INTRODUZIONE ALL'HACKING

Pre-requisiti: Network(4)

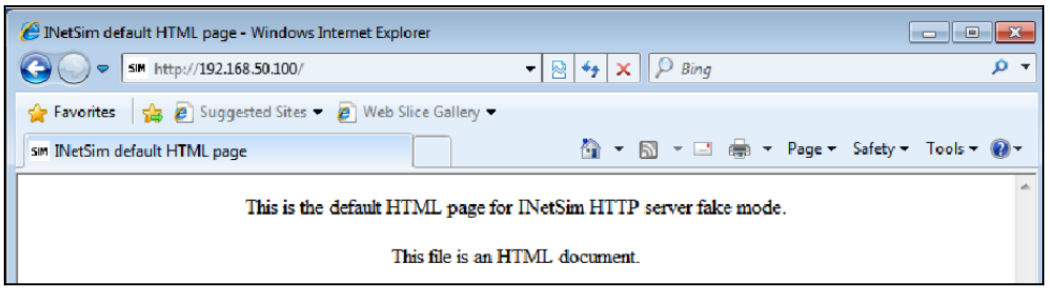
PACKET CAPTURE CON WIRESHARK

Ping da macchina Linux(192.168.50.100) a Macchina Windows 7 (192.168.50.102)

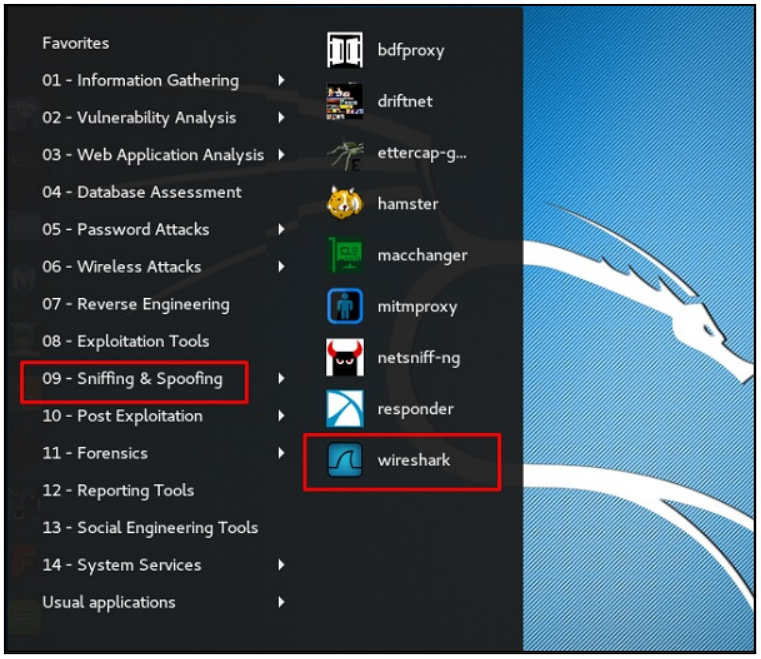
```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.50.102 -c 4
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.
64 bytes from 192.168.50.102: icmp_seq=1 ttl=128 time=0.348 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=0.213 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=0.248 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=0.266 ms

── 192.168.50.102 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3491ms
rtt min/avg/max/mdev = 0.213/0.268/0.348/0.049 ms
```

Utilizzo l'utility di InetSim per l'emulazione di servizi Internet

```
┌──(root㉿kali)-[~]
└─# inetsim
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory:      /var/log/inetsim/
Using data directory:     /var/lib/inetsim/
Using report directory:   /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
=== INetSim main process started (PID 9184) ===
Session ID:     9184
Listening on:   0.0.0.0
Real Date/Time: 2023-06-19 09:19:34
Fake Date/Time: 2023-06-19 09:19:34 (Delta: 0 seconds)
 Forking services...
  * dns_53_tcp_udp - started (PID 9186)
  * smtp_25_tcp - started (PID 9189)
  * time_37_udp - started (PID 9202)
  * smtps_465_tcp - started (PID 9190)
  * pop3_110_tcp - started (PID 9191)
  * ftps_990_tcp - started (PID 9194)
  * chargen_19_tcp - started (PID 9211)
  * chargen_19_udp - started (PID 9212)
  * pop3s_995_tcp - started (PID 9192)
  * tftp_69_udp - started (PID 9195)
  * irc_6667_tcp - started (PID 9196)
  * ntp_123_udp - started (PID 9197)
  * http_80_tcp - started (PID 9187)
  * finger_79_tcp - started (PID 9198)
  * ident_113_tcp - started (PID 9199)
  * discard_9_tcp - started (PID 9207)
  * ftp_21_tcp - started (PID 9193)
  * syslog_514_udp - started (PID 9200)
  * time_37_tcp - started (PID 9201)
  * https_443_tcp - started (PID 9188)
  * daytime_13_udp - started (PID 9204)
  * discard_9_udp - started (PID 9208)
  * daytime_13_tcp - started (PID 9203)
  * quotd_17_tcp - started (PID 9209)
  * echo_7_tcp - started (PID 9205)
  * quotd_17_udp - started (PID 9210)
  * echo_7_udp - started (PID 9206)
  * dummy_1_udp - started (PID 9214)
  * dummy_1_tcp - started (PID 9213)
 done.
Simulation running.
```



Catturo i pacchetti con Wireshark



Source	Destination	Protocol	Length	Info
127.0.0.1	127.0.0.1	TCP	74	43376 → 80 [SYN] Seq=0 Win=65495 Len=0 MS
127.0.0.1	127.0.0.1	TCP	74	80 → 43376 [SYN, ACK] Seq=0 Ack=1 Win=654
127.0.0.1	127.0.0.1	TCP	66	43376 → 80 [ACK] Seq=1 Ack=1 Win=65536 Le
127.0.0.1	127.0.0.1	HTTP	497	GET / HTTP/1.1
127.0.0.1	127.0.0.1	TCP	66	80 → 43376 [ACK] Seq=1 Ack=432 Win=65152
127.0.0.1	127.0.0.1	TCP	216	80 → 43376 [PSH, ACK] Seq=1 Ack=432 Win=6
127.0.0.1	127.0.0.1	TCP	66	43376 → 80 [ACK] Seq=432 Ack=151 Win=6540
127.0.0.1	127.0.0.1	HTTP	324	HTTP/1.1 200 OK (text/html)
127.0.0.1	127.0.0.1	TCP	66	43376 → 80 [ACK] Seq=432 Ack=409 Win=6515
127.0.0.1	127.0.0.1	TCP	66	43376 → 80 [FIN, ACK] Seq=432 Ack=409 Win
127.0.0.1	127.0.0.1	TCP	66	80 → 43376 [FIN, ACK] Seq=409 Ack=433 Win
127.0.0.1	127.0.0.1	TCP	66	43376 → 80 [ACK] Seq=433 Ack=410 Win=6553