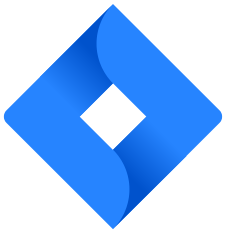


Cyber Safety Solutions

Otman Hmich & Michael Andreoli

Chi siamo?

La nostra azienda è nata dall'unione di un White Hat e un Black Hat, mettiamo a disposizione le nostre conoscenze, maturate grazie alla difesa e all'attacco dei sistemi informatici. Ci dedichiamo a proteggere le informazioni e le risorse digitali delle aziende di tutte le dimensioni. Fondata nel 2024, la nostra missione è fornire soluzioni di sicurezza all'avanguardia per prevenire, rilevare e rispondere alle minacce cibernetiche.

Perchè scegliere Cyber Safety Solutions?

In un mondo in cui le minacce informatiche sono in costante evoluzione, offriamo un approccio proattivo e completo alla sicurezza informatica. I nostri servizi includono:

- **Valutazione della Sicurezza**: Identificazione delle vulnerabilità e delle potenziali minacce con audit di sicurezza completi e penetration testing avanzati.
- **Gestione delle Minacce**: Monitoraggio continuo e risposta immediata agli incidenti per garantire che la vostra azienda sia sempre un passo avanti rispetto agli attaccanti.
- **Consulenza e Formazione**: Assistenza nella creazione di strategie di sicurezza personalizzate e programmi di formazione per sensibilizzare e preparare il personale aziendale.
- **Soluzioni di Sicurezza Personalizzate**: Implementazione di tecnologie di sicurezza su misura, tra cui firewall, sistemi di prevenzione delle intrusioni (IPS), e soluzioni di crittografia avanzate.

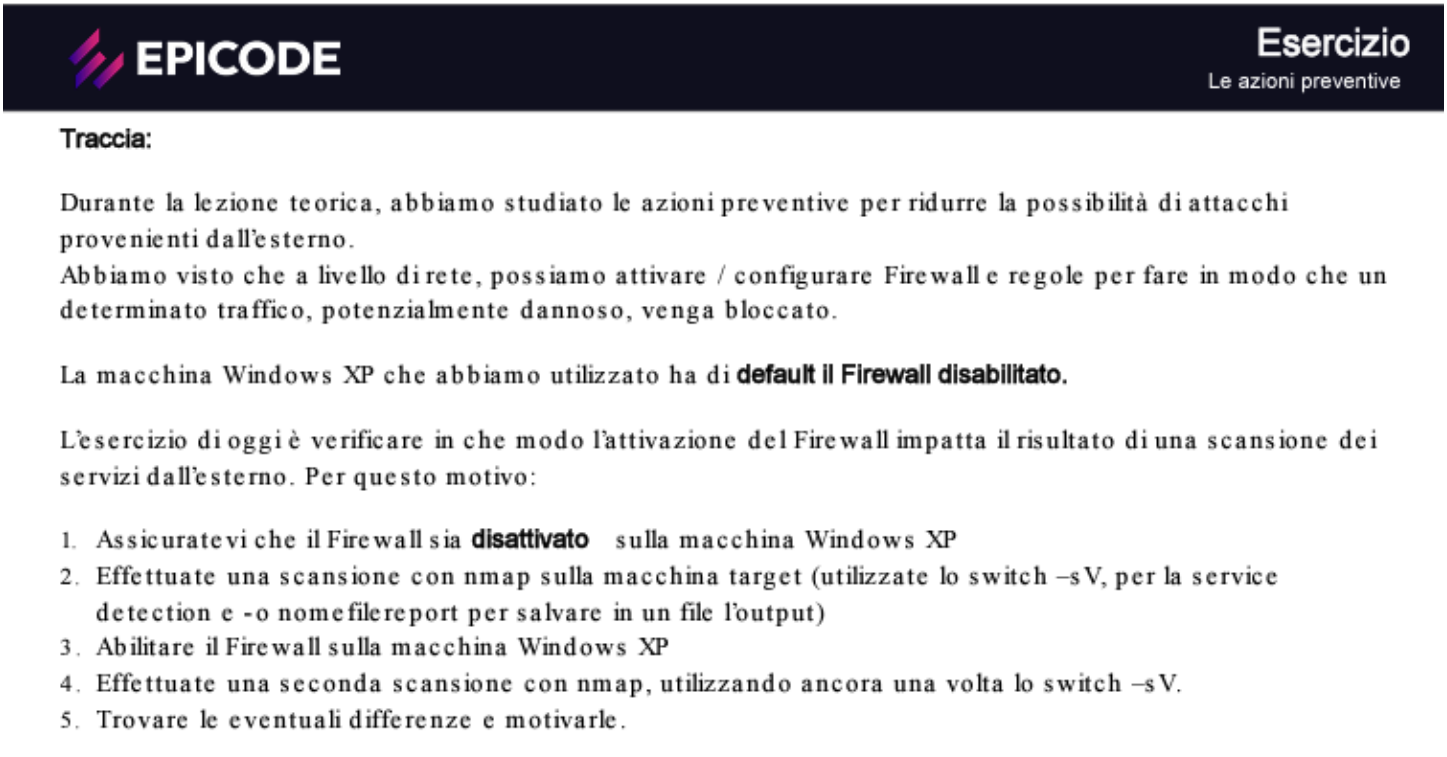
In cosa ci distinguiamo?

- **Esperienza e Competenza**: Il nostro team è composto da esperti certificati con anni di esperienza nel settore della sicurezza informatica.
- **Tecnologie Avanzate**: Utilizziamo strumenti e tecnologie all'avanguardia per proteggere la vostra azienda dalle minacce più recenti e sofisticate.
- **Approccio Personalizzato**: Siamo dedicati a comprendere le specifiche esigenze della vostra azienda per fornire soluzioni di sicurezza su misura.
- **Affidabilità e Riservatezza**: Garantiamo la massima discrezione e riservatezza nella gestione dei vostri dati e delle vostre informazioni.

La Nostra Visione

Immaginiamo un futuro in cui le aziende possano operare in totale sicurezza nel mondo digitale. Il nostro impegno è quello di costruire soluzioni innovative e affidabili che proteggano il cuore delle vostre operazioni aziendali, permettendovi di concentrarvi sulla crescita e sull'innovazione.

Giorno 1



EPICODE

Esercizio
Le azioni preventive

Traccia:

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.

3

Step by Step

Scansione della rete

Ci preoccupiamo di effettuare un'approfondita scansione della rete in modo da avere una precisa idea di cosa succede su quali porte.

Remediation

Andiamo ad attivare il firewall su Windows XP in modo da filtrare il traffico in entrata e bloccare potenziali minacce.

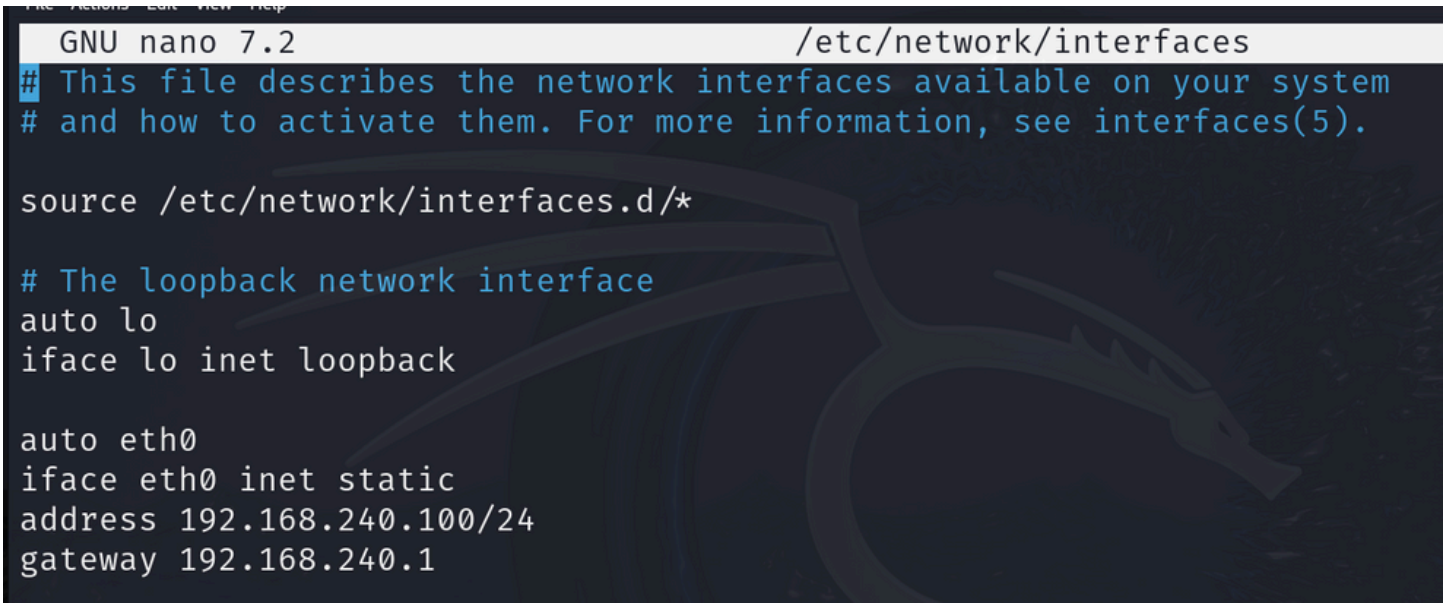
Check

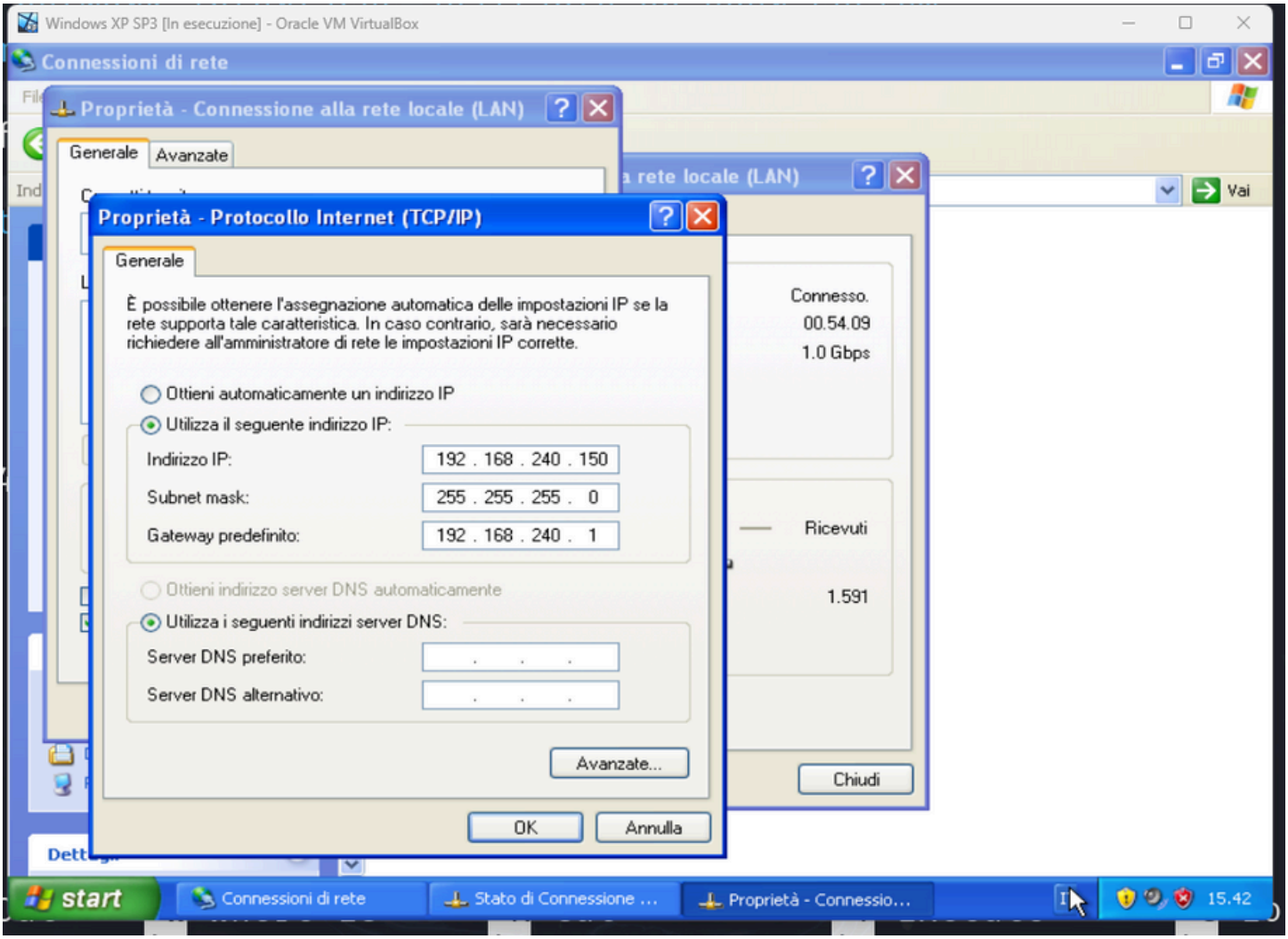
Effettuiamo una nuova scansione e prendiamo nota delle differenze per assicurarci che le nostre azioni abbiano avuto effetto.

Process

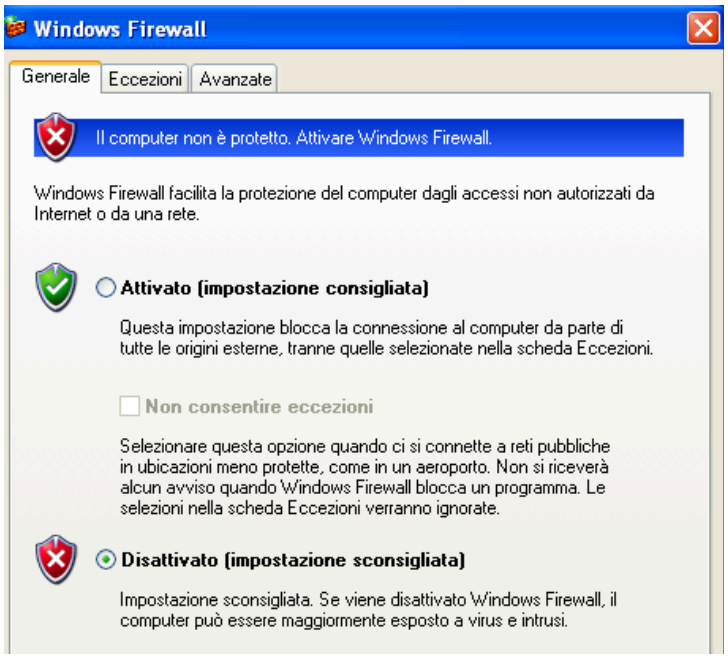
IP Configuration

Andiamo a impostare gli indirizzi IP delle nostre macchine virtuali come richiesto dalla traccia.



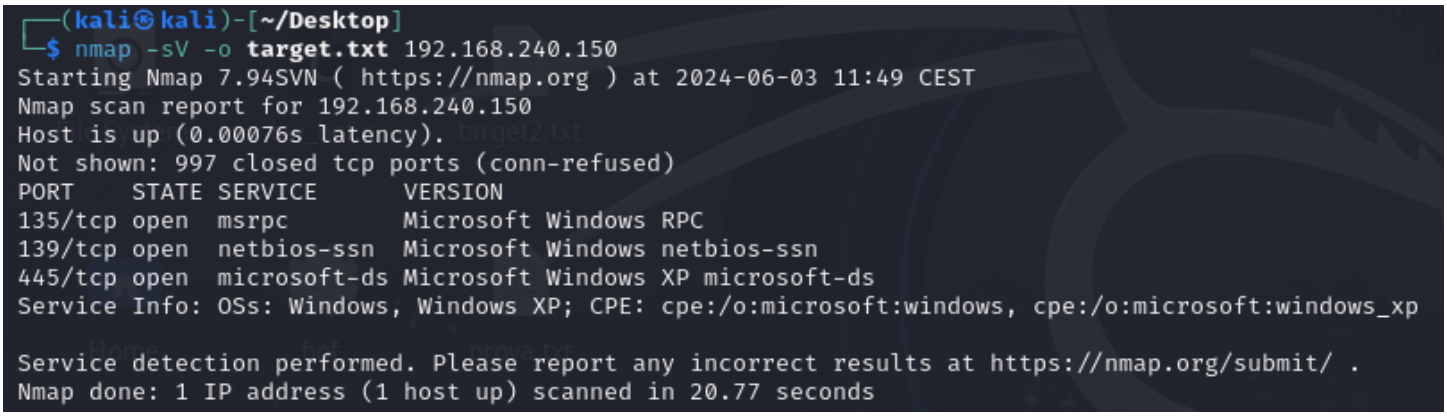


NMAP con firewall disattivo



Andiamo ad effettuare una scansione con nmap sulla nostra macchina windows utilizzando l'opzione -sV per stabilire le porte aperte, le

informazioni e la versione dei servizi attivi, per poi salvare l'output su un file di testo.



Da questa scansione possiamo notare che abbiamo controllato 1000 porte, 997 hanno rifiutato la connessione, perché sono chiuse o perché filtrate. Le 3 porte restanti, risultano aperte con i servizi e le versioni, mostrate nell'immagine.

Porte e servizi associati

- **Porta 135 (msrpc):**
  - Utilizzata pe rle chiamate di procedura remota di Microsoft (RPC).
  - È una porta critica per le funzionalità di rete di Windows e può essere un vettore di attacco se non adeguatamente protetta.

- **Porta 139 (netbios-ssn):**
  - Utilizzata dal servizio NetBIOS per sessioni di rete su TCP/IP.
  - Tipicamente usata per condivisioni di file o stampanti.

- **Porta 445 (microsoft-ds):**
  - Utilizzata per la condivisione di file e stampanti tramite SMB (Server Message Block) su TCP/IP.
  - Sostituisce la funzionalità del NetBIOS sulle reti più moderne.

NMAP con firewall attivo


```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV -o target2.txt 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 12:01 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 3.36 seconds
```

Dopo aver effettuato la scansione notiamo che il dispositivo sembra essere offline, questo perchè il firewall ci impedisce di pingare la macchina.

```
  -Pn: Treat all hosts as online -- skip host discovery
```

Utilizziamo lo switch ***-Pn*** in modo da evitare il ping e occuparsi subito della service discovery.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV -Pn -o target2.txt 192.168.240.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 12:01 CEST
Nmap scan report for 192.168.240.150
Host is up.
All 1000 scanned ports on 192.168.240.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 218.11 seconds
```

Conclusione

Scansione con firewall disattivo

Eseguendo la scansione con ***nmap*** siamo riusciti ad avere accesso alle porte aperte e a scoprire i servizi atttivi per riuscire a sfruttarle a

nostro piacimento per effettuare accessi da remoto, installare backdoor oppure inserire del codice malevolo.

Scansione con firewall attivo

Attivando il firewall abbiamo riscontrato l'impossibilitàà di eseguire il test di ping e utilizzando l'opzione ***-Pn*** abbiamo cercato di bypassare il test per procedere direttamente alla service discovery, non avendo peerò certezza dello stato delle porte, in quanto il firewall ci blocca l'accesso.

Preventivo

Preventivo n°: 1

Cliente:

Nome del Cliente

Indirizzo azienda Cliente

P.IVA/C.F.

Data: 03/06/2024

Valido fino a: 13/06/2024

Voci/Servizi	Quantità	Prezzo	Iva	Totale
Network Scan	16 ore (8hx2)	1600€	352€ (22%)	1952€
Penetration Test	32 ore (16hx2)	3200€	704€ (22%)	3904€
Remediation Actions	32 ore (16hx2)	3200€	704€ (22%)	3904€
Spese di Viaggio	300€ x 2	600€	132€	732€

Subtotale 8600€

Iva 1892€

Totale 10.492€

Giorno 2

EPICODE

Esercizio

Business continuity & disaster recovery

Traccia:

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»
- Terremoto sull'asset «edificio primario»

3

EPICODE

Esercizio

Business continuity & disaster recovery

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%

4

ALE: Annualized loss expectancy.

Valore delle perdite stimate nell'arco di un anno.

ALE = SLE * ARO.

SLE: Single loss expectancy.

Valore delle perdite in caso di un determinato evento.

ARO: Annualized Rate of Occurence.

Stima della frequenza con cui un particolare evento di rischio si verifica in un anno.

SLE = AV * EF.

AV: Asset Value.

Valore dell'asset.

EF: Exposure Factor.

La percentuale di danno o perdita che si stima avverrà a causa dell'evento specifico.

Inondazione Asset Edificio Secondario:

SLE = 150.000€ * 40% = 60.000€

ALE = 60.000€ * 0.02 = ***1.200€***

Terremoto Asset Datacenter:

SLE = 100.000€ * 95% = 95.000€

ALE = 95.000€ * 0.03 = ***2.850€***

Incendio Asset Edificio Primario:

SLE = 350.000€ * 60% = 210.000€

ALE = 210.000€ * 0.05 = ***10.500€***

Incendio Asset Edificio Secondario:

SLE = 150.000€ * 50% = 75.000€

ALE = 75.000€ * 0.05 = ***3.750€***

Inondazione Asset Edificio Primario:

SLE = 350.000€ * 55% = 192.500€

ALE = 192.500€ * 0.02 = ***9.650€***

Terremoto Asset Edificio Primario:

SLE = 350.000€ * 80% = 280.000€

ALE = 280.000€ * 0.03 = ***8.400€***
