

Consegna:

Lolli Vanessa



Esercizio

Traccia e requisiti

Nell'esercizio di oggi metteremo insieme le competenze acquisite finora. Lo studente verrà valutato sulla base della risoluzione al problema seguente.

Requisiti e servizi:

- Kali Linux ☐ IP 192.168.32.100
- Windows 7 ☐ IP 192.168.32.101
- HTTPS server: attivo
- Servizio DNS per risoluzione nomi di dominio: attivo

Traccia:

Simulare, in ambiente di laboratorio virtuale, un'architettura client server in cui un client con indirizzo 192.168.32.101 (Windows 7) richiede tramite web browser una risorsa all'hostname epicode.internal che risponde all'indirizzo 192.168.32.100 (Kali).

Si intercetti poi la comunicazione con Wireshark, evidenziando i MAC address di sorgente e destinazione ed il contenuto della richiesta HTTPS.

Ripetere l'esercizio, sostituendo il server HTTPS, con un server HTTP. Si intercetti nuovamente il traffico, evidenziando le eventuali differenze tra il traffico appena catturato in HTTP ed il traffico precedente in HTTPS. Spiegare, motivandole, le principali differenze se presenti.

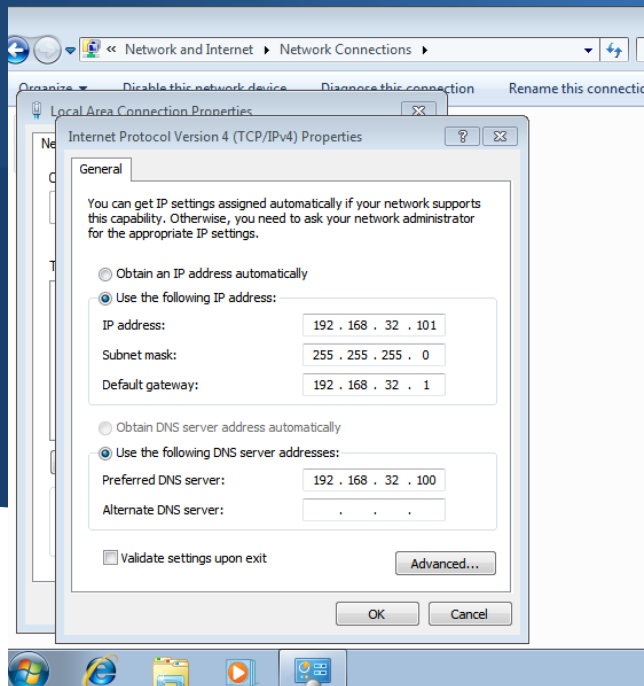
2

Soluzione:

Impostazione IP delle macchine virtuali:

Per modificare l'IP delle due macchine virtuali, come da consegna, ho eseguito due passaggi diversi per le due macchine virtuali.

- Per Kali Linux, dal terminale ho mandato il comando "sudo nano /etc/network/interfaces" e da qui modificato l'indirizzo IP in 192.168.32.100 ed infine il gateway in 192.168.32.1
- Per Windows 7 ho effettuato l'accesso dal pannello di configurazione delle reti, selezionato la scheda di rete ed infine da Internet protocol vs 4 ho modificato l'IP in 192.168.32.101 , impostato il gateway uguale a quello di Kali ed infine aggiunto il PREFERRED DNS SERVER inserendo l'indirizzo IP di Kali Linux . (Vedi Figura)



Utilizzo dell'utility InetSim per l'emulazione di servizi internet sulle due macchine virtuali:

Utilizzeremo InetSim per simulare servizi di rete su un sistema isolato; in questo caso la traccia chiede di simulare un'architettura client server in cui il client Windows 7 richiede tramite web browser una risorsa all'hostname 'epicode.internal' che risponde all'indirizzo di Kali.

Nel fare ciò, configuriamo InetSim modificando alcune impostazioni nel file di configurazione con il seguente comando: **`'sudo nano/etc/inetsim/inetsim.conf'`**, da qui commentiamo tutti i servizi fatta eccezione del servizio DNS, HTTP e HTTPS che ci consentiranno di accedere al sito internet. Fatto ciò modifichiamo il service bind address in 0.0.0.0 ed infine modifichiamo il DNS static aggiungendo **`'dns_static epicode.internal 192.168.32.100'`** come mostrato in figura.

```
File Actions Edit View Help
GNU nano 7.2
#####
# dns_default_hostname
#
# Default hostname to return with DNS replies
#
# Syntax: dns_default_hostname <hostname>
#
# Default: www
#
#dns_default_hostname somehost

#####
# dns_default_domainname
#
# Default domain name to return with DNS replies
#
# Syntax: dns_default_domainname <domain name>
#
# Default: inetsim.org
#
#dns_default_domainname some.domain

#####
# dns_static
#
# Static mappings for DNS
#
# Syntax: dns_static <fqdn hostname> <IP address>
#
# Default: none
#
#dns_static www.foo.com 10.10.10.10
#dns_static ns1.foo.com 10.70.50.30
#dns_static ftp.bar.net 10.10.20.30
#dns_static epicode.internal 192.168.32.100

#####
# dns_version
#
# DNS version
#
# Syntax: dns_version <version>
#
# Default: "INetSim DNS Server"
#
#dns_version "9.2.4"

^G Help      ^O Write Out  ^W Where Is   ^K Cut
^X Exit      ^R Read File  ^\ Replace    ^U Paste
```

In seguito, lanciando il comando ‘sudo inetsim’ inizierà la simulazione.

```
kali-linux-2023.3-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox : 1
File Macchina Visualizza Inserimento Dispositivi Aiuto
File Actions Edit View Help
(kali@kali)-[~]
$ sudo inetsim
[sudo] password for kali:
kali
Sorry, try again.
[sudo] password for kali:
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 1587) ==
Session ID: 1587
Listening on: 0.0.0.0
Real Date/Time: 2023-11-18 10:26:38
Fake Date/Time: 2023-11-18 10:26:38 (Delta: 0 seconds)
Forking services ...
* dns_53_tcp_udp - started (PID 1597)
print() on closed filehandle MLOG at /usr/share/perl5/Net/DNS/Nameserver.pm line 399.
print() on closed filehandle MLOG at /usr/share/perl5/Net/DNS/Nameserver.pm line 399.
* http_80_tcp - started (PID 1598)
* https_443_tcp - started (PID 1599)
done.
Simulation running.
```

3) Richiesta tramite il web browser della risorsa:

Una volta iniziata la simulazione, apriamo da windows 7 una pagina web e immettiamo nella barra di ricerca 'http://epicode.internal/' ed infine 'httpS://epicode.internal/', in questo modo verranno visualizzati siti internet :

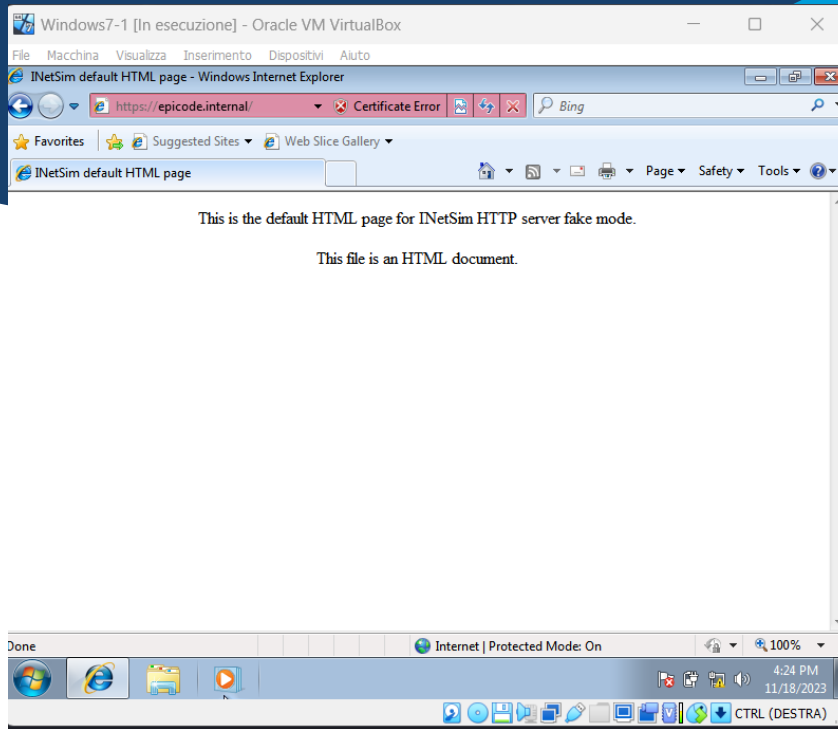


Figura 1 HTTPS

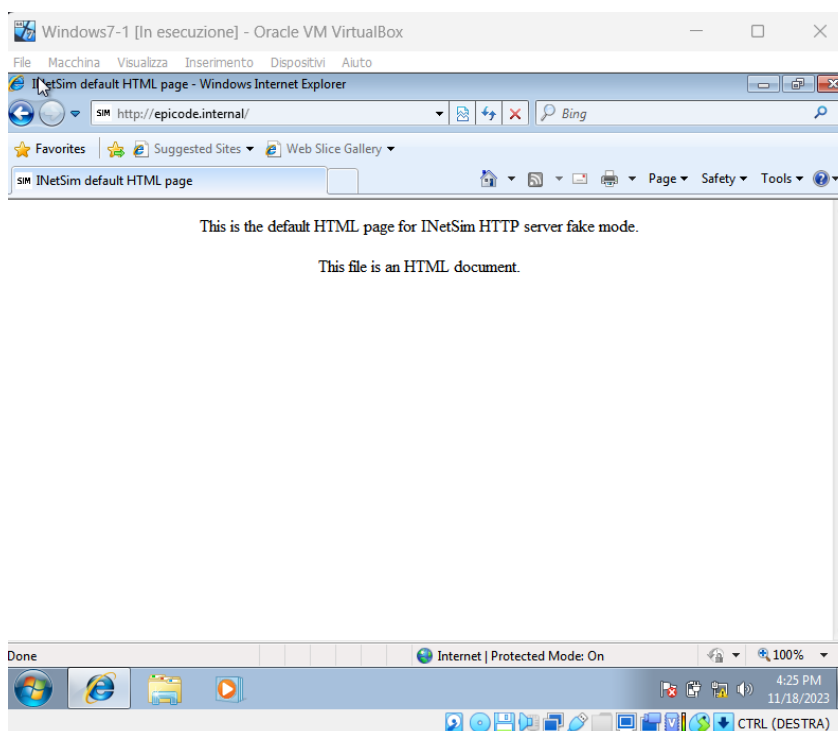


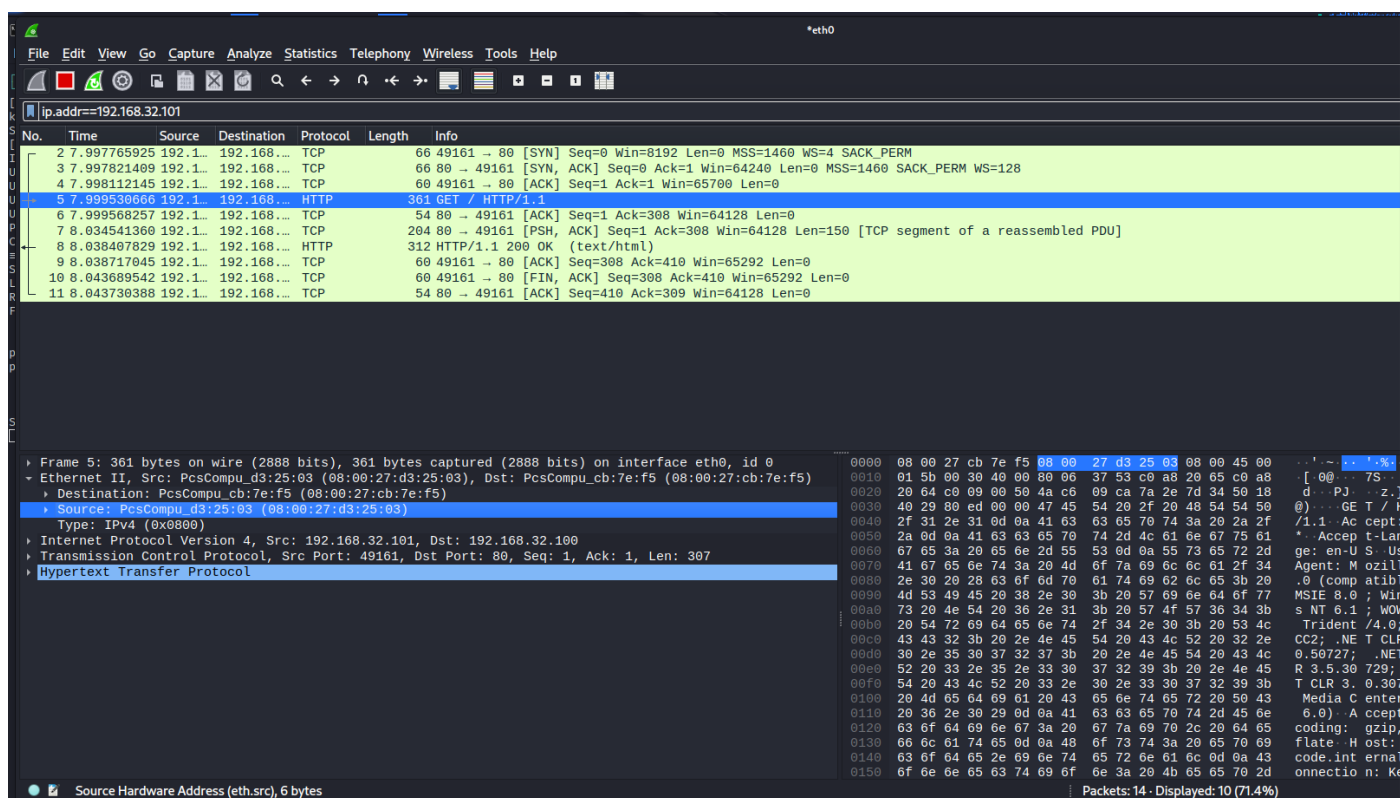
Figura 2 HTTP

4) Cattura di pacchetti con Wireshark

Wireshark è un software di analisi di rete open source utilizzato per l'ispezione e la risoluzione dei problemi delle reti. Consente di catturare e analizzare i pacchetti di dati che passano attraverso una rete in tempo reale.

Visitando dal web browser gli indirizzi citati in precedenza, ovvero HTTP e HTTPS si intercettano i pacchetti in transito su Wireshark.

- Analizzando i pacchetti in transito per http avremo:



Come mostrato in figura, essendo un sito http quindi non criptato, possiamo intercettare e leggere il contenuto HTML della pagina.

Infine analizzando il MAC address di un pacchetto (Source) ed il MAC address di Windows 7 (Physical address) vedremo che i due coincidono. (Vedi in figura)

```
C:\Windows\system32\cmd.exe
WINS Proxy Enabled. . . . . : No
Ethernet adapter Local Area Connection:

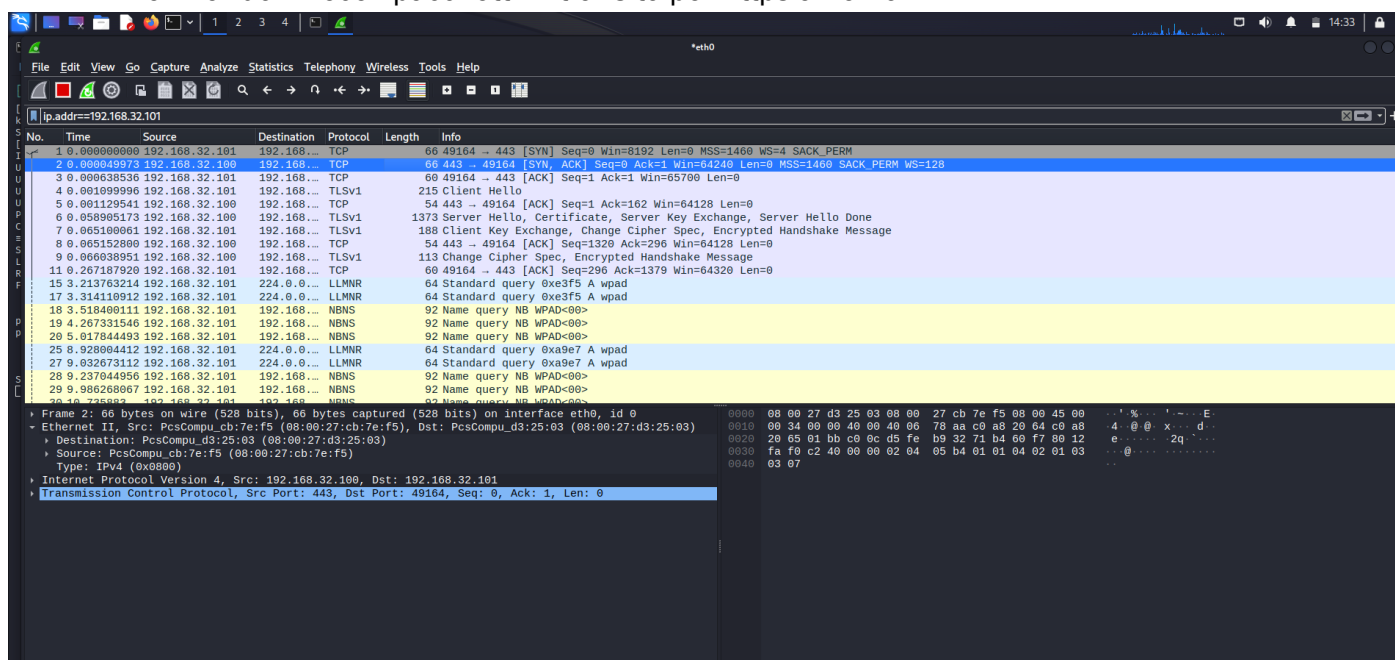
Connection-specific DNS Suffix  : 
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address. . . . . : 08-00-27-D3-25-03
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::7c72:67e9:5dc9:e02b%11(Preferred)
IPv4 Address. . . . . : 192.168.32.101(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.32.1
DHCPv6 IAID . . . . . : 235405351
DHCPv6 Client DUID. . . . . : 00-01-00-01-2C-CF-29-CB-08-00-27-D3-25-03

DNS Servers . . . . . : 192.168.32.100
NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter isatap.{AF22D32A-03D6-476F-B8AF-14AA3E6C90A1}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  : 
Description . . . . . : Microsoft ISATAP Adapter
Physical Address. . . . . : 00-00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
```

- Analizzando invece i pacchetti in transito per https avremo:



Differenze tra il traffico di rete HTTP e HTTPS

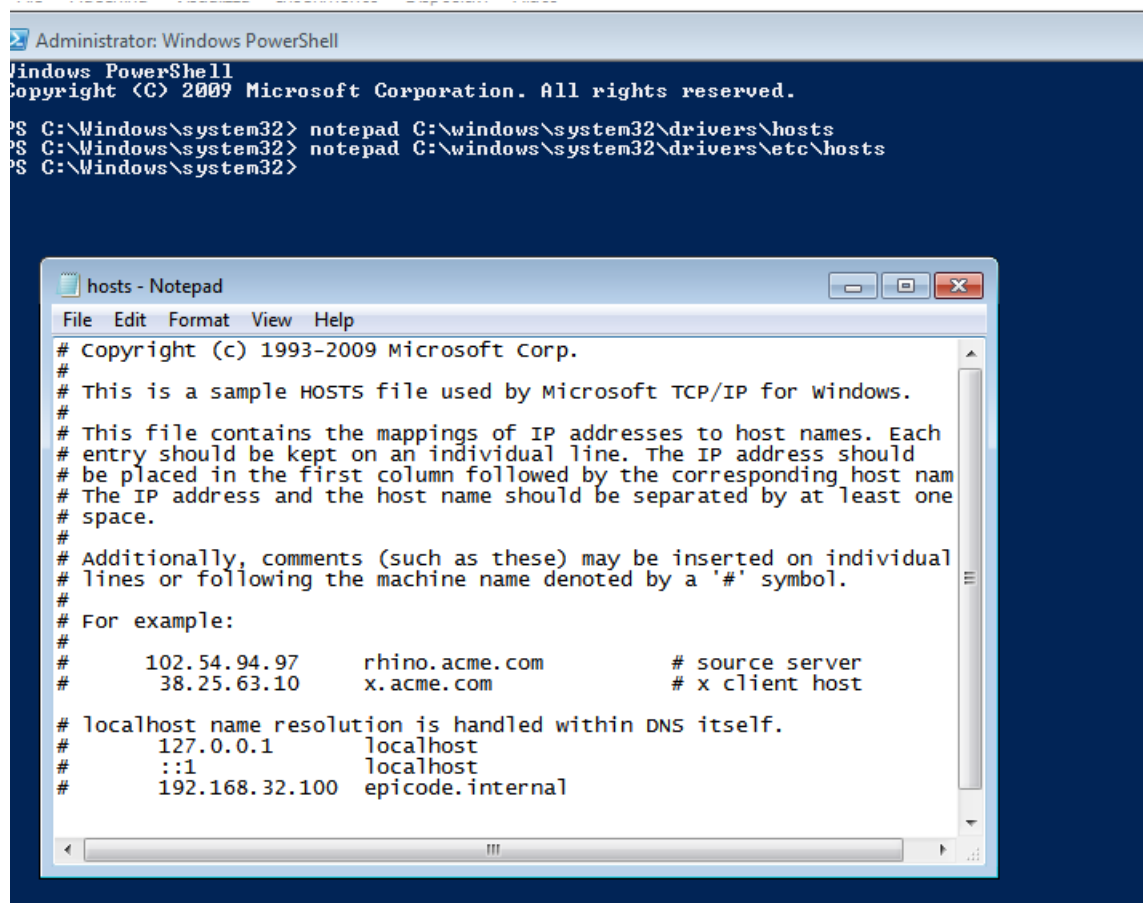
Tra le maggiori differenze che possiamo notare che:

- **HTTP**: Utilizza il protocollo TCP (Transmission Control Protocol) sulla porta 80 di default, Trasmette dati in chiaro, senza crittografia. Le informazioni, inclusi username, password e contenuti, sono visibili in formato testo, Tutti i dati, inclusi i dettagli delle richieste e delle risposte, sono visibili in formato testo leggibile, Solitamente utilizza la porta 80, Senza sicurezza incorporata, vulnerabile agli attacchi di tipo man-in-the-middle.
- **HTTPS**: Utilizza il protocollo TLS (Transport Layer Security) per la crittografia, comunemente sovrapposto a TCP sulla porta 443, Utilizza TLS per crittografare il traffico tra il client e il server. Ciò garantisce la riservatezza e l'integrità delle informazioni scambiate, rendendo più difficile per gli attaccanti intercettare o manipolare il traffico, Anche se è possibile vedere l'inizio della comunicazione TLS, il contenuto effettivo è crittografato e non è facilmente

leggibile nel pacchetto catturato senza la chiave di decrittazione, Solitamente utilizza la porta 443, Aggiunge un livello di sicurezza crittografica per proteggere i dati durante la trasmissione, riducendo il rischio di intercettazioni malevole.

METODO ALTERNATIVO PER CONFIGURARE IL DNS SU WINDOWS 7:

Aprendo il prompt di Windows molti comandi non vengono riconosciuti in quanto vengono richiesti privilegi amministrativi, conviene quindi utilizzare un sistema con privilegi più elevati (Powershell); una volta aperto Powershell come amministratore e inserendo il comando **'notepad C:\Windows\System32\drivers\etc\hosts'** siamo in grado di accedere al file host . Una volta aperto il file host ho aggiunto la riga **'192.168.32.100 epicode.internal'** ed infine salvato il file host. (vedi figura)



The image shows a Windows PowerShell window running as Administrator. The command prompt displays the following commands and output:

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> notepad C:\windows\system32\drivers\hosts
PS C:\Windows\system32> notepad C:\windows\system32\drivers\etc\hosts
PS C:\Windows\system32>
```

Below the PowerShell window, a Notepad window titled "hosts - Notepad" is open, displaying the contents of the hosts file:

```
File Edit Format View Help
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host nam
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com          # source server
#       38.25.63.10       x.acme.com              # x client host
#
# localhost name resolution is handled within DNS itself.
#       127.0.0.1         localhost
#       ::1               localhost
#       192.168.32.100    epicode.internal
```