Task 31/01/25: Cisco Cyber Ops

Traccia 1

Utilizzo di Windows PowerShell:

In questo laboratorio, esploreremo alcune delle funzioni di PowerShell.

Traccia 2

Utilizzo di Wireshark per Esaminare il Traffico HTTP e HTTPS:

In questo laboratorio, completa i seguenti obiettivi:

- Catturare e visualizzare il traffico HTTP
- Catturare e visualizzare il traffico HTTPS

Task 31/01/25: Cisco Cyber Ops

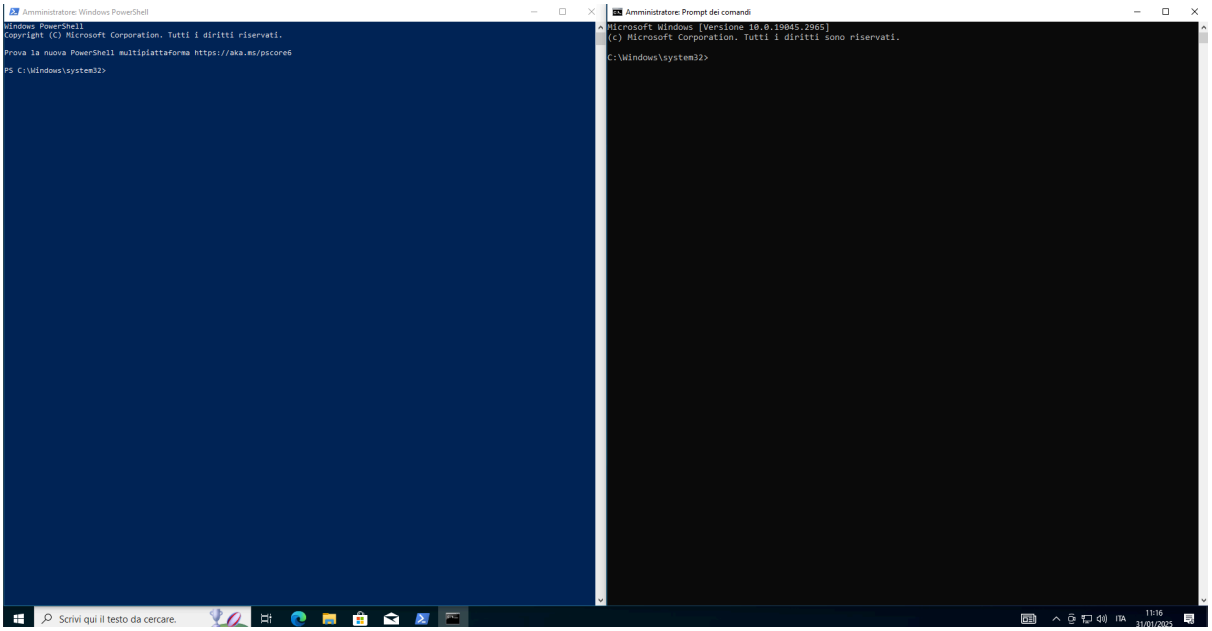
Report

Utilizzo di Windows PowerShell

Scenario

PowerShell is a powerful automation tool. It is both a command console and a scripting language. In this lab, you will use the console to execute some of the commands that are available in both the command prompt and PowerShell. PowerShell also has functions that can create scripts to automate tasks and work together with the Windows Operating System.

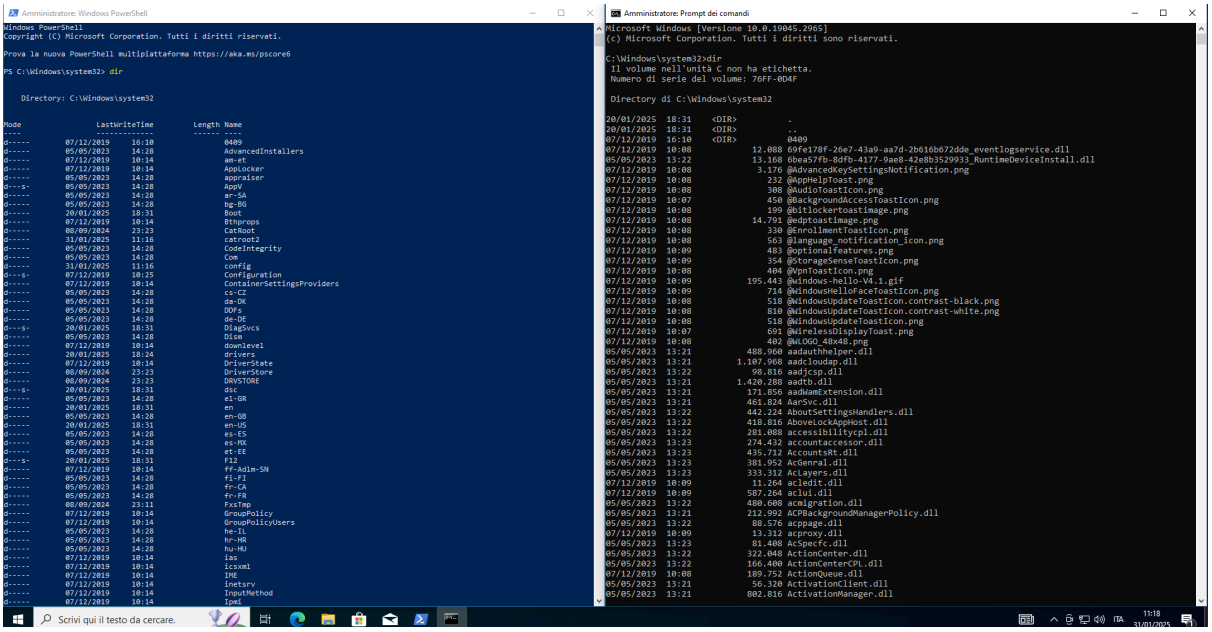
Part 1: Access PowerShell console.
a. Click Start. Search and select powershell.
b. Click Start. Search and select command prompt.



Part 2: Explore Command Prompt and PowerShell commands.
a. Enter dir at the prompt in both windows.
What are the outputs to the dir command?
The dir command was executed in both Command Prompt (cmd) and PowerShell.

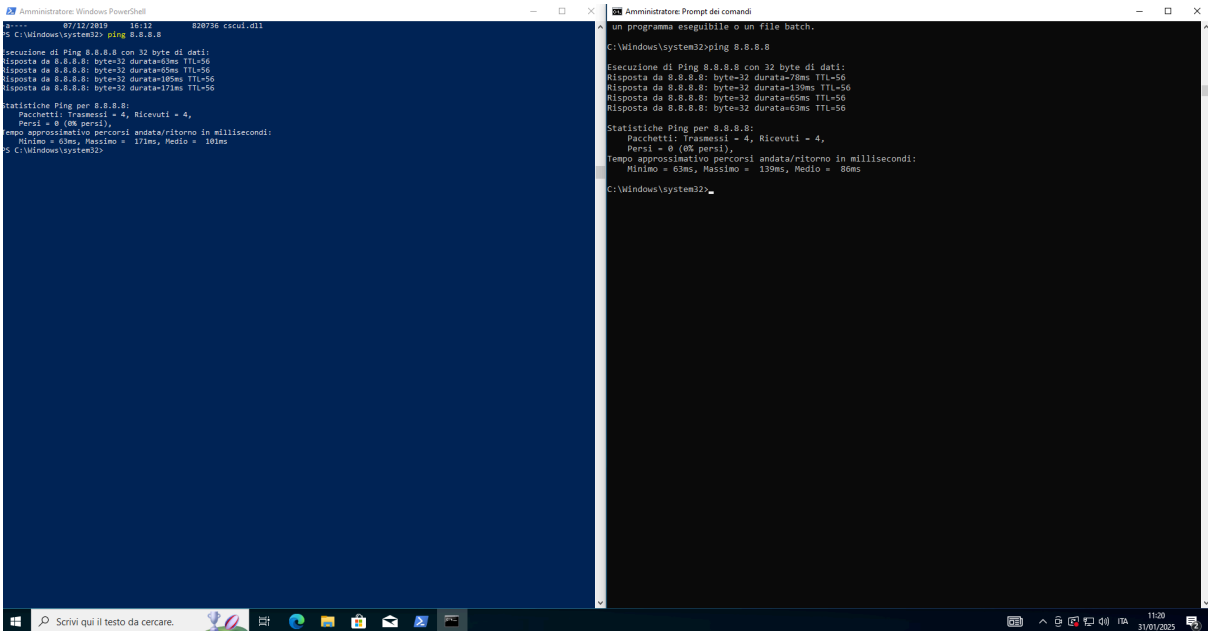
- Command Prompt (cmd) output:
  - Displayed a list of files and directories within C:\Windows\System32.
  - The output includes file names, extensions, sizes, and timestamps.
  - Some notable files include .dll, .png, .exe, and .sys files.
- PowerShell (dir alias for Get-ChildItem) output:
  - Displayed a structured list of directories within C:\Windows\System32.
  - Information shown includes:
    - Mode: Specifies whether it's a directory (d-----) or file (-a----).

- LastWriteTime: Last modification date of the item.
- Length: Size (only for files).
- Name: Name of the file or folder.



b. Try another command that you have used in the command prompt, such as ping, cd, and ipconfig. What are the results?
The ping command was executed for the IP address 8.8.8.8 (Google's public DNS server).

- Results in both cmd and PowerShell:
  - Four packets were sent and successfully received.
  - No packet loss (0% loss).
  - Response times ranged between 63ms and 171ms.
  - TTL (Time to Live) value was 56.
  - Average response time varied:
    - PowerShell: 101ms average.
    - Command Prompt: 86ms average.



Part 3: Explore cmdlets.

a. PowerShell commands, cmdlets, are constructed in the form of verb-noun string. To identify the PowerShell command to list the subdirectories and files in a directory, enter Get-Alias dir at the PowerShell prompt.

What is the PowerShell command for dir?

In PowerShell, dir is an alias for the Get-ChildItem cmdlet.

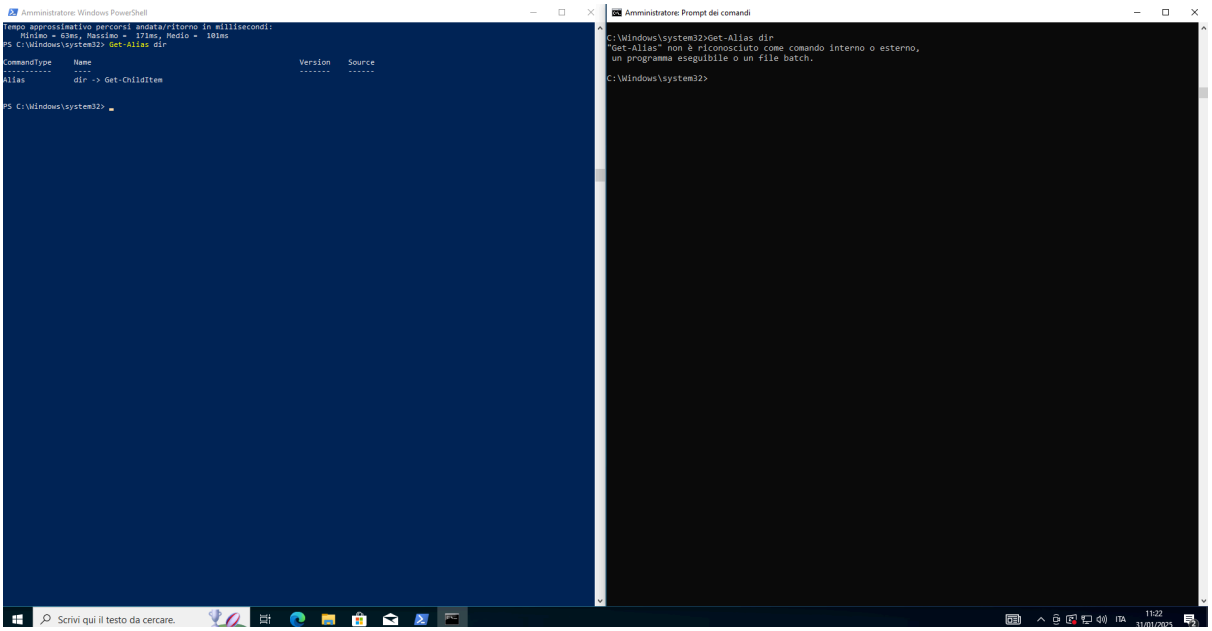
Command Used to Verify This: Get-Alias dir

- Output: dir -> Get-ChildItem
- This confirms that dir in PowerShell maps to Get-ChildItem.

To list files using PowerShell, you can use: Get-ChildItem

b. For more detailed information about cmdlets, perform an internet search for Microsoft powershell cmdlets.

c. Close the Command Prompt window when done.



Part 4: Explore the netstat command using PowerShell.

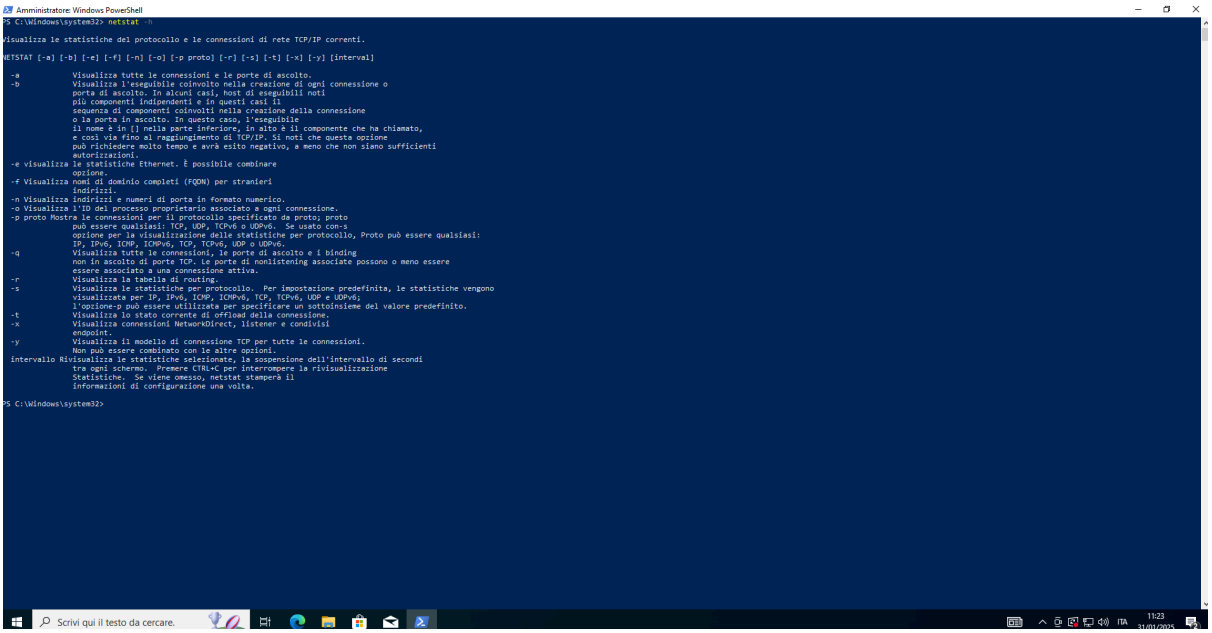
a. At the PowerShell prompt, enter netstat -h to see the options available for the netstat command.

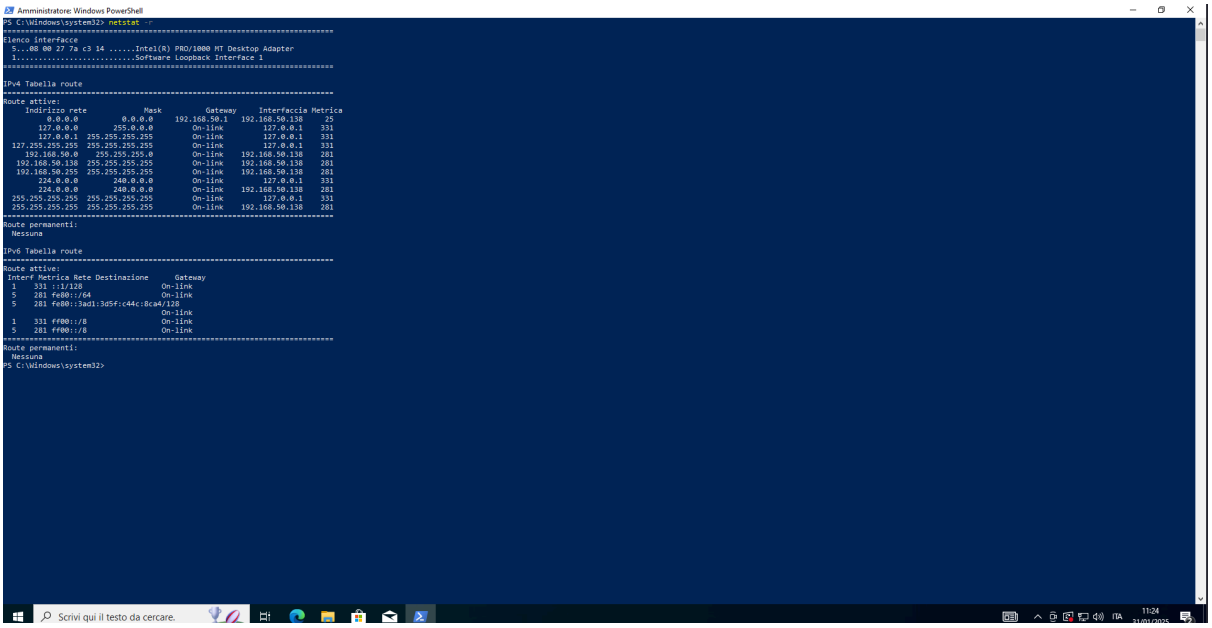
b. To display the routing table with the active routes, enter netstat -r at the prompt.

What is the IPv4 gateway?

The IPv4 gateway can be identified in the netstat -r command output.

- IPv4 Default Gateway: 192.168.50.1
- This is the local router IP address that routes traffic outside the local network.





c. Open and run a second PowerShell with elevated privileges. Click Start. Search for PowerShell and right-click Windows PowerShell and select Run as administrator. Click Yes to allow this app to make changes to your device.

d. The netstat command can also display the processes associated with the active TCP connections. Enter the netstat -abno at the prompt.

e. Open the Task Manager. Navigate to the Details tab. Click the PID heading so the PID are in order.

f. Select one of the PIDs from the results of netstat -abno. PID 756 is used in this example.

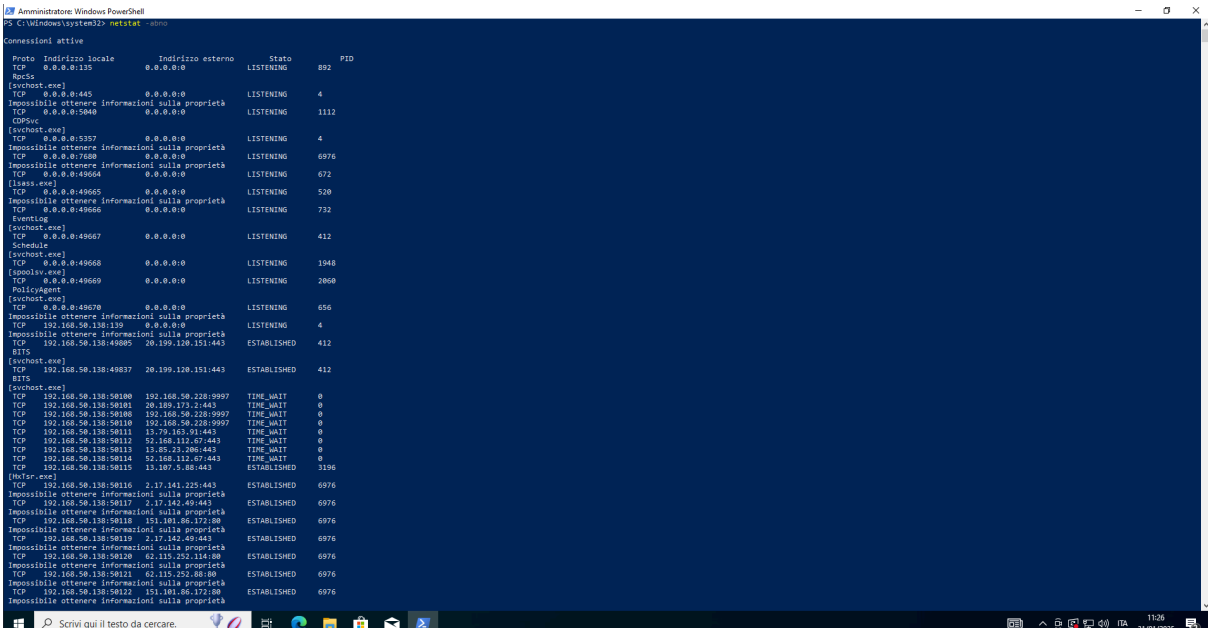
g. Locate the selected PID in the Task Manager. Right-click the selected PID in the Task Manager to open the Properties dialog box for more information.

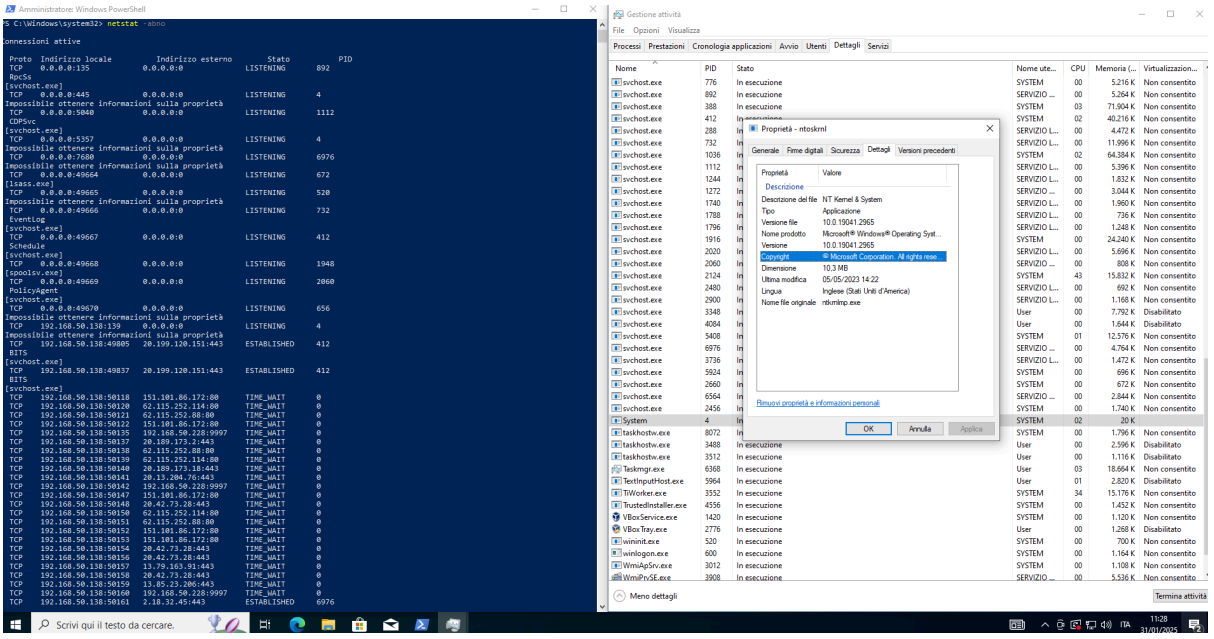
What information can you get from the Details tab and the Properties dialog box for your selected PID?

From the Task Manager (Gestione attività) → Details tab → Properties (Proprietà) window:

- The selected PID (Process ID) is linked to ntoskrnl.exe.
- Key information retrieved:
  - File Name: ntoskrnl.exe
  - Description: NT Kernel & System

    - Type: System file
    - File Version: 10.0.19041.2965
    - Product Name: Microsoft Windows® Operating System
    - Copyright: Microsoft Corporation
    - Size: 10.3 MB
    - Original File Name: ntkrnlmp.exe
    - Last Modified Date: 05/05/2023 14:22
- Additional insights from the Details tab:
    - The Process ID (PID) can be cross-referenced with network connections using netstat -abno.
    - The process is a critical system file, likely associated with Windows Kernel operations.





Part 5: Empty recycle bin using PowerShell.

PowerShell commands can simplify management of a large computer network. For example, if you wanted to implement a new security solution on all servers in the network you could use a PowerShell command or script to implement and verify that the services are running. You can also run PowerShell commands to simplify actions that would take multiple steps to execute using Windows graphical desktop tools.

a. Open the Recycle Bin. Verify that there are items that can be deleted permanently from your PC. If not, restore those files.

b. If there are no files in the Recycle Bin, create a few files, such as text file using Notepad, and place them into the Recycle Bin.

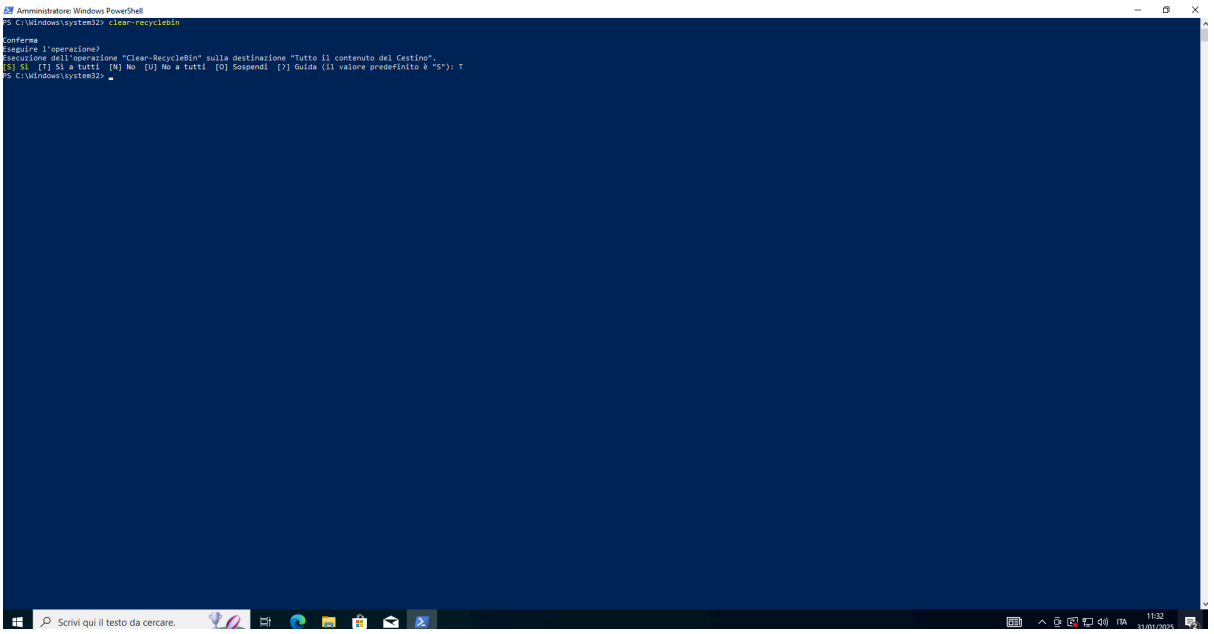
c. In a PowerShell console, enter clear-recyclebin at the prompt.

What happened to the files in the Recycle Bin?

The PowerShell command Clear-RecycleBin was executed.

Command: Clear-RecycleBin

- Effect:
  - The system prompted for confirmation before permanently deleting the files.
  - No user input was visible (T was typed, possibly a typo or incomplete response).
  - If confirmed (Y or S), all files in the Recycle Bin were deleted permanently.



Reflection Question

PowerShell was developed for task automation and configuration management. Using the internet, research commands that you could use to simplify your tasks as a security analyst. Record your findings.

Here are some PowerShell commands that can help in cybersecurity and SOC analyst tasks:

Get currently logged-in users: Get-WmiObject -Class Win32_ComputerSystem | Select-Object UserName

List all active users: Get-WmiObject -Class Win32_LoggedOnUser

Get OS information: Get-ComputerInfo | Select-Object WindowsVersion, WindowsBuildLabEx, OSArchitecture

Check open network connections: Get-NetTCPConnection | Where-Object {$_.State -eq "Established"}List listening ports: Get-NetTCPConnection | Where-Object {$_.State -eq "Listen"}Display network adapters and IP configuration: Get-NetIPAddress

Perform traceroute: Test-NetConnection -TraceRoute google.com
List running processes: Get-Process | Sort-Object -Property CPU -Descending | Select-Object -First 10Check running services: Get-Service | Where-Object {$_.Status -eq "Running"}
Get detailed process information for a specific PID: Get-Process -Id <PID>
Identify suspicious processes (non-Microsoft processes): Get-Process | Where-Object {$_.Path -notlike "*Windows*"}
Display failed login attempts: Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4625}
Get recent PowerShell history: Get-History
List recently modified files (last 24 hours): Get-ChildItem -Path C:\ -Recurse | Where-Object {$_.LastWriteTime -gt (Get-Date).AddDays(-1)}
Export logs: Get-EventLog -LogName Security -Newest 50 | Export-Csv -Path C:\logs\SecurityLogs.csv
Kill suspicious processes: Stop-Process -Id <PID> -Force
Disable a user account: Disable-LocalUser -Name "SuspiciousUser"
Remove malicious scheduled tasks: Get-ScheduledTask | Where-Object {$_.State -eq "Running"} | Stop-ScheduledTask

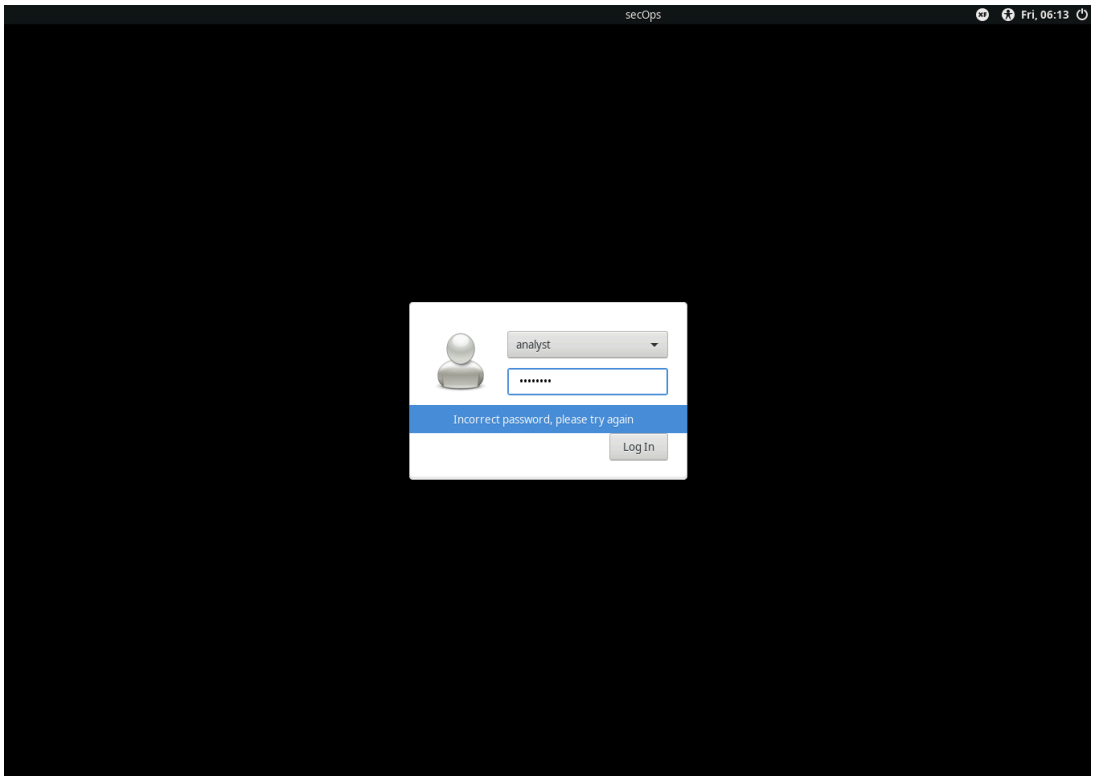
Utilizzo di Wireshark per Esaminare il Traffico HTTP e HTTPS

Scenario

HyperText Transfer Protocol (HTTP) is an application layer protocol that presents data via a web browser. With HTTP, there is no safeguard for the exchanged data between two communicating devices.
With HTTPS, encryption is used via a mathematical algorithm. This algorithm hides the true meaning of the data that is being exchanged. This is done through the use of certificates that can be viewed later in this lab. Regardless of HTTP or HTTPS, it is only recommended to exchange data with websites that you trust. Just because a site uses HTTPS does not mean it is a trustworthy site. Threat actors commonly use HTTPS to hide their activities.
In this lab, you will explore and capture HTTP and HTTPS traffic using Wireshark.

Capture and View HTTP Traffic
In this part, you will use tcpdump to capture the content of HTTP traffic. You will use command options to save the traffic to a packet capture (pcap) file. These records can then be analyzed using different applications that read pcap files, including Wireshark.

Step 1: Start the virtual machine and log in.
Start the CyberOps Workstation VM. Use the following user credentials:
Username: analyst
Password: cyberops



Step 2: Open a terminal and start tcpdump.

a. Open a terminal application and enter the command ip address.

b. List the interfaces and their IP addresses displayed in the ip address output.

c. While in the terminal application, enter the command sudo tcpdump –i enp0s3 –s 0 –w httpdump.pcap. Enter the password cyberops for the user analyst when prompted.

This command starts tcpdump and records network traffic on the enp0s3 interface.

The -i command option allows you to specify the interface. If not specified, the tcpdump will capture all traffic on all interfaces.

The -s command option specifies the length of the snapshot for each packet. You should limit snaplen to the smallest number that will capture the protocol information in which you are interested. Setting snaplen to 0 sets it to the default of 262144, for backwards compatibility with recent older versions of tcpdump.

The -w command option is used to write the result of the tcpdump command to a file. Adding the extension .pcap ensures that operating systems and applications will be able to read to file. All recorded traffic will be printed to the file httpdump.pcap in the home directory of the user analyst.

Use the man pages for tcpdump to determine the usage of the -s and -w command options.

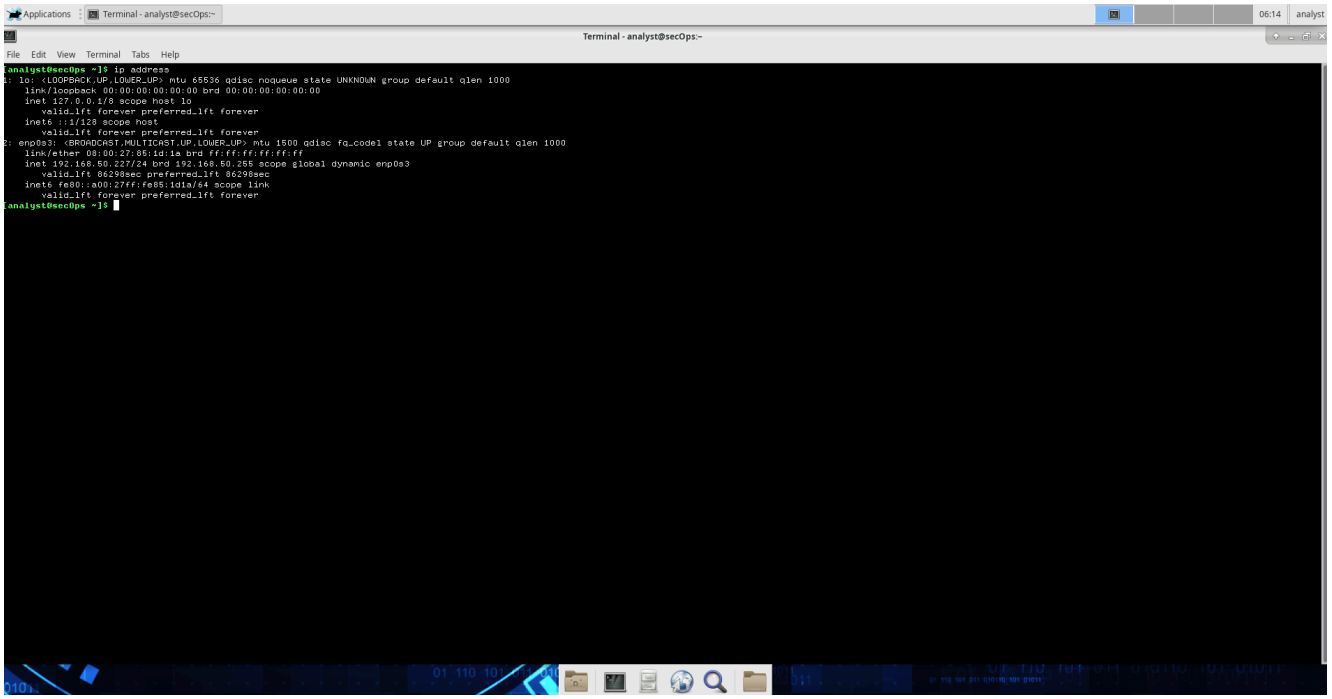
d. Open a web browser from the launch bar within the CyberOps Workstation VM. Navigate to http://www.altoromutual.com/login.jsp

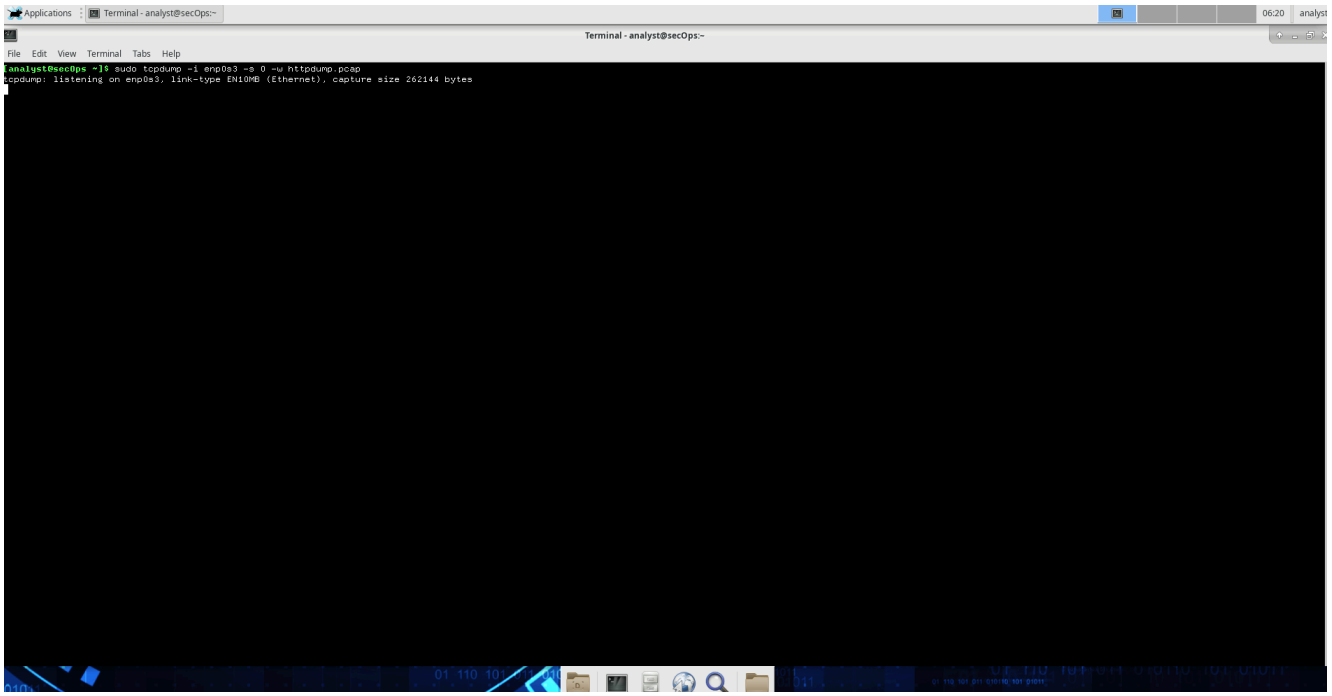
Because this website uses HTTP, the traffic is not encrypted. Click the Password field to see the warning pop up.

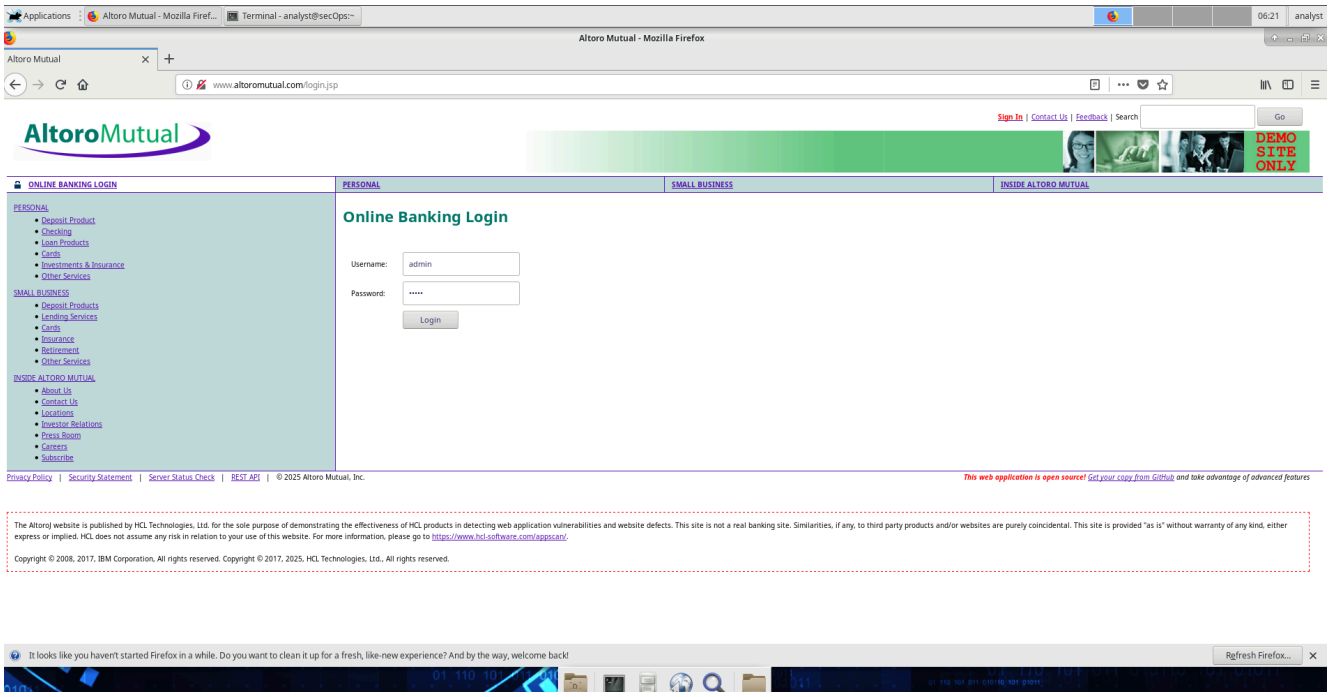
e. Enter a username of Admin with a password of Admin and click Login.

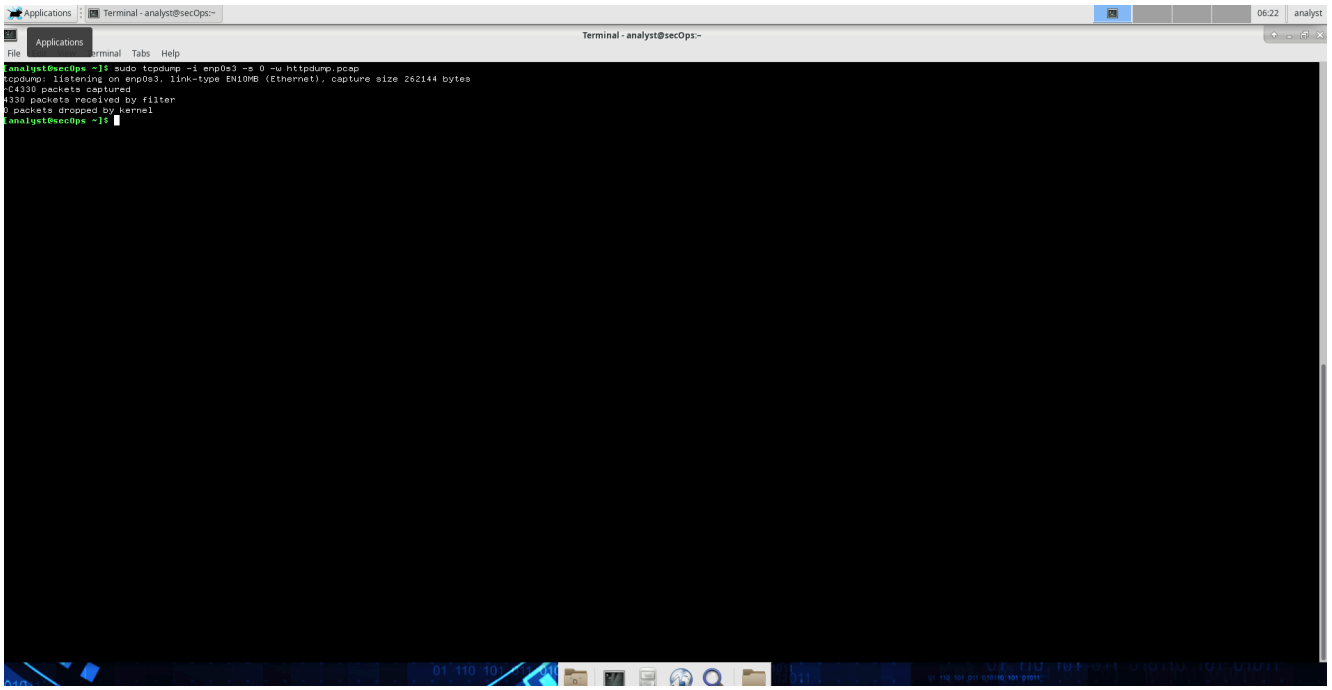
f. Close the web browser.

g. Return to the terminal window where tcpdump is running. Enter CTRL+C to stop the packet capture.




Applications
Terminal - analyst@secOps:~
06:20
analyst
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes


Applications
Altoro Mutual - Mozilla Firef...
Terminal - analyst@secOps:~
06:21
analyst
Altoro Mutual - Mozilla Firefox
Altoro Mutual
www.altoromutual.com/login.jsp
AltoroMutual
Sign In | Contact Us | Feedback | Search
Go
DEMO SITE ONLY
ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
Online Banking Login
Username: admin
Password: •••••
Login
Privacy Policy | Security Statement | Server Status Check | REST API | © 2025 Altoro Mutual, Inc.
This web application is open source! Get your copy from GitHub and take advantage of advanced features
The Altoro website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to https://www.hcl-software.com/appscan/.
Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2025, HCL Technologies, Ltd., All rights reserved.
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...



Step 3: View the HTTP capture.

The tcpdump, executed in the previous step, printed the output to a file named httpdump.pcap. This file is located in the home directory for the user analyst.

a. Click the File Manager icon on the desktop and browse to the home folder for the user analyst. Double-click the httpdump.pcap file, in the Open With dialog box scroll down to Wireshark and then click Open.

b. In the Wireshark application, filter for http and click Apply.

c. Browse through the different HTTP messages and select the POST message.

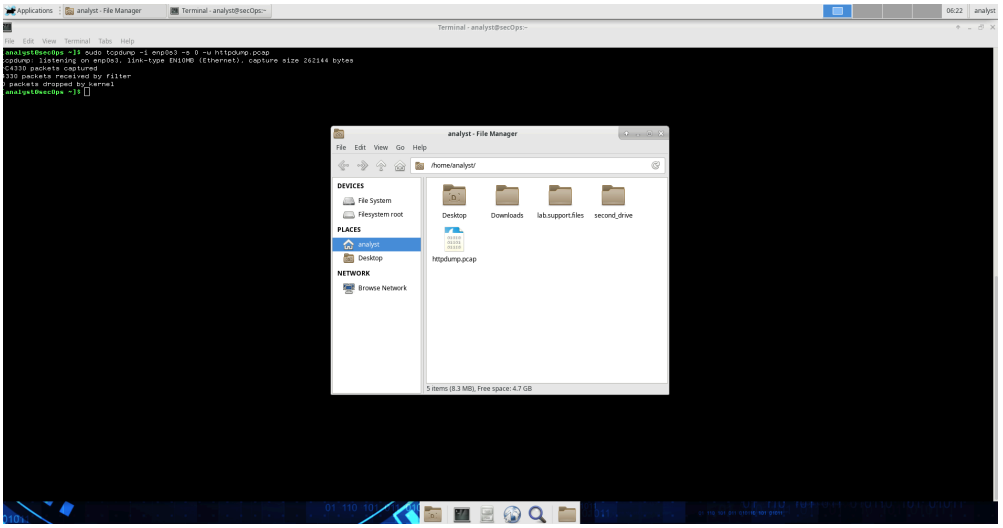
d. In the lower window, the message is displayed. Expand the HTML Form URL Encoded: application/x-www-form-urlencoded section.

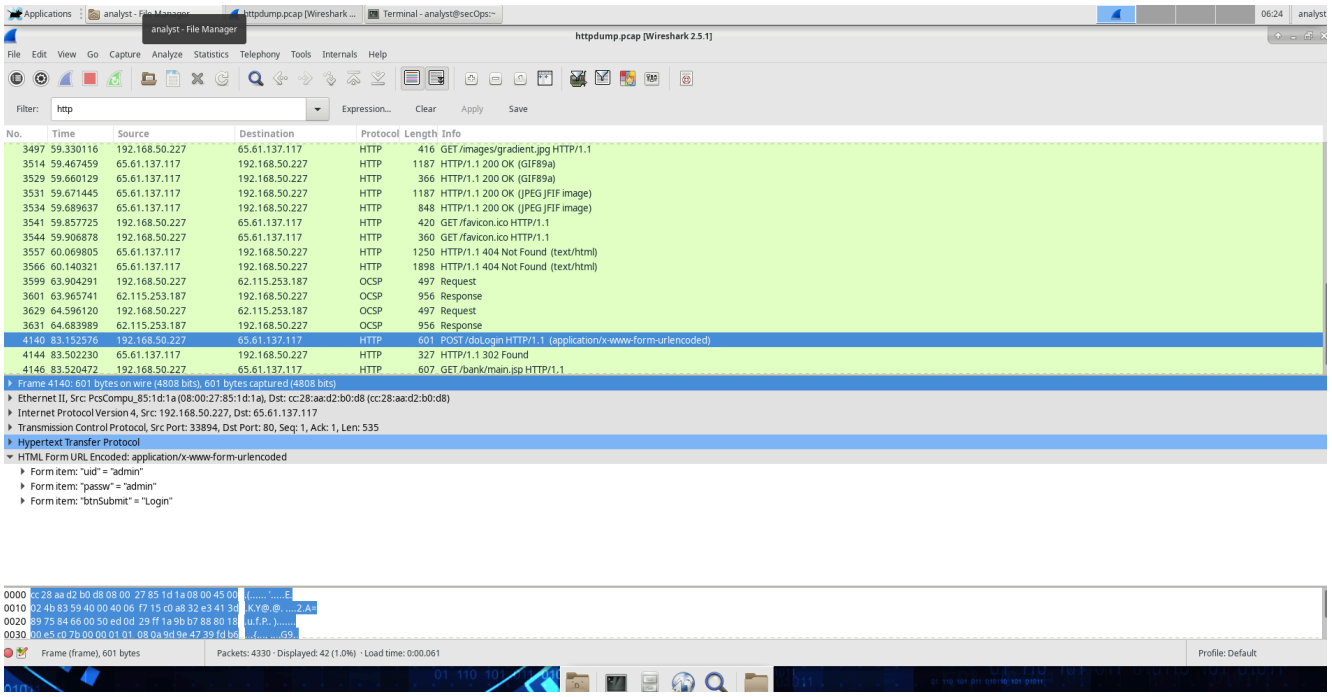
What two pieces of information are displayed?

In the packet capture analysis, two key pieces of information are displayed:

- The communication between the client (192.168.50.227) and the server (34.120.208.123) using TLS 1.2 over port 443.
- The application data, which appears encrypted, showing that HTTPS is in use instead of HTTP.

e. Close the Wireshark application.





Capture and View HTTPS Traffic

You will now use tcpdump from the command line of a Linux workstation to capture HTTPS traffic. After starting tcpdump, you will generate HTTPS traffic while tcpdump records the contents of the network traffic. These records will again be analyzed using Wireshark.

Step 1: Start tcpdump within a terminal.

a. While in the terminal application, enter the command sudo tcpdump –i enp0s3 –s 0 –w httpsdump.pcap. Enter the password cyberops for the user analyst when prompted.

his command will start tcpdump and record network traffic on the enp0s3 interface of the Linux workstation. If your interface is different than enp0s3, please modify it when using the above command. All recorded traffic will be printed to the file httpsdump.pcap in the home directory of the user analyst.

b. Open a web browser from the launch bar within the CyberOps Workstation VM. Navigate to www.netacad.com.

Note: If you receive a “Secure Connection Failed” webpage it probably means the date and time are incorrect. Update the day and time with the following command, changing to the current day and time:

What do you notice about the website URL?

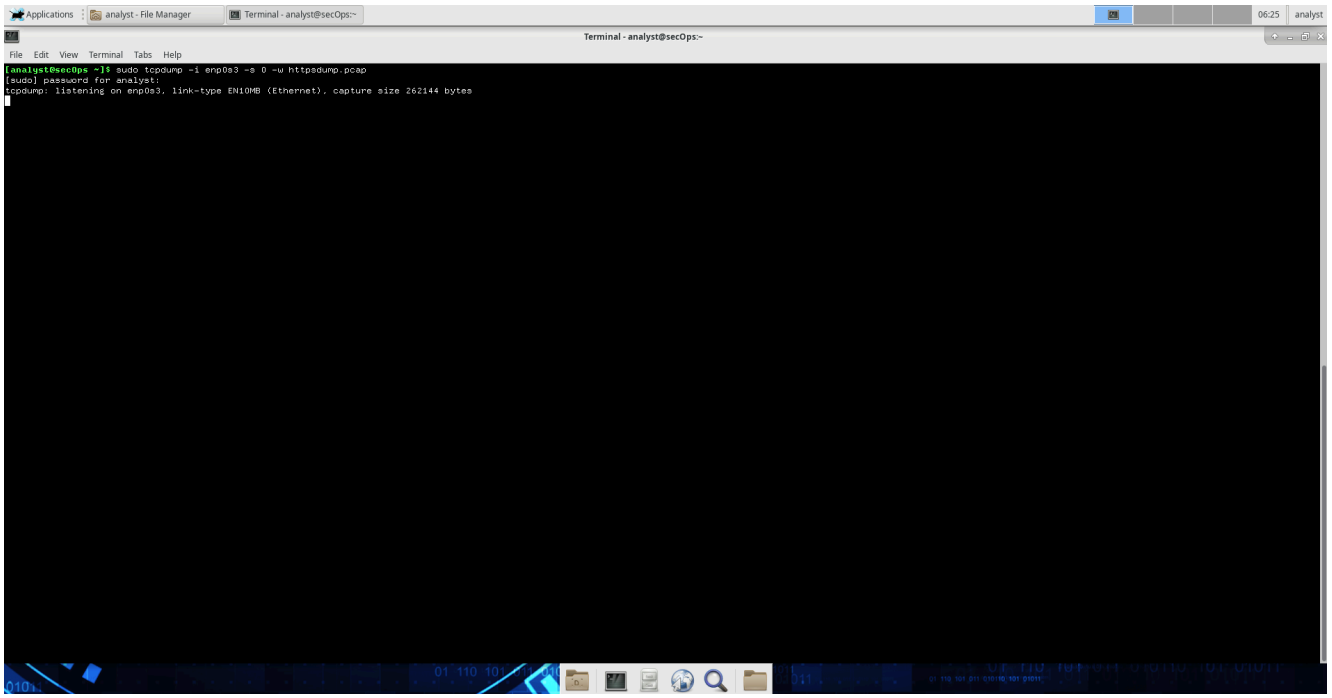
The website URL now starts with "https://", indicating that the communication is encrypted using TLS (Transport Layer Security). This is different from the previous capture where HTTP was used, meaning the data was transmitted in plaintext.

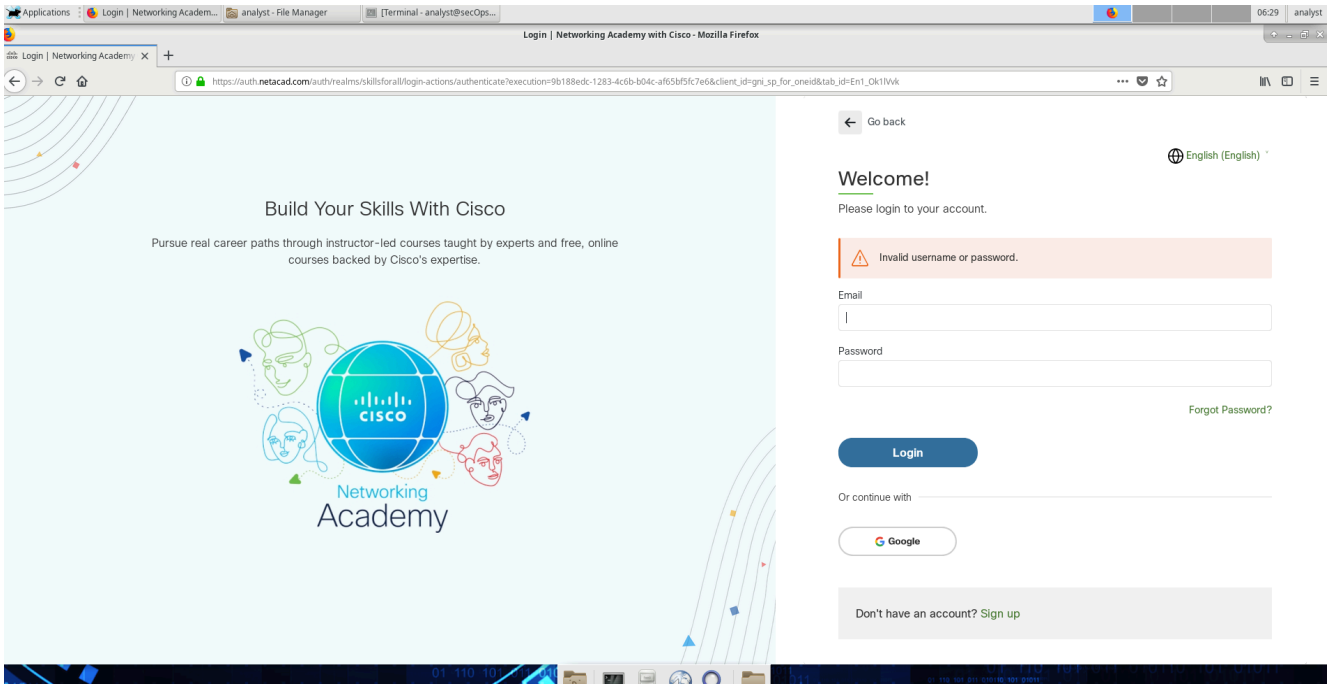
c. Click Log in.

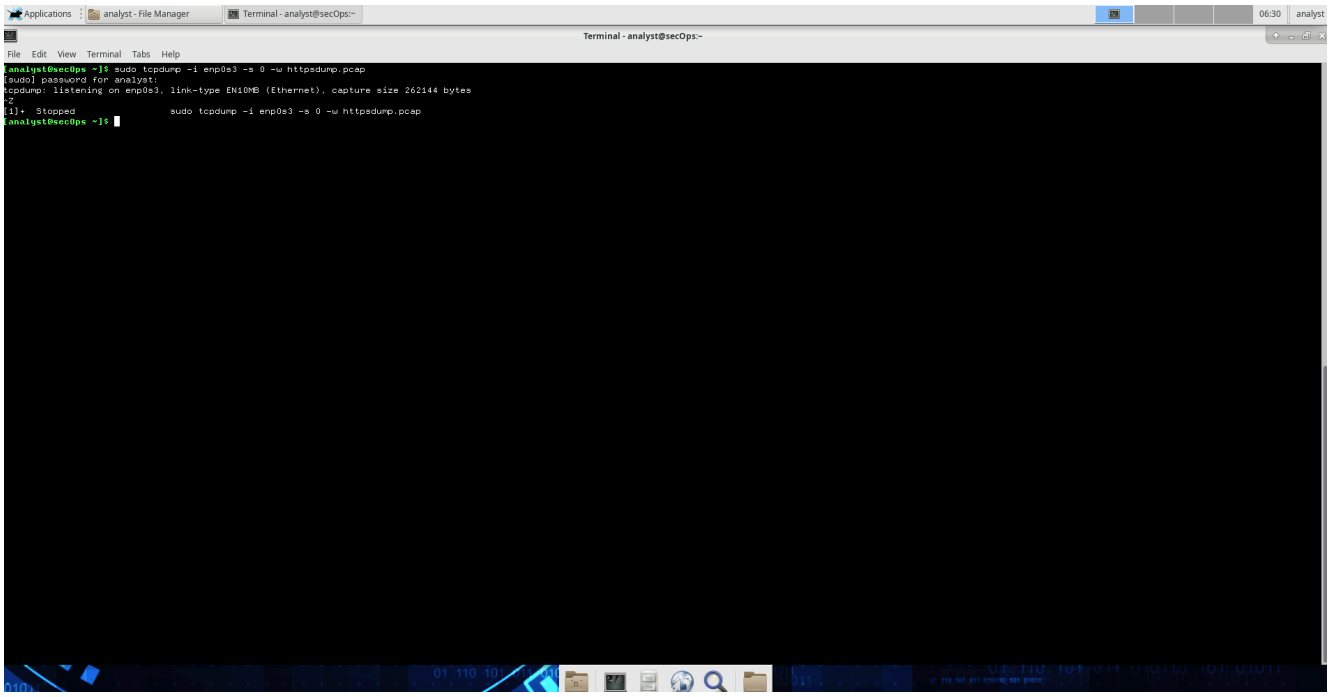
d. Enter in your NetAcad username and password. Click Next.

e. Close the web browser in the VM.

f. Return to the terminal window where tcpdump is running. Enter CTRL+C to stop the packet capture.


Applications
analyst - File Manager
Terminal - analyst@secOps:~
06:25
analyst
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes


Applications
Login | Networking Academ...
analyst - File Manager
[Terminal - analyst@secOps...
06:29
analyst
Login | Networking Academy with Cisco - Mozilla Firefox
Login | Networking Academy
https://auth.netacad.com/auth/realms/skillsforall/login-actions/authenticate?execution=9b188edc-1283-4c6b-b04c-af65bf5fc7e6&client_id=gni_sp_for_oneid&tab_id=En1_Ok1lVvk
Build Your Skills With Cisco
Pursue real career paths through instructor-led courses taught by experts and free, online courses backed by Cisco's expertise.
Networking Academy
Go back
English (English)
Welcome!
Please login to your account.
Invalid username or password.
Email
Password
Forgot Password?
Login
Or continue with
Google
Don't have an account? Sign up



Step 2: View the HTTPS capture.

The tcpdump executed in Step 1 printed the output to a file named httpsdump.pcap. This file is located in the home directory for the user analyst.

a. Click the Filesystem icon on the desktop and browse to the home folder for the user analyst. Open the httpsdump.pcap file.

b. In the Wireshark application, expand the capture window vertically and then filter by HTTPS traffic via port 443.

Enter tcp.port==443 as a filter, and click Apply.

c. Browse through the different HTTPS messages and select an Application Data message.

d. In the lower window, the message is displayed.

What has replaced the HTTP section that was in the previous capture file?

The TLSv1.2 protocol has replaced the previous HTTP traffic. Instead of seeing plaintext HTTP requests and responses, we now see encrypted Application Data packets in the capture.

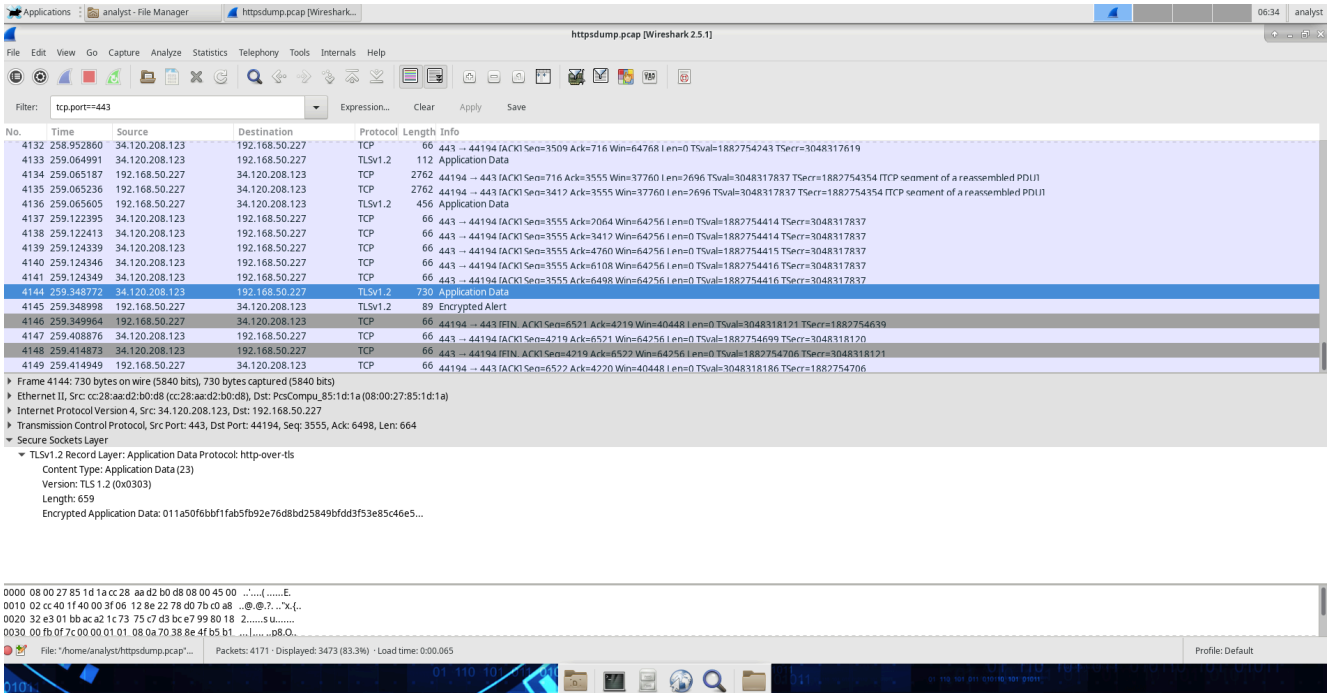
e. Completely expand the Secure Sockets Layer section.

f. Click the Encrypted Application Data.

Is the application data in a plaintext or readable format?

No, the application data is encrypted. Unlike in the HTTP capture where credentials were visible in plaintext, the HTTPS capture only shows encrypted application data, making it unreadable without the proper decryption key.

g. Close all windows and shut down the virtual machine.



Reflection Questions

1. What are the advantages of using HTTPS instead of HTTP?

Using HTTPS provides several advantages over HTTP, including:

- Encryption: Protects data from being intercepted and read by unauthorized parties.
- Integrity: Ensures that data is not altered during transmission.
- Authentication: Verifies that the website is legitimate and not an imposter.
- User Trust: Users are more likely to trust and interact with a site that has HTTPS.

2. Are all websites that use HTTPS considered trustworthy?

No, not all HTTPS websites are trustworthy. While HTTPS ensures encryption, it does not guarantee that a website is legitimate.

- Phishing sites can still use HTTPS to appear more credible.
- A site could have a valid TLS certificate but still contain malicious content.
- Users should check for EV certificates, organization details, and site legitimacy before trusting sensitive information to an HTTPS website.