

EVILCORP
IF IT WORKS DONT TOUCH IT

REPORT

BY EVILCORP

Scritto da: Andrea Di Benedetto

Graphic Designer: Lorenzo Franchi

Direttore Tecnico: Samuele Aversa

Approvato da: Mario Reitano

Giugno 2024

INDICE S9

L0	0
Chi siamo	1
Missione e Visione Aziendale	2
Team Group	3
Regole di Ingaggio	4
I Nostri Prezzi	5
L1	6
Introduzione	7
Obiettivo	8
Configurazione VM	9
V.A. con Firewall Disattivato	10
V.A. con Firewall Attivato	11
Conclusioni	12
L2	
Obiettivo	13
Glossario.....	14
Analisi Formula.....	15
Casistica Incendio.....	16
Casistica Terremoto	17
Casistica Inondazione	18
Conclusioni	19



Chi siamo

Nome Azienda: EvilCorp
Settore: Amministrazione

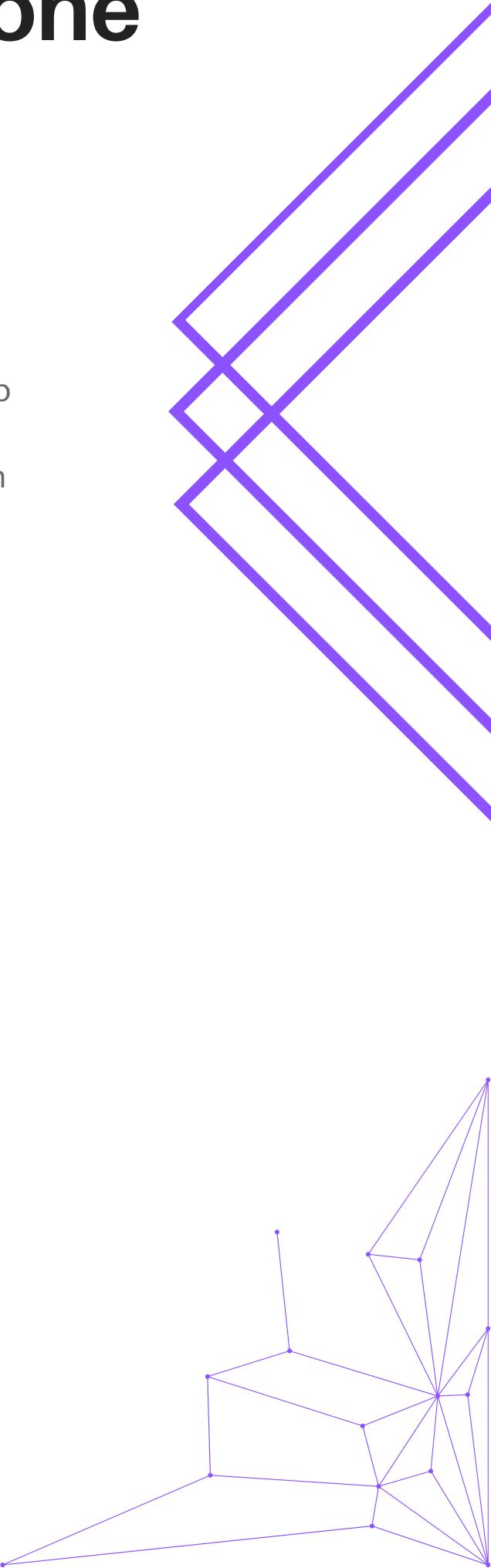
Descrizione dell'Azienda

EvilCorp è un'azienda immaginaria che si occupa di amministrazione. EvilCorp fornisce servizi di amministrazione per altre aziende, gestendo dati sensibili e informazioni riservate. La sicurezza delle loro reti e dei loro dati è cruciale per mantenere la fiducia dei loro clienti e rispettare le normative.



Missione e visione aziendale

Come parte del nostro impegno per garantire la sicurezza informatica, EvilCorp ha incaricato un team di pentester di eseguire un Vulnerability Assessment e un Penetration Testing della rete aziendale. Questo report descrive il processo e le regole di ingaggio, nonché una bozza dei costi operativi.



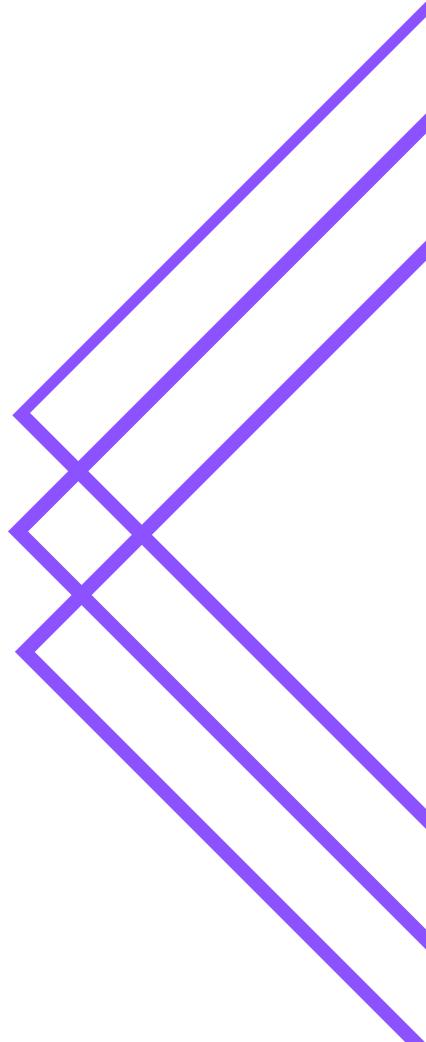
Regole di ingaggio

Le regole di ingaggio definiscono i limiti e le aspettative del nostro lavoro di pentesting. Di seguito sono riportate le regole stabilite per questo incarico:

- 1. Autorizzazione:** EvilCorp ha fornito l'autorizzazione scritta per eseguire la scansione e i test di penetrazione sulla loro rete.
- 2. Scopo del Test:** Le scansioni verranno effettuate solo sugli indirizzi IP forniti dall'azienda.
- 3. Preventivo:** Viene stilato un preventivo del lavoro completo.
- 4. Perimetro d'azione:** Si determina l'area della rete aziendale su cui effettuare i test.
- 5. Ore di Lavoro:** Il team lavorerà dalle 9:00 alle 17:00, dal lunedì al venerdì.
- 6. Impatto sul Sistema:** I test saranno condotti in modo da minimizzare qualsiasi impatto sui sistemi di produzione.
- 7. Riservatezza:** Tutte le informazioni raccolte durante il test saranno mantenute riservate e utilizzate solo ai fini del test.
- 8. Strumenti:** Si presentano gli strumenti utilizzati dai pentester per effettuare l'analisi di rete.

Team Group

Siamo un piccolo team di quattro professionisti, ognuno con una solida esperienza nel campo della cybersecurity. La nostra combinazione di competenze specifiche ci permette di affrontare efficacemente le sfide del settore, assicurando soluzioni innovative e sicure per proteggere al meglio i nostri sistemi e dati.



REFERENCE LINKEDIN

Cliccando sui nostri nomi sarete reindirizzati sulle nostre pagine linkedin



[Andrea
Di Benedetto](#)



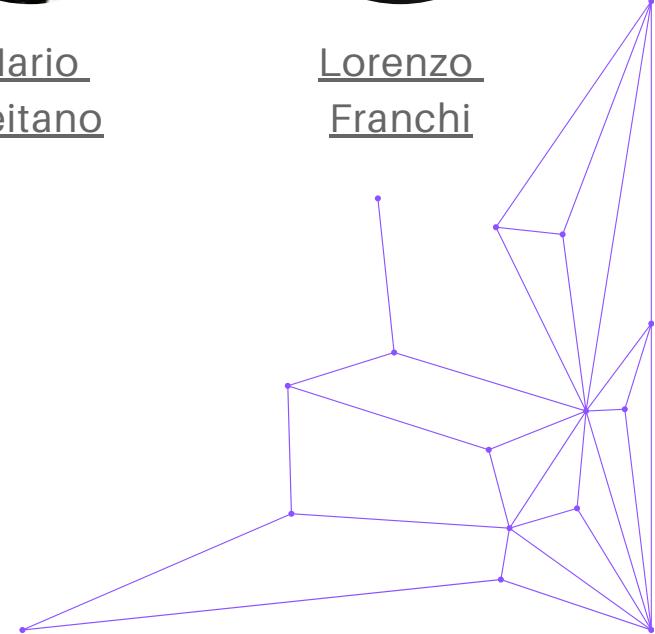
[Samuele
Aversa](#)



[Mario
Reitano](#)



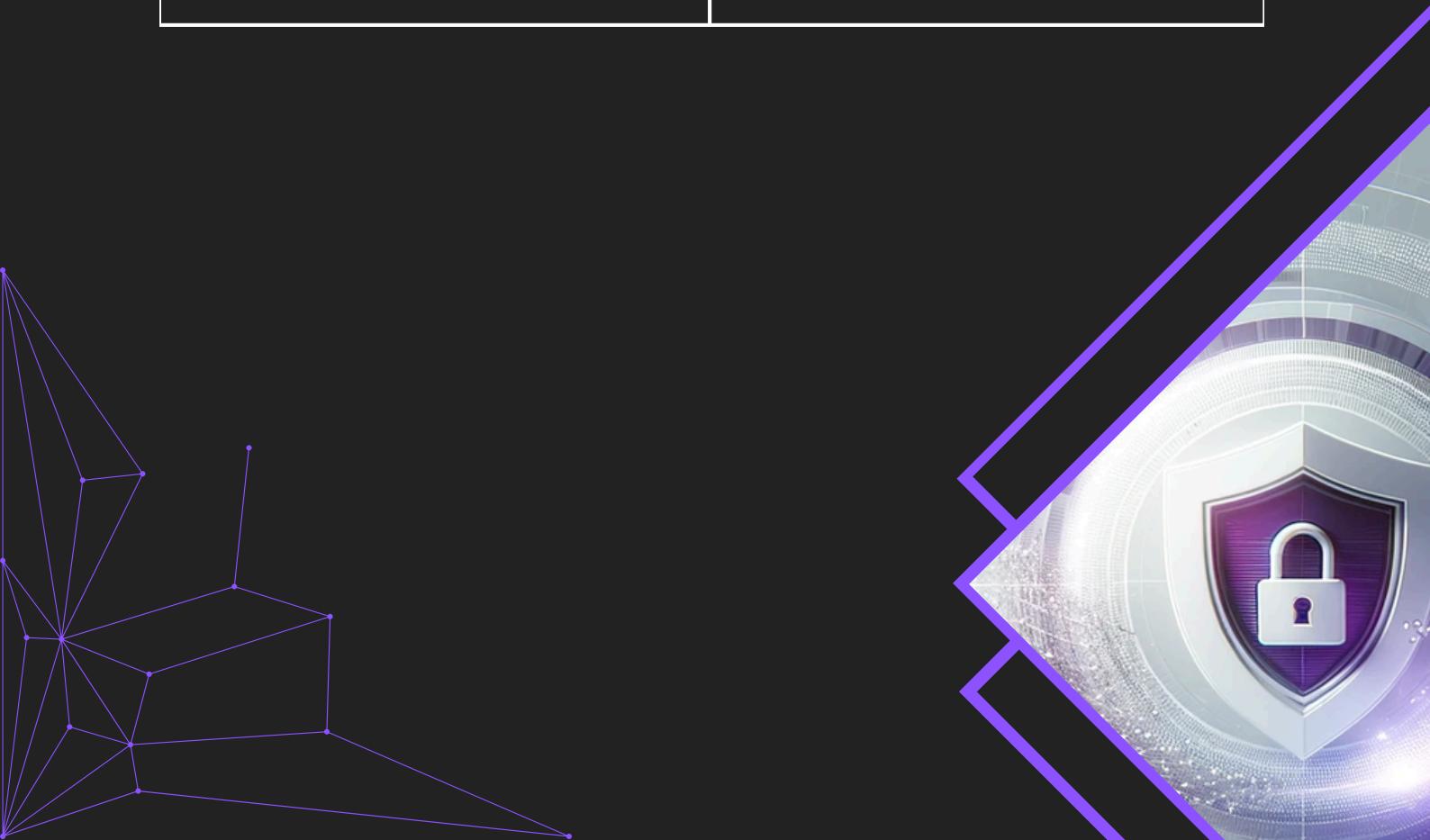
[Lorenzo
Franchi](#)



I Nostri Prezzi

Budget stimato per il progetto

Analisi Vulnerabilità	32.000 €
work	work
in	in
progress	progress

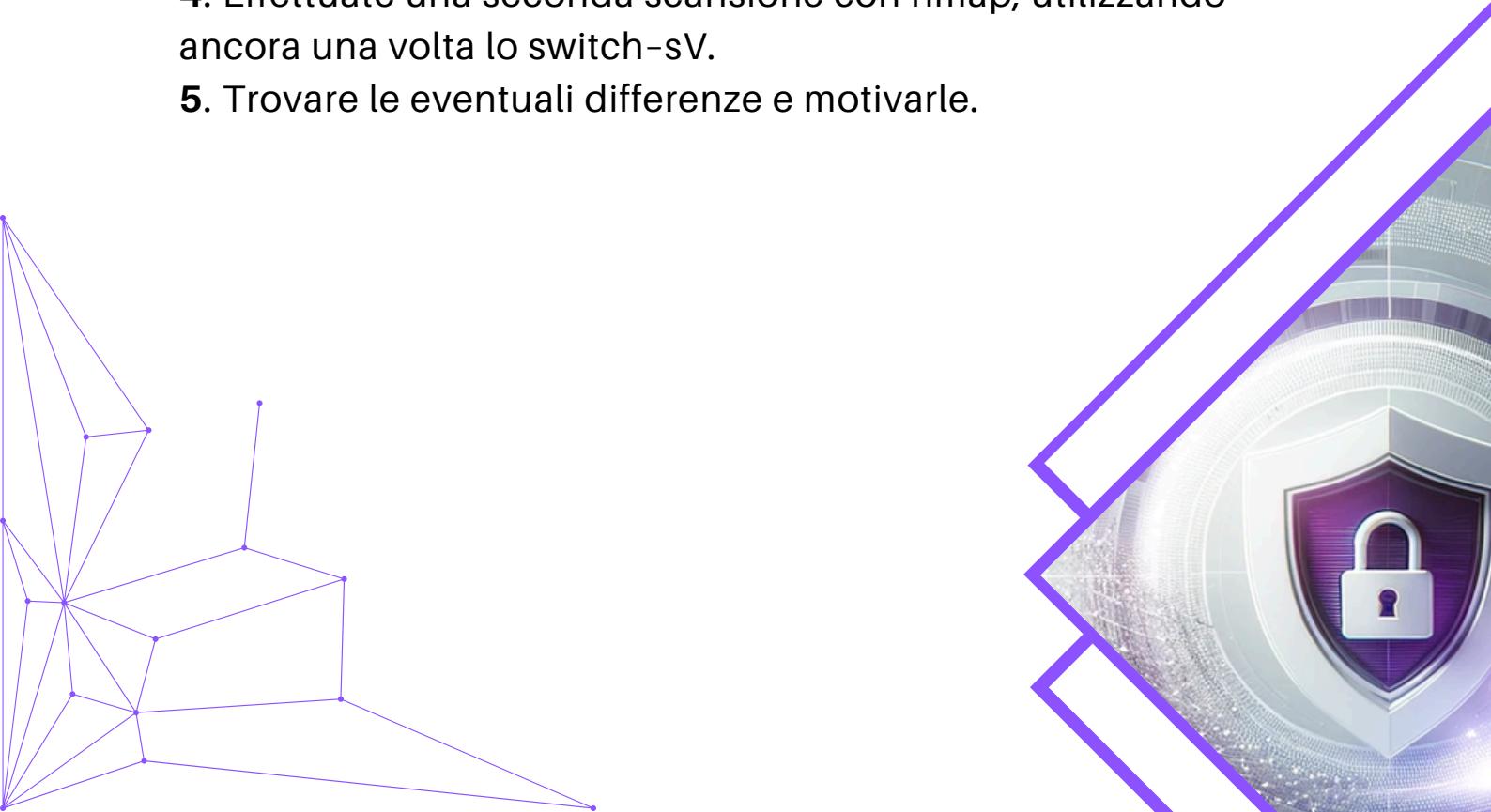


L1

Durante la lezione teorica, abbiamo studiato le azioni preventive per ridurre la possibilità di attacchi provenienti dall'esterno. Abbiamo visto che a livello di rete, possiamo attivare / configurare Firewall e regole per fare in modo che un determinato traffico, potenzialmente dannoso, venga bloccato. La macchina Windows XP che abbiamo utilizzato ha di default il Firewall disabilitato.

L'esercizio di oggi è verificare in che modo l'attivazione del Firewall impatta il risultato di una scansione dei servizi dall'esterno. Per questo motivo:

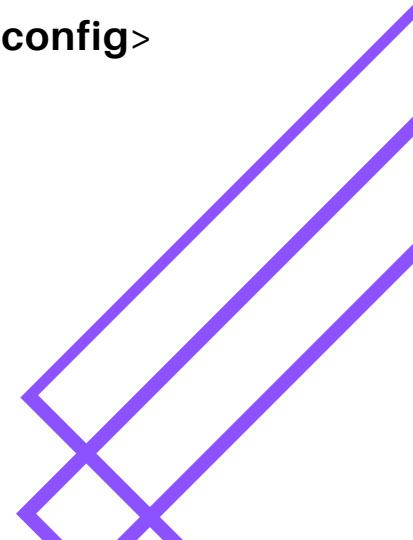
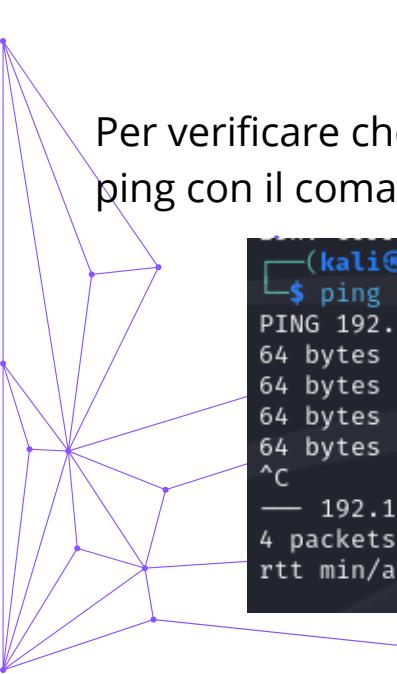
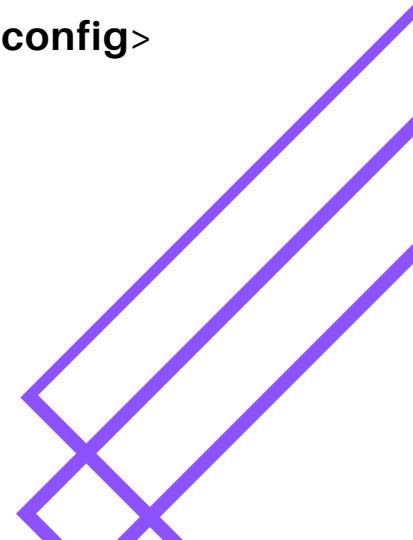
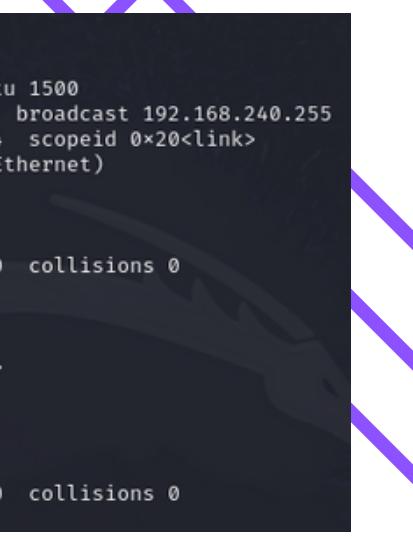
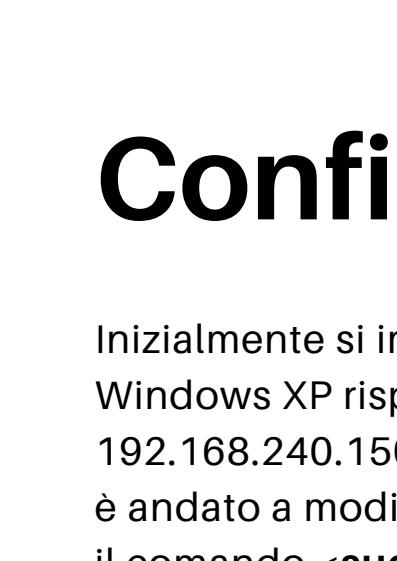
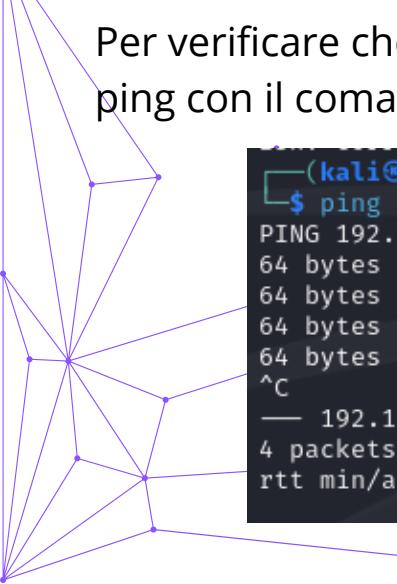
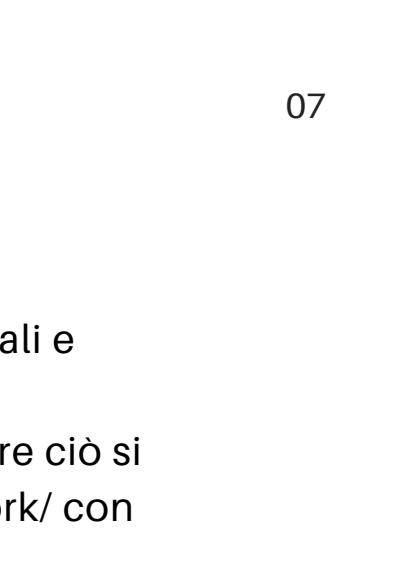
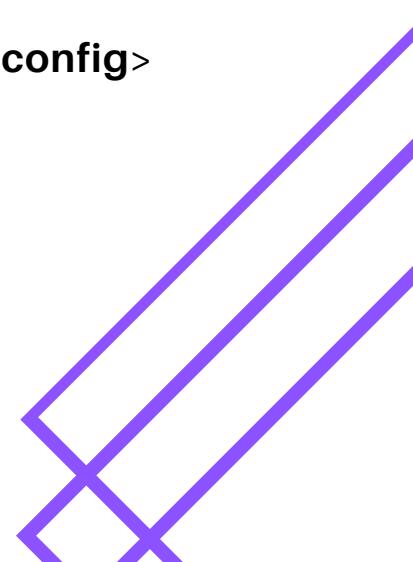
- 1.** Assicuratevi che il Firewall sia disattivato sulla macchina Windows XP
- 2.** Effettuate una scansione con nmap sulla macchina target (utilizzate lo switch-sV, per la service detection e -o nomefilereport per salvare in un file l'output)
- 3.** Abilitare il Firewall sulla macchina Windows XP
- 4.** Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch-sV.
- 5.** Trovare le eventuali differenze e motivarle.

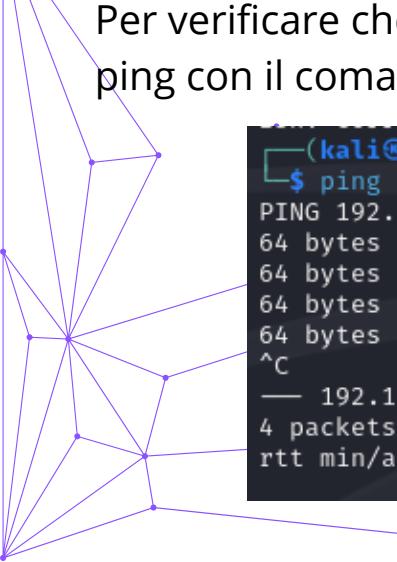
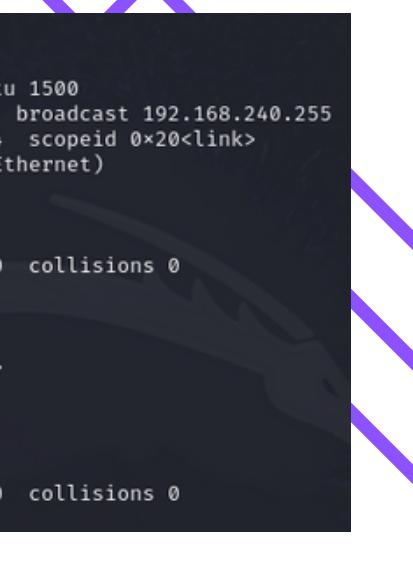


Configurazione VM

Inizialmente si impostano gli indirizzi IP della macchina Kali e Windows XP rispettivamente a 192.168.240.100 e 192.168.240.150, così come richiesto dalla traccia. Per fare ciò si è andato a modificare il file interfaces al PATH /etc/network/ con il comando **<sudo nano /etc/network/interfaces>**.

Dopo aver fatto un reboot delle macchine, il comando **<ifconfig>** su Kali e il comando **<ipconfig>** su Windows XP dimostra l'effettivo cambio di indirizzi IP.


Prompt dei comandi

```
Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Epicode_user>ipconfig

Configurazione IP di Windows

Scheda Ethernet Connessione alla rete locale <LAN>:

    Suffisso DNS specifico per connessione:
    Indirizzo IP . . . . . : 192.168.240.150
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.240.1

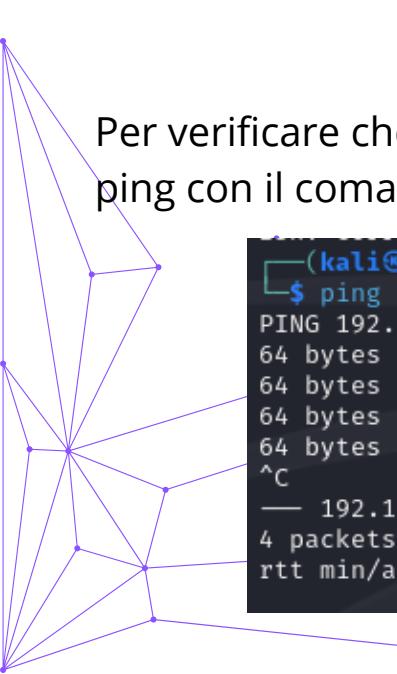
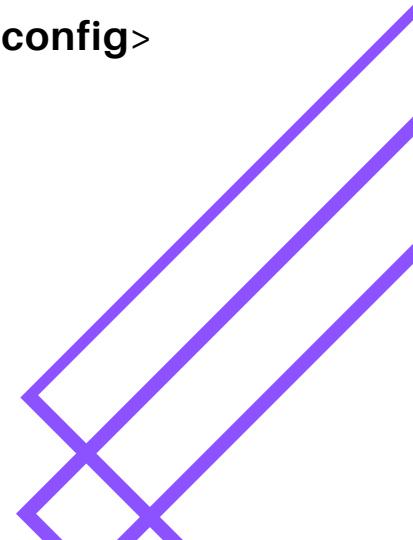
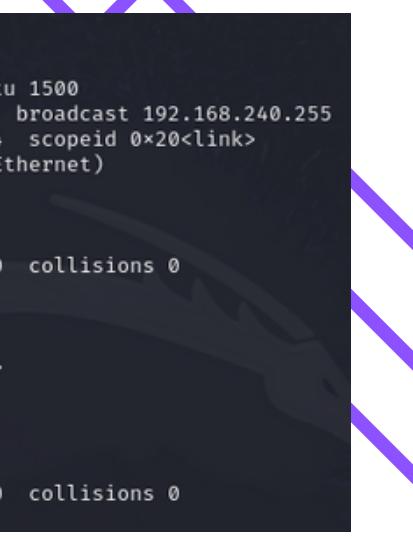
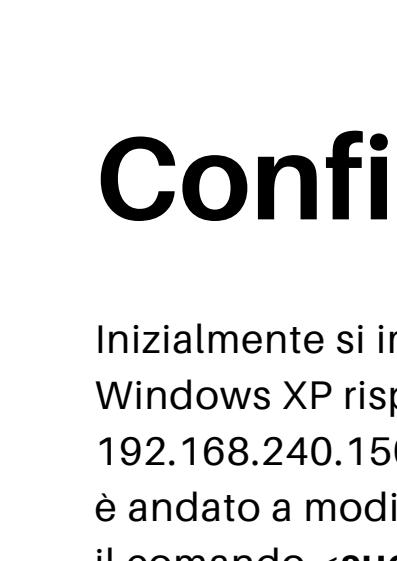
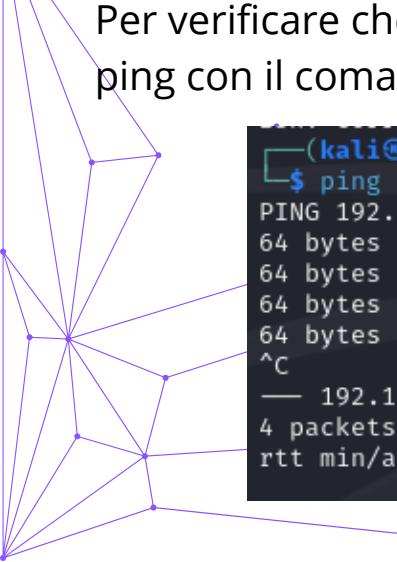
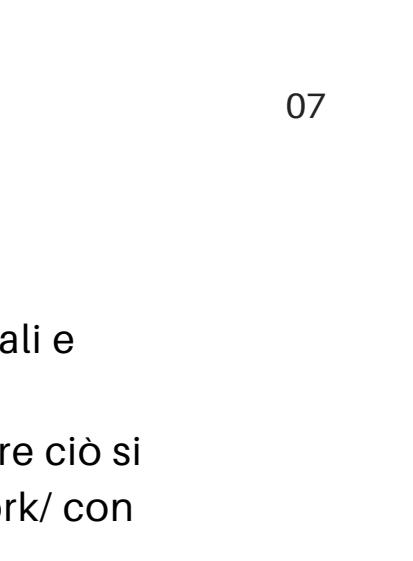
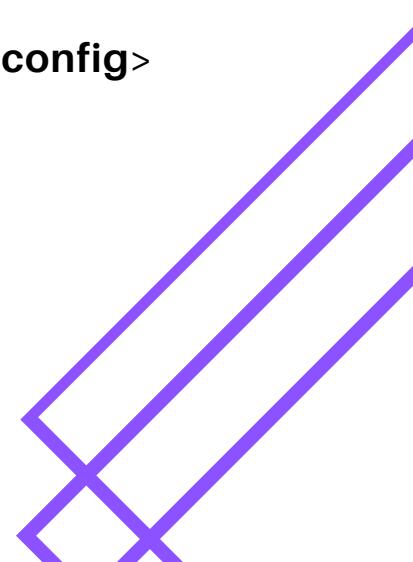
C:\Documents and Settings\Epicode_user>
```

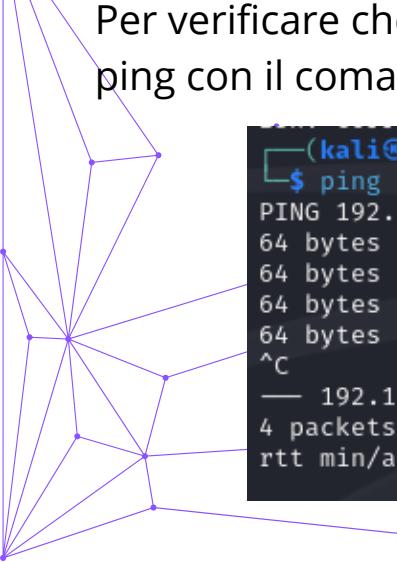
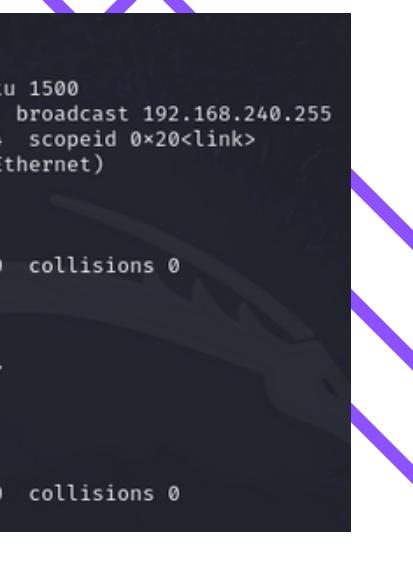
(kali㉿kali)-[~]

```
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.240.100 netmask 255.255.255.0 broadcast 192.168.240.255
      inet6 fe80::a00:27ff:fe1e:364a prefixlen 64 scopeid 0x20<link>
        ether 08:00:27:1e:36:4a txqueuelen 1000 (Ethernet)
          RX packets 13 bytes 1932 (1.8 KiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 24 bytes 3086 (3.0 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 4 bytes 240 (240.0 B)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 4 bytes 240 (240.0 B)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Per verificare che le due macchine sono connesse tra loro si effettua un ping con il comando **<ping indirizzo_ip_WinXP>**

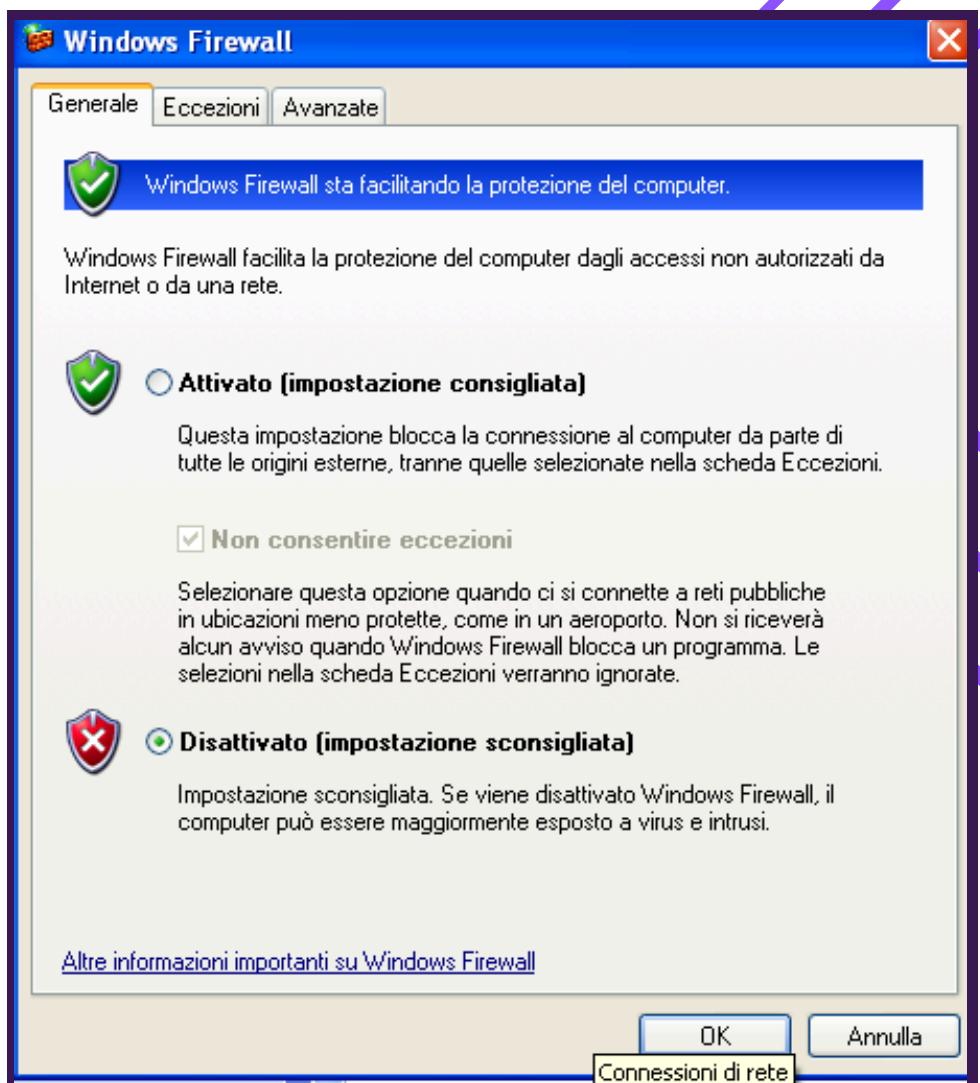




```
(kali㉿kali)-[~]
$ ping 192.168.240.150
PING 192.168.240.150 (192.168.240.150) 56(84) bytes of data.
64 bytes from 192.168.240.150: icmp_seq=1 ttl=128 time=0.437 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=0.250 ms
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=0.701 ms
64 bytes from 192.168.240.150: icmp_seq=4 ttl=128 time=0.306 ms
^C
--- 192.168.240.150 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3059ms
rtt min/avg/max/mdev = 0.250/0.423/0.701/0.173 ms
```

V.A. con Firewall Disattivato

In questa fase viene disattivato il firewall di Windows XP per verificare la sua efficacia in caso di possibili attacchi provenienti dall'estero.

Il firewall di Windows XP è una funzionalità di sicurezza integrata nel sistema operativo progettata per monitorare e controllare il traffico di rete in entrata e in uscita. Funziona bloccando le connessioni non autorizzate e permettendo solo quelle che sono esplicitamente consentite dall'utente o dai programmi installati, contribuendo a proteggere il computer da accessi non autorizzati e attacchi esterni.



V.A. con Firewall Disattivato

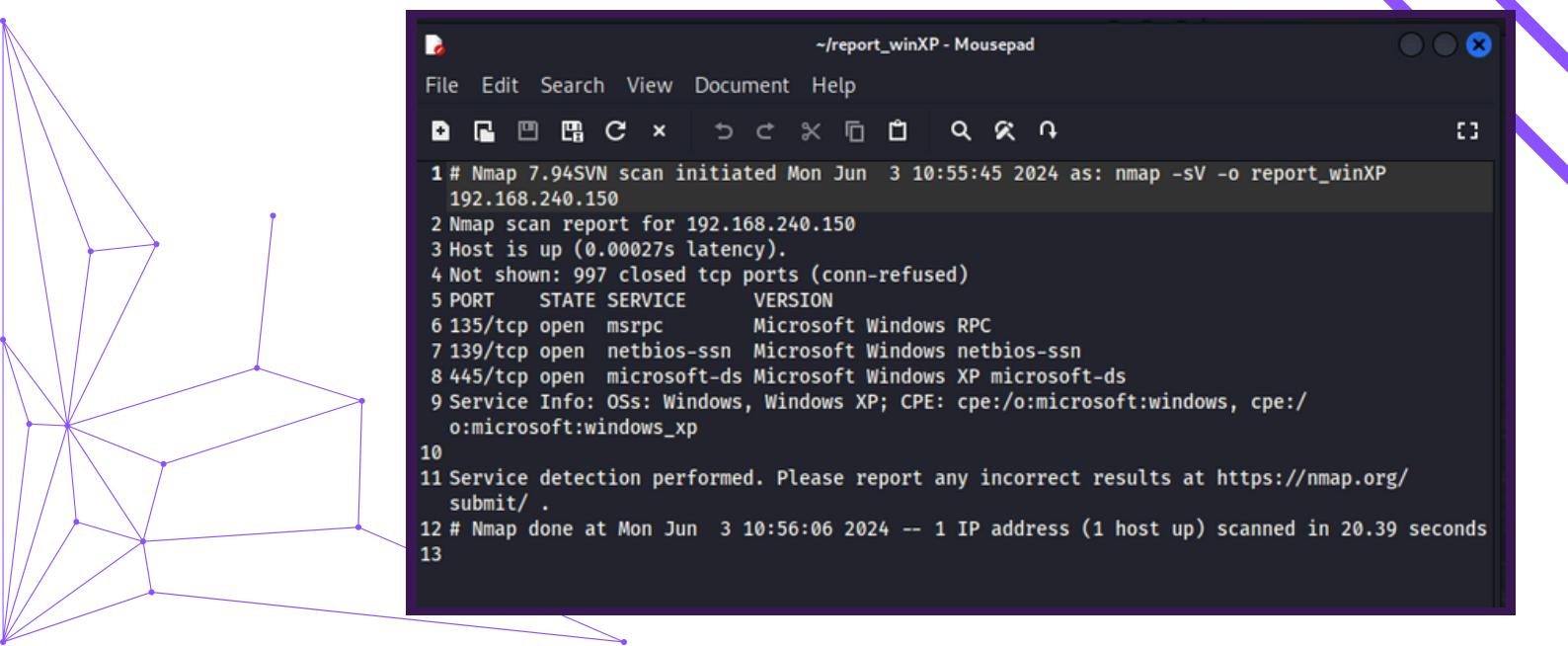
In questa fase viene disattivato il firewall di Windows XP per verificare l'efficacia in caso di possibili attacchi provenienti dall'esterno.

Questo permette di fare una scansione della rete dalla nostra macchina Kali utilizzando lo strumento nmap: con il comando **<nmap -sV indirizzo_ip_WinXP -o report_WinXP>** infatti si è potuta fare una scansione di tutte le porte e servizi attivi sulla macchina target WinXP.

-sV questa opzione permette di rilevare i servizi in esecuzione su ciascun host e di determinare le versioni specifiche di questi servizi.

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.240.150 -o report_winXP
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 10:55 CEST
Nmap scan report for 192.168.240.150
Host is up (0.00027s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

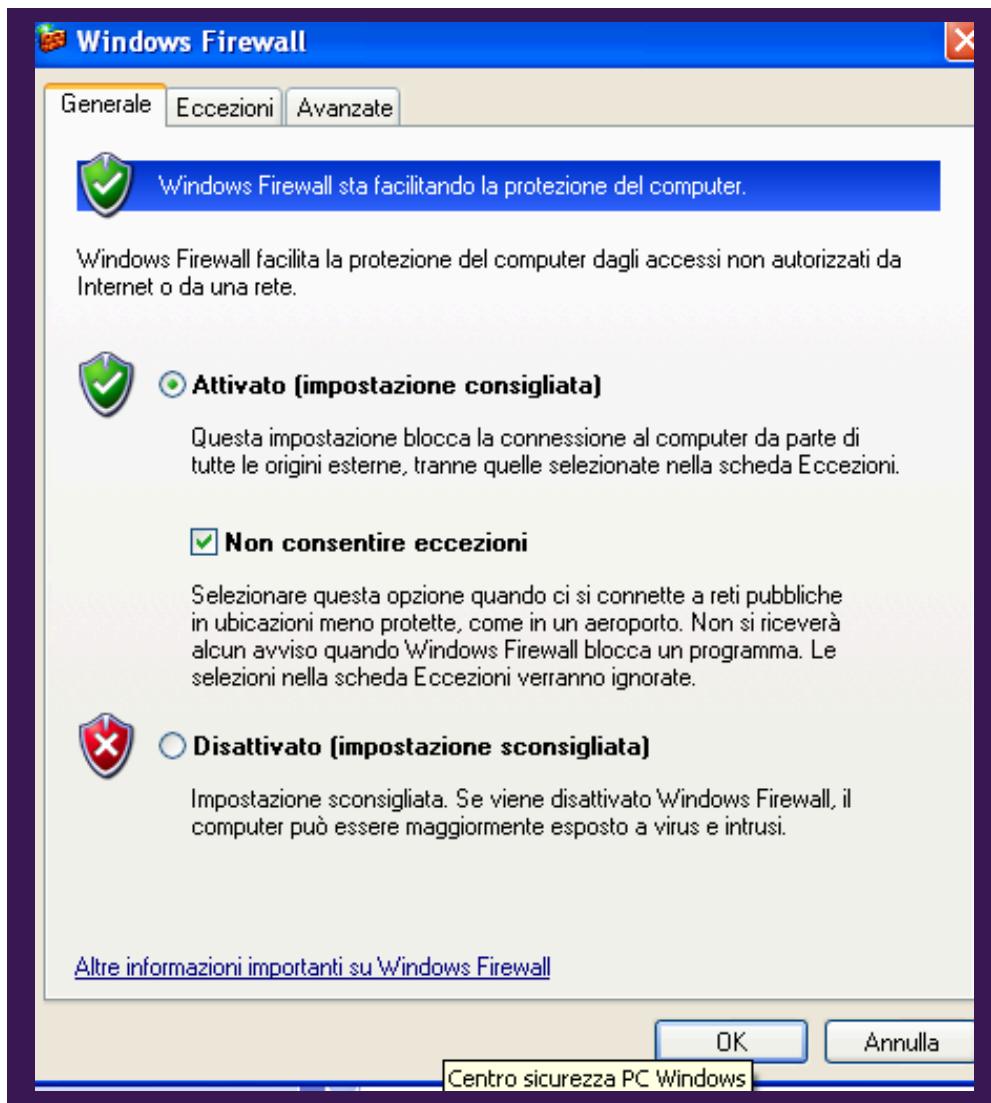
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.39 seconds
```



```
~/report_winXP - Mousepad
File Edit Search View Document Help
File Edit View Insert Document Help
1 # Nmap 7.94SVN scan initiated Mon Jun  3 10:55:45 2024 as: nmap -sV -o report_winXP
192.168.240.150
2 Nmap scan report for 192.168.240.150
3 Host is up (0.00027s latency).
4 Not shown: 997 closed tcp ports (conn-refused)
5 PORT      STATE SERVICE      VERSION
6 135/tcp    open  msrpc        Microsoft Windows RPC
7 139/tcp    open  netbios-ssn   Microsoft Windows netbios-ssn
8 445/tcp    open  microsoft-ds Microsoft Windows XP microsoft-ds
9 Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
10
11 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
12 # Nmap done at Mon Jun  3 10:56:06 2024 -- 1 IP address (1 host up) scanned in 20.39 seconds
13
```

V.A. con Firewall Attivo

Successivamente, per verificare l'efficacia del firewall si è rifatta una scansione della rete aziendale con quest'ultimo attivo. A livello di rete, possiamo attivare / configurare Firewall e regole per fare in modo che un determinato traffico, potenzialmente dannoso, venga bloccato.



V.A. con Firewall Attivo

11

Quando si utilizza Nmap per scansionare un sistema Windows con il firewall attivo, i risultati mostrano in genere meno dettagli sulle porte a causa del blocco operato dal firewall. Durante queste scansioni, è comune trovare:

1. Porte chiuse o filtrate: La maggior parte delle porte viene bloccata dal firewall, risultando inaccessibili o mostrate come chiuse da Nmap.
2. Ritardi nella scansione: Il firewall può causare ritardi o ignorare completamente i pacchetti di scansione, influenzando la velocità e l'efficacia di Nmap.
3. Errori e avvisi: Nmap potrebbe segnalare errori indicando che le porte sono filtrate, suggerendo che il firewall sta impedendo l'accesso.
4. Informazioni limitate sui servizi: Le informazioni raccolte dalle porte aperte sono spesso ridotte, limitando la visibilità dei servizi in esecuzione.
5. False Positivi: Il firewall può causare falsi positivi, facendo apparire alcune porte come chiuse o filtrate anche quando non lo sono.

```
(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150 -o report_winXP_firewall
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 11:05 CEST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.11 seconds
```



Conclusioni

In conclusione, la scansione Nmap eseguita su un sistema Windows ha rivelato differenze significative nei risultati a seconda dello stato del firewall. Con il firewall disattivato, la scansione ha identificato un numero maggiore di porte aperte e servizi attivi, suggerendo una superficie di attacco più ampia e potenziali vulnerabilità accessibili.

Al contrario, con il firewall attivato, la scansione ha mostrato un numero significativamente ridotto di porte aperte, indicando una protezione più robusta contro accessi non autorizzati. La presenza del firewall ha dimostrato la sua efficacia nel filtrare il traffico di rete e nel proteggere il sistema da potenziali attacchi.

Questi risultati sottolineano l'importanza di mantenere attivo il firewall come componente essenziale della sicurezza di rete. Il confronto tra le due scansioni evidenzia chiaramente il ruolo critico del firewall nella protezione delle risorse del sistema e nel mantenimento dell'integrità e della riservatezza dei dati.



L2

Durante la lezione teorica, abbiamo affrontato gli argomenti riguardanti la business continuity e disaster recovery. Nell'esempio pratico di oggi, ipotizziamo di essere stati assunti per valutare quantitativamente l'impatto di un determinato disastro su un asset di una compagnia. Con il supporto dei dati presenti nelle tabelle che seguono, calcolare la perdita annuale che subirebbe la compagnia nel caso di:

- Inondazione sull'asset «edificio secondario»
- Terremoto sull'asset «datacenter»
- Incendio sull'asset «edificio primario»
- Incendio sull'asset «edificio secondario»
- Inondazione sull'asset «edificio primario»

Dati:

ASSET	VALORE
Edificio primario	350.000€
Edificio secondario	150.000€
Datacenter	100.000€

EVENTO	ARO
Terremoto	1 volta ogni 30 anni
Incendio	1 volta ogni 20 anni
Inondazione	1 volta ogni 50 anni

EXPOSURE FACTOR	Terremoto	Incendio	Inondazione
Edificio primario	80%	60%	55%
Edificio secondario	80%	50%	40%
Datacenter	95%	60%	35%

Prima di iniziare

Un **asset** è una risorsa, un bene o un diritto di proprietà che ha un valore economico. Può essere tangibile (immobili, macchinari, merci) o intangibile (marchi, brevetti, competenze). Gli asset sono importanti perché generano valore e sono fondamentali per il successo di un'azienda o individuo.

Le compagnie resilienti predispongono piani e procedure per ridurre gli effetti di un evento catastrofico naturale o di un attacco ed assicurare la continuità operativa, queste pratiche prendono il nome di «business continuity plan» e «disaster recovery».

BUSINESS CONTINUITY PLAN

Il business continuity plan (BCP), piano per la continuità del business, ha lo scopo principale di dettagliare le policy e le procedure per minimizzare gli impatti negativi sull'operatività di una compagnia a valle di un evento catastrofico / attacco, e ad assicurare la continuità delle operazioni svolte dalla compagnia anche in situazioni di emergenza.

Il business continuity plan si compone di quattro step principali:

- Pianificazione e scopo;
- Business impact assessment (BIA), ovvero valutazione degli impatti sul business (può essere qualitativo o quantitativo);
- Business planning, ovvero piano di continuità operativa;
- Approvazione ed implementazione.

DISASTER RECOVERY

Il Disaster recovery planning (DRP) può essere visto come il complemento tecnico al BCP, mentre da un lato il BCP copre le tematiche di governance (pianificazione e gestione), il disaster recovery planning include i controlli tecnici da implementare per la riduzione del rischio e per il recupero dei servizi a valle di un evento catastrofico.



Analisi Formula

Nel business continuity plan, la fase di Business Impact Assessment (BIA) ha lo scopo principale di identificare le risorse critiche di una compagnia e le potenziali minacce alle quali esse sono esposte. Durante questa fase avviene l'identificazione delle priorità e dei rischi, la valutazione delle probabilità e degli impatti.

In questo esercizio ci si è concentrati su una valutazione quantitativa degli impatti di un determinato disastro su un asset della compagnia. A tal fine sono stati usati le seguenti definizioni:

- **Annualized Rate of Occurrence (ARO)**: indica il tasso annuale di occorrenza di un evento e la sua probabilità è espressa in numero di volte che l'evento si è verificato nel corso di un anno.
- **Exposure Factor (EF)**: indica la percentuale di asset che verrebbe impattato a seguito del verificarsi di un determinato evento.
- **Single Loss Expectancy (SLE)**: dà una misura monetaria della perdita che si subirebbe al verificarsi dell'evento, calcolato come il prodotto tra il **valore dell'asset (AV)** e la percentuale impattata in caso di evento (EF):

$$\text{SLE} = \text{AV} * \text{EF}$$

- **Annualized Loss Expectancy (ALE)**: il valore della perdita subita in un arco temporale di un anno, che si calcola come:

$$\text{ALE} = \text{SLE} * \text{ARO}$$

«tabella di riferimento»

INCENDIO

Danni agli asset in caso di incendio:

1. Strutturali:

- Crolli parziali o totali di pareti, solai e tetti.
- Compromissione della stabilità strutturale a causa del calore.

2. Non strutturali:

- Distruzione di mobili, attrezzature e arredi.
- Danni agli impianti elettrici, idraulici e di condizionamento.

3. Infrastrutturali:

- Rottura di tubazioni e condutture, causando perdite di acqua o gas.
- Danni a strade, ponti e altre infrastrutture adiacenti.

Prevenzione dei danni agli asset in caso di incendio:

1. Strutturali:

- Utilizzo di materiali ignifughi.
- Installazione di barriere antincendio.
- Manutenzione regolare delle strutture.

2. Non strutturali:

- Installazione di sistemi di rilevazione e allarme antincendio.
- Utilizzo di arredamenti e attrezzature ignifughi.
- Implementazione di piani di evacuazione e sicurezza.

3. Infrastrutturali:

- Ispezione e manutenzione regolare delle tubazioni.
- Installazione di sistemi di spegnimento automatico (sprinkler).
- Creazione di vie di fuga e accessi per i mezzi di soccorso.

Incendio

Asset	Valore dell'asset	Fattore di esposizione	Frequenza ARO	Perdita annuale
Edificio Primario	€350.000	60%	1/20 anni (0,05)	€10.500
Edificio Secondario	€150.000	50%	1/20 anni (0,05)	€3.750
Datacenter	€100.000	60%	1/20 anni (0,05)	€3.000

FORMULE UTILIZZATE:

$$SLE = AV * EF$$

$$ALE = SLE * ARO$$

«tabella di riferimento»

TERREMOTO

Danni agli asset in caso di terremoto:

1. Strutturali:

- Crolli parziali o totali delle fondamenta, pareti, solai e tetti.
- Crepe e fratture in muri, travi e colonne.
- Deformazioni delle strutture portanti.

2. Non strutturali:

- Caduta di mobili, scaffali e apparecchiature.
- Danni agli impianti elettrici, idraulici e di condizionamento.

3. Infrastrutturali:

- Rottura delle tubazioni, causando perdite d'acqua o gas.
- Danni a strade, ponti e ferrovie, ostacolando soccorsi ed evacuazioni.

Prevenzione dei danni agli asset in caso di terremoto:

1. Strutturali:

- Progettazione antisismica.
- Utilizzo di materiali resistenti.
- Retrofit sismico per edifici esistenti.

2. Non strutturali:

- Ancoraggio di mobili e apparecchiature.
- Barriere antisismiche per finestre e porte.

3. Infrastrutturali:

- Rafforzamento delle tubazioni.
- Manutenzione e rinforzo di strade e ponti.

Terremoto

Asset	Valore dell'asset	Fattore di esposizione	Frequenza ARO	Perdita annuale
Edificio Primario	€350.000	80%	1/30 anni (~0,03)	€8.400
Edificio Secondario	€150.000	80%	1/30 anni (~0,03)	€3.600
Datacenter	€100.000	95%	1/30 anni (~0,03)	€2.850

FORMULE UTILIZZATE:

$$SLE = AV * EF$$

$$ALE = SLE * ARO$$

«tabella di riferimento»

INONDAZIONE

Danni agli asset in caso di inondazione:

1. Strutturali:

- Danni alle fondamenta, pareti e pavimenti.
- Erosione e indebolimento delle strutture portanti.

2. Non strutturali:

- Distruzione di mobili, attrezzature e arredi.
- Danni agli impianti elettrici, idraulici e di condizionamento.

3. Infrastrutturali:

- Rottura di tubazioni e condutture, causando perdite di acqua o gas.
- Danni a strade, ponti e altre infrastrutture adiacenti.

Prevenzione dei danni agli asset in caso di inondazione:

1. Strutturali:

- Costruzione sopra il livello di piena.
- Utilizzo di materiali resistenti all'acqua.
- Installazione di barriere contro l'acqua e sistemi di drenaggio.

2. Non strutturali:

- Sollevamento di mobili e attrezzature da terra.
- Utilizzo di materiali impermeabili per arredi e finiture.
- Implementazione di sistemi di rilevazione e allarme per inondazioni.

3. Infrastrutturali:

- Manutenzione e miglioramento dei sistemi di drenaggio e delle condutture.
- Creazione di argini e bacini di contenimento.
- Pianificazione di vie di fuga e accessi per i mezzi di soccorso.

Inondazione

Asset	Valore dell'asset	Fattore di esposizione	Frequenza ARO	Perdita annuale
Edificio Primario	€350.000	55%	1/50 anni (0,02)	€3.850
Edificio Secondario	€150.000	40%	1/50 anni (0,02)	€1.200
Datacenter	€100.000	35%	1/50 anni (0,02)	€700

FORMULE UTILIZZATE:

$$SLE = AV * EF$$

$$ALE = SLE * ARO$$

CONCLUSIONI

In conclusione, i costi per queste calamità naturali sono purtroppo molto alti. Raccomandiamo di tenere dei fondi in caso di emergenza e invitiamo caldamente a eseguire dei controlli annuali per il mantenimento delle infrastrutture. Avere una buona formazione del personale è essenziale in caso di emergenza e potrebbe salvare molte vite.

Scenario	Asset	Valore dell'asset	Fattore di esposizione	Frequenza ARO	Perdita annuale
Terremoto su "Edificio primario"	Edificio Primario	€350.000	80%	1/30 anni (~0,03)	€8.400
Incendio su "Edificio primario"	Edificio Primario	€350.000	60%	1/20 anni (0,05)	€10.500
Inondazione su "Edificio primario"	Edificio Primario	€350.000	55%	1/50 anni (0,02)	€3.850
Terremoto su "Edificio secondario"	Edificio Secondario	€150.000	80%	1/30 anni (~0,03)	€3.600
Incendio su "Edificio secondario"	Edificio Secondario	€150.000	50%	1/20 anni (0,05)	€3.750
Inondazione su "Edificio secondario"	Edificio Secondario	€150.000	40%	1/50 anni (0,02)	€1.200
Terremoto su "Datacenter"	Datacenter	€100.000	95%	1/30 anni (~0,03)	€2.850
Incendio su "Datacenter"	Datacenter	€100.000	60%	1/20 anni (0,05)	€3.000
Inondazione su "Datacenter"	Datacenter	€100.000	35%	1/50 anni (0,02)	€700

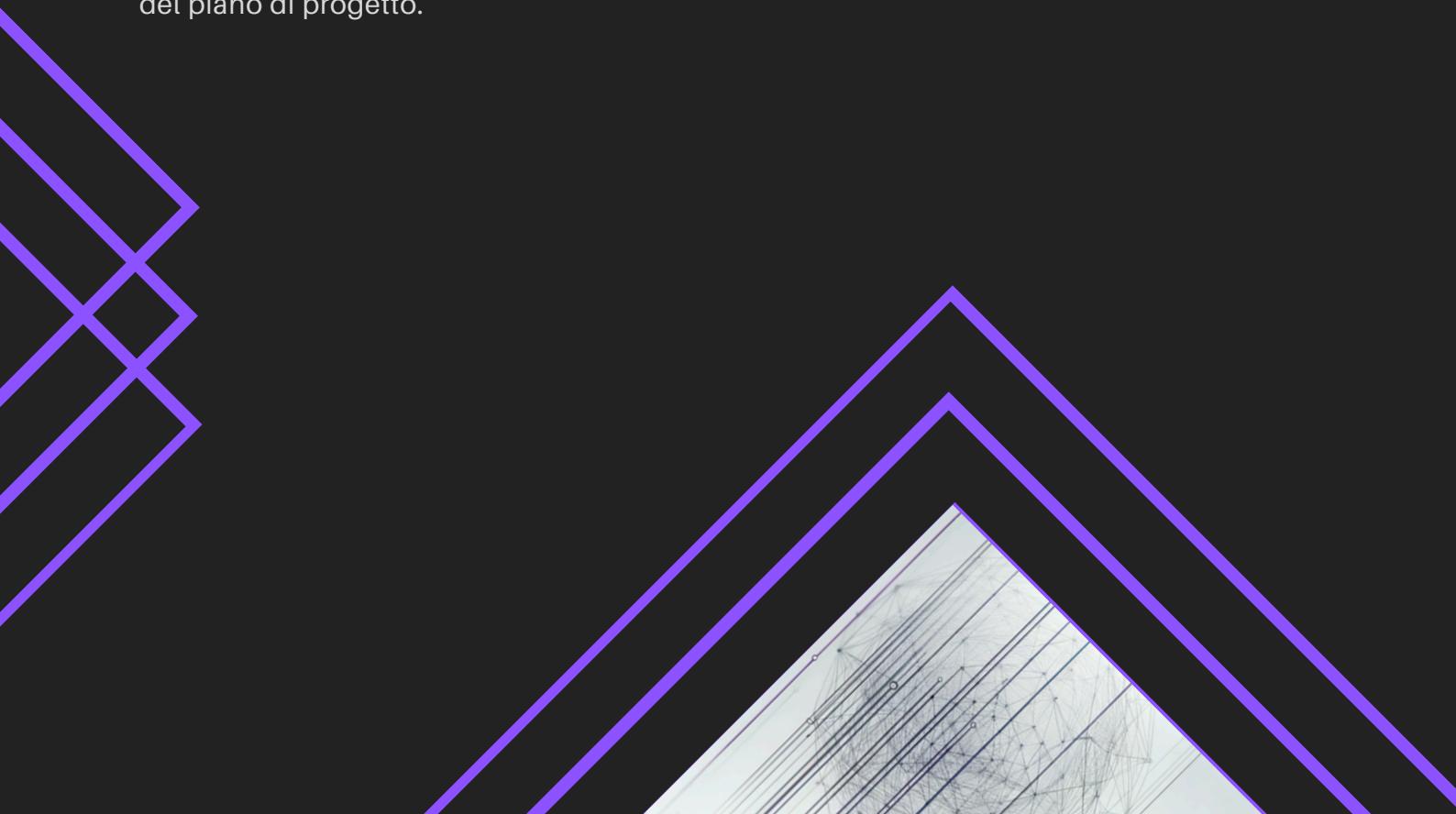
WORK IN PROGRESS

Progetto online

Realizziamo contenuti coinvolgenti, apprezzati e desiderati da tutti gli utenti online.

Che tu scelga di avere un report mensile o trimestrale, ci sono dei consigli che puoi imparare e che ti aiuteranno a redigere report brillante. Innanzitutto è necessario che il report sia rilevante per il tuo pubblico. Selezionare le giuste informazioni tra una marea di dati fa la differenza nel supportare gli obiettivi della tua squadra e della tua azienda. In secondo luogo, tieni presente che le statistiche dei social media non hanno senso se considerate isolatamente. Per questo è necessario collegare i dati attuali con quelli precedenti. Infine, oltre a non essere esagerato, il tuo report dovrebbe sempre rispondere alla domanda "e quindi?"

Un grande progetto prevede la supervisione di molti aspetti, spesso da parte di persone diverse. Per un lancio di successo, i project manager si affidano a un piano di progetto ben strutturato che garantisca l'adempimento degli obiettivi in tempo e nel budget. Un piano di progetto è un documento approvato e impiegato per definire gli obiettivi del progetto, sottolineare il suo scopo, monitorarne le attività e mitigare i rischi. Deve saper rispondere a domande basilari tra cui: qual è lo scopo del progetto, quali sono le attività previste, chi sarà responsabile di cosa, quando dovrebbe concludersi? Non deve essere confuso con il diagramma di Gantt che, invece, illustra le sequenze, la durata e l'arco temporale di ogni singola attività del progetto. Il suddetto diagramma è solo una parte del piano di progetto.



Budget

Budget stimato per la campagna

Brand 1	30.000 €
Brand 2	50.000 €
Brand 3	35.000 €
Totale	115.000 €

Analisi

Dobbiamo lavorare più duramente in alcune aree.

I nostri visitatori sono giovani adulti tra i 21 e i 35 anni.

Dobbiamo sintonizzarci di più con i loro interessi.

Al giorno d'oggi, gli smartphone sono ovunque e l'enorme impatto dei social media nel guidare il comportamento dei consumatori è innegabile. Per questo motivo sia i grandi brand che quelli più piccoli sfruttano le piattaforme digitali nel tentativo di conquistare quote di mercato. Ma essere online non è abbastanza - i brand devono prendere coscienza del comportamento online dei propri clienti, utilizzando quei dati per trarne un guadagno.

Aree di miglioramento

Assicuriamoci che i nostri contenuti soddisfino le aree di interesse.

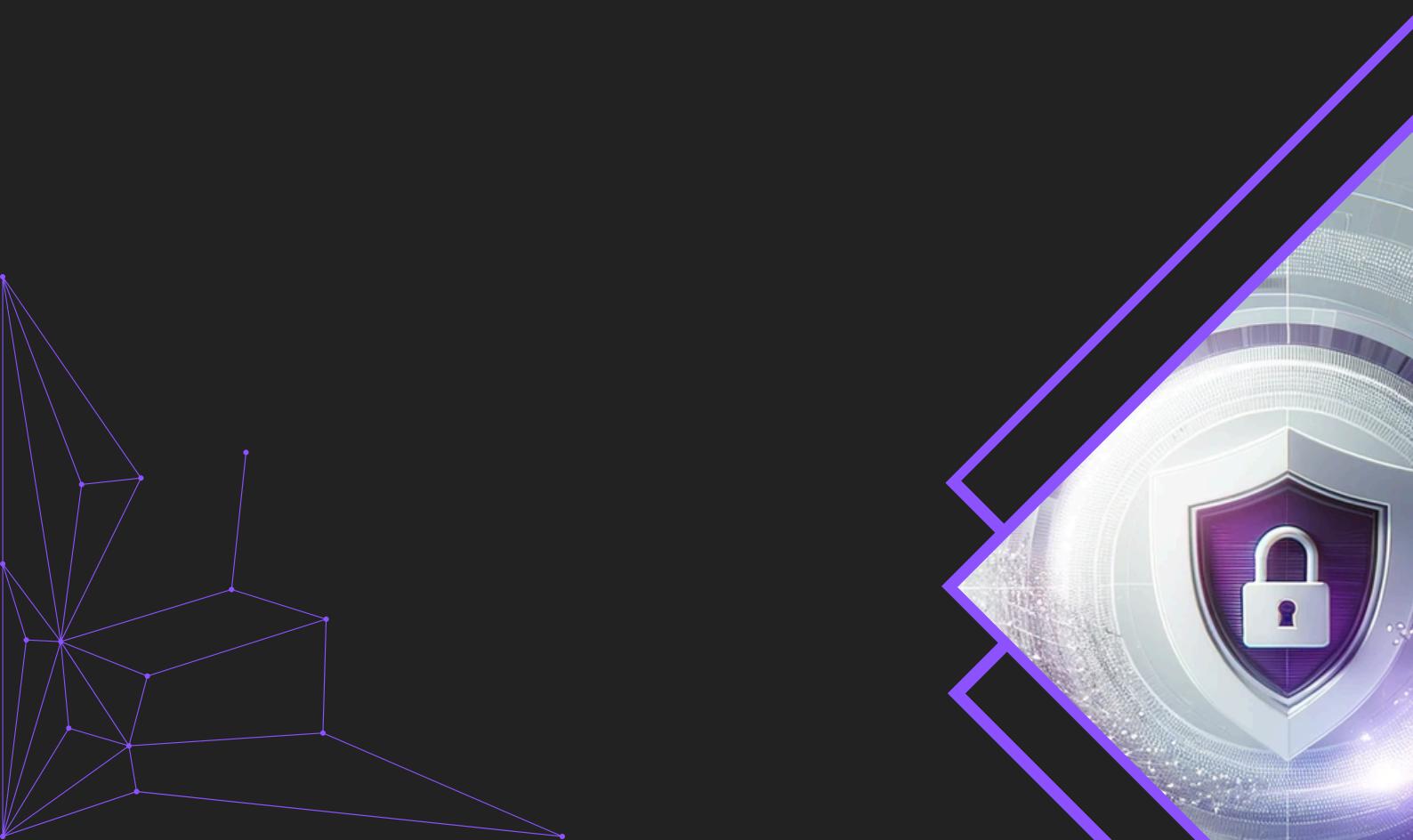
Dobbiamo inserire più informazioni che risultino utili per i nostri lettori.

Dobbiamo fare in modo che consiglino il nostro sito a famigliari e amici.

Prima ancora di scrivere il tuo report, prenditi del tempo per considerarne i destinatari. Una buona regola generale è ricordare che più alta è la posizione dello stakeholder nella scala organizzativa, più succinto deve essere il report.

Obiettivi

Durante la lezione teorica, abbiamo studiato le azioni preventive per ridurre la possibilità di attacchi provenienti dall'esterno. Abbiamo visto che a livello di rete, possiamo attivare / configurare Firewall e regole per fare in modo che un determinato traffico, potenzialmente dannoso, venga bloccato. La macchina Windows XP che abbiamo utilizzato ha di default il Firewall disabilitato. L'obiettivo di oggi è verificare in che modo l'attivazione del Firewall impatta il risultato di una scansione dei servizi dall'esterno. Per questo motivo: 1. Assicuratevi che il Firewall sia disattivato sulla macchina Windows XP 2. Effettuate una scansione con nmap sulla macchina target (utilizzate lo switch-sV, per la service detection e -o nomefilereport per salvare in un file l'output) 3. Abilitare il Firewall sulla macchina Windows XP 4. Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch-sV. 5. Trovare le eventuali differenze e motivarle.



Obiettivi futuri

Su cosa dobbiamo lavorare il prossimo anno

Il passo successivo è decidere quali parametri ti interessano.

Di seguito alcuni parametri con cui puoi iniziare:

1. Crescita dei follower - il numero di persone che hai raggiunto
2. Volume degli influencer - le persone influenti nel tuo network
3. Volume di post - il numero delle volte in cui hai condiviso contenuti
4. Reach rate - il numero di utenti che hanno visto il tuo post
5. Engagement totale - quantità di interazione generata da ciascun post
6. Engagement per follower - engagement generato da ciascun post



Conosci il team esecutivo

Le persone con cui parliamo solamente online sono quelle più impegnate.

Ora che conosci la tua audience e i parametri, puoi iniziare a elaborare il tuo report. Inizia presentando la situazione generale. Fornisci un'istantanea che riassume l'andamento della tua attività sui social media. In questa sede puoi fare un controllo generale e valutare l'andamento delle tue piattaforme nel periodo sul quale ti stai focalizzando. Ricorda che non devi inserire tutti i parametri in una pagina. Semplifica la fruizione da parte del tuo pubblico selezionando solo i tre o quattro parametri più importanti. Poi fornisci alcuni punti chiave che ti aiuteranno a introdurre agevolmente l'altra parte del tuo report.

Ciao andrea

*Soluzioni Digitali Greppi
si occupa di tutte le
attività sui social media di
SoluzioniDigitali snc.*

Dopo aver presentato una panoramica dei tuoi social media, puoi illustrare i tuoi obiettivi e le tue iniziative più importanti. Inizia con l'identificare gli obiettivi che la squadra si è stabilita per il periodo in questione e collegali a obiettivi aziendali di portata maggiore. Se la squadra ha intrapreso iniziative importanti, menzionalo in questa sede. Ricordati di non esagerare e di puntare sui tuoi obiettivi principali. Inoltre, presenta i dati attraverso grafici intuitivi che illustrino il progresso che hai fatto mese dopo mese. In questo modo avrai l'opportunità di illustrare il miglioramento nel tempo della tua attività sui social, così come il modo in cui questa ha contribuito positivamente allo sviluppo dell'azienda.

Sebbene sia importante menzionare l'andamento attuale della situazione, non dipingere un quadro troppo roseo. Assicurati di rammentare i limiti delle tue iniziative e di elaborare un piano d'azione da poter attuare per risolvere tali difficoltà in futuro.

