

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

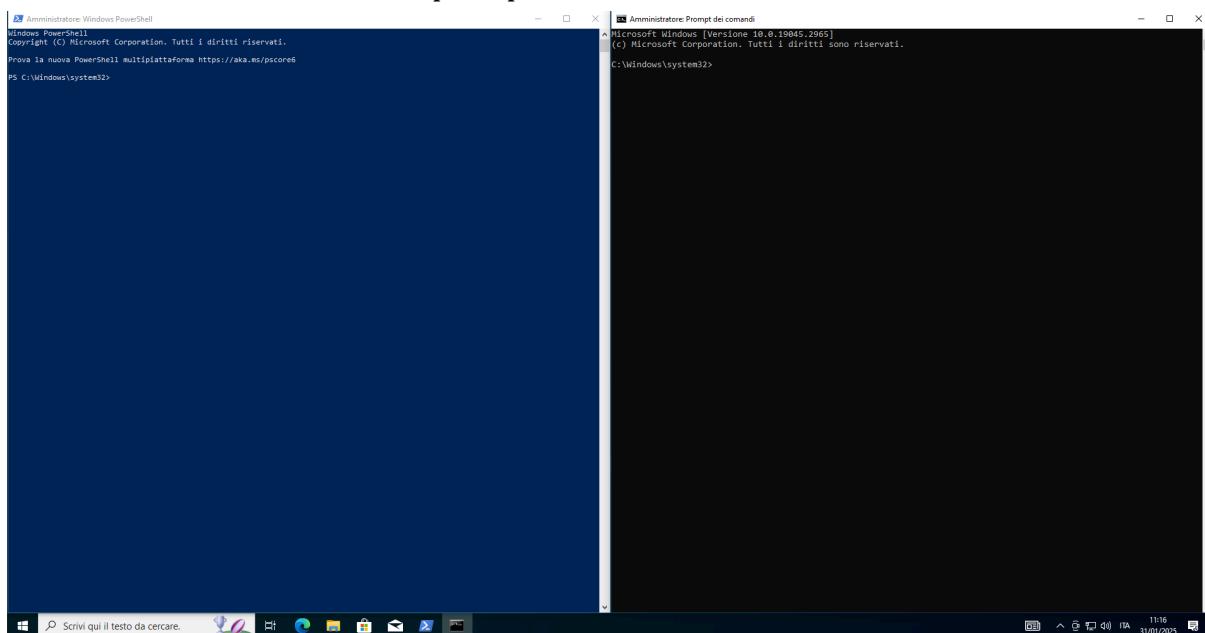
Utilizzo di Windows PowerShell

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.

- Click Start. Search and select powershell.
- Click Start. Search and select command prompt.



Part 2: Explore Command Prompt and PowerShell commands.

- 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.

```
Administrator: Windows PowerShell
Copyright (C) Microsoft Corporation. Tutti i diritti riservati.

Prova la nuova PowerShell multiplattaforma https://aka.ms/powershell

PS C:\Windows\system2> dir

Directory: C:\Windows\system32

Name                           Length  LastWriteTime
----                           ----  -
d-----          AdvancedInstallers
d-----          AppLocker
d-----          appraiser
d-----          ar-SA
d-----          bg-BG
d-----          Configuration
d-----          ConfigurationSettingsProviders
d-----          cs-CZ
d-----          da-DK
d-----          de-DE
d-----          DiagVcvs
d-----          drivers
d-----          downlevel
d-----          DriverStore
d-----          DriverStore
d-----          e1-GR
d-----          en-GB
d-----          en-US
d-----          es-ES
d-----          es-MX
d-----          et-EE
d-----          fr-CA
d-----          fr-FR
d-----          FxTm
d-----          GroupPolicy
d-----          GroupPolicyUsers
d-----          he-IL
d-----          hu-HU
d-----          id-ID
d-----          icxaml
d-----          IME
d-----          InputMethod
d-----          InputMethod
d-----          Ipmi

Administrator: Prompt dei comandi
Microsoft Windows [Versione 10.0.19045.2065]
(c) Microsoft Corporation. Tutti i diritti sono riservati.

C:\Windows\system2>dir
Il volume nell'unità C non ha etichetta.
Numero di serie del volume: 76F8-0D4F

Directory di C:\Windows\system32

Name                           Length  LastWriteTime
----                           ----  -
d-----          .
d-----          .
d-----          0449
d-----          12.088 06/05/2023 10:10 0449\felidz-26ef7d3a9-a97d-2b610b672dde_eventlogservice.dll
d-----          13.174 06/05/2023 10:10 0449\felidz-26ef7d3a9-a97d-2b610b672dde_kineticdeviceinstall.dll
d-----          5.174 07/12/2019 10:08 0449\AdvancedKeySettingNotification.dll
d-----          232 07/12/2019 10:08 0449\AppBarToastIcon.png
d-----          308 07/12/2019 10:08 0449\AudioToasterIcon.png
d-----          456 07/12/2019 10:08 0449\BitlockerToImageIcon.png
d-----          14.791 07/12/2019 10:08 0449\BitLockerToImage.png
d-----          336 07/12/2019 10:08 0449\EnrollmentToastIcon.png
d-----          556 07/12/2019 10:08 0449\GetAppIconFromImageIcon.png
d-----          481 07/12/2019 10:08 0449\OptionalFeatures.png
d-----          354 07/12/2019 10:09 0449\StorageSenseIcon.png
d-----          404 07/12/2019 10:08 0449\WinToastIcon.png
d-----          195.000 07/12/2019 10:09 0449\WinToastIcon.contrast-100.gif
d-----          716 07/12/2019 10:09 0449\WindowsHelloFaceToastIcon.png
d-----          518 07/12/2019 10:08 0449\WindowsUpdateToastIcon.contrast-black.png
d-----          518 07/12/2019 10:08 0449\WindowsUpdateToastIcon.contrast-white.png
d-----          691 07/12/2019 10:07 0449\WirelessDisplayToast.png
d-----          404 07/12/2019 10:08 0449\WLGO_48x48.png
d-----          488 07/12/2019 10:08 0449\WindowsHelpAndSupport.dll
d-----          1.187.960 05/05/2023 13:21 0449\WindowsHelpAndSupport.dll
d-----          98.816 05/05/2023 13:22 0449\adicsp.dll
d-----          1.426.288 05/05/2023 13:23 0449\adbdb.dll
d-----          153.700 05/05/2023 13:23 0449\adbdnension.dll
d-----          461.824 05/05/2023 13:21 0449\aeasvc.dll
d-----          442.224 05/05/2023 13:22 0449\AboutSettingHandlers.dll
d-----          418.816 05/05/2023 13:22 0449\AboveClockAppHost.dll
d-----          203.320 05/05/2023 13:22 0449\BackgroundTask.dll
d-----          274.432 05/05/2023 13:23 0449\accountaccessor.dll
d-----          435.712 05/05/2023 13:23 0449\AccountSR.dll
d-----          381.072 05/05/2023 13:23 0449\AcGeneral.dll
d-----          353.192 05/05/2023 13:23 0449\AcLogon.dll
d-----          11.264 07/12/2019 10:09 0449\acledit.dll
d-----          587.264 07/12/2019 10:09 0449\acldui.dll
d-----          488.000 05/05/2023 13:22 0449\AcLogonManager.dll
d-----          212.960 05/05/2023 13:21 0449\ACPBackgroundManagerPolicy.dll
d-----          88.576 05/05/2023 13:22 0449\apcpage.dll
d-----          13.312 07/12/2019 10:09 0449\apcoxy.dll
d-----          31.408 05/05/2023 13:22 0449\apcsp.dll
d-----          32.044 05/05/2023 13:22 0449\ActionCenter.dll
d-----          166.480 05/05/2023 13:22 0449\ActionCenterPCL.dll
d-----          189.752 07/12/2019 10:08 0449\ActionQueue.dll
d-----          50.520 05/05/2023 13:21 0449\ActivationClient.dll
d-----          802.916 05/05/2023 13:21 0449\ActivationManager.dll
```

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.

```
PS C:\Windows\system32> Get-Alias dir
Tempo approssimativo percorso andata/ritorno in millisecondi:
Nome          Durata (ms)  Percorso
----          -----  -----
dir           18ms       PS C:\Windows\system32> Get-Alias dir
Get-Alias è un comando interno o esterno,
un programma eseguibile o un file batch.
C:\Windows\system32>
```

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.

```

PS C:\Windows\system32> netstat -n
Visualizza le statistiche del protocollo e le connessioni di rete TCP/IP correnti.
NETSTAT [-a] [-b] [-c] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [interval]
-a Visualizza tutte le connessioni e le porte di ascolto.
-b Visualizza i componenti indipendenti per ogni connessione o porta di ascolto. In alcuni casi, host di eseguibili noti più componenti indipendenti e in questi casi i connetti visibili sono solo quelli che costituiscono la connessione o la porta in ascolto. In questo caso, l'eseguibile listing non mostra il nome del componente che ha chiamato, e così via fino al raggiungimento di TCP/IP. Si noti che questa opzione può richiedere molto tempo e avrà esito negativo, a meno che non siano sufficienti memoria e tempo disponibili.
-c visualizza le statistiche Ethernet. È possibile combinare opzione.
-f visualizza le connessioni completi (FONI) per strati dati.
-n visualizza i numeri di porta in formato numerico.
-o visualizza l'ID del processo proprietario associato a ogni connessione.
-p proto mostra le connessioni per il protocollo specificato da proto; proto può essere IP, ICMP, ICMPv6, TCP, TCPv6, UDP o UDPv6.
-q Visualizza le statistiche per protocollo. Per impostazione predefinita, le statistiche vengono visualizzate per IP, ICMP, TCP, TCPv6, UDP e UDPv6; l'opzione -q può essere utilizzata per specificare un sottoinsieme del valore predefinito.
-s Visualizza lo stato corrente di offload della connessione.
-t Visualizza le connessioni Network-to-Direct, listener e condivisi endpoint.
-y Visualizza il modello di connessione TCP per tutte le connessioni.
-H Mostra i host.
-i visualizza le statistiche selezionate, la sospensione dell'intervallo di secondi tra ogni schermata. Premere CTRL+C per interrompere la rivedutizzazione.
-S Stabilisce se si deve visualizzare o stampare le informazioni di configurazione una volta.

PS C:\Windows\system32>

```

```

PS C:\Windows\system32> netstat -rn
=====
Gennaio interfaccia
5...00 00 27 7a c3 14 ..... Intel(R) PRO/1000 MT Desktop Adapter
..... Software Loopback Interface 1
=====
IPv4 Tabella route
=====
Rete Destinazione Gateway Metrica
Indirizzo rett. Mask Interfaccia Metrica
0.0.0.0 0.0.0.0 192.168.1.1 192.168.1.1 1
127.0.0.0 255.255.255.255 On-link 127.0.0.1 331
127.0.0.1 255.255.255.255 On-link 127.0.0.1 331
127.255.255.255 255.255.255.255 On-link 127.255.255.255 331
192.168.0.0 255.255.255.0 On-link 192.168.0.1 1
192.168.0.1 255.255.255.255 On-link 192.168.0.1 1
192.168.50.0 255.255.255.0 On-link 192.168.50.138 281
192.168.50.138 255.255.255.255 On-link 192.168.50.138 281
192.168.50.139 255.255.255.0 On-link 192.168.50.139 281
192.168.50.139 255.255.255.255 On-link 192.168.50.139 281
124.0.0.0 240.0.0.0 On-link 127.0.0.1 331
124.0.0.0 240.0.0.0 On-link 192.168.50.138 281
255.255.255.255 255.255.255.255 On-link 192.168.50.138 281
255.255.255.255 255.255.255.255 On-link 192.168.50.138 281
Route permanenti:
Nessuno
IPv6 Tabella route
=====
Rete Destinazione Gateway Metrica
Interf Metrica Rete Destinazione Gateway
0...00000000000000000000000000000000 On-link
5 281 f#000::/64 On-link
5 281 f#000::1:3d0fc44c8ca#4128 On-link
1 331 f#000::/8 On-link
1 281 f#000::/8 On-link
Route permanenti:
Nessuno
PS C:\Windows\system32>

```

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 -abn.
- The process is a critical system file, likely associated with Windows Kernel operations.

```
C:\Windows\system32> netstat -abn
Connessioni attive
Proto Indirizzo locale Indirizzo esterno Stato PID
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 892
[svchost.exe]
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
Impossibile ottenere informazioni sulla proprietà
TCP 0.0.0.0:5940 0.0.0.0:0 LISTENING 1112
[CDPSvc]
[svchost.exe]
TCP 0.0.0.0:5357 0.0.0.0:0 LISTENING 4
Impossibile ottenere informazioni sulla proprietà
TCP 0.0.0.0:7680 0.0.0.0:0 LISTENING 6976
Impossibile ottenere informazioni sulla proprietà
TCP 0.0.0.0:9964 0.0.0.0:0 LISTENING 672
[svchost.exe]
TCP 0.0.0.0:9965 0.0.0.0:0 LISTENING 520
Impossibile ottenere informazioni sulla proprietà
TCP 0.0.0.0:9966 0.0.0.0:0 LISTENING 732
Eventuale
[svchost.exe]
TCP 0.0.0.0:49867 0.0.0.0:0 LISTENING 411
Scheduale
[svchost.exe]
TCP 0.0.0.0:99668 0.0.0.0:0 LISTENING 1948
[spoolsv.exe]
TCP 0.0.0.0:49669 0.0.0.0:0 LISTENING 2060
PolicyAgent
[svchost.exe]
TCP 0.0.0.0:49670 0.0.0.0:0 LISTENING 656
Impossibile ottenere informazioni sulla proprietà
TCP 192.168.50.138:119 0.0.0.0:0 LISTENING 4
Impossibile ottenere informazioni sulla proprietà
TCP 192.168.50.138:49800 20.199.120.151:443 ESTABLISHED 412
[svchost.exe]
TCP 192.168.50.138:49837 20.199.120.151:443 ESTABLISHED 412
[svchost.exe]
TCP 192.168.50.138:50100 192.168.50.230:9997 TIME_WAIT 0
TCP 192.168.50.138:50101 192.168.50.230:9997 TIME_WAIT 0
TCP 192.168.50.138:50102 192.168.50.230:9997 TIME_WAIT 0
TCP 192.168.50.138:50103 192.168.50.230:9997 TIME_WAIT 0
TCP 192.168.50.138:50104 192.168.50.230:9997 TIME_WAIT 0
TCP 192.168.50.138:50105 192.168.50.230:9997 TIME_WAIT 0
TCP 192.168.50.138:50106 192.168.50.230:9997 TIME_WAIT 0
TCP 192.168.50.138:50107 192.168.50.230:9997 TIME_WAIT 0
TCP 192.168.50.138:50108 192.168.50.230:9997 TIME_WAIT 0
TCP 192.168.50.138:50109 192.168.50.230:9997 TIME_WAIT 0
TCP 192.168.50.138:50110 192.168.50.230:9997 TIME_WAIT 0
TCP 192.168.50.138:50111 52.168.112.67:443 TIME_WAIT 0
TCP 192.168.50.138:50112 52.168.112.67:443 TIME_WAIT 0
TCP 192.168.50.138:50113 52.168.112.67:443 TIME_WAIT 0
TCP 192.168.50.138:50114 52.168.112.67:443 TIME_WAIT 0
TCP 192.168.50.138:50115 13.107.5.88:443 ESTABLISHED 3196
[ntkrnlmp.exe]
TCP 192.168.50.138:50116 2.17.141.225:443 ESTABLISHED 6976
Impossibile ottenere informazioni sulla proprietà
TCP 192.168.50.138:50117 0.0.0.0:0 ESTABLISHED 6976
Impossibile ottenere informazioni sulla proprietà
TCP 192.168.50.138:50118 0.0.0.0:0 ESTABLISHED 6976
Impossibile ottenere informazioni sulla proprietà
TCP 192.168.50.138:50119 2.17.141.49:443 ESTABLISHED 6976
TCP 192.168.50.138:50120 62.115.252.114:88 ESTABLISHED 6976
Impossibile ottenere informazioni sulla proprietà
TCP 192.168.50.138:50121 0.0.0.0:0 ESTABLISHED 6976
Impossibile ottenere informazioni sulla proprietà
TCP 192.168.50.138:50122 15.1.204.66:172.00 TIME_WAIT 0
TCP 192.168.50.138:50123 192.168.50.230:9997 TIME_WAIT 0
TCP 192.168.50.138:50124 62.115.252.114:88 TIME_WAIT 0
TCP 192.168.50.138:50125 62.115.252.48:80 TIME_WAIT 0
TCP 192.168.50.138:50126 62.115.252.114:88 TIME_WAIT 0
TCP 192.168.50.138:50127 62.115.252.114:88 TIME_WAIT 0
TCP 192.168.50.138:50128 62.115.252.114:88 TIME_WAIT 0
TCP 192.168.50.138:50129 62.115.252.114:88 TIME_WAIT 0
TCP 192.168.50.138:50130 62.115.252.114:88 TIME_WAIT 0
TCP 192.168.50.138:50131 62.115.252.48:80 TIME_WAIT 0
TCP 192.168.50.138:50132 151.191.86.172:80 TIME_WAIT 0
TCP 192.168.50.138:50133 151.191.86.172:80 TIME_WAIT 0
TCP 192.168.50.138:50134 20.42.73.28:443 TIME_WAIT 0
TCP 192.168.50.138:50135 20.42.73.28:443 TIME_WAIT 0
TCP 192.168.50.138:50136 20.42.73.28:443 TIME_WAIT 0
TCP 192.168.50.138:50137 20.42.73.28:443 TIME_WAIT 0
TCP 192.168.50.138:50138 20.42.73.28:443 TIME_WAIT 0
TCP 192.168.50.138:50139 13.107.5.88:443 TIME_WAIT 0
TCP 192.168.50.138:50140 13.107.5.88:443 TIME_WAIT 0
TCP 192.168.50.138:50141 2.18.32.45:443 ESTABLISHED 6976
```

Nome utente	CPU	Memoria (...	Virtuallizzata...
SYSTEM	00	5.216 K	Non consentito
SERVIZIO	00	5.264 K	Non consentito
SYSTEM	03	71.904 K	Non consentito
SERVIZIO	02	40.160 K	Non consentito
SERVIZIO	00	4.472 K	Non consentito
SYSTEM	00	11.996 K	Non consentito
SERVIZIO	02	64.384 K	Non consentito
SYSTEM	00	5.396 K	Non consentito
SERVIZIO	00	1.832 K	Non consentito
SYSTEM	03	3.000 K	Non consentito
SERVIZIO	00	1.960 K	Non consentito
SERVIZIO	00	736 K	Non consentito
SYSTEM	00	1.248 K	Non consentito
SYSTEM	00	24.240 K	Non consentito
SERVIZIO	00	5.696 K	Non consentito
SERVIZIO	00	808 K	Non consentito
SYSTEM	43	15.332 K	Non consentito
SERVIZIO	00	602 K	Non consentito
SERVIZIO	00	1.168 K	Non consentito
User	00	7.792 K	Disabilitato
User	00	1.644 K	Disabilitato
SYSTEM	01	12.576 K	Non consentito
SERVIZIO	00	4.764 K	Non consentito
SERVIZIO	00	1.472 K	Non consentito
SYSTEM	00	459 K	Non consentito
SYSTEM	00	672 K	Non consentito
SERVIZIO	00	2.844 K	Non consentito
SYSTEM	00	1.740 K	Non consentito
SYSTEM	02	20 K	
SYSTEM	00	1.796 K	Non consentito
User	00	2.596 K	Disabilitato
User	00	1.912 K	Disabilitato
User	03	18.664 K	Non consentito
User	01	2.820 K	Disabilitato
SYSTEM	34	15.176 K	Non consentito
SYSTEM	00	1.452 K	Non consentito
SYSTEM	00	1.120 K	Non consentito
User	00	1.268 K	Disabilitato
SYSTEM	00	700 K	Non consentito
SYSTEM	00	1.164 K	Non consentito
SERVIZIO	00	1.108 K	Non consentito
SERVIZIO	00	5.536 K	Non consentito

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.

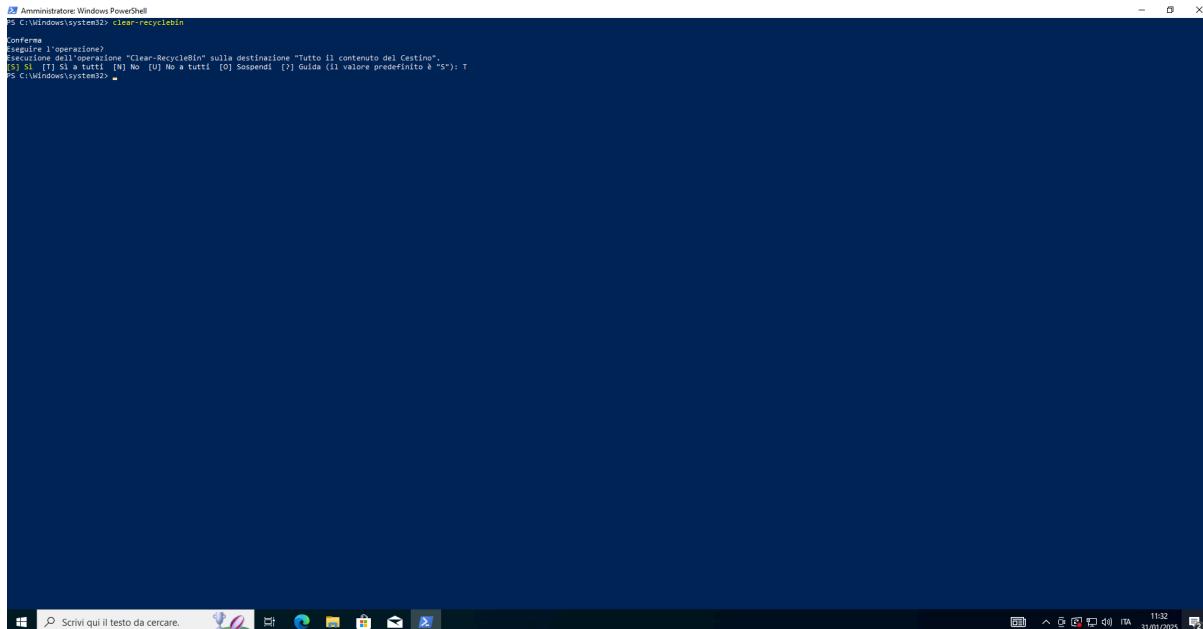
- a. Open the Recycle Bin. Verify that there are items that can be deleted permanently from your PC. If not, restore those files.
- b. If there are no files in the Recycle Bin, create a few files, such as text file using Notepad, and place them into the Recycle Bin.
- c. In a PowerShell console, enter 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.



```
PS C:\Windows\system32> clear-recyclebin
Conferma l'operazione
Eseguire l'operazione "Clear-RecycleBin" sulla destinazione "Tutto il contenuto del Cestino".
[S] Si [T] Si a tutti [N] No [U] No a tutti [O] Sospendi [?] Guida ([i] valore predefinito è "S"): T
PS C:\Windows\system32>
```

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

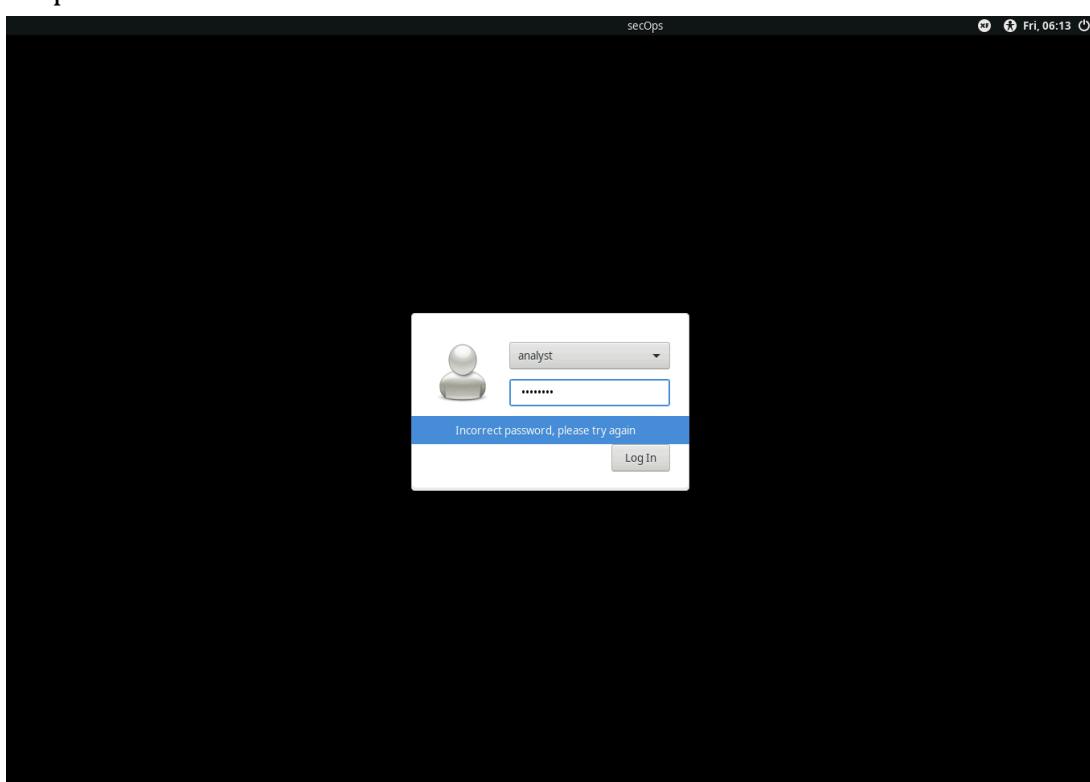
In this part, you will use tcpdump to capture the content of HTTP traffic. You will use command options to save the traffic to a packet capture (pcap) file. These records can then be analyzed using different applications that read pcap files, including Wireshark.

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.

- Open a terminal application and enter the command ip address.
- List the interfaces and their IP addresses displayed in the ip address output.
- 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.

- 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.

- Enter a username of Admin with a password of Admin and click Login.
- Close the web browser.
- Return to the terminal window where tcpdump is running. Enter CTRL+C to stop the packet capture.

```
analyst@secOps ~]$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 127.255.255.255 scope host lo
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:05:id:1a brd ff:ff:ff:ff:ff:ff
    inet 192.168.60.227/24 brd 192.168.60.255 scope global dynamic enp0s3
        valid_lft 86400sec preferred_lft 86400sec
    inet 192.168.60.227/24 brd 192.168.60.255 scope link
        valid_lft forever preferred_lft forever
analyst@secOps ~]$
```

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

```

01 110 101 011 010101 101 010111 01 110 101 011 010101 101 010111

Altoro Mutual - Mozilla Firefox 06:21 analyst

Altoro Mutual

www.altoromutual.com/login.jsp

Sign In | Contact Us | Feedback | Search | Go

DEMO SITE ONLY

AltoroMutual

ONLINE BANKING LOGIN

PERSONAL

- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SIMPLY BUSINESS

- Deposit Products
- Lending Services
- Cards
- Insurance
- Business
- Other Services

INSIDE ALTORO MUTUAL

- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

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 Altoroj 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.



```
analyst@secOps: ~$ sudo tcpdump -i enp0s3 -w 0 -u httpdump.pcap
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
4380 packets captured
4380 packets received by filter
4380 packets discarded by kernel
analyst@secOps: ~$
```

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.

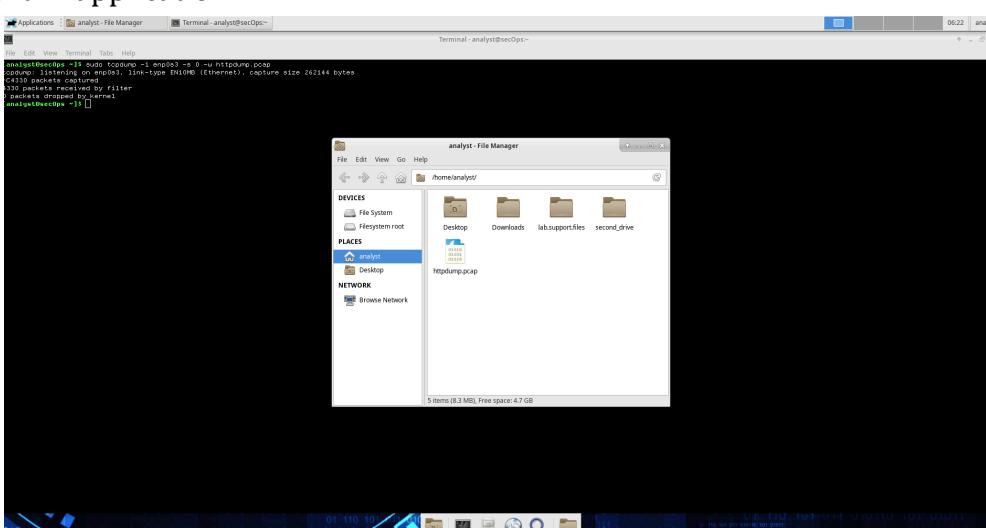
d. In the lower window, the message is displayed. Expand the HTML Form URL Encoded: application/x-www-form-urlencoded section.

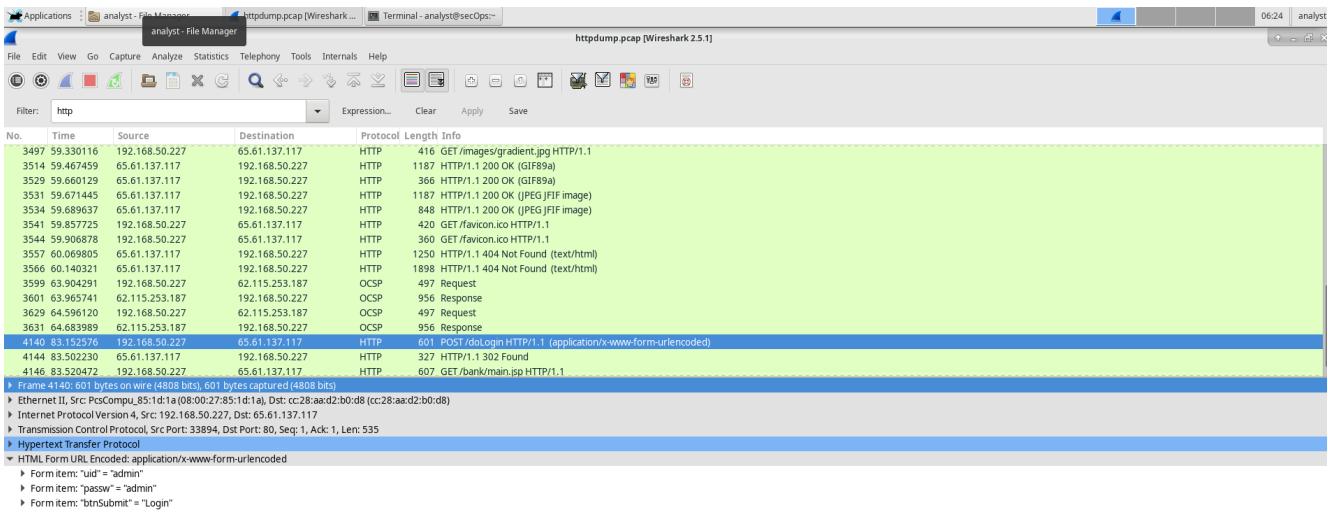
What two pieces of information are displayed?

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.





0000	xx:28:aa:d2:b0:d8 08:00:27:85:1d:1a	...:....E
0010	02:4b:83:59:40:00 00:40:06:17:15:0a	a8:32:e3:41:3d:K.Y@.2.A=
0020	09:75:84:00:00:50	ed:0d:29:f1:a9:b7:88:80:18:u.f.P.
0030	00:5e:cd:76:00:00:01:01:08:0a:4d:9e:47:39:0d:b6:4t:....G9:	

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.

This 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.

```
[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
```

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.



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](#)

```
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
[1]+  Stopped                  sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap
analyst@secOps:~$
```

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.

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

- Browse through the different HTTPS messages and select an Application Data message.
- In the lower window, the message is displayed.

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

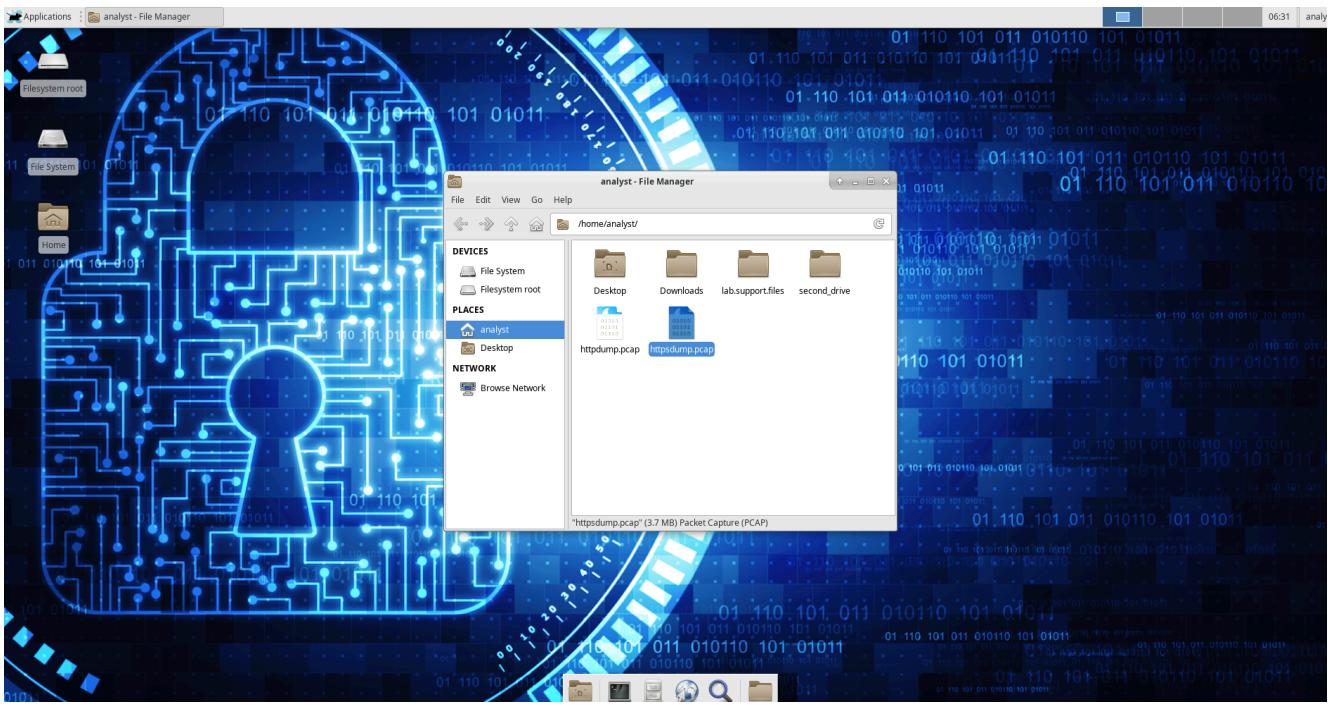
The TLSv1.2 protocol has replaced the previous HTTP traffic. Instead of seeing plaintext HTTP requests and responses, we now see encrypted Application Data packets in the capture.

- Completely expand the Secure Sockets Layer section.
- 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.

- Close all windows and shut down the virtual machine.



Applications analyst - File Manager httpsdump.pcap [Wireshark...]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp.port==443 Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
4132	258.952860	34.120.208.123	192.168.50.227	TCP	66	443 -> 44194 [ACK] Seq=3509 Ack=716 Win=64768 Len=0 TSval=1882754243 TSerr=3048317619
4133	259.064991	34.120.208.123	192.168.50.227	TLSv1.2	112	Application Data
4134	259.065187	192.168.50.227	34.120.208.123	TCP	2762	44194 -> 443 [ACK] Seq=716 Ack=3555 Win=37760 Len=2696 TSval=3048317837 TSerr=1882754354 TCP segment of a reassembled PDU
4135	259.065238	192.168.50.227	34.120.208.123	TCP	2762	44194 -> 443 [ACK] Seq=3412 Ack=3555 Win=37760 Len=2696 TSval=3048317837 TSerr=1882754354 TCP segment of a reassembled PDU
4136	259.065609	192.168.50.227	34.120.208.123	TLSv1.2	456	Application Data
4137	259.122395	34.120.208.123	192.168.50.227	TCP	66	443 -> 44194 [ACK] Seq=3555 Ack=2064 Win=64256 Len=0 TSval=1882754414 TSerr=3048317837
4138	259.122413	34.120.208.123	192.168.50.227	TCP	66	443 -> 44194 [ACK] Seq=3555 Ack=3412 Win=64256 Len=0 TSval=1882754414 TSerr=3048317837
4139	259.124339	34.120.208.123	192.168.50.227	TCP	66	443 -> 44194 [ACK] Seq=3555 Ack=4760 Win=64256 Len=0 TSval=1882754415 TSerr=3048317837
4140	259.124349	34.120.208.123	192.168.50.227	TCP	66	443 -> 44194 [ACK] Seq=3555 Ack=6498 Win=64256 Len=0 TSval=1882754416 TSerr=3048317837
4141	259.124349	34.120.208.123	192.168.50.227	TCP	66	443 -> 44194 [ACK] Seq=3555 Ack=6498 Win=64256 Len=0 TSval=1882754416 TSerr=3048317837
4144	259.348772	34.120.208.123	192.168.50.227	TLSv1.2	730	Application Data
4145	259.348999	192.168.50.227	34.120.208.123	TLSv1.2	89	Encrypted Alert
4146	259.349964	192.168.50.227	34.120.208.123	TCP	66	44194 -> 443 [FIN, ACK] Seq=6521 Ack=4219 Win=40448 Len=0 TSval=3048318121 TSerr=1882754639
4147	259.408876	34.120.208.123	192.168.50.227	TCP	66	443 -> 44194 [ACK] Seq=4719 Ack=6521 Win=40448 Len=0 TSval=1882754639 TSerr=3048318120
4148	259.414873	34.120.208.123	192.168.50.227	TCP	66	443 -> 44194 [FIN, ACK] Seq=4219 Ack=6522 Win=40456 Len=0 TSval=1882754639 TSerr=3048318121
4149	259.414949	192.168.50.227	34.120.208.123	TCP	66	44194 -> 443 [ACK] Seq=6522 Ack=4220 Win=40448 Len=0 TSval=3048318186 TSerr=1882754706

Frame 4144: 730 bytes on wire (5840 bits), 730 bytes captured (5840 bits)
Ethernet II, Src: CC:28:AA:D2:B0:D8 (cc:28:aa:d2:b0:d8), Dst: PCoCompu_85-1d:1a (08:00:27:85:1d:1a)
Internet Protocol Version 4, Src: 34.120.208.123, Dst: 192.168.50.227
Transmission Control Protocol, Src Port: 443, Dst Port: 44194, Seq: 3555, Ack: 6498, Len: 664
Secure Sockets Layer
TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
Content-Type: Application Data (23)
Version: TLS 1.2 (0x0303)
Length: 659
Encrypted Application Data: 011a50f6bbffab5fb92e768bd25849bfd3f53e85c46e5...



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.