

Net Raiders

BUILD WEEK 1

PROGETTAZIONE MODELLO DI RETE

PENTESTING THETA



OGNI ATTACCO HACKER COSTA IN MEDIA ALL'AZIENDA **3,7 MILIONI DI EURO**



Secondo l'edizione 2022 del “Cost of a data breach report” di Ibm, in Italia, nel 2022 il costo medio di un cyberattacco è stato di 3,7 milioni di euro.

Da anni, ormai, il conto sale: nel 2021 era di 100.000 euro in meno. Il motivo è presto detto: privati e (soprattutto) imprese stanno digitalizzando una porzione sempre più ampia delle proprie attività. Si tratta di un processo necessario, che porta – senza dubbio – enormi vantaggi, ma espone a nuovi rischi.

Per questo motivo i Netraiders si impegnano a mantenere il web un posto più sicuro, per tutti e soprattutto per le aziende per cui lavoriamo. Oggi è la volta dell'azienda Theta.





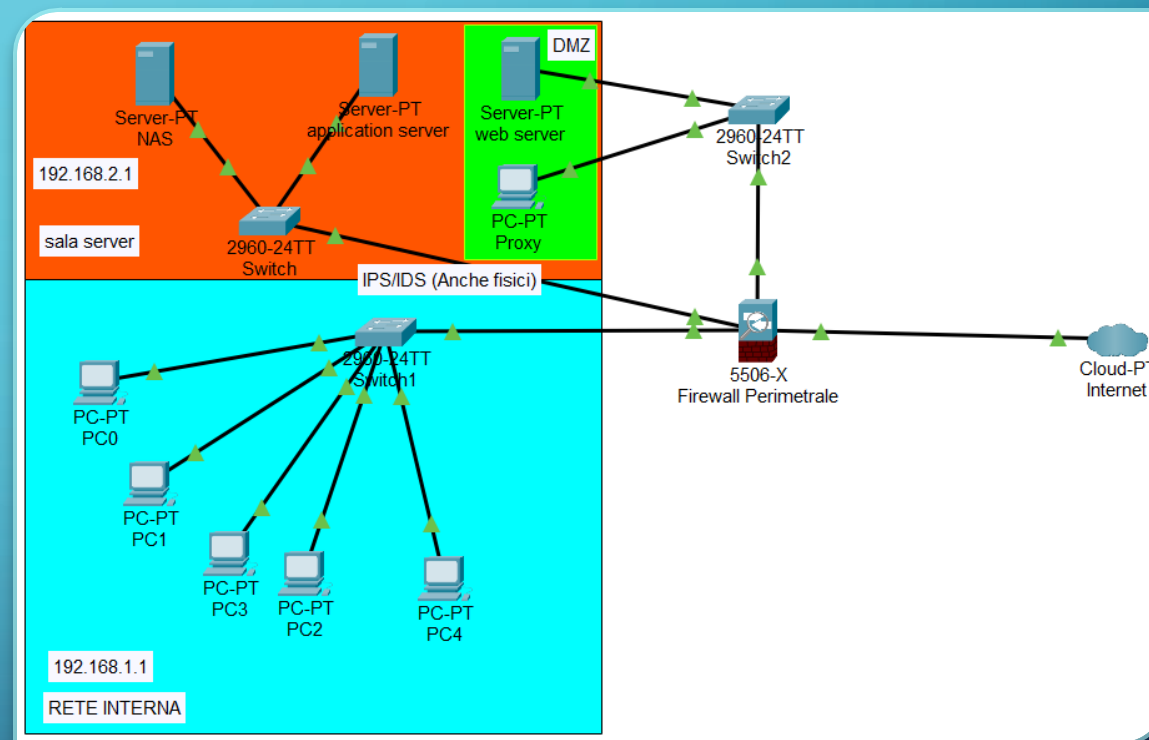
A cartoon illustration depicting a choice between two paths. In the foreground, a person with brown hair, wearing a blue shirt and dark shorts, stands at the start of a dirt path that splits into two. The path is flanked by green grass with some grey rocks. In the center of the fork, there is a wooden signpost with two arrows pointing in opposite directions. The left path leads up a hill to a bright, sunny sky where a large, white castle with blue roofs sits atop a rocky cliff. The right path leads up a hill to a dark, stormy sky with purple lightning bolts, where a dark, gothic-style castle sits atop a rocky cliff. The overall scene is a metaphor for choosing between investing in cybersecurity and not doing so.

**AZIENDA CHE INVESTE
IN CYBERSECURITY**

**AZIENDA CHE
NON LO FA**

THETA – DESIGN DI RETE

- FIREWALL PERIMETRALE
- DMZ
- IPS/IDS (anche fisico, installando un modulo di accesso fingerprint e porta blindata alla sala server)
- MFA per accesso application server
- Computer PROXY per maggiore sicurezza sul web
- DHCP



PREVENTIVO DESIGN DI RETE



Preventivo NetRaiders per Theta

	Quantità / ore	Costo unitario	Costo totale
Requisiti			
Firewall (Cisco ASA 5506-K9)		€ 1.500,00	€ 1.500,00
PC Desktop a scopo di proxy		€ 1.200,00	€ 1.200,00
Cablaggio Ethernet CAT7, misurato in metri	1000	€ 1,50	€ 1.500,00
Modulo accesso biometrico (fingerprint) per Sala Server		€ 500,00	€ 500,00
Porta blindata per Sala Server		€ 4.000,00	€ 4.000,00
Manodopera, comprende IVA			
Sopralluogo e progettazione, pentest, architettura di rete	230	€ 50,00	€ 11.500,00
Configurazione Firewall	12	€ 50,00	€ 600,00
Installazione accesso biometrico e porta blindata	4	€ 50,00	€ 200,00
Manodopera operai per installazioni	16	€ 50,00	€ 800,00
Prezzo totale del preventivo			€ 21.800,00
			€ 21.500,00
include assistenza ordinaria post-vendita			Gratuita
Annuale, 2 anni			
Eventuali optional			
Corso sicurezza informatica anti-phishing per N° dipendenti	30	€ 100,00	€ 3.000,00
Servizio VPN, piano annuale , N° dipendenti	30	€ 240,00	€ 7.200,00
Configurazione VPN	8	€ 50,00	€ 400,00
Assistenza straordinaria			
Giornaliero, Feriale, in loco, dalle 8 alle 20		€ 100,00	€ 100,00
Assistenza straordinaria, festiva/notturna			
Giornaliero, Festivo, in loco, dalle 8 alle 20		€ 200,00	€ 200,00

PENTESTING



- **Vulnerability Scanner:** verifica delle porte aperte nel web server, in cerca di criticità.
- **HTTP methods:** verifica dei vari verbi HTTP utilizzati nell'application Server
- **Bruteforce:** Verifica della robustezza di login nelle varie interfacce dell'application server (PhpMyAdmin, DVWA, DVWA/Vulnerabilities)

Net Raiders 

VULNERABILITY SCANNER

```
scan host 192.168.50.101 dalla porta 0 alla porta 65535 terminata.
```

```
Riepilogo porte aperte:
```

```
21 ( ftp ), 22 ( ssh ), 23 ( telnet ), 25 ( smtp ), 53 ( domain ), 80 ( http ), 111 ( sunrpc ), 139 ( netbios-ssn ), 445 ( microsoft-ds ), 512 ( exec ),  
513 ( login ), 514 ( shell ), 1099 ( rmiregistry ), 1524 ( ingreslock ), 2049 ( nfs ), 2121 ( iprop ), 3306 ( mysql ), 3632 ( distcc ), 5432 ( postgresql  
) , 5900, 6000 ( x11 ), 6667 ( ircd ), 6697 ( ircs-u ), 8009, 8180, 8787, 33733, 37758, 52633, 60906
```

Dal test effettuato possiamo notare alcune criticità riguardo determinate porte aperte.

- Porta 23 Telnet: si tratta di un servizio di comunicazione remota ormai obsoleto, che invia le informazioni e le riceve senza utilizzare la crittografia, per questo motivo è molto esposto a qualsiasi tipo di minaccia. Da rimpiazzare almeno con la porta 22, SSH, avente crittografia end to end e autenticazione sicura.
- Se possibile, rimpiazzare la porta 80 HTTP con la 443 HTTPS, per rendere la navigazione più sicura.
- In generale, porre particolare attenzione a tutte le porte che non offrono una connessione criptata/sicura

METODI HTTP

Dalla verifica dei metodi HTTP usati, si può notare che in ogni pagina scansionata, non ci sono metodi HTTP abilitati. Lo status è 200, quindi la pagina funziona. Probabilmente ciò è dovuto dal fatto che siamo di fronte a una pagina statica: se la pagina è statica e non richiede alcuna interazione dinamica con il server, e quindi potrebbe non richiedere l'uso di metodi HTTP. In questo caso, il server potrebbe semplicemente restituire il contenuto della pagina senza necessità di ulteriori azioni.



```
(kali㉿kali)-[~/Desktop/progetto]
$ python http_methods.py
Inserire Host/IP del sistema target: 192.168.50.101
Inserire la porta del sistema target (default: 80):
Inserire path da controllare (default /):
http://192.168.50.101:80/
Lo status e' : 200
I metodi abilitati sono: None
```

```
(kali㉿kali)-[~/Desktop/progetto]
$ python http_methods.py
Inserire Host/IP del sistema target: 192.168.50.101
Inserire la porta del sistema target (default: 80):
Inserire path da controllare (default /): /phpMyAdmin/
http://192.168.50.101:80/phpMyAdmin/
Lo status e' : 200
I metodi abilitati sono: None
```

```
(kali㉿kali)-[~/Desktop/progetto]
$ python http_methods.py
Inserire Host/IP del sistema target: 192.168.50.101
Inserire la porta del sistema target (default: 80):
Inserire path da controllare (default /): /dvwa/
http://192.168.50.101:80/dvwa/
Lo status e' : 200
I metodi abilitati sono: None
```

```
(kali㉿kali)-[~/Desktop/progetto]
$ python http_methods.py
Inserire Host/IP del sistema target: 192.168.50.101
Inserire la porta del sistema target (default: 80):
Inserire path da controllare (default /): /dvwa/vulnerabilities/brute/
http://192.168.50.101:80/dvwa/vulnerabilities/brute/
Lo status e' : 200
I metodi abilitati sono: None
```




BRUTEFORCE PHPMYADMIN

Grazie allo script creato, abbiamo forzato username e password di phpMyAdmin in maniera piuttosto veloce, in quanto il sito non era protetto da password. Consigliamo **CATEGORICAMENTE** l'utilizzo di password lunghe e di difficile individuazione.

```
(kali㉿kali)-[~/Desktop/progetto/bruteforce]
guest -

Log in!

user: guest
password:

PWNED BY

/ $$ / $$ / $$$$$$ / $$$$$$ / $$$$$$ / $$$$$$ / $$$$$$ / $$$$$$ / $$$$$$ / $$$$$$ / $$$$$$ / $$$$$$ /
| $$$ | $$ | $$_ / | $$_ / | $$_ $$_ / $$_ $$_ | $$_ / | $$_ $$_ | $$_ / | $$_ $$_ / $$_ $$_ /
| $$$$ | $$ | $$$ / | $$$ / | $$$ \ $$$ / $$$ \ $$$ | $$$ | $$$ \ $$$ | $$$ \ $$$ | $$$ \ $$$ /
| $$ $$ $$_ / $$$$ | $$$ | $$$$$$ / $$$$$$ | $$$ | $$$ | $$$ | $$$ | $$$$$$ / $$$$$$ /
| $$ $$$$ | $$_ / | $$$ | $$_ $$$ | $$_ $$$ | $$$ | $$$ | $$$ | $$$ | $$$ | $$$ | $$$ | $$$ | $$$ |
| $$$ \ $$$ | $$$ / | $$$ | $$$ \ $$$ | $$$ | $$$ | $$$ | $$$ | $$$ | $$$ | $$$ | $$$ | $$$ | $$$ |
| $$$ \ $$$ | $$$ / | $$$ | $$$ | $$$ | $$$ / $$$$$$ | $$$$$$ / $$$$$$ | $$$ | $$$ | $$$ /
```



BRUTEFORCE DVWA

Per quanto riguarda la vulnerabilità di DVWA, siamo riusciti ad individuare sia l'username che la password. In aggiunta, abbiamo individuato anche il PHPSESSID, ossia un cookie che ci permette di effettuare il bruteforce all'interno del sito, una volta entrati. Anche per questo login si consiglia un cambio **CATEGORICO** almeno della password.

```

—(kali㉿kali)-[~/Desktop/progetto/bruteforce]
guest - westwood
admin - password

Log in!
username: admin
password: password

PHPSESSID:
dfe7c6ab484b3db73226c58002720db0

PWNED BY

/$$ /$$ /$$$$$$$$ /$$$$$$$$ /$$$$$$$ /$$$$$$$ /$$$$$$$ /$$$$$$$ /$$$$$$$ /$$$$$$$ /$$$$$$$
| $$$ |$$| $$ _____/|_ $$ _/| $$ _ $$ /$$ _$$|_ $$ _/| $$ _ $$| $$ _____/| $$ _ $$ /$$ _$$
| $$$| $$| $$ | $$ \ $$| $$ \ $$| $$ \ $$| $$ \ $$| $$ \ $$| $$ \ $$| $$ \ $$| $$ \ $$|
| $$ $$ $| $$$$ | $$ | $$$$$$/| $$$$$$/| $$ | $$ | $$ | $$| $$$$ | $$$$$$/| $$$$$$/
| $$ $$$$| $$ _/| $$ | $$ _ $$| $$ _ $$| $$ | $$ | $$ | $$| $$ _/| $$ _ $$ \ _____ $$
| $$\ $$$$| $$ | $$ | $$ \ $$| $$ _ $$| $$ | $$ | $$ | $$| $$ \ $$ /$$ \ $$
| $$ \ $$| $$$$$$ | $$ | $$ | $$| $$ | $$ /$$$$$| $$$$$$/| $$$$$$/| $$ | $$| $$$$$$/
| _/ \_/| _____/ | _/ | _/ | _/ | _/ | _/ | _/ | _/ | _/ \ _____/

```

A decorative graphic consisting of white circuit-like lines and circles on a blue background, positioned on the right side of the page.

[illegible]

Fig.1

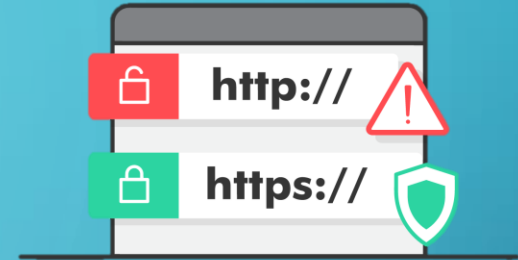
```
Cookie = {
    "PHPSESSID": sessid,
    "security": 'low'
}
```

Fig.2





BULLET POINTS



- MFA (Multi Factor Authenticator): Limiterebbe l'accesso ai soli dipendenti, grazie magari ad un app dedicata di authenticator, per evitare l'intrusione di malintenzionati.
- Corso di sicurezza informatica (almeno livello base) per tutti i dipendenti dell'azienda.
- Uso di Password con almeno 8 caratteri, una lettera maiuscola, un numero e un carattere speciale (es: '!'). Questo renderebbe la password di difficile individuazione.
- Cambio password periodico ogni 3 mesi con password completamente diversa dalla precedente
- Chiusura porte inutilizzate più vulnerabili, ad esempio l'obsoleta porta 23 Telnet
- Utilizzo connessioni sicure/cryptate
- Modifica parametri di sicurezza all'interno del sito, per renderlo effettivamente più sicuro ed impenetrabile

The background is a complex digital interface. At the top center is a large circular window showing a server room with blue-lit racks. Surrounding this are various icons: a shield, a monitor, a person, a gear, and others, all connected by a network of thin lines. A large, dark, semi-transparent rectangle is centered over the image, containing the text.

**DOMANDE, DUBBI,
PERPLESSITA'?**