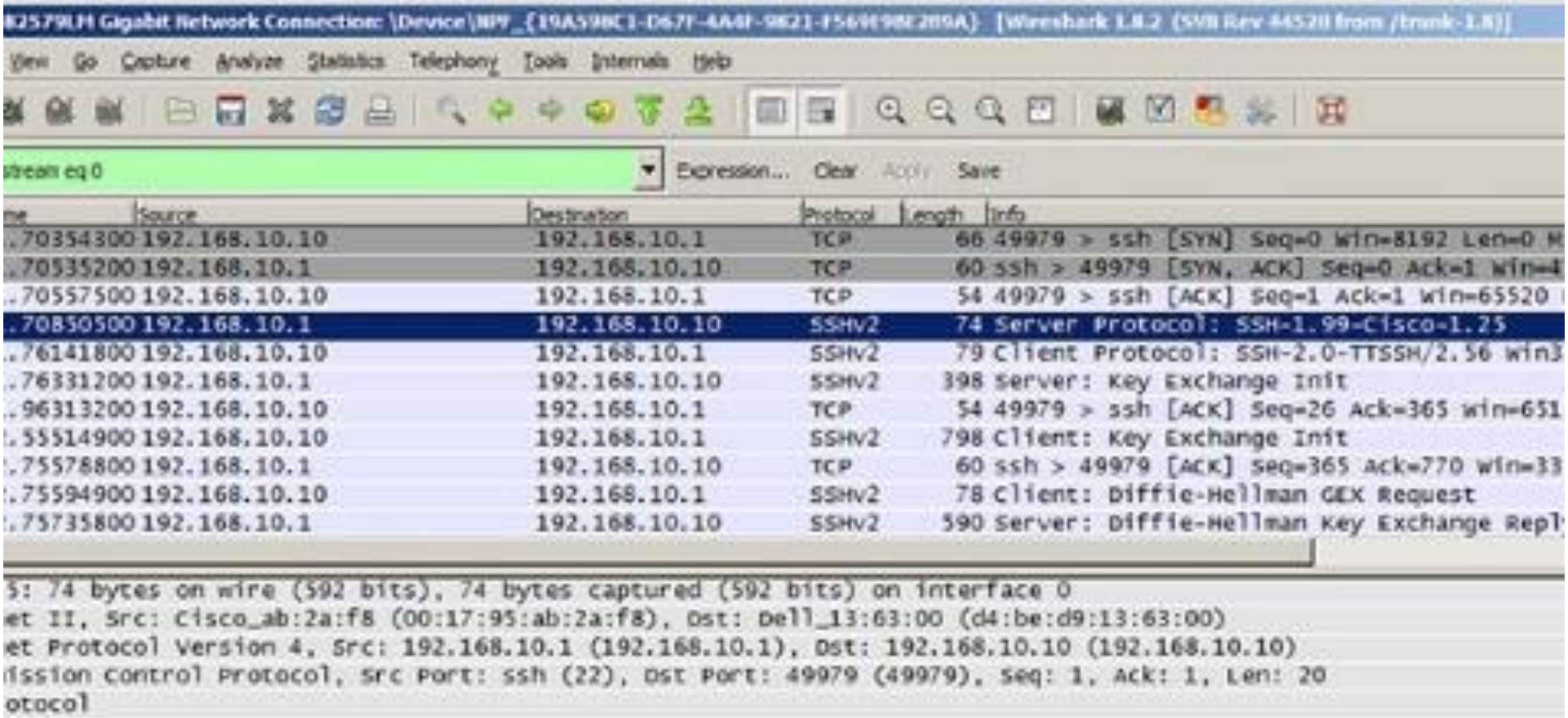


```
............

User Access Verification

Username: .........................P...........vt100..BBoobb
.
Password: cisco
.
R1>eenn
.
Password: class
.
R1#
```

Wireshark SSH Capture

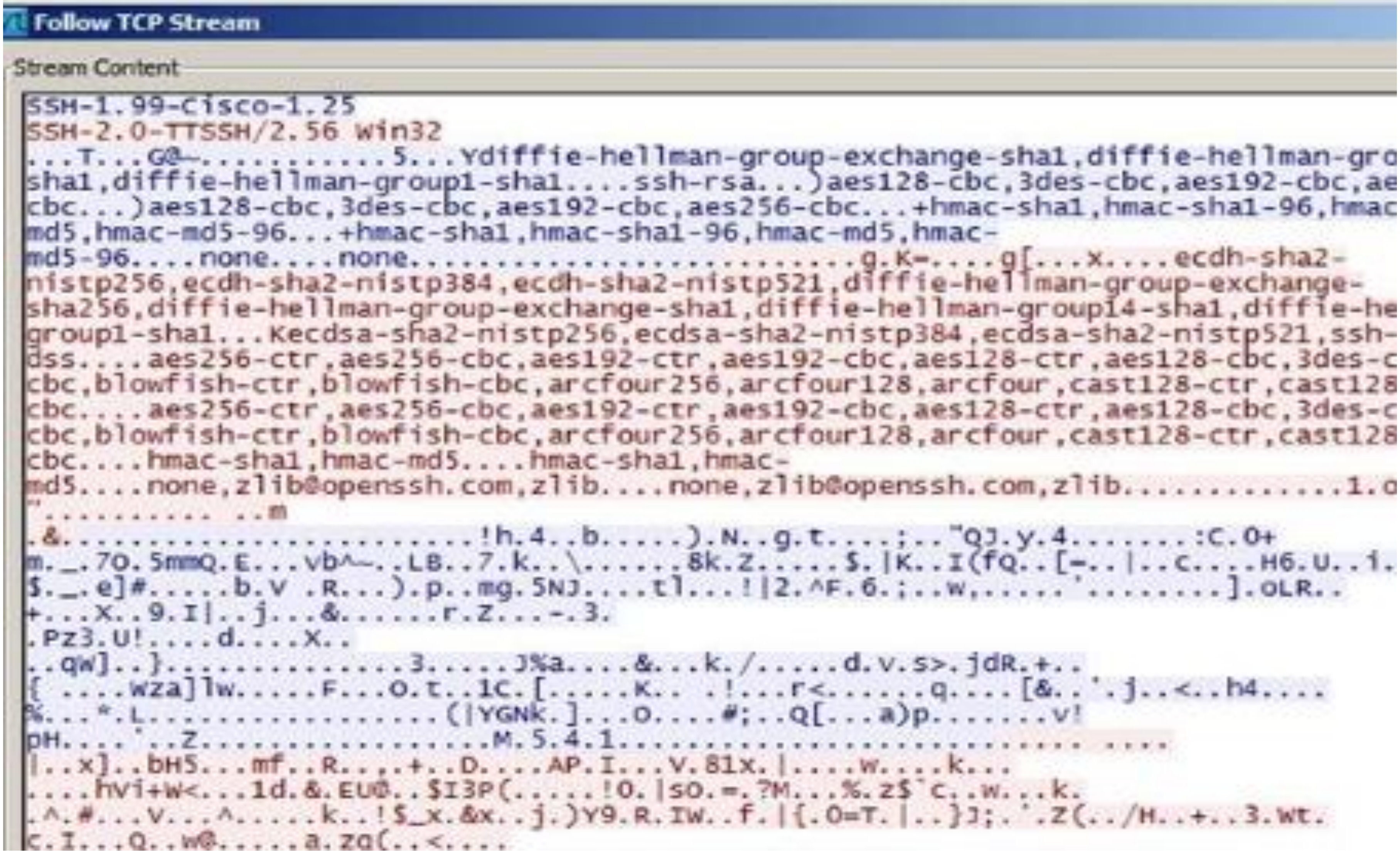

82579LM Gigabit Network Connection: \Device\NPF_{19A598C1-D67F-4A4F-9821-F569E98E2B9A} [Wireshark 1.8.2 (SVN Rev 44520 from /trunk-1.8)]
View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

stream eq 0

```
me          Source             Destination          Protocol Length Info
.70354300 192.168.10.10      192.168.10.1         TCP        66 49979 > ssh [SYN] Seq=0 Win=8192 Len=0 M
.70535200 192.168.10.1       192.168.10.10        TCP        60 ssh > 49979 [SYN, ACK] Seq=0 Ack=1 Win=4
.70557500 192.168.10.10      192.168.10.1         TCP        54 49979 > ssh [ACK] Seq=1 Ack=1 Win=65520
.70850500 192.168.10.1       192.168.10.10        SSHv2      74 Server Protocol: SSH-1.99-Cisco-1.25
.76141800 192.168.10.10      192.168.10.1         SSHv2      79 Client Protocol: SSH-2.0-TTSSH/2.56 Win3
.76331200 192.168.10.1       192.168.10.10        SSHv2     398 Server: Key Exchange Init
.96313200 192.168.10.10      192.168.10.1         TCP        54 49979 > ssh [ACK] Seq=26 Ack=365 Win=651
.55514900 192.168.10.10      192.168.10.1         SSHv2     798 Client: Key Exchange Init
.75578800 192.168.10.1       192.168.10.10        TCP        60 ssh > 49979 [ACK] Seq=365 Ack=770 Win=33
.75594900 192.168.10.10      192.168.10.1         SSHv2      78 Client: Diffie-Hellman GEX Request
.75735800 192.168.10.1       192.168.10.10        SSHv2     590 Server: Diffie-Hellman Key Exchange Repl
```

```
5: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
et II, Src: Cisco_ab:2a:f8 (00:17:95:ab:2a:f8), Dst: Dell_13:63:00 (d4:be:d9:13:63:00)
et Protocol Version 4, Src: 192.168.10.1 (192.168.10.1), Dst: 192.168.10.10 (192.168.10.10)
ission Control Protocol, Src Port: ssh (22), Dst Port: 49979 (49979), Seq: 1, Ack: 1, Len: 20
otocol
```

Username and Password Encrypted



```
SSH-1.99-Cisco-1.25
SSH-2.0-TTSSH/2.56 Win32
...T...G@~..............5...Ydiffie-hellman-group-exchange-sha1,diffie-hellman-gro
sha1,diffie-hellman-group1-sha1....ssh-rsa...)aes128-cbc,3des-cbc,aes192-cbc,ae
cbc...)aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc...+hmac-sha1,hmac-sha1-96,hmac
md5,hmac-md5-96...+hmac-sha1,hmac-sha1-96,hmac-md5,hmac-
md5-96....none....none.........................g.K=....g[...x....ecdh-sha2-
nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-
sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-he
group1-sha1...Kecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ssh-
dss....aes256-ctr,aes256-cbc,aes192-ctr,aes192-cbc,aes128-ctr,aes128-cbc,3des-c
cbc,blowfish-ctr,blowfish-cbc,arcfour256,arcfour128,arcfour,cast128-ctr,cast128
cbc....aes256-ctr,aes256-cbc,aes192-ctr,aes192-cbc,aes128-ctr,aes128-cbc,3des-c
cbc,blowfish-ctr,blowfish-cbc,arcfour256,arcfour128,arcfour,cast128-ctr,cast128
cbc....hmac-sha1,hmac-md5....hmac-sha1,hmac-
md5....none,zlib@openssh.com,zlib....none,zlib@openssh.com,zlib..............1.o
"
.......... ..m
.&.........................!h.4..b.....).N..g.t....;.."QJ.y.4........:C.O+
m._.7O.5mmQ.E...vb^~..LB..7.k..\......8k.Z.....$.|K..I(fQ..[-..|..C....H6.U..i.
$._.e]#.....b.V .R...).p..mg.5NJ....tl...!|2.^F.6.;..w,..... .........].OLR..
+...X..9.I|..j...&.......r.Z...-.3.
.Pz3.U!....d....X..
..qw]..}...............3.....J%a....&...k./.....d.v.s>.jdR.+..
{ ....wza]lw.....F...O.t..1C.[.....K..  .!...r<......q....[&..'.j..<..h4....
%...*.L....................(|YGNk.]...O....#;..Q[...a)p.......v!
pH....'..Z...................M.5.4.1............................... ....
|..x]..bH5...mf..R...,.+..D....AP.I...V.81x.|.....w....k...
....hvi+w<...1d.&.EU@..$I3P(......!O.|sO.=.?M...%.z$`c..w...k.
.^.#...V...^.....k..!$_x.&x..j.)Y9.R.IW..f.|{.O=T.|..}J;.'.Z(../H..+..3.Wt.
c.I...Q..w@.....a.zq(..<....
```

Server Hardening
Administrative Measures

Securing Ports and Services - Cyber criminals exploit the services running on a system because they know that most devices run more services or programs than they need. An administrator should look at every service to verify its necessity and evaluate its risk. Remove any unnecessary services.

Privileged Accounts - Cyber criminals exploit privileged accounts because they are the most powerful accounts in the organization. Privileged accounts have the credentials to gain access to systems and they provide elevated, unrestricted access. Administrators use these accounts to deploy and manage operating systems, applications, and network devices. These account should be secured or removed to mitigate these risks.

Group Policies - In most networks that use Windows computers, an administrator configures Active Directory with Domains on a Windows Server. An administrator configures user account policies such as password policies and lockout policies by adding users to groups and setting policy at a group level.

Enable Logs and Alerts - A log records events as they occur on a system. Log entries make up a log file, and a log entry contains all of the information related to a specific event. Logs that relate to computer security have grown in importance.

Server Hardening

Physical Protection of Server

Power - A critical issue in protecting information systems is electrical power systems and power considerations. A continuous supply of electrical power is critical in today's massive server and data storage facilities.

Heating, Ventilation, and Air Conditioning (HVAC) - HVAC systems are critical to the safety of people and information systems in the organization's facilities. When designing modern IT facilities, these systems play a very important role in the overall security. HVAC systems control the ambient environment (temperature, humidity, airflow, and air filtering) and must be planned for and operated along with other data center components such as computing hardware, cabling, data storage, fire protection, physical security systems and power.

Hardware Monitoring - Hardware monitoring is often found in large server farms. A server farm is a facility that houses hundreds or thousands of servers for companies.

7.3 Network Hardening

Cisco | Networking Academy®
Mind Wide Open™

Network Hardening

Securing Network Devices

Operation Centers - The Network Operation Center (NOC) is one or more locations containing the tools that provide administrators with a detailed status of the organization’s network. The NOC is ground zero for network troubleshooting, performance monitoring, software distribution and updates, communications management, and device management.

Switches, Routers, and Network Appliances - Network devices ship with either no passwords or default passwords.

- **Network switches** are the heart of the modern data communication network. The main threat to network switches are theft, hacking and remote access, attacks against network protocols like ARP/STP or attacks against performance and availability.
- **VLANs -** provide a way to group devices within a LAN and on individual switches. VLANs use logical connections instead of physical connections.

Network Hardening

Securing Network Devices (Cont.)

- **Firewalls -** are hardware or software solutions that enforce network security policies. A firewall filters unauthorized or potentially dangerous traffic from entering the network.
- **Routers -** Routers form the backbone of the Internet and communications between different networks. Routers communicate with one another to identify the best possible path to deliver traffic to different networks. Routers use routing protocols to make routing decision.
- **Wireless and Mobile Devices** - Wireless and mobile devices have become the predominant type of devices on most modern networks. They provide mobility and convenience but pose a host of vulnerabilities. These vulnerabilities include theft, hacking and unauthorized remote access, sniffing, man-in-the-middle attacks, and attacks against performance and availability.
- **Network and Routing Services** - Cyber criminals use vulnerable network services to attack a device or to use it as part of the attack. Securing network services ensures that only necessary ports are exposed and available. Network services include; DHCP, DNS, ICMP, Routing Services (RIP-OSPF-ISS), NTP and others.

Network Hardening

Voice and Video Equipment

VoIP Equipment - uses networks such as the Internet to make and receive phone calls. The equipment required for VoIP includes an Internet connection plus a phone.

Cameras - An Internet camera sends and receives data over a LAN and/or the Internet. A user can remotely view live video using a web browser on a wide range of devices including computer systems, laptops, tablets, and smartphones. Cameras come in various forms including the traditional security camera.

Videoconferencing Equipment - allows two or more locations to communicate simultaneously using telecommunication technologies. These technologies take advantage of the new high definition video standards. Videoconferencing is now part of normal day-to-day operations in industries like the medical field.

Network and IoT Sensors - One of the fastest sectors of information technology is the use of intelligent devices and sensors. The computer industry brands this sector as the Internet of Things (IoT). Businesses and consumers use IoT devices to automate processes, monitor environmental conditions, and alert the user of adverse conditions.

7.4 Physical Security

Cisco | Networking Academy®
Mind Wide Open™

Physical Security

Physical Access Control

Fencing and Barricades - Physical barriers are the first thing that comes to mind when thinking about physical security. This is the outermost layer of security, and these solutions are the most publicly visible. A perimeter security system typically consists of perimeter fence system, security gate system, bollards, vehicle entry barriers and guard shelters.

Biometrics - are the automated methods of recognizing an individual based on a physiological or behavioral characteristic. Biometric authentication systems include measurements of the face, fingerprint, hand geometry, iris, retina, signature, and voice. Biometric technologies can be the foundation of highly secure identification and personal verification solutions.

Badges and Access Logs – A badge allows an individual to gain access to an area with automated entry points. An entry point can be a door, a turnstile, a gate, or other barrier. Access badges use various technologies such as a magnetic stripe, barcode, or biometrics. The system logs the transaction for later retrieval. Reports reveal who entered what entry points at what time.

Physical Security

Surveillance

Guards and Escorts - All physical access controls including deterrent and detection systems ultimately rely on personnel to intervene and stop the actual attack or intrusion. In highly secure information system facilities, guards control access to the organization’s sensitive areas.

Video and Electronic Surveillance – This type of surveillance can supplement or in some cases, replace security guards. The benefit of video and electronic surveillance is the ability to monitor areas even when no guards or personnel are present, the ability to record and log surveillance videos and data for long periods, and the ability to incorporate motion detection and notification.

RFID and Wireless Surveillance – These types of surveillance are used to manage and locate important information system assets.

7.5 Chapter Summary

Cisco | Networking Academy®
Mind Wide Open™

Chapter Summary

Summary

- This chapter discussed the technologies, processes and procedures that cybersecurity specialists use to defend the systems, devices, and data that make up the network infrastructure.
- Host hardening includes securing the operating system, implementing an antivirus solution, and using host-based solutions such as firewalls and intrusion detection systems.
- Server hardening includes managing remote access, securing privileged accounts, and monitoring services.
- Data protection includes file access control and implementing security measures to ensure the confidentiality, integrity, and availability of data.
- Device hardening also involves implementing proven methods of physically securing network devices. Protecting a cybersecurity domain is an on-going process to secure an organization’s network infrastructure and requires a constant vigilance against threats.

Cisco | Networking Academy®

Mind Wide Open™