CUORE ANDREA

27-10-2022

MODIFICA PRIORITY DEL FIREWALL

E

SNIFFING PACCHETTI DI UNA RETE CREATA SU KALI

TASK:

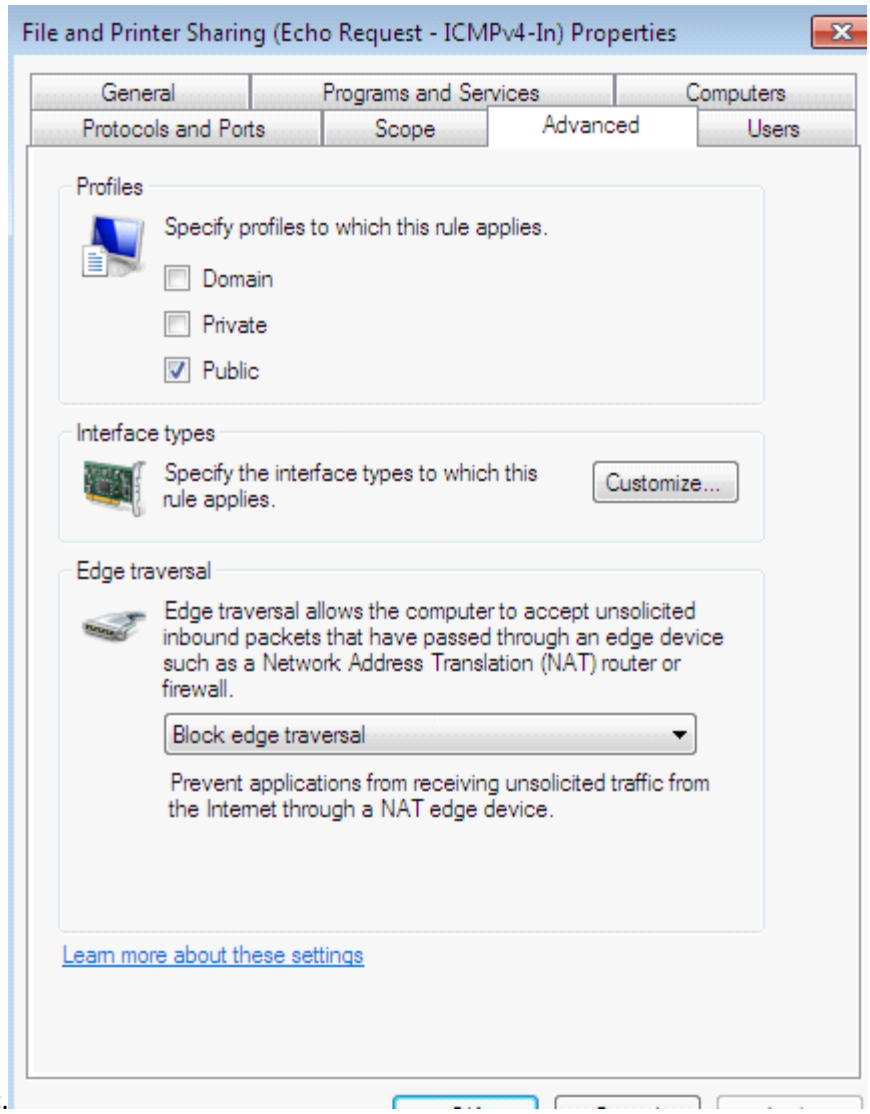
L'esercizio di oggi mira a consolidare le conoscenze acquisite nella lezione del mattino. Vedremo due esercizi: I) la configurazione di una policy sul firewall windows; II) una packet capture con Wireshark. Vedremo anche come simulare alcuni servizi di rete con un tool pre-installato su Kali Linux (InetSim)

Esercizio:

- Configurare policy per il ping da macchine Linux a Macchina Windows nel nostro laboratorio
- Utilizzo dell'utility InetSim per l'emulazione di servizi Internet
- Cattura di pacchetti con Wireshark

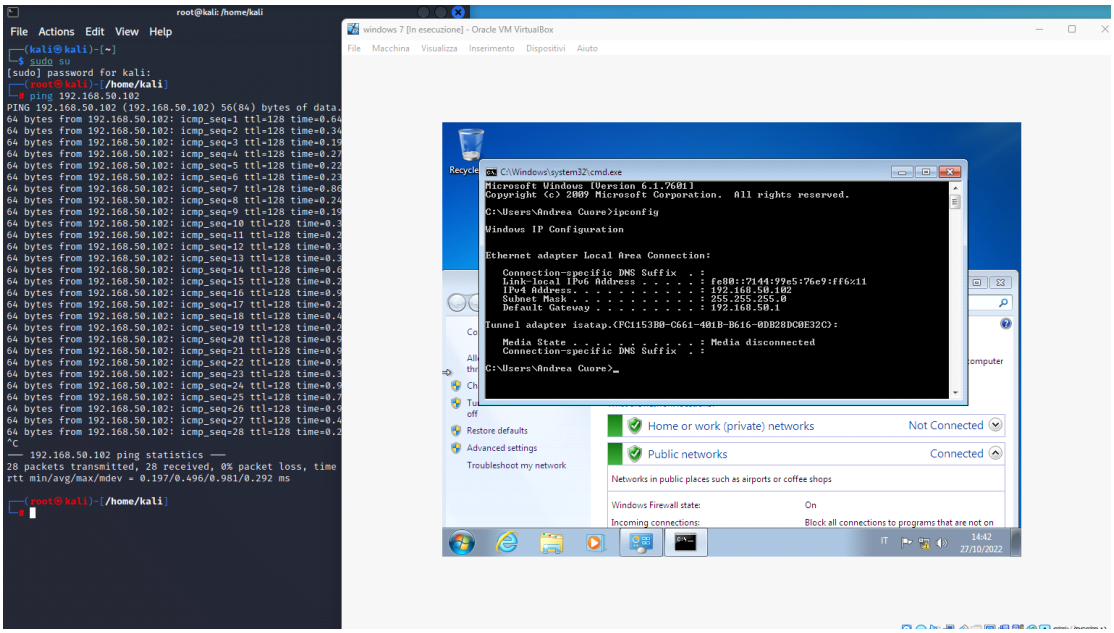
MODIFICA PRIORITY DEL FIREWALL E PING ALLA MACCHINA.

Per la riuscita di un ping mediante una macchina kali su una macchina windows con firewall attivato, è necessario modificare la priority del firewall stesso. La priority che ci interessa modificare e la File and Printer Sharing (Echo Request - IPv4) impostanto i profili autorizzati ad effettuare questa azione, da



Private a Public.

Successivamente sarà possibile effettuare il ping dalla nostra macchina Kali, accedendo alla nostra macchina Kali e scrivendo il comando da terminale ping 192.168.50.102



UTILIZZO WIRESHARK E AVVIO INETSIM

Lavorando su rete locale senza conessione ad internet mi sono avvalso del tool inetshark per simulare un collegamento di tipo HTTP alla rete e successivamente sniffare i vari pacchetti con il tool Wireshark.

Ho inizialmente avviato il Tool Inetsim per controllare quale fosse il patch di configurazione che è risultato essere /etc/inetsim/inetsim.conf, successivamente ho abilitato il fake Http (per un eventuale test su invio di file) ed ho inserito il codice IP macchina in aggiunta al IP e DNS di default

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/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 1140) ===
Session ID:     1140
Listening on:   127.0.0.1
Real Date/Time: 2022-10-27 08:44:43
Fake Date/Time: 2022-10-27 08:44:43 (Delta: 0 seconds)
 Forking services...
  * irc_6667_tcp - started (PID 1156)
  * echo_7_udp - started (PID 1166)
  * daytime_13_tcp - started (PID 1163)
  * dns_53_tcp_udp - started (PID 1146)
  * dummy_1_tcp - started (PID 1173)
  * discard_9_tcp - started (PID 1167)
  * time_37_tcp - started (PID 1161)
  * syslog_514_udp - started (PID 1160)
  * ident_113_tcp - started (PID 1159)
  * ntp_123_udp - started (PID 1157)
  * time_37_udp - started (PID 1162)
  * finger_79_tcp - started (PID 1158)
  * discard_9_udp - started (PID 1168)
  * chargen_19_udp - started (PID 1172)
  * echo_7_tcp - started (PID 1165)
  * tftp_69_udp - started (PID 1155)
  * chargen_19_tcp - started (PID 1171)
  * quotd_17_tcp - started (PID 1169)
  * dummy_1_udp - started (PID 1174)
  * pop3s_995_tcp - started (PID 1152)
  * quotd_17_udp - started (PID 1170)
  * daytime_13_udp - started (PID 1164)
  * smtp_25_tcp - started (PID 1149)
  * pop3_110_tcp - started (PID 1151)
  * https_443_tcp - started (PID 1148)
  * smtps_465_tcp - started (PID 1150)
  * ftps_990_tcp - started (PID 1154)
  * ftp_21_tcp - started (PID 1153)
  * http_80_tcp - started (PID 1147)
 done.
Simulation running.
```

Di seguito riportate le sezioni di modifica DNS ed IP

```
##############################################
# dns_default_ip
#
# Default IP address to return with DNS replies
#
# Syntax: dns_default_ip <IP address>
#
# Default: 127.0.0.1
#
#dns_default_ip 10.10.10.1
#dns_default_ip 192.168.50.100
```

```
##############################################
# service_bind_address
#
# IP address to bind services to
#
# Syntax: service_bind_address <IP address>
#
# Default: 127.0.0.1
#
#service_bind_address 10.10.10.1
#service_bind_address 192.168.50.100
```