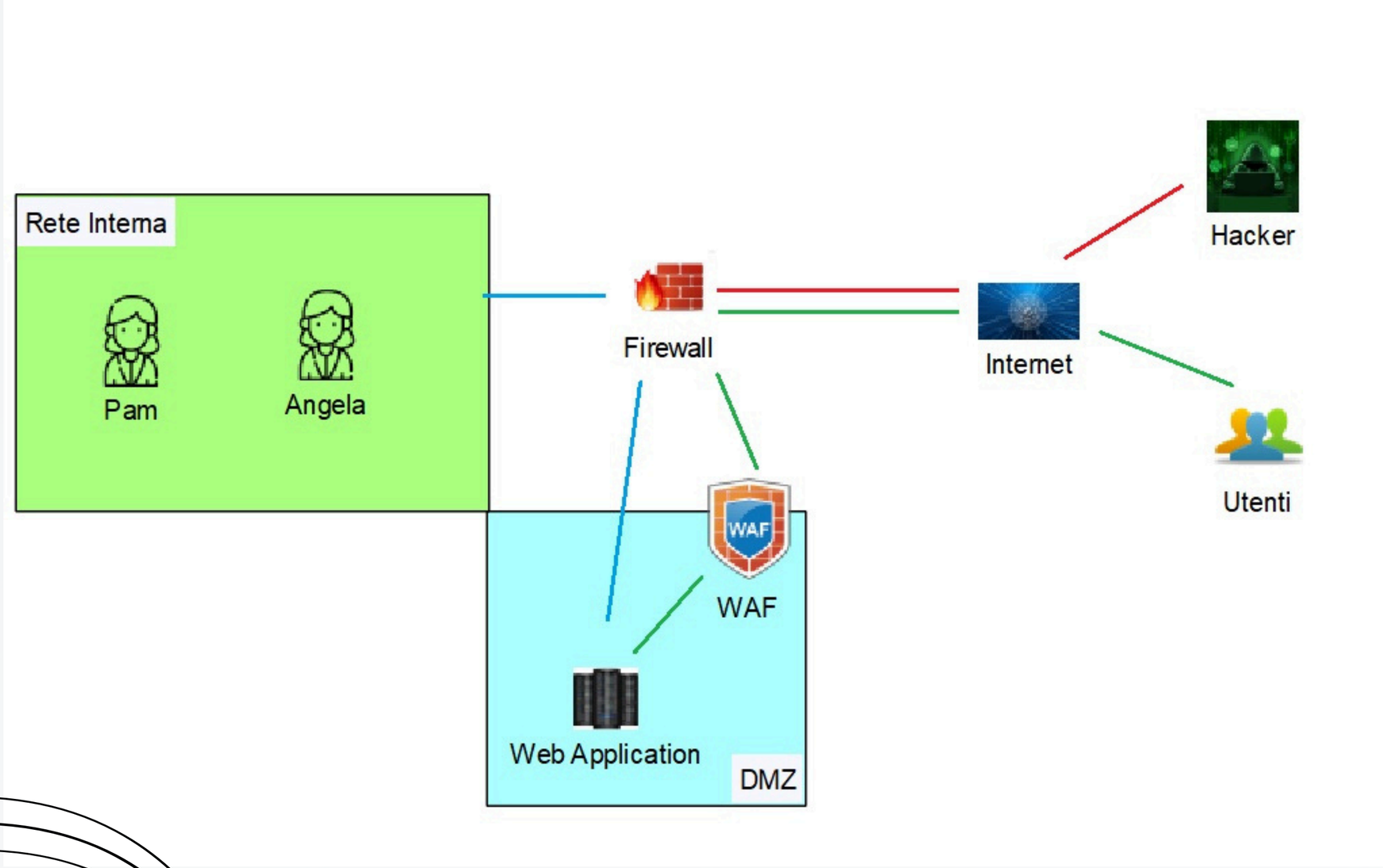
ANDREA
FALIERO

# PROGETTO

## S9-L5

# TRACCIA

1. Azioni preventive : quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni. È richiesta sola modifica
2. Impatti sul business : l'applicazione Web subisce un attacco di tipo l'applicazione non raggiungibile per 10 minuti . DDoS dall'esterno che rende Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media minuto gli utenti spendono ogni 1.200 € sulla piattaforma di e-commerce . Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica
3. Response : l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura in slide 2 con la soluzione proposta .
4. Soluzione completa : unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)
5. Modifica «più aggressiva» dell'infrastruttura: anche una soluzione al punto 2) integrando eventuali altri elementi di sicurezza (integrando Budget 5000-10000 euro. Eventualmente fare più proposte di spesa

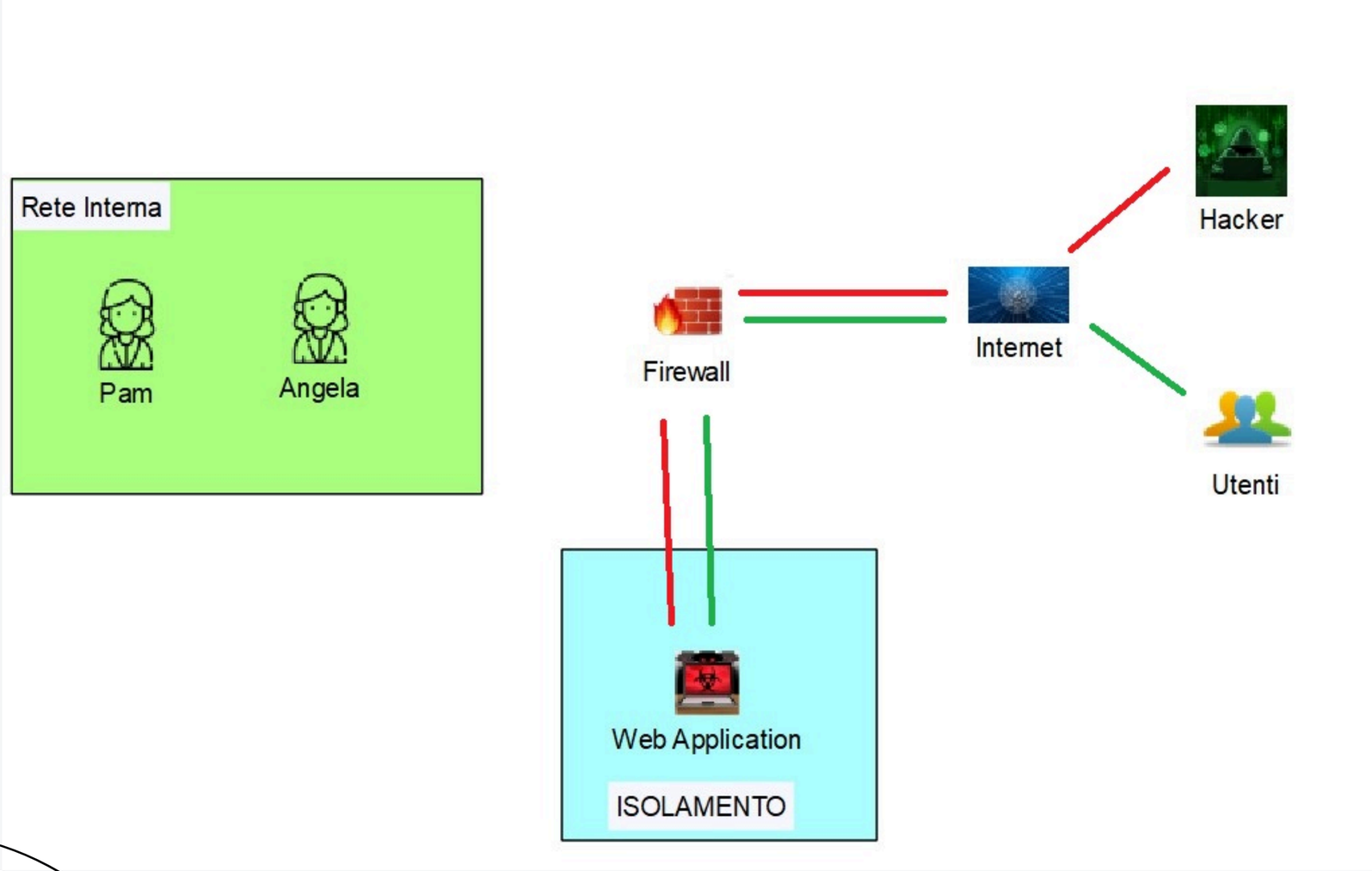

Rete Interna
Pam
Angela
Firewall
Internet
Hacker
Utenti
WAF
WAF
Web Application
DMZ

# ESERCIZIO 1

Un attacco DDoS che rende l'applicazione non raggiungibile per 10 minuti ha un impatto diretto sui ricavi dell'azienda. Considerando che gli utenti spendono in media 1.200 € al minuto vuol dire che per quei 10 minuti la perdita netta per l'azienda ammonta a 12.000€ (tenendo buone queste stime l'azienda ha un fatturato medio giornaliero di circa 1.7 Mln di euro). in questo calcolo però non viene considerato che questo disservizio può avere impatti su potenziali perdite a lungo termine dovute a danni alla reputazione, perdita di clienti, costi di ripristino e potenziali sanzioni legali da parte dei clienti e/o fornitori.

Calcolo dell'impatto:
Impatto = Entrate per minuto × Durata del downtime
Impatto = 1.200 € × 10
Impatto Totale = 12.000€.

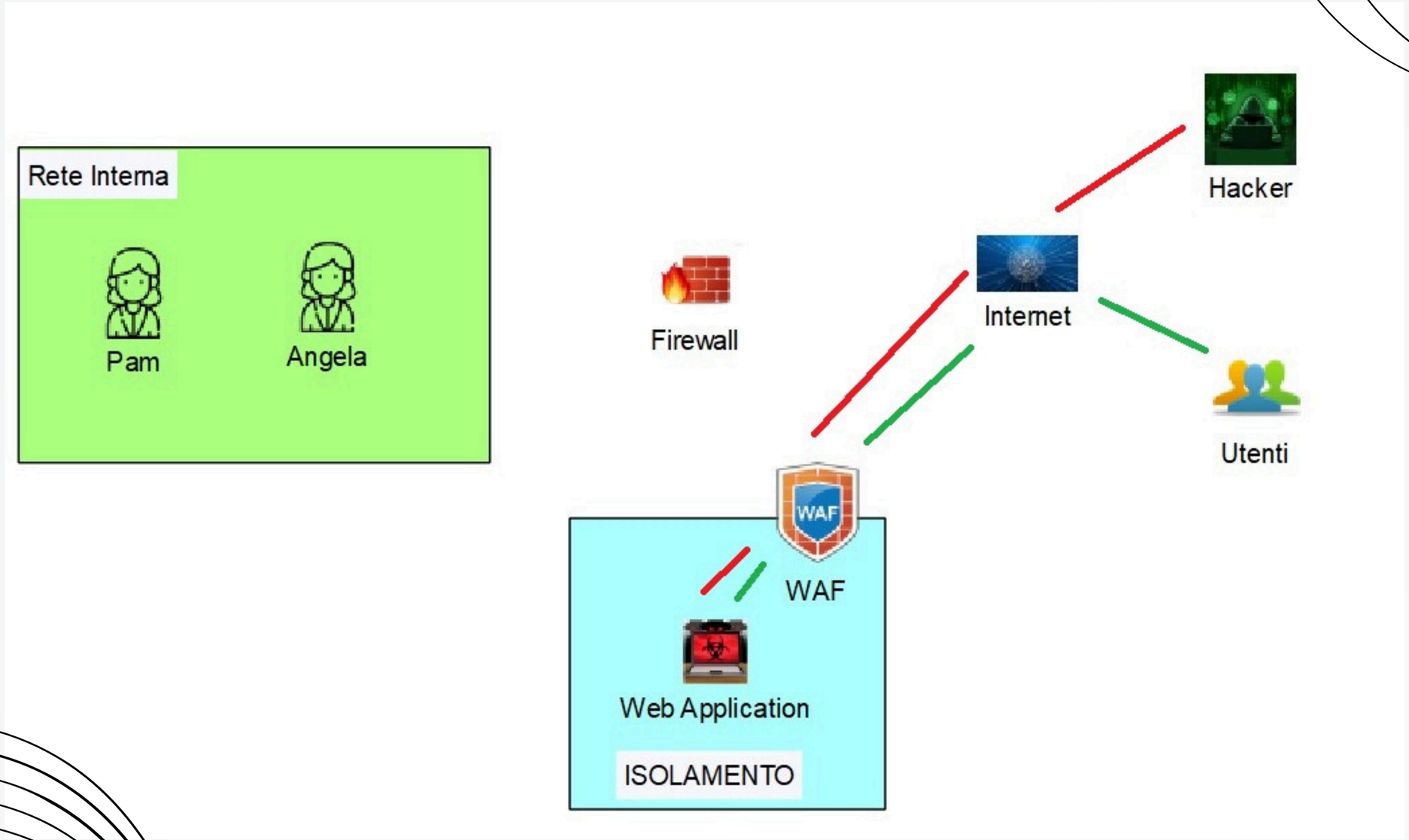
# ESERCIZIO 2




Misure di risposta per contenere l'infezione:

- Isolare il server infetto: Disconnettere il server infetto dalla rete per evitare la propagazione del malware.
- Segmentare la rete: Implementare VLAN per isolare segmenti critici della rete.
- Aggiornare le regole del firewall: Bloccare la comunicazione tra il server infetto e altri sistemi.

# ESERCIZIO 3


Rete Interna
Pam
Angela
Firewall
Hacker
Internet
Utenti
WAF
WAF
Web Application
ISOLAMENTO

# ESERCIZIO 4

Proposta di spesa 1:

- Firewall di nuova generazione (NGFW):
- Costo: 2.781,04 €
- Web Application Firewall (WAF):
- Costo: 4.440,00 €
- Intrusion Detection and Prevention System (IDPS):
- Costo: 2.000,00 €
- Sistema di Monitoraggio della Sicurezza (SIEM):
- Costo: 2750,00€

TOTALE: € 11.971,04

# ESERCIZIO 5

Proposta di spesa 2:

- Firewall di nuova generazione (NGFW):
- Costo: 2.800 €
- Web Application Firewall (WAF):
- Costo: 3.600 €
- Intrusion Detection and Prevention System (IDPS):
- Costo: 2.150 €
- Sistema di Monitoraggio della Sicurezza (SIEM):
- Costo: 3.600 €
- Content Delivery Network (CDN) con DDoS Protection:
- Costo: 3.800 €

TOTALE : ~ 15950 €

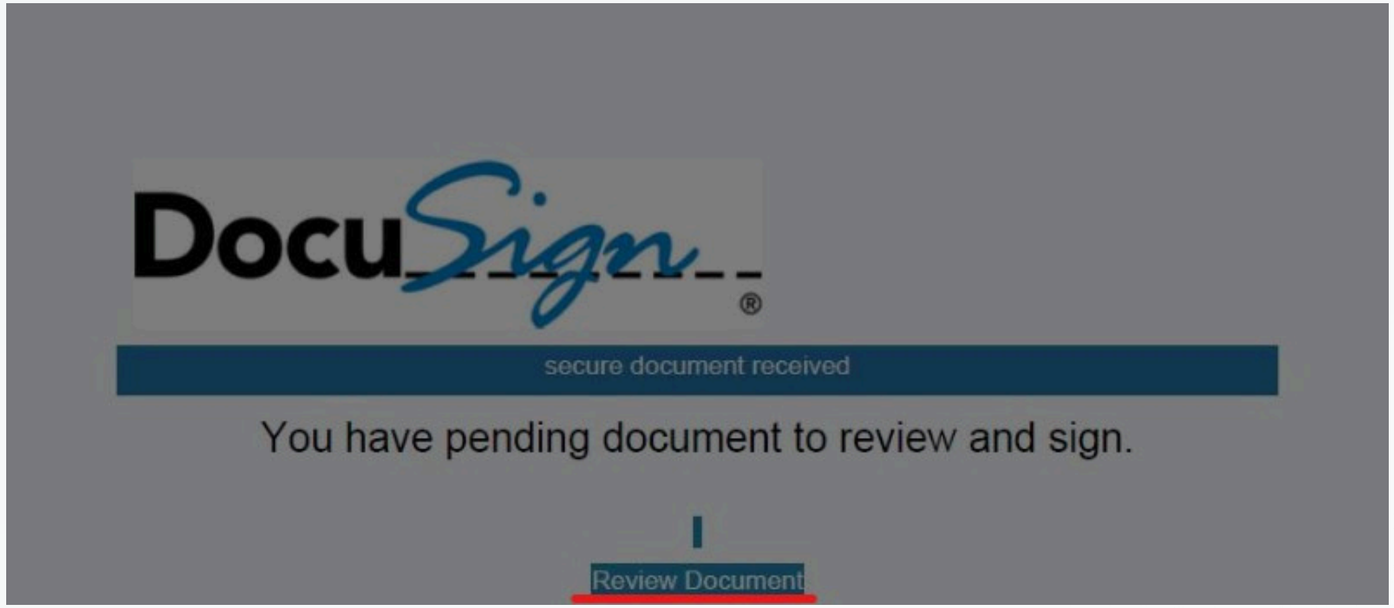
# ESERCIZIO 5

Nel primo URL ci troviamo di fronte al più classico dei phishing ovvero è una forma di attacco informatico in cui un attaccante si maschera da entità fidata per indurre gli utenti a rivelare informazioni sensibili come credenziali di accesso, dati finanziari e informazioni personali. Gli attacchi di phishing sono spesso eseguiti tramite email, messaggi di testo o siti web falsi.

Indicatori di Compromissione (IOC)
Per identificare potenziali attacchi di phishing, è importante riconoscere alcuni indicatori comuni:

1. Email sospette: Indirizzi email falsificati, errori grammaticali, e richieste urgenti di informazioni personali.
2. Link ingannevoli: URL che imitano siti legittimi ma con lievi variazioni ortografiche.
3. Allegati pericolosi: File allegati che, se aperti, possono installare malware.

in questo caso possiamo notare come il link malevolo sia annidato nel reindirizzamento per la revisione del documento.




# BONUS 1

In questo caso invece ci troviamo di fronte al malware più temuto (giustamente) da tutte le aziende, ovvero un ransomware (dalla parola ransom = riscatto), è una forma di malware che cripta i dati delle vittime e richiede un riscatto per ripristinarne l'accesso. Gli attacchi ransomware sono diventati una delle minacce informatiche più significative, colpendo individui, aziende e istituzioni

Indicatori di Compromissione (IOC)
Gli indicatori comuni di un'infezione ransomware includono:

1. File criptati: Estensioni insolite o file inaccessibili.
2. Messaggi di riscatto: Notifiche che richiedono il pagamento per decriptare i file.
3. Attività di rete anomala: Comunicazioni con server di comando e controllo.
4. Processi sospetti: Processi in esecuzione che non fanno parte delle normali operazioni del sistema.

Azioni Preventive

1. Backup regolari: Mantenere backup aggiornati e offline dei dati critici.
2. Aggiornamento software: Installare regolarmente patch e aggiornamenti di sicurezza non appena il reparto IT lo indica.
3. Educare il personale sui rischi dei malware e delle pratiche di sicurezza.
4. Soluzioni di sicurezza: Utilizzare antivirus, firewall e strumenti di rilevamento delle minacce.

# BONUS 2

# CONCLUSIONI

L'esercizio ha dimostrato con successo la capacità di ottenere una sessione remota Meterpreter sulla macchina vittima e di raccogliere le informazioni richieste. Le informazioni raccolte includono la configurazione di rete e la tabella di routing della macchina vittima, come richiesto.