UNIVERSITÀ DEGLI STUDI DI BARI
"ALDO MORO"

DIPARTIMENTO DI INFORMATICA
Corso di Laurea in
Informatica e Tecnologie per la Produzione del Software

Tesi di Laurea in
Reti di calcolatori + laboratorio

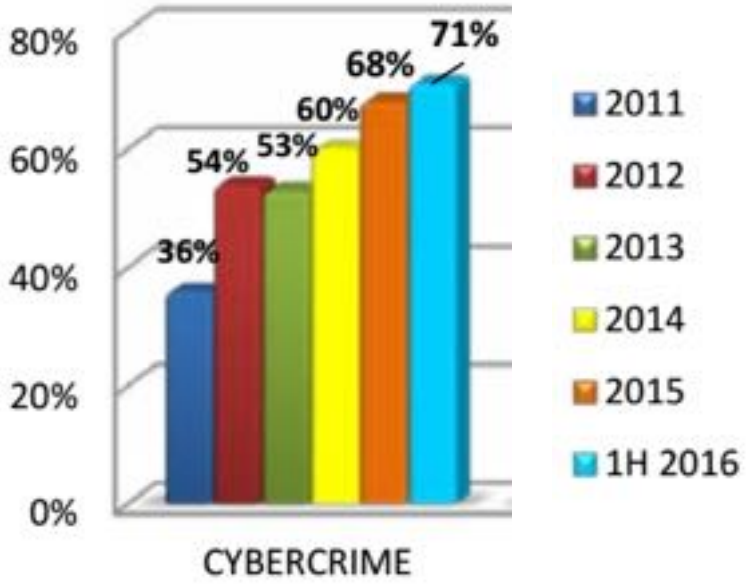
Utilizzo di next-generation firewall per l'analisi e l'implementazione di nuove tecniche di protezione delle reti telematiche

Relatore:
Prof. Michele Scalera
Correlatore:
Dott. Emanuele Magno

Laureando:
Domenico Picerno

Scopi degli attacchi informatici

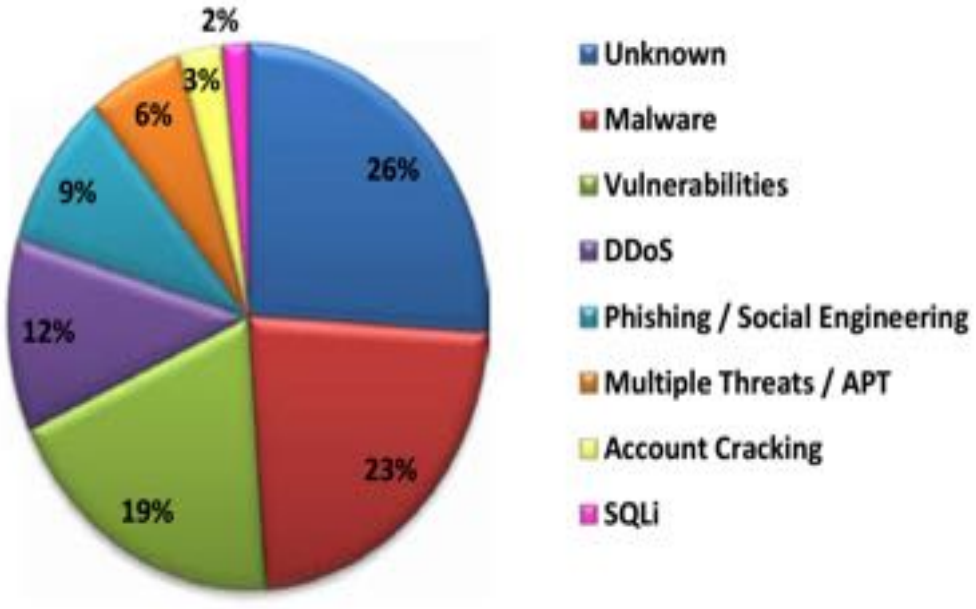
Distribuzione percentuale degli attaccanti 2011- 1H 2016



Analisi clusit

- Continuo incremento degli attacchi alle reti telematiche
- Danni arrecati principalmente a scopo di lucro
- Necessità di studiare ed implementare nuove tecniche di difesa

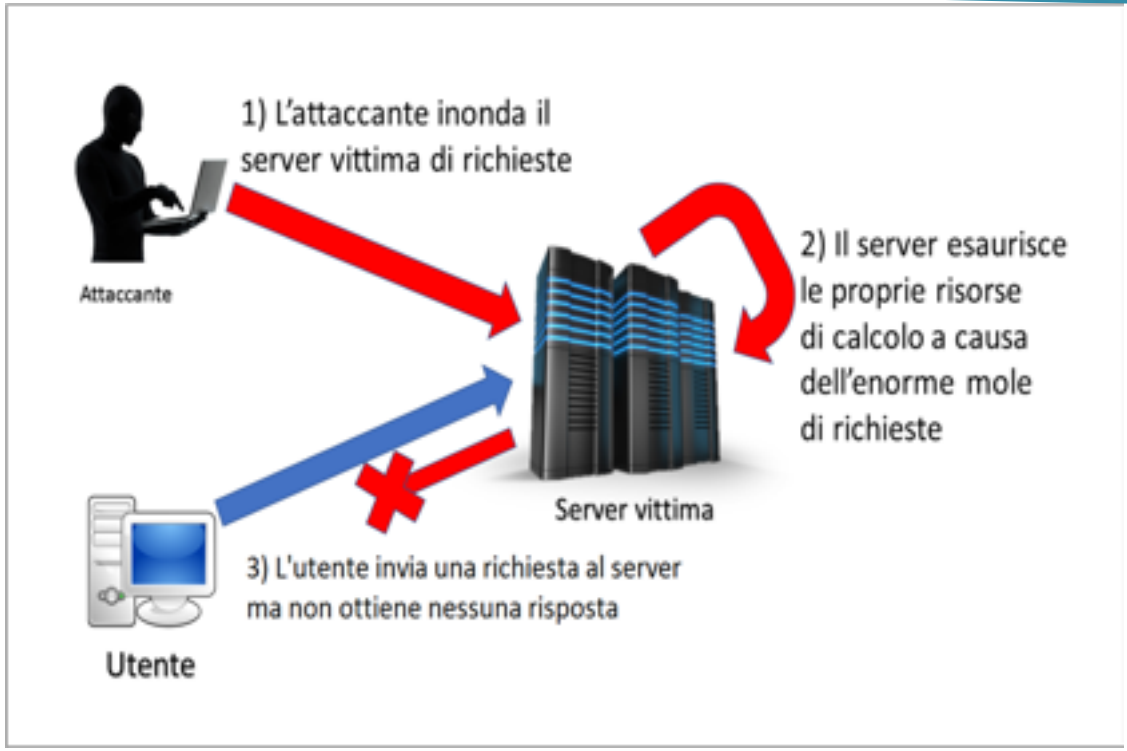
Tipologia di attacchi informatici



Rapporto 2016 sulla Sicurezza ICT in Italia - Aggiornamento Giugno 2016

- Molte tipologie ancora sconosciute
- Malware ancora tra i metodi di attacco più utilizzati (virus, worm, trojan, ram scraper, ransomware)
- Le vulnerability dei sistemi software possono anche essere sfruttate per attacchi DoS e DDoS

Gli attacchi Denial of Service (DoS)

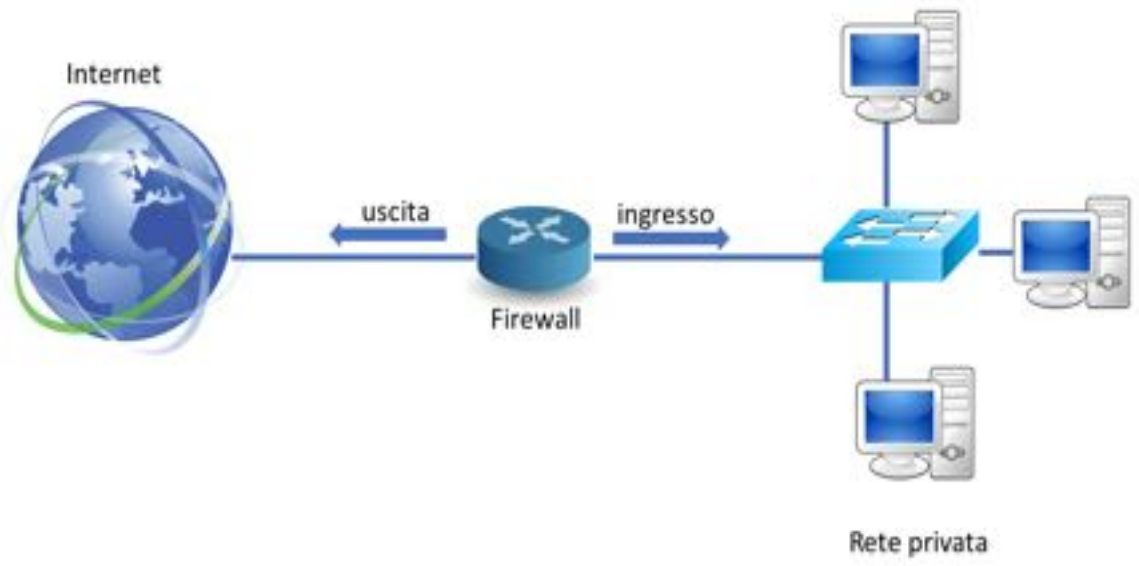


- Singolo attaccante
- Interruzione dell'erogazione di servizi da parte della vittima
- Può essere effettuato sfruttando molti protocolli basati su TCP (HTTP) o UDP (DNS, NTP, NetBIOS)
- Se effettuato da più attaccanti simultaneamente si tratta di Distributed Denial of Service (DDoS)

Gli attacchi Denial of Service (DoS)

- Possibile interruzione dei servizi per giorni
- Si basano sulla ricerca dei punti deboli della rete vittima
- Definizione di policy orientate alla protezione utilizzando anche strumenti di ultima generazione come NGFW

Next-generation firewall (NGFW)



Firewall tradizionale:

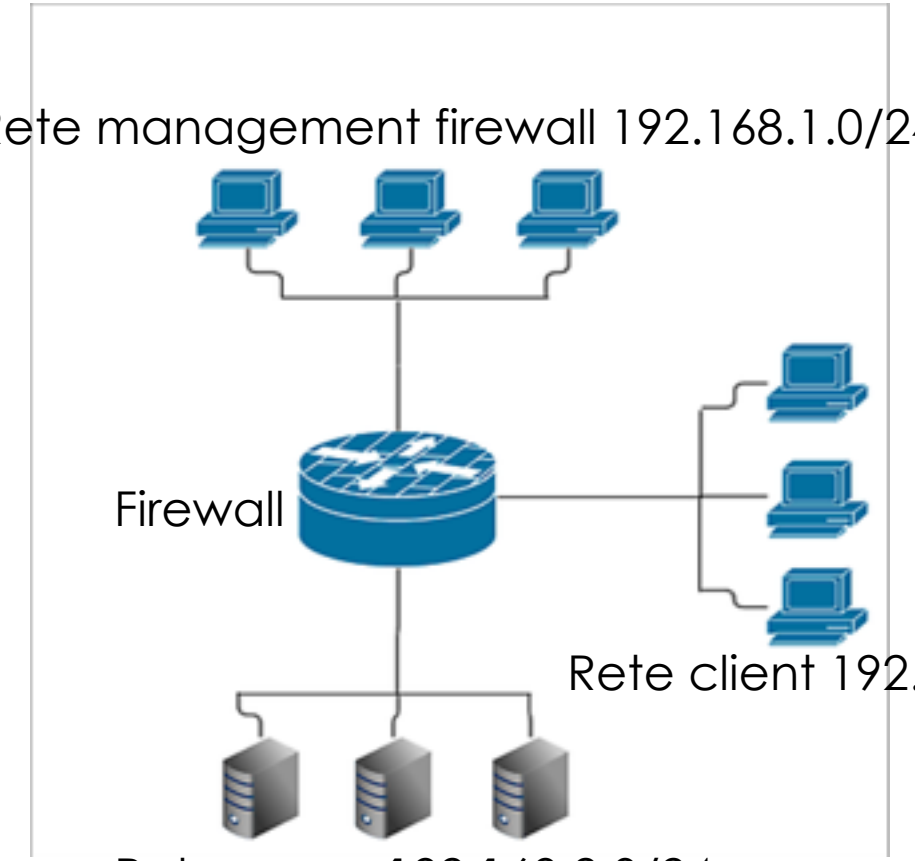
- Hardware, software o combinazione delle due
- Si basa sulla creazione delle regole di protezione
- Non consente controlli accurati su protocolli di alto livello della pila ISO/OSI

Next-generation firewall (NGFW)

NGFW

- Evoluzione del firewall tradizionale
- Meccanismo di stateful inspection
- Controllo dei comportamenti dei client
- Gestione accurata del traffico
- Prevenzione dalle intrusioni
- Filtraggio contenuti web
- Ispezione virus

Progetto dell'esperimento

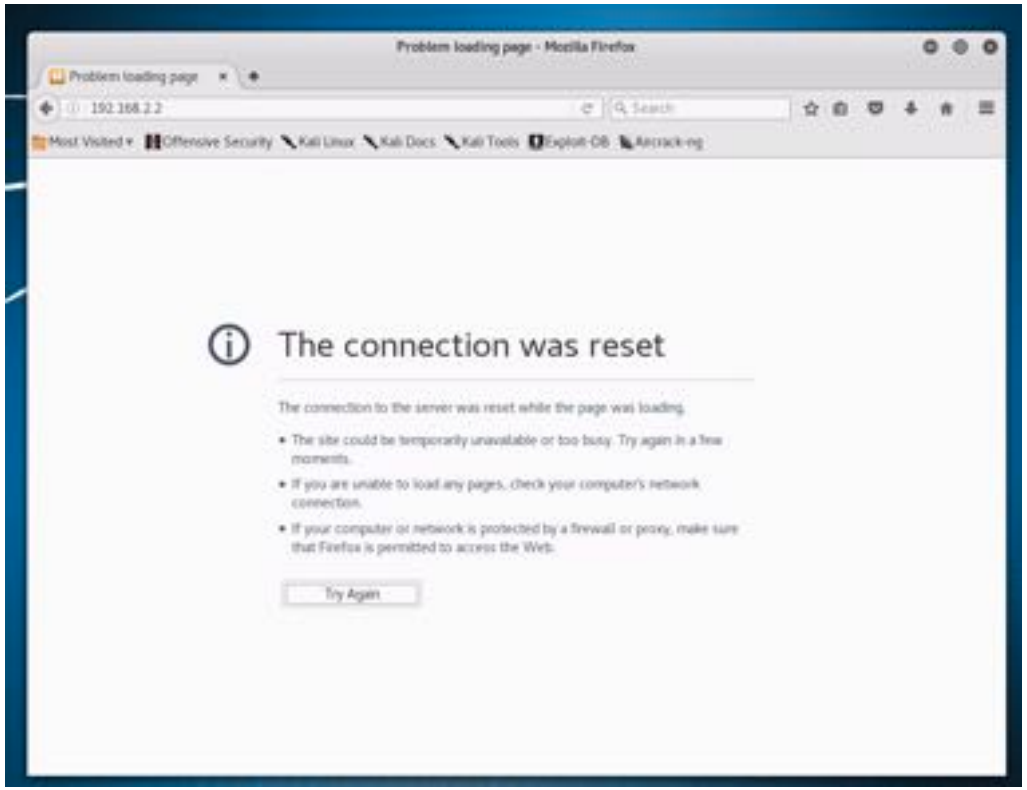


- Ambiente completamente virtualizzato
- Composizione di 3 reti: client, server e management
- Rete server con server web Apache e server DNS BIND9
- NGFW al centro della rete
- Limite di banda impostato a 50Mbps (45Mbps per il download di dati e 5Mbps per l'upload)
- 3 regole di protezione per consentire comunicazioni HTTP, DNS e PING

Attacco Slowloris

- Diretto ai soli server web Apache
- Apertura numerosi slot di comunicazione
- Continuo invio di richieste HTTP GET incomplete
- L'attesa di ulteriori informazioni porta il server web in DoS

Attacco Slowloris



- Comando utilizzato

perl slowloris.pl -dns 192.168.2.2 -port 80 -num 500 -timeout 5

Parametri:

- -num= numero threads
- -dns= indirizzo IP vittima
- -port= porta da attaccare
- -timeout= tempo reinvio richiesta

Attacco Slowloris

- Grafico di utilizzo rete da parte del server

Attacco DNS-Amplification

DoS con amplificazione

- Tipologia di attacco basta sul meccanismo di amplificazione: risposta del server molto pesante (in byte) rispetto alla richiesta
- Tecnica utilizzabile su molti protocolli basati su UDP (DNS, NTP, LDAP)

DNS-Amplification

- Si basa sui server open-resolver
- Richiesta di informazioni inutili per aumentare il peso della risposta
- Utilizzo del comando DIG ANY
- Ai nomi da risolvere vengono associati molti record spazzatura

Attacco DNS-Amplification

- Fattore di amplificazione ottenuto nei test di laboratorio: 57,4
- Attacco sferrato utilizzando il tool **Saddam**, basato sull'utilizzo del comando DIG ANY

- Comando utilizzato:

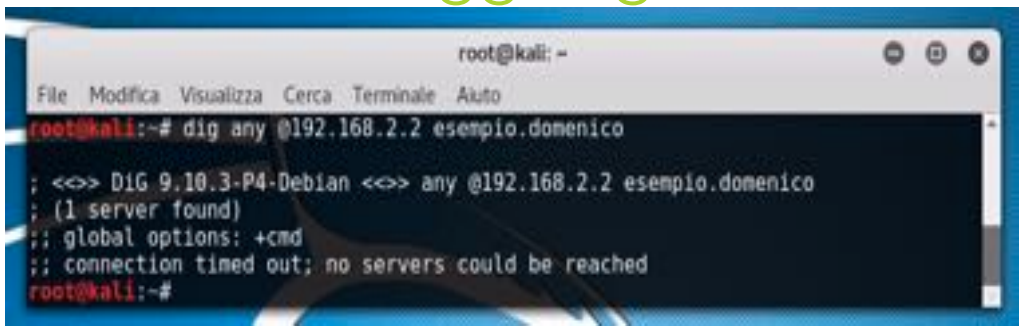
python Saddam.py 192.168.3.3 –dns=list.txt:esempio.domenico -t 100

Parametri utilizzati:

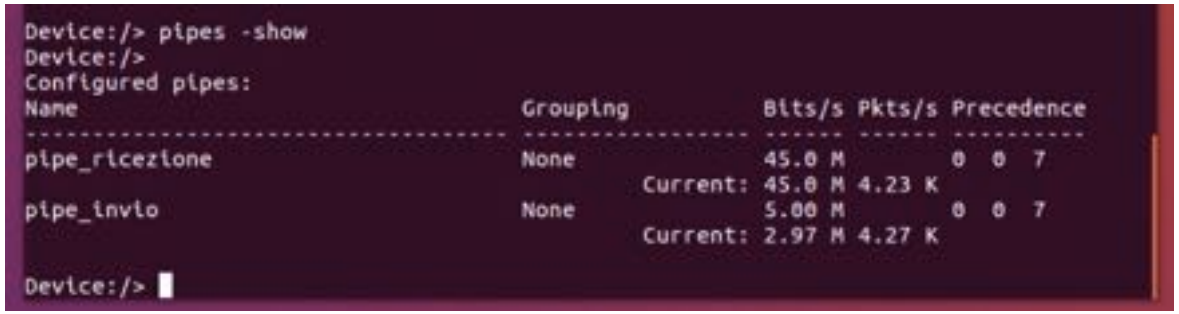
- -t = numero threads
- list.txt= file contenente indirizzo server vittima
- esempio.domenico= indirizzo da tradurre

Attacco DNS-Amplification

Server dns irraggiungibile

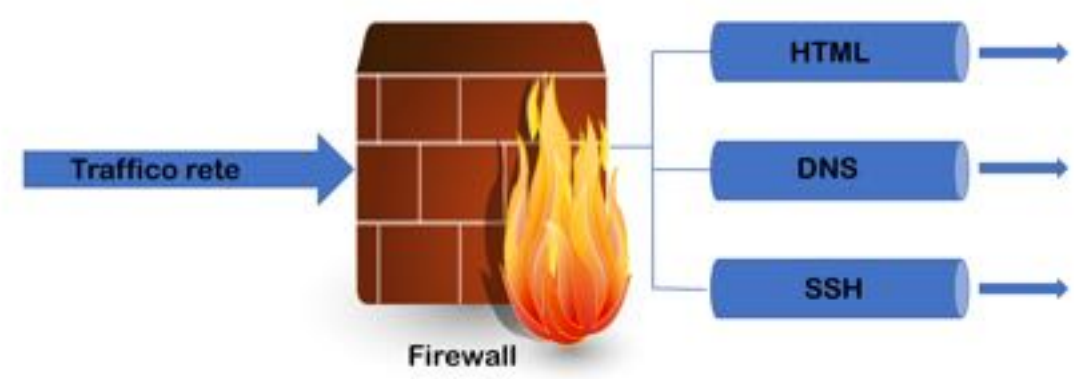


Saturazione dei 45Mbps dedicati al download



Incremento dell'utilizzo medio della CPU del server dal 65% al 96,3%

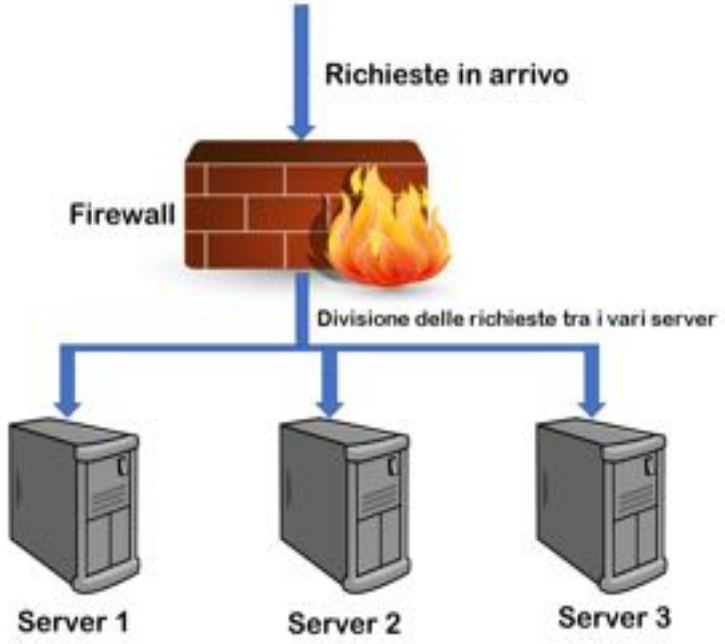
Tecniche di protezione avanzate: Pipe & Pipe Rules



Pipe

- Canali concettuali in cui fluisce il traffico dati
- Creabili per ogni protocollo
- Assegnazione limite di bandwidth
- Vengono utilizzate nelle pipe rules
- In caso di attacco DoS, viene saturata solo quella in cui fluisce il protocollo sotto attacco mentre le altre restano inalterate

Tecniche di protezione avanzate: Server load balancing



- Divisione del carico di rete tra i vari server
- Algoritmi di divisione: Round-robin e Connection-rate
- Continuo monitoraggio dei server con messaggi di controlli basati su ICMP, HTTP o TCP
- In caso di sovraccarico di un server, le richieste vengono dirottate su altri calcolatori più liberi

Tecniche di protezione avanzate: Threshold rules

- Regole comportamentali
- Individuazione e reazione contro livelli anomali di connessione
- Permettono di bloccare l'host che ha attivato la regola
- Soglia di attivazione esprimibile in numero di connessioni attive o per connessioni aperte al secondo

Implementazione tecniche di protezione: pipe e pipe rules

Creazione due nuove pipe:

- Una con limite di 10Mbps
- Una con limite di 35Mbps

Utilizzo delle pipe in due nuove pipe rules:

- Pipe da 35Mbps utilizzata per il protocollo DNS
- Pipe da 10Mbps utilizzata per il protocollo HTTP

Implementazione tecniche di protezione: Server load balancing

Per protezione protocollo HTTP

Protocolli di monitoraggio utilizzati:

- ICMP
- HTTP

Algoritmo di divisone richieste utilizzato:

- Round-robin

Per protezione protocollo DNS

Protocolli di monitoraggio utilizzati:

- ICMP
- TCP (su porta 53)

Algoritmo di divisione richieste utilizzato:

- Connection-rate

Implementazione tecniche di protezione: Threshold rules

Per protezione protocollo HTTP

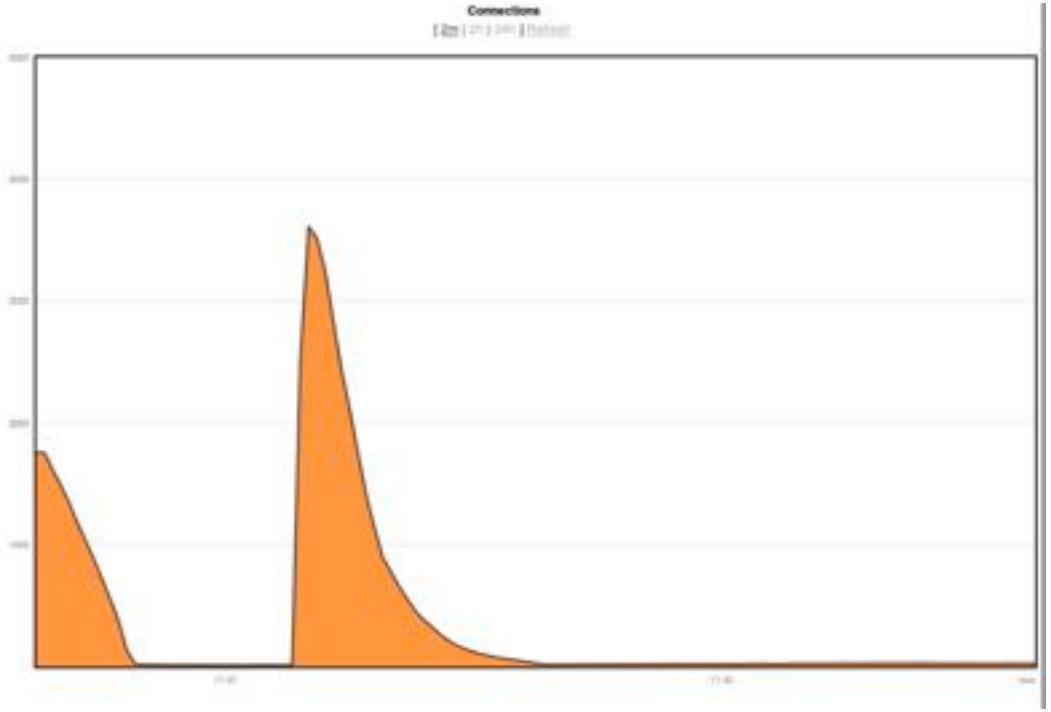
- Controllo per connessioni attive
- Valore soglia impostato a 100 connessioni
- Blacklist dell'host solo per protocollo HTTP

Per protezione protocollo DNS

- Controllo per connessioni effettuate al secondo
- Valore soglia impostato a 3800 connessioni al secondo
- Blacklist dell'host per tutti i protocolli

Test di attacco DNS-Amplification

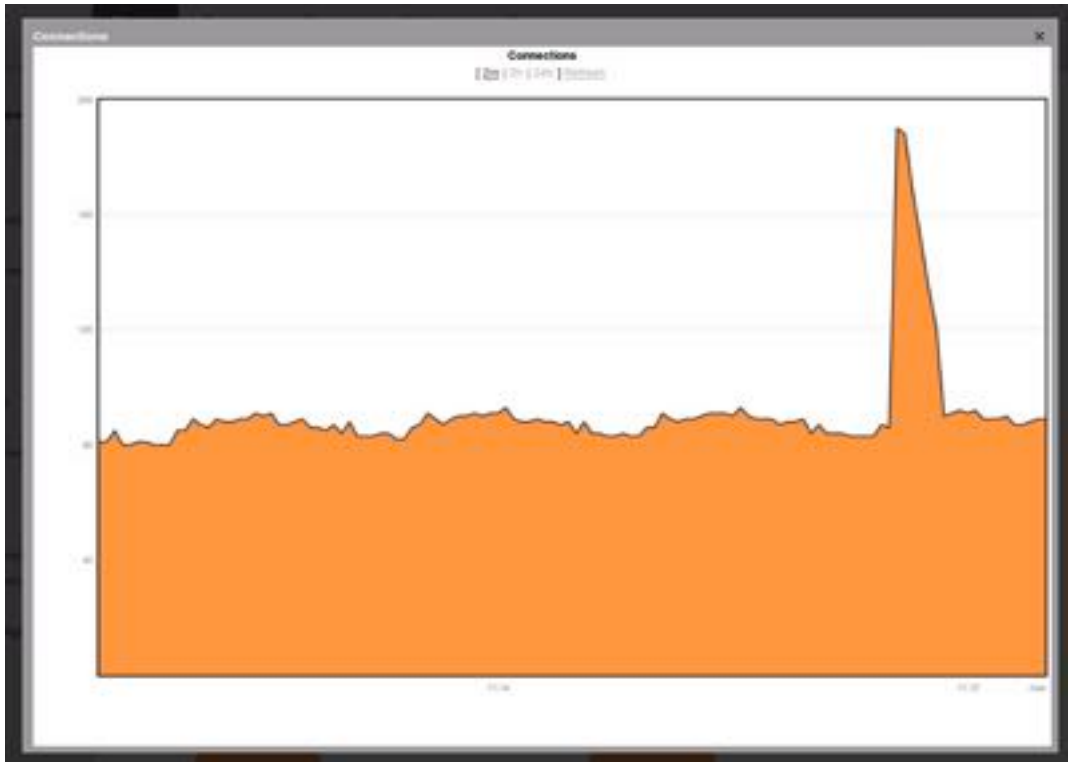
Grafico connessioni dell'NGFW durante l'attacco



- Picco corrispondente all'inizio dell'attacco
- Una volta raggiunto il valore soglia 3800 tutte le connessioni vengono chiuse

Test di attacco Slowloris

Grafico connessioni dell'NGFW durante l'attacco



- Picco corrispondente all'inizio dell'attacco
- Una volta raggiunto il valore soglia 100, tutte le connessioni vengono chiuse

Conclusioni

- Scenario: utilizzando tool liberamente reperibili su Internet, è possibile sferrare attacchi informatici anche di grande potenza.
- Consapevolezza dell'importanza della sicurezza
- Soluzione: investimento in policy di sicurezza (risorse umane, ricerca)
- Trend: applicazione tecniche AI per protezione (utilizzando ad es. BIG DATA)

Grazie per l'attenzione