

Report esercizio

Argomento: Attacchi DoS (Denial of Service) - Simulazione di un UDP Flood

Requisiti del Programma:

Input dell'IP Target:

Il programma deve richiedere all'utente di inserire l'IP della macchina target.

Input della Porta Target:

Il programma deve richiedere all'utente di inserire la porta UDP della macchina target.

Costruzione del Pacchetto:

La grandezza dei pacchetti da inviare deve essere di 1 KB per pacchetto.

Suggerimento: per costruire il pacchetto da 1 KB, potete utilizzare il modulo random per la generazione di byte casuali.

Numero di Pacchetti da Inviare:

Il programma deve chiedere all'utente quanti pacchetti da 1 KB inviare.

Flusso Operativo del codice

L'utente specifica:

IP del target: Indirizzo IPv4 della macchina bersaglio.

Porta UDP: Numero di porta compreso tra 0 e 65535.

Numero di pacchetti: Quantità totale di pacchetti UDP da inviare.

Lo script:

Crea un socket UDP utilizzando `socket.AF_INET` e `socket.SOCK_DGRAM`.

Genera pacchetti di 1 KB pieni di dati casuali tramite `random._urandom()`.

Invia ogni pacchetto utilizzando `sendto()`.

Stampa il numero del pacchetto inviato per il monitoraggio.

Gestione degli Errori:

Se si verifica un errore durante la creazione del socket o l'invio dei pacchetti, lo script stampa un messaggio di errore specifico.

Alla fine, il socket viene chiuso per liberare risorse.

Ripetizione o Uscita:

Alla fine dell'attacco, l'utente può scegliere se ripetere l'attacco o terminare l'esecuzione.

Limitazioni Tecniche:

Invio Sequenziale: I pacchetti vengono inviati uno alla volta, riducendo la velocità massima.

Mancanza di Multi-threading: L'aggiunta di più thread migliorerebbe notevolmente le prestazioni.

Controllo delle Prestazioni Assente: Lo script non misura il tempo impiegato o la velocità di invio.

Effettuato scan di rete per identificare le porte aperte sulla macchina WindowsXP

Comando: `sudo nmap -sU -p 1-1024 192.168.50.102`

```
(kali@kali)-[~]
└─$ sudo nmap -sU -p 1-1024 192.168.50.102
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-11 14:22 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.102
Host is up (0.0018s latency).
Not shown: 1023 open/filtered udp ports (no-response)
PORT      STATE SERVICE
137/udp    open  netbios-ns
MAC Address: 08:00:27:5C:8D:1C (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 16.81 seconds
```

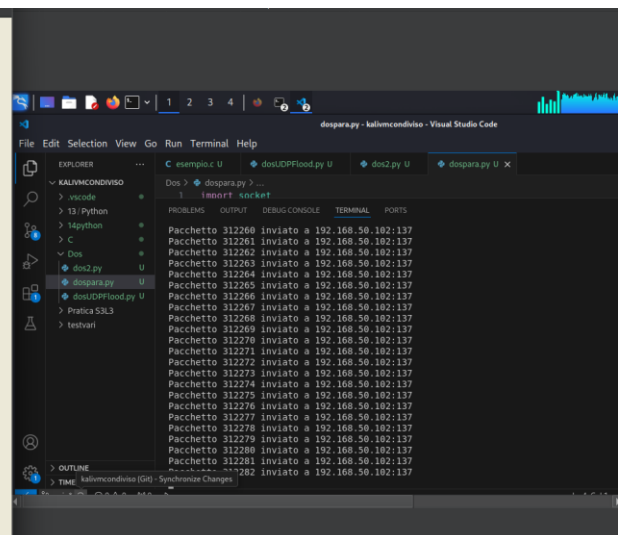
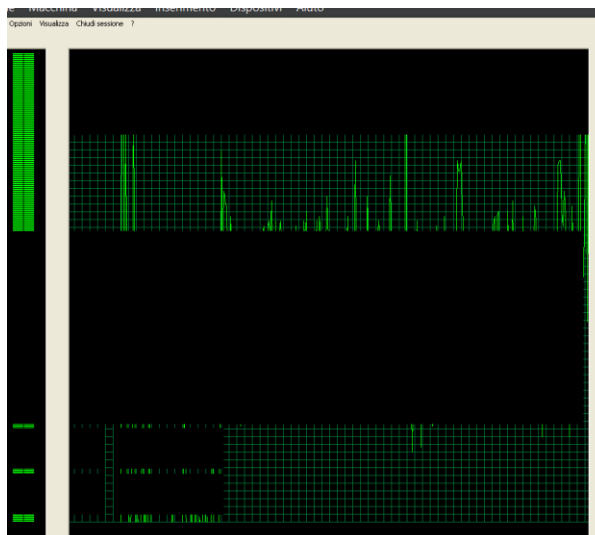
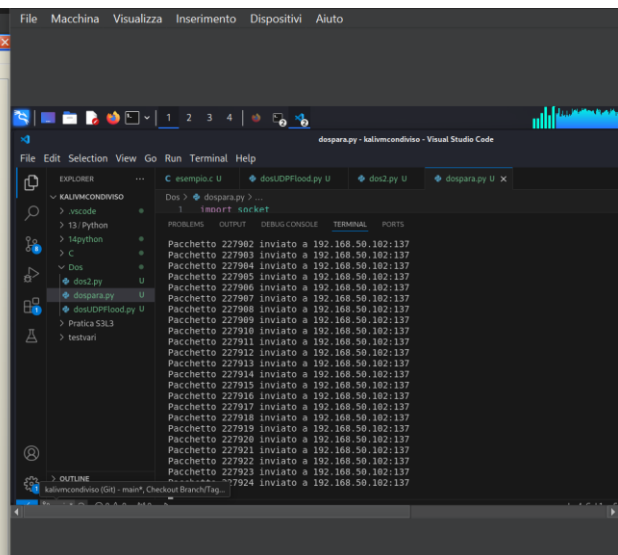
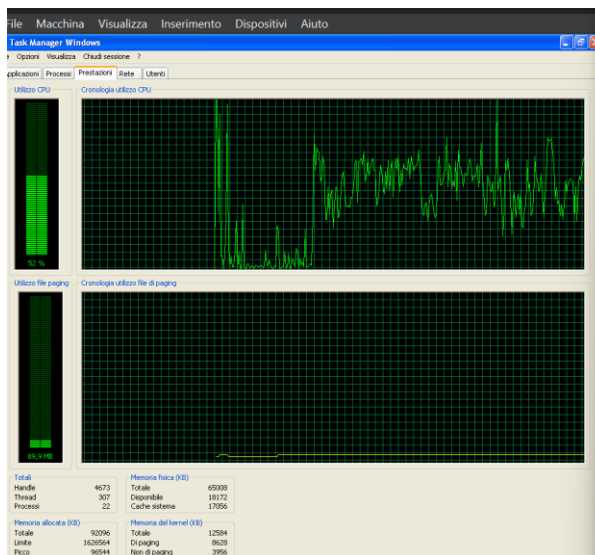
Porta UDP 137: Utilizzata da NetBIOS Name Service (NBNS) per la risoluzione dei nomi su reti basate su Windows.

Windows XP usa NBNS per convertire i nomi NetBIOS in indirizzi IP (una funzione simile al DNS).

Un attacco UDP Flood verso questa porta tenta di saturare il servizio NetBIOS, rendendo difficoltosa la risoluzione dei nomi e, in alcuni casi, causando instabilità al sistema.

Osservazioni durante il Test

Utilizzo delle risorse:



Capturing from eth0						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
Apply a display filter ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
67910	33.413679542	192.168.50.100	192.168.50.102	NBNS	1066	Unknown operation (3)[Malf
67911	33.413780909	192.168.50.100	192.168.50.102	NBNS	1066	Unknown operation (3)[Malf
67912	33.413879506	192.168.50.100	192.168.50.102	NBNS	1066	Unknown operation (3)[Malf
67913	33.414020889	192.168.50.100	192.168.50.102	NBNS	1066	Unknown operation (3)[Malf
67914	33.414147005	192.168.50.100	192.168.50.102	NBNS	1066	Unknown operation (3)[Malf
67915	33.414265097	192.168.50.100	192.168.50.102	NBNS	1066	Unknown operation (3)[Malf
67916	33.414385569	192.168.50.100	192.168.50.102	NBNS	1066	Unknown operation (3)[Malf
67917	33.414505836	192.168.50.100	192.168.50.102	NBNS	1066	Unknown operation (3)[Malf
67918	33.414625013	192.168.50.100	192.168.50.102	NBNS	1066	Unknown operation (3)[Malf
67919	33.414743564	192.168.50.100	192.168.50.102	NBNS	1066	Unknown operation (3)[Malf

▶ Frame 1: 1066 bytes on wire (8528 bits), 1066 bytes captured (8528 b ▶ Ethernet II, Src: PCSSystemtec_ad:25:87 (08:00:27:ad:25:87), Dst: PC ▶ Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.50.10 ▶ User Datagram Protocol, Src Port: 52422, Dst Port: 137 ▶ NetBIOS Name Service ▶ [Malformed Packet: NBNS] ▶ [Expert Info (Error/Malformed): Malformed Packet (Exception occur [Malformed Packet (Exception occurred)] [Severity level: Error] [Group: Malformed]	0000 08 00 27 5c 8d 1c 08 00 27 0010 04 1c 4c 72 40 00 40 11 04 0020 32 66 cc c6 00 89 04 08 ea 0030 e4 a7 c1 41 7a a1 3c a0 64 0040 71 95 64 32 d5 5a 26 f0 49 0050 0f b3 3a 5f 88 18 9a d6 c8 0060 f9 b0 c9 1b 73 74 6e bb d6 0070 95 52 f3 38 62 dc dd ec f6 0080 43 22 2e ec 6a 90 5f 0d 72 0090 37 5a 2b a1 13 fe f1 58 f7 00a0 75 0f 16 78 33 f5 dc f7 79 00b0 4a 8d 4c 48 71 46 5c 91 de
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Dettagli del Protocollo NBNS

NBNS è utilizzato per la risoluzione dei nomi NetBIOS in reti basate su Windows.

Porta tipica: 137 (UDP).

Quando un pacchetto è etichettato come "Malformed," significa che i dati catturati non rispettano le specifiche del protocollo.

Pacchetti Randomici: Lo script `udp_flood` sta inviando pacchetti con contenuti casuali generati da `random._urandom`. Questi pacchetti non contengono dati validi per il protocollo NBNS.

Risultato osservato: Wireshark rileva pacchetti NBNS "malformati," confermando che il traffico generato è casuale e non conforme al protocollo.

Conclusioni per il Report sull'Esercizio UDP Flood

Risultati Principali

L'esercizio ha dimostrato come un attacco UDP Flood possa saturare un servizio vulnerabile come NetBIOS Name Service (NBNS) sulla porta UDP 137 di Windows XP. La simulazione ha evidenziato l'efficacia dell'invio massivo di pacchetti casuali in ambienti di test controllati. Le seguenti osservazioni sono emerse durante il test:

Traffico Generato:

Pacchetti UDP di 1 KB generati casualmente sono stati rilevati tramite Wireshark come "malformati," indicando che il traffico non segue uno standard specifico del protocollo NBNS.

Comportamento del Target:

Windows XP ha risposto gestendo alcuni pacchetti NBNS, ma il sistema è diventato meno reattivo con l'aumentare del carico, confermando l'efficacia del test.

Limitazioni Ricontrate

Pacchetti Malformati:

I pacchetti inviati sono casuali e non conformi agli standard NBNS, riducendo l'efficacia dell'attacco per test specifici.

Invio Sequenziale:

L'invio di pacchetti è sequenziale, limitando le prestazioni. L'introduzione di multi-threading migliorerebbe l'efficienza.

Assenza di Feedback Avanzato:

Sebbene il programma mostri il rendimento finale, mancano metriche più dettagliate come i tempi medi di risposta del target.

Ottimizzazione delle Prestazioni: Aggiungere multi-threading o multiprocessing per migliorare la velocità di invio dei pacchetti.

Protocollo Simulato Realistico: Includere pacchetti conformi agli standard NBNS per test più precisi.

Miglioramento dell'Interfaccia: Integrare ulteriori metriche come il tempo medio di risposta e la percentuale di pacchetti ricevuti con successo.