



STRUMENTI DI TESTING DELLA RETE

6 SETTEMBRE 2024



Programma della presentazione

Progetto 1: Port Scanner

Progetto 2: Interrogatore verbi HTTP

Progetto Bonus: Rilevatore socket



Progetto n. 1: Port Scanner



Introduzione al Port Scanner

Scopo del Programma:

Scansionare le porte di un indirizzo IP fornito dall'utente per identificare porte aperte e relative servizi.

Utilità:

Fornire un report sulla sicurezza della rete.

- Verifica della sicurezza della rete;
- Gestione delle risorse di rete;
- Troubleshooting e diagnosi;
- Conformità alle normative di sicurezza;
- Prevenzione accessi non autorizzati.



Funzionamento

Input Utente:

L'utente inserisce indirizzo IP, porta iniziale e porta finale.

Ciclo di scansione:

Il programma scansiona ogni porta nell'intervallo indicato.

Connessione TCP:

Verifica se la porta è aperta.

Risultati:

Stampa sul terminale la lista di porte aperte e dei relative servizi



Esempio di output

```
Inserisci l'indirizzo IP da scansione: 192.168.1.248
Inserisci il numero di porta da cui iniziare la scansione: 20
Inserisci il numero di porta con cui terminare la scansione: 80
Attualmente in scan: porta 20
Attualmente in scan: porta 21
Attualmente in scan: porta 22
Attualmente in scan: porta 23
Attualmente in scan: porta 24
Attualmente in scan: porta 25
Attualmente in scan: porta 26
Attualmente in scan: porta 27
Attualmente in scan: porta 28
Attualmente in scan: porta 29
Attualmente in scan: porta 30
```

```
Risultati della scansione:
Porta 21: Aperta | Servizio: ftp
Porta 22: Aperta | Servizio: ssh
Porta 23: Aperta | Servizio: telnet
Porta 25: Aperta | Servizio: smtp
Porta 53: Aperta | Servizio: domain
Porta 80: Aperta | Servizio: http
```

```
La scansione è terminata.
```




Progetto n. 2: Interrogatore verbi HTTP



Introduzione all'Interrogatore verbi

Scopo del Programma:

Verificare e interrogare metodi HTTP supportati.

Utilità:

Facilitare la gestione e la sicurezza di applicazioni web e server.

- Verifica dei metodi HTTP supportati;
- Sicurezza e conformità;
- Troubleshooting e diagnosi;



Funzionamento

Input Utente:

L'utente inserisce l'URL o l'indirizzo IP target.

Invio richiesta:

Il programma scansiona ogni porta nell'intervallo indicato.

Stampa dei verbi abilitati e presentazione del menù:

Il programma entra in un loop che presenta un menù interattivo all'utente, permettendogli di scegliere quale verbo verificare.

Risultati:

Stampa sul terminale la risposta ricevuta in base al verbo selezionato.



Esempio di output

```
Inserisci l'URL o l'IP del target da interrogare: 192.168.1.248
```

```
Metodi HTTP abilitati per 192.168.1.248:
```

- GET
- POST
- PUT
- DELETE

```
Scegli un verbo HTTP:
```

```
Digita 1 per GET;
```

```
Digita 2 per POST;
```

```
Digita 3 per PUT;
```

```
Digita 4 per DELETE;
```

```
Digita 0 per terminare il programma.
```

```
La tua scelta: █
```

```
La tua scelta: 1
```

```
Risposta web: 200
```

```
·  
·  
·
```

```
Scegli un verbo HTTP:
```




Progetto bonus: Rilevatore socket di rete



Introduzione al rilevatore socket di rete

Scopo del Programma:

Lo scopo del programma è catturare i pacchetti di rete in tempo reale analizzando le connessioni attive e visualizzando un'analisi dettagliata delle intestazioni IP e TCP.

Utilità:

L'utilizzo di questo programma è consigliato per mantenere la rete aziendale sicura, efficiente e ben gestita, facilitando la risoluzione dei problemi e il monitoraggio delle risorse di rete.

- Monitoraggio della rete;
- Gestione delle connessioni;
- Sicurezza;
- Analisi delle prestazioni;
- Diagnosi dei problemi.i.



Funzionamento

Import dei moduli utilizzati:

- socket
- psutil
- struct

Definizione delle funzioni principali

- parse_ip_header
- parse_tcp_header
- parse_packet_info

Main script e recupero delle connessioni attive

Il programma recupera le connessioni di rete attive fornendo un elenco dettagliato delle connessioni in corso.

Inizio di un loop infinito:

Il programma inizia un ciclo 'while' per ricevere e analizzare i pacchetti.

Stampa dei risultati:

Le informazioni dettagliate vengono stampate sul terminale.



Esempio di output

```
Protocol  Local Address  Remote Address  Status  PID  Process Name
Pacchetto ricevuto: b'E\x00\x004I\x7f@\x00m\x06\xac\x89\x14*AU\xc0\xa8\x01\x94\x01\xbb\xe2\x88)\x97\xf4z\xe6\xe9\x995\x80\x10@\x01'
IP Header:
  Version: 4
  IHL: 5
  TTL: 109
  Protocol: TCP
  Source IP: 20.42.65.85
  Destination IP: 192.168.1.148
TCP Header:
  Source Port: 443
  Destination Port: 57992
UDP      192.168.1.148:68      192.168.1.1:67      NONE      603      NetworkManager
TCP      192.168.1.148:57992  20.42.65.85:443     ESTABLISHED      1635      code
```




PANTER
PWNERS

Cyber Security Solutions

Grazie per
l'attenzione
