Afcat http://www.afflib.org

Localização: Path

Descrição: O Advanced Forensics Format (AFF) é um formato aberto extensível para o armazenamento de imagens de disco e metadados forenses. Afcat copia o conteúdo de um Affile para stdout.

Sintaxe:

afcat [opções] arquivoentrada [... mais arquivosentrada]

Opções:

-s name	Apenas o nome do segmento de saída.
-p nnn	Apenas saída de dados nnn número da página.
-S nnn	Apenas saída de dados (assume 512-byte setores). Setor # 0 é o primeiro
-q quiet	Não imprimir em STDERR se uma página é ignorada.
-n noisy	Diga quando as páginas são ignorados.
-l	Lista todos os nomes do segmento.
-L	Lista os nomes do segmento, comprimentos, e args.
-d Debug	Imprimir os números de página para stderr como dados vai para o stdout.
-b BADFALG	saída de blocos defeituosos (o padrão é NULL).
-v	Imprimir o número de versão e sair.

Observação: nenhuma

Exemplo:

Pressupõe que você tenha um arquivo AFF nomeado como image.aff O afcat mostrará os dados brutos e irá exibi-lo na tela.

BT:~# afcat image.aff
ÁREA © 88m8µ2WÈôfë (qu? Y)? 6por ^ Lœ3Dö i× / V þi »MSA ¿iMþûé (ko ª x ° Yoe § ~ OO \ öi ® 7UúW ÷ GVòQêûûc ¬ Ø SVZ) + SðÐÍ'h #! Ëçå ¿¿¿ž

Amap http://www.thc.org/thc-amap/

Localização: Path

Descrição: O Advanced Forensics Format (AFF) é um formato aberto extensível para o armazenamento de imagens de disco e metadados forenses. Afcat copia o conteúdo de um Affile para stdout.

Sintaxe:

Amap [-A |-B |-P |-W] [-1buSRHUdqv] [[-h]-o arquivo] [-D arquivo] [sec -t/-T] [cons-c] [Retries-C] [-p proto] [-i arquivo] porta-alvo [[porta] ...]

Modos:

-A pedidos	Mapa: enviar gatilhos e analisar as respostas (padrão)
-B	Basta pegar as bandeiras, não envie dispara
-P	no banner ou material de aplicação - seja um (completa-se) Port Scanner
-W	Update - atualizar o banco de dados on-line de impressão digital aplicação!

Opções:

-1	Somente enviar gatilhos para um porto, até 1 de identificação. Speeeeed!
-6	Use IPv6 em vez de IPv4
-b	Imprimir banner ascii de respostas
-i	arquivo Nmap outputfile máquina de leitura óptica para ler as portas de Portas u especificado na linha de comando são UDP (o padrão é TCP)
-R/-S	Não identificam RPC / serviços SSL
-H	não enviar pedido desencadeia marcados como potencialmente nocivos
-U	Don't dump unrecognised respostas (melhor para criação de scripts)
-d	Dump todas as respostas

-v	modo verboso, use duas vezes (ou mais!) para depurar (não recomendado :-)
-q	Não relatório portas fechadas, e não imprimi-las como não identificados
-o	arquivo [-m saída] Escreva para arquivo FILE,-M cria a saída de leitura óptica
-c	CONS quantidade de conexões paralelas para fazer (padrão 32, max 256)
-C	RETRIES Número de reconecta-se no tempo limite (veja-T) (padrão 3)
-T-SEC	Connect timeout na tentativa de conexão em segundos (default 5)
-t SEC	Resposta esperar tempo em segundos (default 5)
-p PROTO	Somente enviar gatilhos para este protocolo FTP (EG)
PORT TARGET	o endereço de destino e a porta (s) para digitalizar (para além)

Observação: "Opções-BQV" são recomendadas, adicione "-1" para o Fast / controle do rush.

Exemplo:

amap-i scan.txt

Arpalert http://www.arpalert.org

Localização: Path

Descrição: este software é usado para o monitoramento de redes Ethernet. Ele escuta em uma interface de rede (sem usar o modo 'promíscuo') e captura todas as conversas de endereço MAC para posterior verificação. Em seguida, ele compara os endereços MAC é detectado com uma lista pré-configurada de endereços MAC autorizados. Se o MAC não está na lista, arpalert lança um comando pré-definido de usuário com o endereço MAC e endereço IP como parâmetros. Este software pode ser executado no modo daemon, ele é muito rápido CPU (Baixo consumo de memória).

Sintaxe:

arpalert [-f config_file] [-i network_interface] [pid_file-p] [exec_script e] [-D log_level] [leases_file-l] [-d] [-f] [v] [-h] [-w] [P] [-V]

Opções:

-f conf_file	arquivo de configuração
-i devices	lista de dispositivos separados por vírgulas de interfaces
-p pid_file	arquivo com o pid do daemon
-e script	script executado alertas
-D loglevel	loglevel (0 a 7)
-l leases	arquivo para armazenar os endereços MAC
-m module	arquivo para módulo de carga
-d	executado como daemon
-F	executado em primeiro plano
-v	dump (despejo) config
-h	ajuda
-w opção debug:	imprime um dump (despejo) de pacotes capturados (loglevel 7)
-P	executado em modo promíscuo
-V	versão

Observação: nenhuma

Exemplo:

1. configurar endereços MAC "amigáveis" em /etc/arpalert/maclist.allow - uma WhiteList de MACs.
2. configure /etc/arpalert/arpalert.conf/ para sua situação particular
3. bt~# arpalert

Burp Suite http://portswigger.net/suite/

Localização: /pentest/web/burpsuite

Descrição: é uma plataforma integrada para atacar aplicações web. Ele contém todas as ferramentas Burp com inúmeras interfaces entre elas destinadas a facilitar e acelerar o processo de atacar um aplicativo. Todas as partes ferramentas do mesmo framework são robustas para lidar com solicitações HTTP, persistência, autenticação, proxies, registro de alerta e extensibilidade. Burp Suite permite que você combine técnicas manuais e automatizados para enumerar, analisar, varrediras de ataque e explorar aplicações web. As várias ferramentas Burp trabalhar eficazmente em conjunto para compartilhar informações e permitir conclusões identificadas no âmbito de uma ferramenta para formar a base de um ataque usando outro.

Sintaxe: nenhuma

Tutorial

http://portswigger.net/intruder/help.html
http://portswigger.net/proxy/help.html
http://portswigger.net/scanner/help.html

Observação: nenhuma

Exemplo: nenhuma

Cisco Auditing Tool

Localização: /pentest/cisco/cisco-auditing-tool

Descrição:
é um script em Perl que analisa roteadores Cisco para vulnerabilidades comum. Verifica facilmente por senhas padrão, nomes oferecidos em wordlist comunitários e/o bug históricos do IOS. Inclui suporte para plugins e varredura de vários hosts.

Sintaxe:

./CAT [opções]

Opções:

-h	hostname (para varreduras de host único)
-f	hostFile (para a varreduras de vários hosts)
-p	porta padrão porta 23
-w	wordlist lista de palavras para adivinhação
-a	passlist lista de senhas para adivinhação
-i	ioshist verifica por bugs históricos no IOS
-l	logfile arquivo para log para, tela padrão
-q	modo silencioso (sem saída de tela)

Observação: nenhuma

Exemplo:

./CAT -h 192.168.1.100 -w wordlist comunitário -a passwords -i

Cisco Global Exploiter

Localização: /pentest/cisco/cisco-global-exploiter

Descrição: é um script que os alvos de vulnerabilidades no Cisco Internetwork Operating System (IOS) e produtos Catalyst. É expressamente aconselhável avisar os utilizadores a atualizar o firmware dos equipamentos CISCO para fechar os buracos (holes) que este script está explorando. Quando o script é executado contra o host, exibe opções de menu para o usuário executar.

Sintaxe:

/cge.pl -h [host] -v [número vulnerabilidade]

Opção (Tabela de Vulnerabilidades):

1	Cisco 677/678 Telnet estouro de buffer (buffer overflow)
2	Cisco IOS Router Denial of Service (DoS)
3	Cisco IOS HTTP Auth
4	Cisco IOS HTTP Configuration Arbitrary Administrative Access (Configuração Arbitrária de Acesso administrativo)
5	Cisco Catalyst SSH Protocol Mismatch Denial of Service (DoS)
6	Cisco 675 Web Administration Denial of Service (DoS)
7	Cisco Catalyst 3500 XL Remote Arbitrary Command (Comando Arbitrário Remoto)
8	Software Cisco IOS HTTP Request Denial of Service (DoS)
9	Cisco 514 UDP Flood Denial of Service (DoS)

Observação: nenhuma

Exemplo:

./cge.ph -h 192.168.1.100 -v 1

Exemplo:

Airsnarf http://airsnarf.shmoo.com/

Localização: /pentest/wireless/airsnarf-0.2

Descrição: é um simples utilitário de configuração de acesso sem fio ponto à ponto projetado para demonstrar como um rogue AP pode roubar nomes de usuário e senhas de wireless hotspots públicos. Airsnarf foi desenvolvido e lançado para demonstrar a vulnerabilidade inerente a um 802.11b hotspots público - obtendo nomes de usuário e senhas de usuários através de confusos DNS e redirecionamentos HTTP a partir de um concorrente AP.

Sintaxe:

./airsnarf

Opções: nenhum

Observação: Encontre um ponto de acesso que pretende imitar e atualizar os arquivos cfg na conformidade.

Autopsy http://www.sleuthkit.org/autopsy/index.php

Localização: Path

Descrição: é uma interface gráfica para a linha de comando digital de instrumentos de investigação do The Sleuth Kit. Juntos, eles permitem que você para investigar o sistema de arquivos e volumes de um computador.

Sintaxe:

./autopsy

Opções: nenhuma

Observação: nenhuma

Exemplo:

Abra o Firefox no link http://localhost:9999/autopsy

Copy Router Config

Localização: /pentest/cisco/copy-router-config

Descrição:
é um script em Perl que analisa roteadores Cisco para vulnerabilidades comum. Verifica facilmente por senhas padrão, nomes oferecidos em wordlist comunitários e/o bug históricos do IOS. Inclui suporte para plugins e varredura de vários hosts.

Sintaxe:

./copy-copy-config.pl [router-ip] [tftp-serverip] [community]

Opções: nenhuma

Observação: nenhuma

Exemplo:

./copy-copy-config.pl 192.168.1.100 192.168.1.110 public

Gooscan http://johnny.ihackstuff.com/

Localização: /pentest/enumeration/google/gooscan

Descrição: é uma ferramenta que automatiza consultas em motores de pesquisa do Google, mas com turbo. Essas consultas são especialmente concebidos para encontrar possíveis vulnerabilidades em páginas da web. Pense "CGI scanner" que nunca se comunica diretamente com o servidor Web de destino, uma vez que todas as consultas são enviadas ao Google, e não para o alvo. Esta ferramenta é muito poderosa e irá violar os termos de serviço do Google, se não usados corretamente. O arquivo README é muito informativo e bem escrito.

Sintaxe:

./gooscan -t www.google.com -q "String para Consultar" -s sitealvo.com

Opções:

-q	consultar uma consulta padrão do Google
-i	arquivo consulta uma lista de consultas do Google (veja o README)
-t alvo	Motor do Google/server
-o lista	HTML arquivo_saida formatado com os resultados
-P proxy:	endereço da porta:porta de um proxy GTTP válido para inativos
-v	verbose
-s	local restringe a pesquisa a um domínio
-x	xtra_appliance_fields necessários para varreduras aparelho

Observação: nenhuma

Exemplo:

./gooscan -t www.google.com -q "backtrack" -s remote-exploit.org

Wireshark http://wireshark.org

Localização:

Descrição: é um analisador de protocolo interface de rede. Ele permite que você navegue de forma interativa nos dados dos pacotes a partir de uma rede em tempo real ou de uma captura de arquivo salvo anteriormente. O formato nativo de arquivo de captura do Wireshark é o formato libpcap, que também é o formato usado pelo TCP-dump e várias outras ferramentas. Devido a problemas de marca registrada do projeto de software Ethereal mudou seu nome para Wireshark.

Sintaxe:

wireshark

Opções: nenhuma

Observação: nenhuma

Exemplo: nenhum

Xhydra http://www.thc.org

Localização: Path

Descrição: Este é um GUI para Hydra.

Tutorial:

http://www.youtube.com/watch?v=VPnbEm7ozns

Opções: nenhum

Observação: nenhuma

Exemplo: nenhum

Zenmap http://nmap.org/zenmap/

Localização: /pentest/enumeration/google/gooscan

Descrição: é a GUI oficial do NMAP Security Scanner. É aplicativo multi-plataforma (Linux, Windows, Mac OS X, BSD, etc)de código aberto que visa tornar o Nmap fácil de usar para iniciantes e ao mesmo tempo que fornece funcionalidades avançadas para usuários experientes Nmap. Freqüentemente exames utilizados podem ser guardados como perfis para torná-los fáceis de executar novamente. Através comandos em scripts, permitem a criação interativa de linhas de comando do Nmap. Scan resultados podem ser salvas e exibidas posteriormente. Você pode salvar os resultados da varreduras, que podem ser comparados uns com os outros para ver o que há de diferente. Os resultados de exames recentes são armazenadas em um banco de dados pesquisável. Esta aplicação tem uma interface gráfica.

Sintaxe:

So clicar no ícone do Zenmap

Opções: nenhum

Observação: nenhuma

Exemplo: nenhum

Blueprint http://trifinite.org/trifinite_stuff_blueprinting.html

Localização: /pentest/bluetooth/blueprint

Descrição: é um método remoto para descobrir detalhes sobre dispositivos Bluetooth. Blueprinting pode ser usado para gerar estatísticas sobre os fabricantes e modelos e para saber se existem dispositivos no intervalo definido que tenham problemas com a segurança do Bluetooth.

Sintaxe:

sdptool browse --tree --l2cap XX:XX:XX:XX:XX:XX | ./bp.pl: XX:XX:XX:XX:XX:XX <option>

Opções:

-mkdb	banco de dados de pesquisa não apenas gerar hash
-nomac	não use o MAC/BD_ADDR para pesquisas de banco de dados

Observação: nenhuma

Exemplo: nenhum

Cupp	http://www.remote-exploit.org/codes_cupp.html

Localização: /pentest/password/cupp

Descrição: A forma mais comum de autenticação é a combinação de um nome de usuário e uma senha ou passphrase. Se ambos encontraram valores armazenados dentro de uma tabela armazenada localmente, o usuário é autenticado para uma conexão. A "Força da senha" é a medida da dificuldade de adivinhar ou quebrar a senha através de técnicas de criptografia ou uma biblioteca baseada em testes automatizados de valores alternativos. Uma "senha fraca" pode ser muito curta ou apenas usar caracteres alphanumericos, tornando simples decodificação. Uma "senha fraca" pode ser também uma senha que é facilmente adivinhada por alguém, baseado no perfil do usuário, como um aniversário, apelido, endereço, nome de um animal de estimação ou parente, ou uma palavra comum, como Deus, amor, dinheiro ou senha. É para isso que Cupp foi desenvolvido e ele pode ser usado em situações como testes de penetração legal ou investigações criminais forenses.

Sintaxe:

./cupp.py [OPÇÕES]

Opções:

-h	este menu de perguntas interativa para criação de perfis de senha do usuário
-w	Utilize esta opção para perfil existente dicionário, ou a saída WyD.pl
-V	versão do programaversão do programa

Observação: nenhuma

Exemplo: nenhum

Cisco OCS Mass Scanner http://www.hacklab.tk

Localização: /pentest/cisco/cisco-ocs

Descrição:

Sintaxe:

./ocs xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy

Opções:

xxx.xxx.xxx.xxx	start intervalo IP
yyy.yyy.yyy.yyy	fim intervalo IP

Observação: nenhuma

Exemplo:

./ocs 192.168.1.100 192.168.1.200

Cisco Passwd Scanner

Localização: /pentest/cisco/ciscos

Descrição: fará a varredura em uma rede classe A, B ou C dentro da faixa de endereços IP dos roteadores Cisco que não mudaram sua senha padrão de "cisco".

Sintaxe:

./ciscos [IP] [classe] [opção]

Opções:

Class A scan	Classe A para varredura - ciscos 127 1
Class B scan	Classe B para varredura - ciscos 127.0 2
Class C scan	Classe C para varredura - ciscos 127.0.0 3
-C-threads	<threads> máximas
-t <timeout>	segundos antes do tempo limite de conexão

Observação: Saída armazenados em cisco.txt

Exemplo:

./ciscos 192.168 2 -t 10

OracleSysExec http://www.cqure.net/wp/test/

Localização: /pentest/cisco/oscanner

Descrição: Pode ser executado em modo interativo, permitindo que o usuário especifique os comandos para ser executado pelo servidor, ou no modo automático. No modo automático, netcat é tftpd para o servidor e liga-se uma porta TCP 31337.

Sintaxe:

./oscanner.sh

Oracle Scanner 1.0.6 por patrik@cqure.net
OracleScanner-s-r <ip> <repfile> [opções]

Opções:

-s	<nome_servidor>
-f	<lista_servidor>
-P	<portnr>
-v	Modo verbose

Observação: nenhuma

Exemplo: nenhum

ReverseRaider http://complemento.sourceforge.net/

Localização: /pentest/enumeration/complemento/reverseraider

Descrição: Parte do conjunto de Complemento de ferramentas, um scanner de domínio que usa a força bruta e wordlist para varreduras que encontrem no alvo sub-domínios ou resolução inversa de um intervalo de endereços IP. Ele é semelhante a algumas das funcionalidades em DNSenum. Suporta a permutação wordlist e IPv6.

Sintaxe:

./reverseraider-d Domínio | gama-r [opções]

Opções:

-R	range de IPv4 ou IPv6, para inverter a varredura Exemplos: 192.168.1.1-254 ou 2001:0 DB8:: 1428:57 AB-6344
-D	varredura do domínio, por wordlist (google.com exemplo)
-w	arquivo de wordlist (ver diretório de listas de palavras ...)

Opção extra:

-timeout	pedidos t em segundos
-P	permitir permutação numérico wordlist (default off
-D	nameserver para utilizar (padrão: resolv.conf)
-T	usar TCP em vez de consultas UDP queries
-R	não definir o bit de recursão em consultas

Observação: nenhuma

Exemplo:

Varredura Reversa de uma faixa de IP (no nosso exemplo o proprietário dos hosts é o Google ...):
./reverseraider -r 66.249.93-120

Saída:

google.it	66.249.93.104
ug-in-f102.google.com	66.249.93.102

ug-in-f112.google.com	66.249.93.112
ug-in-f101.google.com	66.249.93.101
ug-in-f100.google.com	66.249.93.100
ug-in-f115.google.com	66.249.93.115
ug-in-f116.google.com	66.249.93.116
ug-in-f118.google.com	66.249.93.118
gsmtp93-2.google.com	66.249.93.114
ug-in-f120.google.com	66.249.93.120

Podemos fazer o mesmo com um intervalo de IPv6 (se o seu servidor de nomes suporta consulta de DNS reverso para IPv6):

./reverseraider -r 2001:4860:0:1001::68-69

Saída:

nf-in-x68.google.com	2001:4860:0:1001::68

Wordlist varredura de um domínio:
./reverseraider -d google.com -w wordlists/fast.list

Saída:

www.l.google.com	74.125.43.103
www.google.com	74.125.43.103
googlemail.l.google.com	74.125.43.18
mail.google.com	74.125.43.18
ns.google.com	216.239.32.10
vpn.google.com	64.9.224.70
vpn.google.com	64.9.224.68
vpn.google.com	64.9.224.69
www.google.com	74.125.43.103
web.google.com	74.125.43.103
www2.l.google.com	74.125.77.103
print.google.com	74.125.77.103
smtp1.google.com	209.85.237.25
smtp.google.com	209.85.237.25

ns.google.com	216.239.32.10
vpn.google.com	64.9.224.68
vpn.google.com	64.9.224.69
vpn.google.com	64.9.224.70

SIPdump	http://www.remote-exploit.org/codes_sipcrack.html

Localização:

Descrição: Use sipdump para despejar SIP Digest autenticações. Se um login for encontrado, o login farejado (sniffing) é gravado o arquivo de dumping.

Sintaxe:

./sipdump [OPÇÕES] <dump file>

Opções:

<dump file>	arquivo onde logins capturados serão gravadas
-i <interface>	interface para escutar
-p <file>	uso pcap arquivo de dados
-m	inserir dados de login manualmente
-f "<filter>"	conjunto de filtros libpcap

Observação: *Você precisa especificar arquivo de despejo

Exemplo:

./sipdump-i eth0 logins.dump

VoIP Hopper http://voiphopper.sourceforge.net/

Localização: /pentest/voip/voiphopper

Descrição: é uma ferramenta de segurança, licenciadaGPLv3, escrito em C, que rapidamente varre em uma VLAN a outra VLAN de Voz, saltando (Hop) sobre switches Ethernet específicos. VoIP Hopper faz isso por que imita o comportamento de um telefone IP, a Cisco, Avaya, Nortel e outros. VoIP Hopper é uma ferramenta de teste VLAN Hop, mas também uma ferramenta para testar a segurança da infra-estrutura de VoIP.

Sintaxe:

./voiphopper <interface>-i-c (0 | 1 | 2)-a-n-v <VLANID>

Por favor, especifique 1 modo opção de base:
CDP Sniff Mode (-c 0)
Exemplo: voiphopper-i eth0-c 0

CDP Spoof Mode com pacotes personalizados (-c 1):

Opções:

-D <string>	(Device ID)
-P <string>	(Port ID)
-C <string>	(Capabilities)
-L <string>	(Platform)
-S <string>	(Software)
-U <string>	(Duplex)

Observação:

Exemplo:

SIP phone firmware:
./voiphopper-i eth0-c 1-SIP00070EEA5086 E ''-P 'Port 1' C-Convidado-Cisco L 'IP Phone 7940 »P003-S'-08-8-00 'U-1

SCCP telefone firmware:

./voiphopper-i eth0-c 1-SEP0070EEA5086 E ''-P 'Port 1' C-Convidado-Cisco L 'IP Phone 7940'-P00308000700 S 'U-1

Falsificação de telefone com o MAC:
./voiphopper-i eth0-m 00:07:0 E: EA: 50:86-c 1-SEP00070EEA5086 E ''-P 'Port 1' C-Convidado-Cisco L 'IP Phone 7940 »P003-S'-08 -8-00 'U-1

Avaya opção DHCP Mode (-a):
./voiphopper-i eth0-um
./voiphopper-i eth0-a-h 00:07:0 E: EA: 50:86

VLAN Hop Mode (-v VLAN ID):
./ voiphopper-i eth0-V 200
./ voiphopper-i eth0-V 200-D-m 00:07:0 E: EA: 50:86

SIPdump http://www.scrt.ch/pages_en/outils.html

Localização: /pentest/web/webshag

Descrição: é uma ferramenta web multi-tarefa e multi-plataforma de auditoria de servidor. Escrito em Python, que reúne as funcionalidades comumente úteis para auditoria em servidores de Web, como o rastreamento, a URL de varredura ou arquivo de difusão. Webshag pode ser usado para fazer a varredura de um servidor web em HTTP ou HTTPS, através de um proxy e usando a autenticação HTTP (Basic e Digest). Além do que se propõe a evasão de funcionalidades inovadoras para IDS, destinadas a fazer correlação entre o pedido mais complexo (por exemplo, usar diferentes requisições aleatórias HTTP Servidor de Proxy). Também fornece funcionalidades inovadoras, como a capacidade de recuperar a lista de nomes de domínio hospedado em uma máquina de destino e difusão de arquivos usando nomes de arquivos gerados dinamicamente (além da lista comum baseada fuzzing). Webshag URL scanner e um arquivo fuzz são destinadas a reduzir o número de falsos positivos e assim produzir resultados em conjuntos. Para este efeito, webshag implementa naa página web, mecanismo fingerprinting resistentes às alterações de conteúdo. Este mecanismo de impressão digital é então utilizado em um algoritmo de remoção de falsos positivos, especialmente destinadas a lidar com "soft 404" em respostas ao servidor. Webshag fornece uma interface de usuário cheia de recursos gráficos intuitivos, bem como interfaces de texto, como base de comando e está disponível para plataformas Linux e Windows, sob licença GPL.

Sintaxe: nenhuma

Tutorial: http://www.scrt.ch/outils/webshag/ws100_manual.pdf

WiSPY GTK http://www.metageek.net

Localização: Path

Descrição: É analisador de espectro de Wifi USB 2,4 GHz e é capaz de gerar gráficos de tráfego WiFi atuais e detectar possíveis interferências.

Sintaxe:

1. Conecte um dispositivo USB Wifi à sua máquina.
2. Kmenu--> !BackTrack--> Radio Network Analysis--> 80211--> All--> WiSPY GTK

Opções: nenhuma

Fórum: http://www.metageek.net/support/forum

Vídeos: http://www.metageek.net/support/videos

XSSS http://www.sven.de/xss
s

Localização: /pentest/web/xsss

Descrição: faz força-bruta de pesquisa de vulnerabilidades XSS solicitando URLs e apresentação de documentos com dados que contêm caracteres especiais de controle HTML e olhando para eles, a resposta do servidor.

Sintaxe:

./xsss [opções] url ...

As opções válidas:
--forms, --queries, --pathinfo --list=arquivo --depth=n --help
--maxcount=n

Opções:

--forms	permite formas de varredura (desativada por padrão)
--noqueries	desativa noqueries consulta de varredura (ativado por padrão)
-list = arquivo	varreduras lista de URLs a partir do arquivo
--depth=n n	mit níveis de recursão. padrão é 5.
--maxcount n	número limite do pedido. Padrão 1000

Observação:

Exemplo:

./xsss --forms http://www.target.com

Btscanner http://www.pentest.co.uk/cgi-bin/viewcat.cgi?cat=downloads

Localização:

Descrição: é uma ferramenta desenhada especificamente para extrair o máximo de informação possível a partir de um dispositivo Bluetooth sem a exigência de parelhamento.

Sintaxe:

btscanner [opções]

Opções:

-help	exibir ajuda
-cfg=<arquivo>	usar <arquivo> para o arquivo de configuração
-no-reset	não redefinir o adaptador Bluetooth antes da varredura

Observação:

Exemplo: nenhum

Xspy

Localização: /pentest/sniffers/xspy

Descrição: Este programa monitora o teclado e ecos cada tecla pressionada. Existe um programa existente chamado xkey.c que faz a mesma coisa, fazendo uso da forma padrão do X Windows para receber eventos keypress. No entanto, quando o terminal está no chamado "modo de segurança" (e durante o login), o servidor não transmiti esses eventos para o programa.

Sintaxe:

./xspy -display <display> -delay <usecs> -up

Opções:

display	especifica um display X
delay	determina a freqüência de pesquisa (0.1 sec é 100000 usecs)
up	desiste de transições de algumas teclas

Observação:

Exemplo: nenhum

CoWPAtty http://www.willhackforsushi.com/Cowpatty.html

Localização:

Descrição: destina-se a auditoria de PSK na pré-seleção compartilhada chave WPA para redes baseadas no protocolo TKIP. Um tempo atrás, Robert Moskowitz publicou um artigo intitulado "Weakness in Passphrase Choice in WPA Interface", que descreveu um ataque de dicionário contra as redes wireless usando o protocolo TKIP com uma chave pré-compartilhada (PSK). Através do fornecimento de um arquivo libpcap que inclui o TKIP four-way handshake, um arquivo de dicionário de senhas para adivinhar e com o SSID para a rede.

Sintaxe:

./cowpatty [options]

Opções:

-h	ajuda
-v	verbose
-f	arquivo dicionário
-d	arquivo de hash(genpmk)
-r	arquivo de captura de pacotes
-s	nome da rede SSID (SSID em uso incluir espaços)
-v	verbose

Observação:

Exemplo: nenhum

Erase_registrations pentest/voip/erase_registrations

Localização:

Descrição: Parte do pacote VOIP Hacking Exposed de ferramentas, essa ferramenta envia um pedido de registo devidamente trabalhada para um telefone SIP com um proxy SIP com a intenção de apagar as informações de contato.

Sintaxe:

interface (por exemplo, eth0)
usuário de destino (por exemplo, "ou john.doe ou 5000, ou "1+210-555-1212")
Addr IPv4 de domínio de destino (ddd.ddd.ddd.ddd)
Addr IPv4 de destino proxy/registrar (ddd.ddd.ddd.ddd)

Opções:

-h	ajuda
-v	modo de saída verbose

Observação: nenhuma

Exemplo: nenhum

PackETH http://packeth.sourceforge.net/

Localização: Path

Descrição: é uma ferramenta GUI para Linux para geração de pacotes para Ethernet. Ele permite a você criar e enviar qualquer pacote possível ou seqüência de pacotes na ethernet. A ferramenta baseada na GUI é bastante auto-explicativa, mas exige um certo grau de conhecimento da tecnologia Ethernet. README é bem escrito e está localizado em: /usr/share/doc/packeth/README.

Sintaxe: nenhuma

Opções: nenhum

Observação: nenhuma

Exemplo: nenhum

Vomit http://vomit.xtdnet.nl/

Localização: /pentest/voip/vomit

Descrição: Voice Over Internet Misconfigured Telefones. Uma ferramenta para Voip, vomit converte uma conversa por telefone Cisco IP em um arquivo de som que pode ser executado com em players comuns. vomit requer um arquivo de saída no tcpdump. vomit não é um sniffer VoIP, mas também poderia ser apesar da nomeação estar provavelmente relacionado com H.323.

Sintaxe:

./vomit [-h] [-d <dispositivo>] [-p <wav>] [-r <arquivo>] [filtro]

Opções:

-d <dispositivo>	uso do <dispositivo> para sniffing (farejar)
-p <wav>	ler este arquivo wav para posterior inserção
-r<arquivo>	use o conteudo do <arquivo> para sniffing (farejar)
-h	ajuda

Observação: nenhuma

Exemplo: nenhum

Xspy

Localização: /pentest/sniffers/xspy

Descrição: Este programa monitora o teclado e ecos cada tecla pressionada. Existe um programa existente chamado xkey.c que faz a mesma coisa, fazendo uso da forma padrão do X Windows para receber eventos keypress. No entanto, quando o terminal está no chamado "modo de segurança" (e durante o login), o servidor não transmitir esses eventos para o programa .

Sintaxe:

./xspy -display <display> -delay <usecs> -up

Opções:

display	especifica um display X
delay	determina a freqüência de pesquisa (0.1 sec é 100000 usecs)
up	desiste de transições de algumas teclas

Observação: nenhuma

Exemplo: nenhum

DBPwAudit http://www.cqure.net/wp/dbpwaudit/

Localização: /pentest/database/dbpwaudit

Descrição: é uma ferramenta Java que permite a realização de auditorias de qualidade para senhas, em drivers de banco de dados diversos. O design do aplicativo permite a fácil adição de drivers de banco de dados adicionais simplesmente copiando novos drivers JDBC para o diretório jdbc. A configuração é realizada em dois arquivos, o arquivo aliases.conf é usado para mapear os condutores e os pseudônimos rules.conf informa o aplicativo como lidar com mensagens de erro do teste. A ferramenta foi testada e conhecida por trabalhar com: Microsoft SQL Server 2000/2005,Oracle 8/9/10/11, IBM DB2 Universal Database, MySQL .

Sintaxe:

./dbpwaudit.sh

DBPwAudit v0.8 por Patrik Karlsson <patrik@cqure.net>
---------- --
DBPwAudit <server>-s-d-D <db> <driver>-U <usuarios>-P <senhas> [opções]

Opções:

-s	Nome do servidor ou endereço.
-p	Porta do servidor de banco/instância.
-d	Banco de dados/nome de instância da auditoria.
-D	O alias do driver para uso (-L para aliases)
-U	arquivo contendo nomes para adivinhar.
-P	Arquivo contendo senhas para adivinhar
-L	driver aliases List.

Observação: nenhuma

Exemplo: nenhum

Bkhive http://packages.debian.org/sid/bkhive

Localização: Path

Descrição: Esta ferramenta é projetada para recuperar o bootkey e syskey de um seção do sistema Windows NT/2K/XP. Então, podemos descriptografar o arquivo SAM com o syskey e fazer dump dos hashes de senha. (by ncuomo).

Sintaxe:

bkhive systemhive keyfile

Opções: nenhuma

Observação: nenhuma

Exemplo:

Supondo que sua unidade do Windows é montada em /mnt/sda1
bkhive /mnt/sda1/WINDOWS/system32/config/system saved-syskey.txt

Dnsmap http://lab.gnucitizen.org/projects/dnsmap

Localização: /pentest/enumeration/dns/dnsmap

Descrição: Realize bruto-force em domínios. A ferramenta pode usar uma wordlist interna, ou trabalhar com um arquivo externo dicionário.

Sintaxe:

./dnsmap <target-domain> [options]

Opções: nenhuma

-w	<wordlist-file>
-r	<results-path>

Observação: nenhuma

Exemplo:

- Subdomínio dnsmap bruteforcing usando built-in word-list:
./dnsmap targetdomain.foo

- Subdomínio bruteforcing usando uma wordlist fornecidos pelo usuário:
./dnsmap targetdomain.foo -w wordlist.txt

- Subdomínio bruteforcing usando o built-in wordlist e salvar os resultados para / tmp:
./dnsmap target-fomain.foo -r /tmp/

- Bruteforcing uma lista de domínios de destino, de forma a granel usar o script bash fornecidas. ou seja:
./dnsmap-bulk.sh domains.txt /tmp/results/

Ettercap-GTK Video:
[http://www.youtube.com/watch?v=o37rc97xdj8&feature=channel_page Passive OS fingerprinting, envenenamento de ARP, sniffer em HTTP e HTTPS]

Video:
[Plugins http://www.youtube.com/watch?v=vS9v0poMr3s&feature=channel_page]

Affix http://www.afflib.org

Localização: Path

Descrição: O Advanced Forensics Format (AFF) é um formato aberto extensível para o armazenamento de imagens de disco e metadados relacionados forenses. O Affix gera relatórios de erros com arquivos AFF e correções..

Sintaxe:

affix [opções] arquivo1 [...]

Opções:

-b	somente relatório arquivos quebrados
-v	exibe o número de versão e sair.

Observação: nenhuma

Exemplo:

affix -b image1.aff

Afstats http://www.afflib.org

Localização: Path

Descrição: O Advanced Forensics Format (AFF) é um formato aberto extensível para o armazenamento de imagens de disco e metadados relacionados forenses. Afstats exibe estatísticas sobre um ou mais arquivos AFF.

Sintaxe:

afstats [opções] arquivo(s)

Opções:

-m	toda a saída em megabytes.
-v	exibr o número de versão e sair

Observação: nenhuma

Exemplo:

afstats -m image2.aff

Name	AF_IMAGESIZE	Compressed	Uncompressed
image2.aff	478	401	960 0 0

Asleap http://asleap.sourceforge.net/

Localização: /pentest/wireless/asleap

Descrição: Esta ferramenta é lançada como uma prova de conceito para demonstrar fraquezas no LEAP e protocolos PPTP.

Sintaxe:

./asleap [opções]

Opções:

-h	ajuda
-r	ler um arquivo libpcap
-i	interface para capturar on
-f	arquivo de dicionário com NT hashes
-n	arquivo de índice para NT hashes
-s	ignorar a verificação sobre se a autenticação foi bem sucedida
-v	verbose
-V	versão
-C	Valor de desafio entre dois delimitado pontos bytes
-R	Valor de resposta entre dois delimitado pontos bytes
-W	arquivo de dicionário ASCII (efeitos especiais)

Observação: nenhuma

Exemplo:

affix -b image1.aff

BruteSSH http://www.edge-security.com/edge-soft.php

Localização: /pentest/password/brutessh

Descrição: Uma ferramenta bruteforcer para sshd baseada em senhas simples usando uma wordlist, sendo muito mais rápido para redes internas. É multithreads (Multitarefa).

Sintaxe:

./brutessh.py [opções]

Opções:

-h	host de destino
-u	usuário para forçar
-d	arquivo de senhas
-t	tarefas (padrão 12, mais pode ser ruim)

Observação: nenhuma

Exemplo:

./brutessh.py -h 192.168.1.100 -u root -d listasenhas.txt

Cryptcat http://cryptcat.sourceforge.net/

Localização: Path

Descrição: é o netcat padrão, reforçado com criptografia twofish com porting para o Windows NT, BSD e Linux. Twofish é cortesia da counterpane e cryptix.

Sintaxe:

cryptcat-k <senha> [opções] <host> <porta#>
cryptcat <senha>-k-l-p <port#> [opções] [host] [porta]

Opções:

-h	host de destino
-u	usuário para forçar
-d	arquivo de senhas
-t	tarefas (padrão 12, mais pode ser ruim)

Observação: Esta versão do cryptcat não suporta a opção de comando -e

Exemplo:
Abra duas janelas.

Na janela 1:
cryptcat ilovebacktrack-k-l-p 4321

Na janela 2:
cryptcat ilovebacktrack K-4321

type: Olá backtrack

Evans Debugger http://www.codef00.com/projects.php#Debugger

Localização: Path

Descrição: A QT4 baseado binário de modo depurador com o objetivo de trabalhar em conjunto com OllyDbg.

Sintaxe: edb

Opções: nenhum

Observação: nenhum

Exemplo: nenhum

Fast-Track http://www.thepentest.com/

Localização: /pentest/exploits/

Descrição: .

Sintaxe:

./fast-track.py [mode]

Opções:

-i	menu interativo
-c	linha de comando
-g	web GUI porta padrão (44444)
-g porta	web GUI a porta que você especificar

Observação:
http://trac.thepentest.com/wiki

Wiki:
http://trac.thepentest.com/wiki

irc.freenode.net
FastTrack #

Vídeos:
SQLPwnage; quebrar a barreira 64kb debug
Fast-Track [http://www.milw0rm.com/video/watch.php?id=95]

Apresentação Shmoocon
Fast-Track [http://vimeo.com/3212613]

Walkthrough
Fast-Track [http://vimeo.com/3212183]

SQLPwnage
Fast-Track [http://vimeo.com/3212460]

SQL Injector POST Attack
Fast-Track [http://vimeo.com/3212473]

Injector SQL Query String Attack
Fast-Track [http://vimeo.com/3212483]

MSSQL Bruter
Fast-Track [http://vimeo.com/3212497]

MS08-067 Buffer Overflow
Fast-Track [http://vimeo.com/3212502]

Internet Explorer estouro de buffer
Fast-Track [http://vimeo.com/3212534]

Autopwnage
Fast-Track [http://vimeo.com/3212542]

Exemplo:

./fast-track.py -i
./fast-track.py -g

Abra Firefox para http://127.0.0.1:44444

GDB GNU Debugger http://sourceware.org/gdb/documentation/

Localização: path

Descrição: o depurador do projeto GNU, permite que você veja o que está acontecendo dentro de outro programa enquanto ele executa - ou que outro programa estava fazendo no momento em que travou. O programa está que sendo depurado pode ser escrito em Ada, C, C + +, Objective-C, Pascal (e muitos outras lingagens de programação). Esses programas podem ser executados na mesma máquina que o GDB (nativa) ou em outra máquina (remota). GDB pode rodar em UNIX e suas variantes mais populares do Microsoft Windows. GDB pode fazer quatro tipos principais de coisas (além de outras coisas, de apoio a estes) para ajudá-lo a pegar os bugs no ato:

1.Iniciar o programa, especificando qualquer coisa que possa afetar o seu comportamento.

2.Fazer o seu programa parar em condições especificadas.

3.Examinar o que aconteceu, quando o programa foi interrompido.

4.Verificar quais coisas mudaram no seu programa, assim você pode experimentar como corrigir os efeitos de um erro e continuar a aprender sobre o outro.

Sintaxe:

gdb

Opções: nenhum

Observação:

Manual do Usuário:

http://sourceware.org/gdb/current/onlinedocs/gdb_toc.html
Manual Internos: http://sourceware.org/gdb/current/onlinedocs/gdbint_toc.html

Exemplo:

./brutessh.py -h 192.168.1.100 -u root -d listasenhas.txt

Abra duas janelas.

Galleta http://sourceforge.net/projects/odessa/files/

Localização: Path

Descrição: é uma ferramenta para extrair informações valiosas (a partir de um investigador forense ponto de vista) a partir de arquivos cookie MS IE. Ele irá extrair o nome do site, os nomes de variáveis e valores. A criação e expirar tempo para essas variáveis e também bandeiras..

Sintaxe:

galleta [opções] <arquivo cookie>

Opções:

-d <delimitador> (TAB por padrão)

Observação: nenhum

Exemplo:

Suponha que termos um cookie MS IE arquivo chamado "cookiesgalore".

galleta -d : cookiesgalore

Genlist

Localização: Path

Descrição: é um programa que retorna uma lista de hosts que estão respondendo a ping. Assim, esta lista pode ser usada para criar uma lista das máquinas e posteriormente, efetuar uma verificação dessas máquinas usando PBNJ ou Nmap.

Sintaxe:

genlist [tipo-entrada] [opções gerais]

Opções:

-n --nmap <path>	caminho para executável Nmap
--inter <interface>	Realize Scan Nmap usando a interface não-padrão

Opções Gerais:

-v --version	Versão
-h --help	Ajuda

Entrada:

-s --scan <alvo>	Ping Alvo Range ex: 10.0.0.*

Observação: nenhum

Exemplo:

Digamos que você queria ver os endereços IP que estavam respondendo a pings na sub-rede 192.168.1.0 255.255.255.0, e depois executar uma varredura do Nmap esses endereços.

genlist -s 192.168.1.* > iplista.txt

nmap -sV -iL iplista.txt

.

Genpmk http://www.wirelessdefence.org/Contents/coWPAttyMain.htm

Localização: /pentest/wireless/cowpatty

Descrição: Parte da suite CoWPAtty de ferramentas, genpmk é usado para precomputar os arquivos de hash de forma semelhante às tabelas do Rainbow é usado para pré-senhas de hash em Windows LANMan attacks.

Sintaxe:

genpmk [opções]

Opções:

-f	arquivo Dicionário
-d	arquivo hash de saída
-s	rede SSID
-h	ajuda
-v	exibe informações verbose
-V	versão do programa

Observação: Após o arquivo de hash precomputing CoWPAtty, executado com o argumento -d.

Exemplo:

./genpmk -f wordlist.txt -d hash.txt -s Linksys

Gerix-Wifi-Cracker http://security-sh3ll.blogspot.com/2009/06/gerix-wifi-cracker.html

Localização: /usr/share/gerix-wifi/buc/bin/gerix_wifi_cracker.mc

Descrição: é GUI para Aircrack-ng, é projetado para pentesting em um Mundo Real, sendo eficiente e de fácil utilização com interface gráfica.

Sintaxe: nenhum

Opções: nenhum

Observação: http://www.youtube.com/watch?v=r0olWYQ-Fsg

Exemplo: nenhum

Goorecon http://www.darkoperator.com

Localização: /pentest/enumeration/goorecon

Descrição: Ruby scritp para a enumeração dos Exércitos, subdomínios e e-mails de um determinado domínio usando o Google.

Sintaxe:

ruby goorecon.rb <tipos> <alvos>

Opções:

-s	enumeração dos subdominios
-e	coletar e-mail

Observação: nenhum.

Exemplo:

ruby goorecon.rb -e www.target.com

ICMP Redirect http://www.phenoelit-us.org/fr/tools.html

Localização: Path

Descrição: Suite de ferramentas IRPAS. Usa os pacotes ICMP de uma máquina/rede e redireciona para outra máquina/rede.

Sintaxe:

icmp_redirect [-v[v[v]]] -i <interface> [-s <rede origem>/<origem mascara>] [-d <rede destino>/<mascara destino>] [-G <gateway IP>] [-w <delay>] [-S <IP address>]

Opções: nenhum

Observação: nenhum.

Exemplo:

icmp_redirect -vvv -eth0 -s 192.168.0.0/255.255.255.0 -d 10.1.1.0/255.255.255.0 -S 172.16.21.22

IDA Pro Free

Localização:

Descrição: Um multi-processador disassembler e depurador.
Info: http://www.hex-rays.com/idapro/.

Sintaxe: nenhum

Opções: nenhum

Observação: nenhum.

Exemplo: nenhum

IRDPresponder http://phenoelit-us.org/irpas/docu.html

Localização: Path

Descrição: Sniffer, que atende a IRDP requests (solicitação) e respostas. Envia atualizações periódicas.

Sintaxe:

irdpresponder-i [dispositivo] [opções]

Opções:

-v	verbose
-P	ativar o modo promíscuo
-i <interface>	interface
-p <preference>	preferência desta entrada (padrão 0)
-l <lifetime>	tempo de vida da entrada (padrão 1800)
-s <spoofed source IP>	talvez você precise do IP
-D <destination IP>	se você não especificar, será usado o endereço do broadcast

Observação: nenhum.

Exemplo: nenhum

ISP http://blog.sebastien.raveau.name/2009_02_01_archive.html

Localização: /pentest/misc/isp

Descrição: O ISP é um script Python que utiliza consultas DNS para determinar o seu provedor permite-lhe enviar o tráfego ou não para a Internet utilizando uma fonte de falsificação de IP (spoofing IE).

Sintaxe:

./isp.py <IP do DNS server>

Opções: nenhum

Observação: este dá falso-positivos quando executar atrás de alguns roteadores NAT!

TTL padrão para 86400
TTL 2 segundos após consulta ao spoofed DNS(falso): 86397

Exemplo:

./isp.py 192.168.1.100

Impacket SAMRDump http://oss.coresecurity.com/projects/impacket.html

Localização: /pentest/python/impacket-examples

Descrição: Uma aplicação que se comunica com o Security Account Manager Remote interface from the DCE/RPC suite. Ele lista as contas de usuário do sistema, partes dos recursos disponíveis e outras informações sensíveis exportados através deste serviço..

Sintaxe:

samrdump.py [username[:password]@]<address> [protocol list...]

Opções: nenhum

Observação: Protocolos disponíveis: ['445/SMB','139/SMB'] Nome de usuário e senha são necessários somente para determinados transportes, por exemplo. SMB

Exemplo: nenhum

JbroFuzz http://www.owasp.org/index.php/Category:OWASP_JBroFuzz

Localização: /pentest/fuzzers/jbrofuzz

Descrição: é um fuzzer de protocolo de aplicações web (web application protocol) que surgiram a partir das necessidades de testes de penetração. Escrito em Java, que permite a identificação de determinadas classes de vulnerabilidades de segurança, por meio da criação de dados malformados e com o servidor/serviço em questão consumir os dados.

Sintaxe: nenhuma

Opções: nenhum

Observação:

vídeo tutorial.
http://downloads.sourceforge.net/jbrofuzz/tutorial-jbrofuzz-0.2.swf?modtime=1162798454&big_mirror=0 Download

vídeo tutorial.
http://video.google.co.uk/videoplay?docid=6388655108193715653&q=jbrofuzz Watch]

Exemplo: nenhum

John http://www.openwall.com/john/

Localização: /pentest/password/jtr

Descrição: aka John the Ripper é um cracker de senha.

Sintaxe: nenhuma

Opções: nenhuma

Observação: nenhum.

Exemplo: nenhum

Kismet http://www.kismetwireless.net/

Localização: Path

Descrição: é um detector de rede wireless 802.11 layer2, sniffer e IDS (sistema de detecção de intrusão). Kismet funciona com qualquer placa wireless que suporta modalidade de monitoramento bruto (rfmon) e pode sniffar tráfego 802.11b, 802.11ae 802.11g. Kismet identifica redes coletando passivamente por pacotes e detectar o padrão chamado nas redes, detectando (e determinado momento, decloaking) redes ocultas e deduzir a presença de redes nonbeaconing através de tráfego de dados.

Sintaxe:

./configure --disable-setuid
make dep && make && make install

Opções: nenhum.

Observação: nenhum.

Exemplo: nenhum

List-Urls

Localização: /pentest/enumeration/list-urls

Descrição: vem em duas formas, a original, que irá analisar a URL de uma página e incluí-los na saída (STDOUT). A segunda forma é a versão 2.0. Isto irá analisar as urls de uma página on-line ou off-line uma página armazenada. Ela então lhe dá a opção para resolver nomes de máquinas e saída de informações em um arquivo ou para saída (STDOUT) em um formato grep.

Sintaxe:

./list-urls.py <web-page>

Opções: nenhum

Observação: nenhum.

Exemplo:

./list-urls.py http://www.target.com

Lodowep

Localização: /pentest/password/lodowep

Descrição: é uma ferramenta para analisar a força da senha de contas em um sistema servidor Lotus Domino. A ferramenta suporta tanto de sessão e autenticação básica. Ele roda 20 conexão simultâneas para adivinhar senhas especificadas em um arquivo de dicionários contra o perfil de usuário fornecido.

Sintaxe:

java -jar lodowep.jar -u <userfile> -p <pwfile> -t <targeturl>

Opções: nenhum

Observação: nenhum.

Exemplo:

java -jar lodowep.jar -u usr.txt -p pw.txt -t
http://www.target.com/catalog.nsf

Lynx http://lynx.isc.org/

Localização: /pentest/password/lodowep

Descrição: é o navegador web de texto.

Sintaxe:

lynx www.target.com

Opções: nenhum

Observação: nenhum.

Exemplo: nenhum

Macchanger http://alobbs.com/macchanger/

Localização: Path

Descrição: A GNU / Linux utilidade para visualizar / manipular o endereço MAC de interfaces de rede.

Sintaxe:

macchanger [opções] dispositivo

Opções:

-h	ajuda
-V	versão
-s	mostra o endereço MAC
-e	não altere os bytes do vendedor
-a	MAC do fabricante aleatório do mesmo tipo
-A	MAC do fabricante aleatório do mesmo tipo ou de qualquer tipo e fabricante
-r	MAC do fabricante aleatório totalmente aleatório
-l	exibi os fabricantes conhecidos
-m	inserir manualmente um endereço MAC

Observação: nenhum.

Exemplo:

macchanger -s eth0

Merge Router Config

Localização: /pentest/cisco/copy-router-config

Descrição: Obtem a configuração do roteador Cisco usando SNMP. Certifique-se de um servidor TFTP está configurado, de preferência em execução a partir de /tmp!.

Sintaxe:

./merge-copy-config.pl [router-ip] [tftp-serverip] <community>

Opções: nenhuma

Observação: nenhum.

Exemplo:

./merge-copy-config.pl 192.168.1.100 192.168.1.110 public

Metacoretex http://sourceforge.net/projects/metacoretex/

Localização:

Descrição: É um scanner de segurança extremamente modular em plugin baseado em um scanner de segurança escrito inteiramente em Java para permitir o uso de drivers JDBC Type IV no scanning de banco de dados. Inicialmente, a maioria dos plugins provavelmente será de DBS.

Sintaxe: nenhuma

Opções: nenhum

Observação: Este programa tem uma interface gráfica que é bastante auto-explicativa.

Exemplo: nenhum

Milw0rm

Localização: /pentest/exploits/milw0rm

Descrição: Um site para a obtenção de prova de conceito (Proof of Concept) e código de exploração (Exploit).

Sintaxe:

grep-i [exploit] sploitlist.txt

grep -i [exploit] sploitlist.txt | cut -d " " -f1 | xargs grep sys | cut -d ":" -f1 | sort -u

---

Opções:

Windows	process.h, string.h, winbase.h, windows.h, winsock2.h
Linux	arpa/inet.h, fcntl.h, netdb.h, netinet/in.h, sys/sockt.h, sys/types.h, unistd.h

Observação: Alguns podem ser feitos para a compilação em Windows, enquanto outros para o Linux. Você pode identificar o ambiente inspecionando os cabeçalhos.

grep "#include" [exploit]

Exemplo:

grep-i ms08 sploitlist.txt

Mini MySqlat0r http://www.scrt.ch/pages_en/minimysqlator.html

Localização: /pentest/database/MiniSqlat0r

Descrição: Uma aplicação multi-plataforma utilizada para auditar sites, com objetivo de descobrir e explorar vulnerabilidades de injeção SQL. É escrito em Java e é utilizado através de uma GUI user-friendly que contém três módulos distintos.

Sintaxe: nenhuma

Opções: nenhuma

Observação:

Este programa tem uma interface gráfica.

http://www.scrt.ch/outils/mms/mms_manual.pdf

Exemplo: nenhuma

Mysqlaudit

Localização: Path

Descrição: Python Script para auditoria básicos de configuração de segurança comuns no MySQL.

Sintaxe:

./mysqlaudit.py <Targer IP> <User> <Password> <Report>

Opções:

Target	O sistema que você quer fazer o assement sobre, a porta 3306 deve ser aberta.
User	Conta de usuário com privelages DBA no servidor para usar a avaliação.
Password	senha para a conta do usuário
Report	Nome do arquivo de texto em que para escrever o relatório.

Observação: nenhum.

Exemplo:

./mysqlaudit.py 192.168.1.100 admin admin scan.txt

Netifera http://netifera.com/

Localização: /pentest/scanners/netifera

Descrição: Uma plataforma modular nova, opensource para criação de ferramentas de segurança de rede. Este projeto oferece muitas vantagens para os desenvolvedores de segurança e os investigadores que querem implementar novas ferramentas, bem como a comunidade de usuários dessas ferramentas. Esta é uma aplicação GUI.

Sintaxe:

./netifera

Opções: nenhuma

Observação:

Tutorial
http://netifera.com/doc/netifera_tutorial_sniffing_module_part1/

Guia de Introdução
http://netifera.com/doc/netifera_getting_started_guide/

Exemplo:

./netifera

OScanner http://www.cqure.net /wp/oscanner/

Localização: /pentest/cisco/oscanner

Descrição: é um framework de avaliação para Oracle desenvolvido em Java. Tem um plugin baseado em arquitetura e vem com um par de plugins que fazem atualmente:

- Enumeração do Sid
- Testes de senhas (comum e dicionário)
- Enumerar versão Oracle
- Enumerar os regras de conta
- Enumerar privilégios de conta
- Enumerar os hashes conta
- Enumerar informações de auditoria
- Enumerar as diretivas de senha
- Enumerar as database links

Os resultados são apresentados em uma árvore gráfica em java.

Sintaxe:

./oscanner.sh

Oracle Scanner 1.0.6 by patrik@cqure.net
OracleScanner -s <ip> -r <repfile> [options]

Opções:

-s	<servername>
-f	<serverlist>
-P	<portnr>
-v	verbose

Observação: nenhum.

Exemplo: nenhum

ObexFTP http://triq.net/obexftp.html

Localização: Path

Descrição: A aplicação ObexFTP permite armazenar e recuperar documentos para a memória do celular - que forma você pode acessar sua agenda, logo, toque, mp3, imagem e armazenamento.

Sintaxe:

obexftp [-i |-b <dispositivo> [-B <chan>] |-U <intf> | t-<dispositivo> | <host>-N] [-c <dir> ...] [-C < dir>] [-l [<dir>]] [-g <arquivo> ...] [-p <arquivo> ...] [-k <arquivo> ...] [-x] [m-<origem> <dest> ...]

Opções:

-i, --irda	usando IrDA transporte (padrão)
-b, --bluetooth <dispositivo>	usar ou procurar um dispositivo Bluetooth
-B, --channel <numero>	usar este canal ao conectar bluetooth
-u, --usb [<intf>]	conectar a uma interface USB ou a lista de interfaces
-t, --tty <dispositivo>	ligar a este TTY utilizando um transporte personalizado
-n, --network <host>	conectar a este host
-U, - uuid	determinado uso uuid(nenhum, FBS, IRMC, S45, Sharp)
-H, - noconn	suprimir ids conexão(cabeçalho não conn)
-S, --nopath	não use o caminho padrão(caminho usar como nome de arquivo)
-c, --chdir <DIR>	chdir
-C, --mkdir <DIR>	mkdir e chdir

-l, --list [<PASTA>]	lista atual/dados pasta chegar e colocar sempre especificar a nome remoto
-g, --get <ORIGEM>	buscar arquivos
-G, --getdelete <ORIGEM>	buscar e apagar (mover) arquivos
-p, --put <ORIGEM>	enviar arquivos
-k, --delete <ORIGEM>	apagar arquivos
-X, --capability	recuperar a capacidade de objeto
-Y, --probe	sonda e características do dispositivo de relatório
-x, --info	recuperar informações (Siemens)
-m, - move <ORIGEM> <DEST>	mover arquivos (Siemens)
-v, - verbose	verbose
-V, - version info	versão para impressão
-h, - help	texto de ajuda

Observação: nenhum.

Exemplo: obexftp-b 00:0F:ED:F1:ED:5E -B 12-L

Opwg http://www.cqure.net/wp/test/

Localização: /pentest/database/oat

Descrição: O Oracle Auditoria Tools é uma ferramenta que pode ser utilizado para auditoria de segurança dentro de servidores de banco de dados Oracle.

Sintaxe:

```
./opwg.sh
Oracle Password Guesser v1.3.1 by patrik@cqure.net
---------------------------------------------------------------------------
OraclePwGuess [options]
```

Opções:

-s*	<servername>
-u	<userfile>
-p	<passfile>
-d	<SID>
-P	<portnr>
-D	disables default pw checks
-C	check for CREATE LIBRARY permissions
-v	be verbose

Observação: nenhum.

Exemplo: nenhum.

Oquery http://www.cqure.net/wp/test/

Localização: /pentest/database/oat

Descrição: O Oracle Auditoria Tools é uma ferramenta que pode ser utilizado para auditoria de segurança dentro de servidores de banco de dados Oracle. A linha de comando minimalista ferramenta de consulta baseada sql.

Sintaxe:

```
./oquery.sh
OracleQuery v1.3.1 by patrik@cqure.net
----------------------------------------------------------
OracleQuery [options]
```

Opções:

-s*	<servername>
-u*	<username>
-p*	<password>
-d*	<SID>
-P	<portnr>
-v	be verbose
-q	<query>
-o	<outfile>
-m	<tabledelimiter>

Observação: nenhum.

Exemplo: nenhum.

Otnsctl http://www.cqure.net /wp/test/

Localização: /pentest/database/oat

Descrição: OracleTNSCtrl - é utilizado para consultar o ouvinte TNS para várias informações, como o utilitário Oracle lsnrctl. É um pouco limitado embora. Use o comando help para ver comandos correntemente implementadas

Sintaxe:

./otnsctl.sh

Oracle TNS Control v1.3.1 by patrik@cqure.net

OracleTNSCtrl [options]

Opções:

-s*	<servername>
-P	<portnr>
-c	command to execute (status/services/version/etc.)
-I*	interactive mode
-v	be verbose

Observação: nenhum

Exemplo: nenhum

Paros Proxy http://www.parosproxy.org/

Localização: /pentest/web/paros

Descrição: Um framework completamente escrito em Java. Todos HTTP e HTTPS de dados entre o servidor e o cliente, incluindo cookies e campos de formulário, pode ser interceptada e modificada

Sintaxe:

Iniciar Paros Proxy.

Configurar o Firefox para usar Paros como o proxy.

Editar> Preferências -> aba Avançado -> aba Rede -> botão Configurações -> Manual Proxy Configuração (localhost:8080)-> usar este proxy para todos os protocolos.

Navegue para na página Web de destino.

Confira a saída em Paros.

Opções:

Observação: http://windowsitpro.com/articles/print.cfm?articleid=94001

Exemplo: nenhum

Pblind http://www.parosproxy.org/

Localização: /pentest/web/paros

Descrição: é pequeno utilitário para ajudar com a exploração das vulnerabilidades de injeção SQL.

Sintaxe:

./pblind [-n -b] iniUrl+injectHere+endUrl

Opções:

-n num	comprimento do resultado esperado (1 tarefa para cada posição) (padrão 20)
-b	[Oracle,MySQL,MSSQL]: se não especificado, fingerprinting é executado

Observação: http://windowsitpro.com/articles/print.cfm?articleid=94001

Exemplo:

./pblind -b mysql "http://localhost/sql.php?id=3+user()"

Powerfuzzer http://www.powerfuzzer.com/

Localização: /pentest/web/powerfuzzer

Descrição: é uma interface gráfica baseada em web altamente automatizado fuzzer derivada de muitos outros fuzzers Open Source disponível (incl. cfuzzer, fuzzled, fuzzer.pl, jbrofuzz, WebScarab, wapiti, Socket Fuzzer) e as informações recolhidas a partir de inúmeros recursos de segurança e sites. É capaz de spidering um website e identificação de fatores de entrada.

Sintaxe:

1. Open Powerfuzzer (Kmenu ->! BackTrack -> Web Application Analysis -> Web (interface) -> Powerfuzzer)
2. Digite um URL no menu Target URL
3. Clique "Scan"

Opções:

Observação: nenhuma

Exemplo: nenhum

Proxychains http://proxychains.sourceforge.net/

Localização: Path

Descrição: Força qualquer conexão TCP feita por qualquer aplicação que usar proxy como o TOR ou qualquer outro em SOCKS4, SOCKS5 ou HTTP(S) proxy..

Sintaxe:

proxychains <aplicação> <destino>

Opções: nenhuma

Observação: nenhuma

Exemplo:

edit /etc/proxychains.conf atender suas finalidades

proxychains target.com telnet

Proxyresolve http://proxychains.sf.net

Localização: Path

Descrição: Usado para resolver nomes de HOST através de Proxy ou TOR.

Sintaxe:

proxyresolv <host>

Opções: nenhuma

Observação: nenhuma

Exemplo:

edit /etc/proxychains.conf conforme as suas necessidades

proxyresolv www.google.com

RFIDIOt ACG http://rfidiot.org/

Localização: /pentest/rfid/RFIDOt

Descrição: Uma coleção de ferramentas e bibliotecas escritos em python para fins de exploração de tecnologia RFID.

Sintaxe:

proxyresolv <host>

Opções: nenhuma

Observação: nenhuma

Exemplo:

Ótimo tutorial escrito por Adam para RFIDIOt.org pode ser encontrado http://www.rfidiot.org/documentation.html

RFIDIOt Frosch http://rfidiot.org/

Localização: /pentest/rfid/RFIDOt

Descrição: Uma coleção de ferramentas e bibliotecas escritos em python para fins de exploração de tecnologia RFID..

Sintaxe:

Ótimo tutorial escrito por Adam at RFIDIOt.org pode ser encontrado http://www.rfidiot.org/documentation.html

Opções: nenhuma

Observação: nenhuma

Exemplo:

Ótimo tutorial escrito por Adam para RFIDIOt.org pode ser encontrado http://www.rfidiot.org/documentation.html

RFIDIOt PCSC http://rfidiot.org/

Localização: /pentest/rfid/RFIDOt

Descrição: Uma coleção de ferramentas e bibliotecas escritos em python para fins de exploração de tecnologia RFID..

Sintaxe:

Ótimo tutorial escrito por Adam at RFIDIOt.org pode ser encontrado http://www.rfidiot.org/documentation.html

Opções: nenhuma

Observação: nenhuma

Exemplo:

Ótimo tutorial escrito por Adam para RFIDIOt.org pode ser encontrado http://www.rfidiot.org/documentation.html

RTDump http://rfidiot.org/

Localização: /pentest/rfid/RFIDOt

Descrição: faz parte do RainbowCrack conjunto de ferramentas utilizadas para despejo de lutar de uma cadeia de arco-íris.

Sintaxe:

./rtdump [caminho_tabelas_rainbow] [rainbow_chain_index]

Opções: nenhuma

Observação:
http://www.antsight.com/zsl/rainbowcrack/optimization/optimization.html

Exemplo: nenhum

RTSort http://rfidiot.org/

Localização: /pentest/password/rcrack

Descrição: faz parte do RainbowCrack, um conjunto de ferramentas usadas para classificar as cadeias rainbow chains e índice dessas cadeias rainbow chains de volta para o arquivo.

Sintaxe:

./rsort caminho_tabelas_rainbow

Opções: nenhuma

Observação:
http://www.antsight.com/zsl/rainbowcrack/optimization/optimization.htm

Exemplo: nenhum

RarCrack http://rarcrack.sourceforge.net/

Localização: /pentest/passwords/rarcrack

Descrição: Usa um algoritmo de força bruta para quebrar as senhas protegidas por senha de arquivos compactados RAR, 7z e zip.

Sintaxe:

rarcrack archive.ext [--threads <2-12>] [--type rar|zip|7z]

Opções:

- help:	mostra a tela de ajuda
- type:	usado para especificar o tipo de arquivo se não detectar
- topics:	número de segmentos para executar, max é 12, o padrão é 2

Observação: A Política de senha específica pode ser configurado através da edição do <targetname>.<ext>.xml.

Este arquivo é gerado automaticamente em tempo de execução

Exemplo:

./rarcrack test.rar --threads 12 --type rar

SA Exploiter http://securestate.com/pages/free-tools.aspx

Localização: /pentest/database/saexploiter

Descrição: é a mais avançada ferramenta GUI disponível de injeção de SQL. Se trata de copiar/colar o shellcode do Metasploit ou usando o seu próprio exe constumizado, SA Exploiter o binário payload não é limitada pela depuração do Windows para 64k como muitas outras ferramentas. Ele automatiza muitas outras tarefas de exploração e é projetado para Windows.

Sintaxe: nenhum

Opções:

Observação: Esta aplicação tem uma interface gráfica.

Exemplo: nenhum

SNMPEnum http://www.filip.waeytens.easynet.be/

Localização: /pentest/enumeration/snmpenum

Descrição: Um simples script Perl para enumerar informações em computadores que estão executando o SNMP.

Sintaxe:

./snmpenum.pl [endereço IP] [community] [configfile]

Opções: nenhuma

Observação: nenhum

Exemplo:

./snmpenum.pl 192.168.1.100 public linux.txt

SPIKE nenhum

Localização: /pentest/fuzzers/spike

Descrição: é uma tentativa de escrever uma fácil API de uso do protocolo genérico que ajuda a fazer engenharia reversa de protocolos de rede nova e desconhecida. Ele apresenta vários exemplos de trabalho. Inclui um servidor web de autenticação NTLM forcer bruta e código de exemplo que analisa aplicações web e DCE-RPC (MSRPC).

Sintaxe:

./snmpenum.pl [endereço IP] [community] [configfile]

Opções: nenhuma

Observação: http://74.125.47.132/search?q=cache:esKkXGhnAWQJ:www.blackhat.com/presentations/bh-usa-02/bh-us-02-aitel-spike.ppt+fuzzer+spike&hl=en&ct=clnk&cd=2&gl=us&client=safari

Exemplo: nenhum

SSHatter

Localização: /pentest/password/sshatter/src

Descrição: é uma tentativa de escrever uma fácil API de uso do protocolo genérico que ajuda a fazer engenharia reversa de protocolos de rede nova e desconhecida. Ele apresenta vários exemplos de trabalho. Inclui um servidor web de autenticação NTLM forcer bruta e código de exemplo que analisa aplicações web e DCE-RPC (MSRPC).

Sintaxe: nenhuma

Opções: nenhuma

Observação: http://freshmeat.net/projects/sshatter/?branch_id=70781&release_id=263196

Exemplo: nenhum

SWFIntruder

Localização: /pentest/web/swfintruder

Descrição: é a primeira ferramenta para testes de segurança em filmes Flash. SWFIntruder é um analisador de tempo de execução para filmes SWF externos. Ela ajuda a encontrar falhas em Flash.

Sintaxe: nenhuma

Opções: nenhuma

Observação:
http://www.owasp.org/index.php/Category:SWFIntruder
Este programa tem uma interface gráfica.

http://www.mindedsecurity.com/labs/fileshare/SWFIntruderTutorial.swf

Exemplo: nenhum

Smb4k http://smb4k.berlios.de/

Localização:

Descrição: Um navegador de rede avançada para o KDE e uma interface para os programas da suite de software Samba. Sua finalidade é oferecer um programa é fácil de usar e que tem tantos recursos quanto possível.

Sintaxe: nenhuma

Opções: nenhuma

Observação:

Esta é uma aplicação GUI.

http://smb4k.berlios.de/handbook/index.html

Exemplo: nenhum

TrueCrypt http://www.truecrypt.org

Localização: Path

Descrição: é um sistema de software para a criação e manutenção de um volume encriptado on-the-fly (dispositivo de armazenamento de dados). On-the-fly significa que a criptografia de dados é automaticamente criptografado ou descriptografado diretamente antes de serem carregados ou salvos, sem qualquer intervenção do usuário. Não há dados armazenados em um volume criptografado pode ser lido (descriptografado) sem usar a senha correta/keyfile(s) ou as chaves de criptografia correta. Sistema de arquivo inteiro é criptografado (por exemplo, nomes de arquivos e pastas, o conteúdo de cada arquivo, espaço livre, metadados, etc).

Sintaxe: nenhuma

Opções: nenhuma

Observação:

Esta é uma aplicação GUI.

http://www.truecrypt.org/docs/tutorial

Exemplo: nenhum

UDPTunnel

Localização: Path

Descrição: é um pequeno programa que cria um túnel de pacotes UDP bidirecional através de uma conexão TCP. Seu objetivo principal(motivação e original) é permitir que as conexões multi-media para atravessar um firewall que permite apenas conexões TCP de saída.

Sintaxe: nenhuma

Opções:

Uso 1:	udptunnel -s TCP-port [-r] [-v] UDP-addr/UDP-port[/ ttl]
Uso 2:	udptunnel -c TCP-addr[/TCP-port] [-r] [-v] UDP-addr/UDP-port[/ttl]
-s	modo servidor, espera para conexões TCP na porta
-c	modo client, conecta para o endereço indicado
-r	modo RTP, conectar/escutar on portas N e N+1 entre ambas UDP e TCP, número da portas
-v	mode verbose, especifique -v várias vezes para aumentar a verbosidade

Observação:

http://www1.cs.columbia.edu/~lennox/udptunnel/

Exemplo: nenhum

USBView http://www.kroah.com/linux/usb/

Localização: Path

Descrição: é um programa que exibe os dispositivos que são conectados ao barramento USB em uma máquina Linux. Ele também exibe informações sobre cada um dos dispositivos. Isso pode ser útil para determinar se um dispositivo está funcionando corretamente ou não.

Sintaxe: nenhuma

Opções: nenhuma

Observação:

Baseado em GUI auto-explicativa

Exemplo: nenhum

VoIPong http://www.enderunix.org/voipong/

Localização: /pentest/voip/voipong

Descrição: é um utilitário que detecta todas as chamadas de voz sobre IP em um pipeline e para aqueles que são codificados G711, dumps conversa real de arquivos em arquivos wave. Ele suporta SIP, H323, Skinny Cisco Client Protocol, RTP e RTCP.

Sintaxe: nenhuma

Opções: nenhuma

-h	ajuda na tela
-v	versão
-f	executado em primeiro plano (não se torne um daemon)
-d	nível de depuração. Níveis válidos são de 0 a 4 default(0).
-c	caminho do arquivo de configuração

Observação:

http://www.enderunix.org/voipong/manual/

Exemplo: nenhum

WarVOX http://warvox.org/

Localização: /pentest/voip/voipong

Descrição: é uma suíte de ferramentas para explorar, classificar e auditoria de sistemas de telefonia. Ao contrário das ferramentas wardialing normal, WarVOX trabalha com o áudio em tempo real de cada chamada e não utiliza um modem diretamente. Este modelo permite WarVOX para encontrar e classificar uma variedade de linhas interessantes, incluindo modems, faxes, caixas de correio de voz, PBXs, loops, tons de discagem, URAs, e transitários. WarVOX fornece a capacidade única de classificar todas as linhas telefônicas em um determinado intervalo, não apenas aquelas ligadas aos modems, permitindo uma auditoria abrangente de um sistema telefônico.

Sintaxe:

ruby warvox.rb

[*] Starting WarVOX on http://127.0.0.1:7777/

=> Booting Mongrel (use 'script/server webrick' to force WEBrick)
=> Rails 2.2.2 application starting on http://127.0.0.1:7777
=> Call with -d to detach
=> Ctrl-C to shutdown server
** Starting Mongrel listening at 127.0.0.1:7777
** Starting Rails with production environment...
** Rails loaded.
** Loading any Rails specific GemPlugins
** Signals ready. TERM => stop. USR2 => restart. INT => stop (no restart).
** Rails signals registered. HUP => reload (without restart). It might not work well.
** Mongrel 1.1.5 available at 127.0.0.1:7777
** Use CTRL-C to stop.

Opções: nenhuma

Observação:

http://warvox.org/

Exemplo: nenhum

WifiZoo http://community.cor
est.com/~hochoa/wif
izoo/index.html

Localização: /pentest/wireless/wifizoo

Descrição: é uma prova de conceito de rede sem fio, chamada sidejacker. Ele trabalha com a idéia de que a maioria das empresas devem forçar a logar com autenticação, passando por cookie de autenticação sem criptografia. Wifizoo permite que você use esse cookie e proxy com o usuário.

Sintaxe:

./wifizoo.py <opções>

Opções: nenhuma

-i <interface>

-c <pcap_file>

Observação: nenhuma

Exemplo:

./wifizoo.py -i ath0

Airolib-ng

Localização: /pentest/wireless/wifizoo

Descrição: Parte da suite aircrack-ng de ferramentas. Airolib-ng é uma ferramenta para o Aircrack-ng para armazenar e gerenciar listas essid e senha, calcular Pairwise Master Keys (PMKs) e usá-los cracking em WPA/WPA2.

Sintaxe:

airolib-ng <database> <operações> [opções]

Opções: nenhuma

--stats	Saída de informações sobre o banco de dados.
--sql <sql>	Executa comando SQL especificado
--clean [all]	o banco de Limpeza de sucata velha. 'all' irá também reduzir tamanho e se possível executar uma verificação de integridade.
--batch	lote Start-processamento todas as combinações de ESSIDs e senhas.
--verify [all]	Verificar se um conjunto de PMKs escolhidos aleatoriamente. Se 'todos' é dado, todos PMK inválido será excluído
--import [essid| passwd] <file> :	Importar um arquivo de texto como uma lista de ESSIDs ou senhas.
--import cowpatty <file>	Importação: um arquivo CoWPAtty.
--export cowpatty <essid> <file> :	Exportar para um arquivo CoWPAtty.

Observação: nenhuma

Exemplo:

./wifizoo.py -i ath0

AIRserv-ng http://www.aircrack-ng.org/doku.php?id=airserv-ng

Localização: Path

Descrição: Parte da suite aircrack-ng de ferramentas. AIRserv-ng é um servidor de placa wireless que permite que múltiplos programas aplicativos sem fio para uso de forma independente uma placa wireless através de um cliente-servidor TCP conexão de rede.

Sintaxe:

AIRserv-ng <opções>

Opções:

-h	ajuda na tela
-p <port>	porta TCP para escutar (padrão: 666)
-d <iface>	interface Wi-Fi para usar
-c <chan>	Canal de usar
-v <level>	Debug padrão (1 a 3; padrão: 1)

Observação:

http://www.aircrack-ng.org/doku.php?id=tutorial

Exemplo: nenhum

Asp-audit http://www.hacker-soft.net/Soft/Soft_2895.htm

Localização: Path

Descrição: asp-audit é uma ferramenta que ajuda a identificar servidores ASP.NET vulneráveis e fracamente configurados.

Sintaxe:

asp-audit.pl [http://target/app/file.aspx] [opções]

Opções:

-bf força bruta para versão ASP.NET usando JS Validate.

Observação: nenhuma

Exemplo:

asp-http://www.target.com/app/file.aspx audit.pl-bf

Buddy-ng

Localização: Path

Descrição: Parte da suite aircrack-ng de ferramentas. Buddy-ng servidor de ecos de volta os pacotes descodificada para o funcionamento do sistema easside-ng para acessar a rede sem fio sem saber a chave WEP. É feito com a AP se descriptografar os pacotes. Não existem parâmetros para buddy-ng. Uma vez invocado, ele escuta na porta TCP 6969 e UDP 6969. O TCP é usado para a ligação permanente entre esside-ng e buddy-ng. UDP é usado para receber pacotes decifrada a partir da AP.

Sintaxe:

buddy-ng

Opções: nenhuma

Observação: nenhuma

Exemplo:

buddy-ng

dnsmap-bulk http://lab.gnucitizen.org/projects/dnsmap

Localização: /pentest/enumeration/dns/dnsmap

Descrição: Executa força-bruta nos domínios. A ferramenta poderá usar uma wordlist interna ou arquivo de dicionário externo.

Sintaxe:

./dnsmap-bulk.sh <arquivo-domínios> <resultados-path>

Opções: nenhuma

Observação: nenhuma

Exemplo:

./dnsmap-bulk.sh domínios.txt /tmp/

Dnswalk

Localização: /pentest/enumeration/dns/dnswalk

Descrição: Um depurador de DNS que executa as transferências de zona de domínio especificado e verifica a base de dados de várias maneiras a sua coerência interna, bem como a precisão.

Sintaxe:

./dnswalk domain
domain MUST end with a '.'

Opções: nenhuma

Observação: nenhuma

Exemplo:

./dnswalk target.com

Dradis http://dradisframework.org/

Localização: /pentest/misc/dradis

Descrição: é uma ferramenta de código aberto para compartilhar informação durante as avaliações de segurança. Ele fornece um repositório centralizado de informações para acompanhar o que foi feito até agora, e que ainda está pela frente..

Sintaxe: veja em Exemplo

Opções: nenhuma

Observação:

The web interface
http://dradisframework.org/videos/dradis2-01.html

Import and export attachments
Video: http://dradisframework.org/videos/dradis2-02.html

Exemplo:

Inicie o servidor

./server/script/server

Usando a opção -p pode especificar o número da porta. Por padrão, o cliente Dradis vai tentar o servidor na porta 3004, se você alterar esse valor, será necessário modificar a configuração do cliente. Por padrão, Dradis escuta no loopback local (127.0.0.1), no entanto, é possível iniciar o servidor para escutar em uma interface diferente com o parâmetro -b:

./server -b 192.138.1.100

Abra o Firefox e vá para https://localhost:3004/

Inicie o cliente

cd cliente

Você terá que escolher entre o console padrão (interface):

ruby dradis.rb -c

ou a interface gráfica:

ruby dradis.rb -g

Dsniff http://monkey.org/~dugsong/dsniff

Localização: Path

Descrição: é uma coleção de ferramentas para auditoria de rede e testes de penetração. dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf e WebSpy para monitorar passivamente uma rede de dados (senhas, e-mail, arquivos, etc.) arpspoof, dnsspoof e macof facilitar a intercepção de tráfego de rede normalmente indisponível para um atacante (por exemplo, devido à camada de comutação-2). sshmitm e webmitm implementar ativo monkey-in-the-middle contra SSH e sessões HTTPS redirecionadas, explorando fracas ligações ad-hoc em PKI.

Sintaxe:

dsniff [-cdmn] [-i interface | -p pcapfile] [-s snaplen] [-f services] [-t trigger[,...]] [-r|-w savefile] [expression]

Opções: nenhuma

Observação: nenhuma

Exemplo: nenhum

Dsniff http://monkey.org/~dugsong/dsniff

Localização: Path

Descrição: é uma coleção de ferramentas para auditoria de rede e testes de penetração. dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf e WebSpy para monitorar passivamente uma rede de dados (senhas, e-mail, arquivos, etc.) arpspoof, dnsspoof e macof facilitar a intercepção de tráfego de rede normalmente indisponível para um atacante (por exemplo, devido à camada de comutação-2). sshmitm e webmitm implementar ativo monkey-in-the-middle contra SSH e sessões HTTPS redirecionadas, explorando fracas ligações ad-hoc em PKI.

Sintaxe:

dsniff [-cdmn] [-i interface | -p pcapfile] [-s snaplen] [-f services] [-t trigger[,...]] [-r|-w savefile] [expression]

Opções: nenhuma

Observação: nenhuma

Exemplo: nenhum

Hcidump http://www.linuxcommand.org/man_pages/hcidump8.html

Localização: Path

Descrição: lê dados brutos do HCI que estão entrando e saindo para um dispositivo Bluetooth e imprime os comandos de tela, eventos e dados de forma legível. Opcionalmente, o dump pode ser gravada em um arquivo simples para ser analisado e o arquivo de dump pode ser analisado em um momento posterior.

Sintaxe:

hcidump [opções] [filtro]

Opções:

-i,--device=hci_dev	HCI dispositivo
-l,--snap-len=len	snap len (em bytes)
-p,--psm=psm	padrão PSM
-m,--manufacturer=compid	padrão manufacturer
-w,--save-dump=file	salva em arquivo dump
-r,--read-dump=file	lê um arquivo dump
-s,--send-dump=host	envia dump para o host
-n,--recv-dump=host	recebe dump de um host
-d,--wait-dump=host	aguarda dump de um host e envia
-t,--ts	exibe time stamps
-a,--ascii	dados de dump em ascii
-x,--hex	dados de dump em hex
-X,--ext	dados de dump em hex e ascii
-R, --raw	dados de dump em raw
-C, --cmtp=psm	PSM para CMTP
-H, --hcrp=psm	PSM para HCRP

-O,	**--obex=channel**	channel para OBEX
-P,	**--ppp=channel**	channel para PPP
-D,	**--pppdump=file**	extrair trafego PPP
-A,	**--audio=file**	extrair dados de audio SCO
-B,	**--btsnoop**	usar arquivo no formato BTSnoop
-V,	**--verbose**	decodificação verbose
-Y,	**--novendor**	nenhum fornecedor ou comandos de eventos
-N,	**--noappend**	não adicionar os arquivos existentes
-4,	**--ipv4**	usar IPv4
-6	**--ipv6**	usar IPv6
-h,	**--help**	listar ajuda
--usage		listar ajuda

Observação: nenhuma

Exemplo: nenhum

Httprint GUI http://net-square.com/httprint

Localização: /pentest/enumeration/www/httprint/win32

Descrição: é um servidor web ferramenta impressão digital. Este programa tem uma interface gráfica

Sintaxe:

Host: adicionar o host que você deseja fazer o scanning (www.target.com exemplo).

Port: escolha a porta que pretende fazer o scanning (exemplo 80).

Opções: nenhuma

Observação: nenhuma

Exemplo: nenhum

Iaxflood http://www.hackingvoip.com/sec_tools.html

Localização: /pentest/voip/iaxflood

Descrição: Uma ferramenta para a ataque DoS para IAX.

Sintaxe:

./iaxflood <origem> <destino> <numero-pacotes>

Opções: nenhuma

Observação: nenhuma

Exemplo: nenhum

Inviteflood	http://www.securelogix.com

Localização: /pentest/voip/inviteflood

Descrição: Uma ferramenta para executar inundações (flooding) SIP/SDP message INVITE sobre UDP/IP.

Sintaxe:

./invitefood

Mandatório

Interface	(por exemplo, eth0)
usuário de destino	(por exemplo, "ou john.doe ou 5000, ou "1+210-555-1212")
domínio de destino	(por exemplo, enterprise.com ou um endereço IPv4)
endereço IPv4 do alvo de inundação(flood)	(ddd.ddd.ddd.ddd) (flood stage)fase de inundação (ou seja, número de pacotes)

Opções

-a	flood tool "From:" alias (e.g. jane.doe)
-i IPv4 origem do IP	[padrão é o endereço IP da interface]
-S srcPort (0 - 65535)	[padrão é conhecido por descartar porta 9]
-D destPort (0 - 65535)	[padrão é conhecido SIP porta 5060]
-l lineString	line used by SNOM [padrão é branco]
-s sleep time	btwn INVITE msgs (usec)
-h	ajuda
-v	Modo de saída verbose

Observação: nenhuma

Exemplo:

./inviteflood eth0 5000 proxy1.target.com
192.168.1.100 1000000

Itrace http://phenoelit-us.org/irpas/docu.html

Localização: Path

Descrição: Um programa que implementa funcionalidade do traceroute usando pacotes ICMP echo request. Portanto, parece que você está apenas usando ping no seu alvo, enquanto você faz traceroute. É muitas vezes ajuda de rastreamento por trás de firewalls.

Sintaxe:

itrace [opções] -i [dispositivo] -d [domínio]

Opções: nenhuma

-v	verbose
-n	inverter IPs de pesquisa (lento!)
-p x	enviar sondas x por hop (padrão 3)
-m x	máxima TTL padrão (30)
-t x	timeout após x segundos (padrão 3)
-i	dispositivo de rede
-d	destino

Observação: nenhuma

Exemplo:

itrace -i eth0 -d target.com

Netenum http://phenoelit-us.org/irpas/docu.html

Localização: Path

Descrição: Parte do conjunto de ferramentas IRAPS, netenum pode ser usado para produzir listas de convidados de outros programas. Não é tão poderoso como ping e outras ferramentas de varredura, mas é simples. Ao dar um tempo limite, ele usa o ICMP Echo Request para encontrar hosts disponíveis. Se você não fornecer um tempo limite, ele apenas imprime um endereço IP por linha, para que você possa usá-los em shell scripts.

Sintaxe:

netenum [dominio] [timout] [verbosidade]

Opções: nenhuma

Observação: nenhuma

Exemplo:

netenum target.com

Se o tempo limite é >0, pings são usados para enumerar. Verbalização é entre 0 (baixo) a 3 (verbose)

Onesixtyone http://www.phreedom.org/solar/onesixtyone/

Localização: Path

Descrição: Um scanner SNMP eficiente. Ela tira proveito do fato de que o SNMP é um protocolo sem conexão e envia todas as solicitações SNMP tão rápido quanto possível. Em seguida, o scanner aguarda as respostas de voltar e registra-los, de forma semelhante ao Nmap varreduras ping.

Sintaxe:

onesixtyone [options] [host] [community]

Opções: nenhuma

-c <communityfile>	arquivo com nomes de comunidade para decifrar
-i <inputfile>	arquivo com host do alvo
-o <outputfile>	registro de log
-d	modo de depuração, use duas vezes para obter mais informações
-w n	esperar n milissegundos entre o envio de pacotes padrão(10)
-q	Modo silencioso, não imprimir log stdout, use com-l

Observação: nenhuma

Exemplo:

onesityone -c dict.txt 192.168.1.100 public

OpenACUNETIX

Localização: /pentest/web/openAcunetix

Descrição: Uma ferramenta scanner em Java de código aberto para procurar vulnerabilidades em aplicações web.

Sintaxe: nenhuma

Opções: nenhuma

Observação: nenhuma

Exemplo:

1. Iniciar openACUNETIX (GUI scanner baseado em web)
2. Digite um URL de destino.
3. Clique em "scan".

Procecia

Localização: /pentest/scanners/propecia

Descrição: Um scanner muito rápido classe C de domínio que procura por uma determinada porta aberta.

Sintaxe:

./propecia [X.X.X] [porta]

Opções: nenhuma

Observação:

https://208.68.239.28/backtrack/wiki/discover.sh

Exemplo:

./propecia 192.168.1 80

Samdump2

Localização: Path

Descrição: Dump Windows 2k/NT/XP hashes de senha (por ncuomo).

Sintaxe:

samdump2 samhive keyfile

Opções: nenhuma

Observação:

http://sourceforge.net/project/showfiles.php?group_id=133599&package_id=222150

Exemplo:

Seu disco rígido do Windows é montado como /mnt/sda1 e um syskey dump do bkhive:] com nome dump.txt:

samdump2 /mnt/sda1/WINDOWS/system32/config/sam dump.txt > hashes.txt

SBD http://tigerteam.se/dl/sbd/

Localização: Path

Descrição: é uma ferramenta Netcat-clone, projetado para ser portátil e oferecem criptografia forte. Ele roda em sistemas Unix-like operacional e no Microsoft Win32. SBD possui características de criptografia AES-CBC-128 + HMAC-SHA1 (por Christophe Devine), a execução do programa (-e opção), porta de origem escolher, reconexão contínua com atraso e algumas outras características interessantes. Apenas o protocolo TCP/IP é suportado.

Sintaxe: nenhuma

Opções: nenhuma

Observação: nenhum

Exemplo: nenhum

SMAP http://www.wormulon .net/smap/

Localização: /pentest/voip/smap

Descrição: envia vários pedidos SIP aguardando respostas SIP DSL router, proxies e os agentes do usuário. Poderia ser considerado um mistura entre nmap e sipsak.

Sintaxe:

./smap [options] <IP | IP:port | IP/mask | host>

Opções: nenhuma

-h	ajuda
-d	aumentar a depuração
-o	permitir fingerprinting (impressões digitais)
-O	permitir fingerprinting (impressões digitais) mais detalhado
-l	modo de aprendizagem (impressões digitais)
-t	TCP
-u	UDP (padrão)
-P0	tratar todos hosts como online - pular descoberta de hosts
-p <port>	porta destino
-r <rate>	messagem limite ms por segundo
-D <domain>	domínio SIP para usar sem levar SIP
-w <timeout>	timeout em ms

Observação: nenhum

Exemplo:

./smap target.com

ou

smap 192.168.1.0/24

Smem

Localização: /pentest/voip/smap

Descrição: faz um exclusão segura das informações ao substituir a memória (RAM), porque o conteúdo da memória pode ser recuperada mesmo após uma parada! O padrão é o modo de segurança (38 gravações)..

Sintaxe:

smem [-flv]

Opções:

-f	modo rápido (e inseguro): no /dev/urandom.
-l	diminui a segurança (uso duas vezes para o modo de insegurança total).
-v	Modo verbose.

Observação: nenhum

Exemplo:

smem-v

Starting Wiping the memory, press Control-C to abort earlier.
Help: "smem -h"
Wipe mode is secure (38 special passes)
Using /dev/urandom for random input.
*******.....

SoapUI http://www.soapui.org

Localização: /pentest/web/soapui

Descrição:

é uma aplicação desktop livre e de código aberto para:

- Inspecionar Web Services
- Invocar Web Services
- Desenvolvimento de Web Services
- Web Services simulação e mocking
- Carga funcional e testes de conformidade dos Web Services

É principalmente destinado a desenvolvedores e testadores fornecendo ou consumindo WSDL ou REST baseados em Web Services(Java, Net, etc). Testes funcionais e de carga pode ser feito tanto de forma interativa em soapUI ou dentro de uma compilação automatizada ou processo de integração utilizando as ferramentas de linha de comando.

Sintaxe: nenhuma

Opções: nenhuma

Observação:

http://www.soapui.org/userguide/index.html

Exemplo: nenhum

Sqlsus http://sqlsus.sf.net/

Localização: nenhuma

Descrição:

é uma injeção de SQL em MySQL e a ferramenta de aquisição, escrito em perl. Através de uma interface de linha de comando que imita um console do MySQL, você pode recuperar o estrutura de banco de dados, injetar uma consulta SQL, download de arquivos do servidor web, upload e controle de um backdoor, e muito mais ... Ele é projetado para maximizar a quantidade de dados recolhidos por web hit servidor, fazendo o melhor uso das funções do MySQL para otimizar a injeção espaço disponível. sqlsus está focada em instalações PHP/MySQL e já integra alguns recursos simples, alguns dos quais são muito específicas para o SGBD. Ela não é e nunca vai ser um scanner de injeção de SQL.

Sintaxe: nenhuma

Opções: nenhuma

Observação: nenhuma

Exemplo: nenhum

SRM http://www.thc.org

Localização: Path

Descrição: não substitui um modo seguro/renomear/excluir do arquivo alvo(s). O padrão é o modo de segurança (38 gravações).

Sintaxe:

srm [-dflrvz] file1 file2 etc

Opções:

-d Ignore o ponto e dois arquivos especiais "." e "..".

-f modo rápido (e inseguro): no /dev/urandom, no modo de sincronizar.

-l diminui a segurança (uso duas vezes para o modo de insegurança total).

-r modo recursivo, apaga todos os subdiretórios.

-v Modo verbose

-z grava e limpa com zeros em vez de dados aleatórios.

Observação: nenhum

Exemplo:

1. touch gonk
2. bt:~# srm -v gonk

Using /dev/urandom for random input.
Wipe mode is secure (38 special passes)
Wiping gonk **********
Removed file gonk ... Done

Tcptraceroute http://michael.toren.net/code/tcptraceroute/

Localização: Path

Descrição: A implementação do traceroute com pacotes TCP. O traceroute mais tradicional envia pacotes UDP ou ICMP ECHO com um TTL de um lado e incrementa o TTL até que o destino foi alcançado. Ao imprimir os gateways que geram o tempo de ICMP excedido mensagens ao longo do caminho, ele é capaz de determinar os pacotes caminho a tomar para chegar ao destino.

Sintaxe:

tcptraceroute [-nNFSAE] [-i interface] [-f first TTL] [-l length] [-q number of queries] [-t tos] [-m max TTL] [-p source port] [-s source address] [-w wait time] host [destination port] [length]

Opções: nenhuma

Observação: nenhum

Exemplo:

tcptraceroute -i eth0 target.com

Tctrace http://phenoelit-us.org/irpas/docu.html

Localização: Path

Descrição: é como itrace um irmão do traceroute mas ele usa pacotes TCP SYN para rastreamento. Isto torna possível para que você possa rastrear através de firewalls. Caso seja um serviço em TCP que é permitido a passagem pelo firewall para fora dos limites de segurança da rede e para rede externa

Sintaxe:

tctrace [-vn] [-pX] [-mX] [-tX] [-DX] [-SX] -i [dispositivo] -d [domínio]

Opções:

-v	verbose
-n	IPs de pesquisa reversa
-pX	enviar sondas X (padrão 3)
-mX	máxima mX TTL (padrão 30)
-tX	timeout X sec (padrão 3)
-DX	porta destino (padrão 80)
-SX	porta origem (padrão 1064)
-i	dispositivo
-d	domínio

Observação: nenhum

Exemplo:

tctrace -i eth0 -d target.com

W3af http://w3af.sourceforge.net/

Localização: /pentest/web/w3af

Descrição: é um framework de ataque e auditoria para aplicações Web. O objetivo do projeto é criar um framework para encontrar e explorar as vulnerabilidades de aplicativos da Web sendo fácil de usar e estender.

Sintaxe:

./w3af_gui

Opções: nenhuma

Observação:

Tutorial part 1
http://pentesterconfessions.blogspot.com/2007/10/how-to-use-w3af-to-audit-web.html

Tutorial part 2
http://pentesterconfessions.blogspot.com/2007/10/w3af-tutorial-part-2.html

Este programa tem uma interface gráfica.

Exemplo: nenhum

Wep_keygen http://airpwn.sourceforge.net/Airpwn.html

Localização: Path

Descrição: Gera uma chave WEP com base na seqüência de entrada

Sintaxe:

wep_keygen <password>

Opções: nenhuma

Observação:

40-bit keys:
0: c4:31:bf:c7:05
1: fe:e9:d1:90:a0
2: 77:0b:73:80:7d
3: 4a:02:30:91:dd

104-bit key:
99:e9:55:55:31:f7:ae:a8:e3:5e:0e:9e:3c

Exemplo:

wep_keygen BackTrack

Afxml http://www.afflib.org

Localização: Path

Descrição: O Advanced Forensics Format (AFF) é um formato aberto extensível para o armazenamento de imagens em disco e metadados forenses. O Afxml gera saídas de metadados de um arquivo AFF em XML.

Sintaxe:

afxml [opções] arquivo

Opções: nenhuma

-v	Basta imprimir o número de versão e sair.
-x	Não incluem infile na saída.
-j segname	Basta imprimir segname para o arquivo. (pode ser repetido).

Observação: nenhuma

Exemplo:

afxml image1.aff

```
<?xml version='1.0' encoding='UTF-8'?>
<affobjects>
<!-- XML generated by afxml version 1.6.31 -->
<affinfo name='image1.aff'>
   <pages>1</pages>
</affinfo>
</affobjects>
```

Grendel-Scan http://grendel-scan.com/

Localização: /pentest/web/Grendel-Scan

Descrição: é um ferramenta open-source de testes de segurança em Web Application. Tem módulo automatizado de testes para a detecção de vulnerabilidades em aplicativos web comum e recursos voltados para a ajudar os testes de penetração (Pentest) manual. O único requisito do sistema é o Java 5, para Windows, Linux ou Macintosh.

Sintaxe:

Iniciar a aplicação.

Na seção "Base URLs" digite a URL completa (http://www.url.com ie) e clique em "Add".

Selecione um diretório de saída, se desejar.

Depois ir para a 'Test Module Selection' e marque 'All Test Modules'.

Ajuste o "Internal Proxy Settings" na caixa de seleção.
Scan Select '-> Start Scan'.

Opções: nenhuma

Observação:

Este programa tem uma interface gráfica.

Exemplo: nenhum

Miredo http://www.remlab.net/miredo/

Localização: /pentest/web/Grendel-Scan

Descrição: é software de Tunneling um open-source Teredo IPv6 . Inclui implementações funcionais de todos os componentes da especificação Teredo (cliente, servidor e relay). Ele foi criado para fornecer conectividade IPv6, mesmo por detrás dispositivos NAT.

Sintaxe:

Requer a utilização de um Miredo-Server].

Edite /etc/miredo/miredo.conf

Então:

miredo [options] [server_name]
Cria uma interface de encapsulamento Teredo para encapsulamento de IPv6 sobre UDP.

Opções:

-c --config	especificar um arquivo de configuração
-f --foreground	executado em primeiro plano ajuda
-h --help	ajuda
-p --pidfile	substituir a localização do arquivo de PID
-u --user	substituir o usuário defina a UID
-V --version	versão

Observação: nenhuma

Exemplo: nenhum

Voiper http://voiper.sourceforge.net/

Localização: /pentest/fuzzers/voiper

Descrição: é um conjunto de ferramentas de segurança que visa permitir com facilidade que desenvolvedores e pesquisadores de segurança, possam testar extensivamente e automaticamente dispositivos de VoIP para vulnerabilidades de segurança. Ele incorpora um conjunto fuzzing construído no framework Sulley fuzzing, uma "ferramenta torturadora" de SIP com base no RFC 4475 e uma variedade de módulos auxiliares para ajudar na detecção de colisão e de depuração.

Sintaxe:

./fuzzer.py [opções]

Opções: nenhuma

Observação:

Muitos cenários e tutoriais http://unprotectedhex.com/voiper-wiki/index.php/VoIPER_Usage_Examples

Exemplo:

./fuzzer.py -f SIPInviteCommonFuzzer -i 192.168.1.100 -p 5060 -a sessions/scen1 -c 0

SSWAP http://www.thc.org

Localização: Path

Descrição: Sobregrava com segurança o espaço de swap. O padrão é o modo de segurança (38 gravações).

Sintaxe:

sswap [-flvz] [-j start] /dev/of_swap_device

Opções:

-f modo rápido (e inseguro): no /dev/urandom no modo de sincronizar.

-j Salte sobre o primeiro número de bytes quando limpar. (padrão 4096)

-l diminui a segurança (use duas vezes para o modo de insegurança total).

-v Modo verbose.

-z limpar e escrever zeros em vez de dados aleatórios no final.

Observação:

Você deve desativar a partição swap antes de usar esse programa!

Exemplo:

```
bt:~# swapoff /dev/sda5
bt:~# sswap -fv /dev/sda5
Wipe mode is secure (38 special passes)
Writing to device /dev/sda5: *********...
```

BAFFLE GUI http://baffle.cs.dartmouth.edu/

Localização: path (baffle --gui)

Descrição: GUI interface para BAFFLE

Sintaxe:

baffle [opções] bssid essid

Opções: Fingerprinting

-i, --interface	A interface de utilização, tanto para a injeção e captação (padrão:ath0)
-j, --inject	A interface a usar para injeção (padrão:ath0)
-c, --capture	A interface de captura de usar para captura (padrão: ath0)
-d, --driver	O driver utilizado para a injeção (padrão: madwifing)
-h, --channel	O canal para escutar (padrão: 11)

Opções: Saída

-f, --fpdiagram	Escrever um diagrama de impressões digitais (footprinting) para cada sonda, utilizando SVGPREFIX
-p, --plot	Gravar um arquivo de lote para cada sonda, utilizando SVGPREFIX

Opções: Formação

-t, --train	treinamento de um novo dispositivo de fingerprint (impressão digital)

Opções comuns:

-v, --verbose	verbose mais detalhados
-?, --help	mostrar esta mensagem
--version	imprimir a versão
-g, --gui	Mostrar GUI

Observação: nenhuma

Exemplo: nenhum

BED http://snake-basket.de/bed.html

Localização: /pentest/fuzzers/bed

Descrição: Esta é uma coleção de scripts para testar automaticamente implementações dos protocolos diferentes para buffer overflow e/ou vulnerabilidades de formato de cadeia, através do envio de um lote de comandos de longas seqüências de um servidor de uma maneira chata e estúpida ... :) Daí o nome, .. ele tenta uma espécie de força-bruta, um ataque sem qualquer plano ... Alguns chamariam isso de um difusor. : P

Sintaxe:

./bed.pl -s [plugin] -t [target] -p [port] -o [timeout] [depends on the plugin]

Opções:

target host de destino para verificação (padrão localhost)

port porta para se conectar (porta padrão standard)

timeout tempo de espera em segundos para aguardar após cada teste (padrão 2 segundos)

Use "bed.pl -s <plugin>" para obter os parâmetros necessários para o plugin.

-s é um parâmetro obrigatório.

Observação: nenhuma

Exemplo:

./bed.pl -s HTTP -t 192.168.1.100

BED 0.5 by mjm (www.codito.de) & eric (www.snake-basket.de)

+ Buffer overflow testing:
testing: 1 HEAD XAXAX HTTP/1.0 .....
testing: 2 HEAD / XAXAX .....
testing: 3 GET XAXAX HTTP/1.0 .....
testing: 4 GET / XAXAX .....

testing: 5 POST XAXAX HTTP/1.0 .....
testing: 6 POST / XAXAX .....
testing: 7 GET /XAXAX .....
testing: 8 POST /XAXAX .....
+ Formatstring testing:
testing: 1 HEAD XAXAX HTTP/1.0 .....
testing: 2 HEAD / XAXAX .....
etc.....

Bluebugger http://www.remote-exploit.org/codes_bluebugger.html

Localização: Path

Descrição:

Sintaxe:

bluebugger [OPTIONS] -a <addr> [MODE]

Opções:

-a <addr>	um endereço Bluetooth do alvo
-m <name>	nome para usar quando conectar (padrão: '')
-d <device>	dispositivos para uso (padrão: '/dev/rfcomm')
-c <channel>	canal para uso (padrão: 17)
-n	No device name lookup
-t <timeout>	tempo limite em segundos para pesquisa de nome (padrão: 5)
-o <file>	salvar em arquivo <file>
Mode:	
info	ler informações do telefone (padrão)
phonebook	ler agenda telefônica (padrão)
messages	ler mensagens SMS (padrão)
dial <num>	número discado
ATCMD	comando personalizado (ex.: '+GMI')

Observação:

Nota: Os modos podem ser combinados, por exemplo, 'info phonebook +GMI'

* Você tem que definir o destino de endereço

Exemplo: nenhum

GISKismet

Localização: Path

Descrição: é uma ferramenta de visualização sem fio recon para representar os dados recolhidos através Kismet em um modo flexível. GISKismet armazena as informações em um banco de dados para que o usuário pode gerar gráficos usando SQL. GISKismet usa atualmente para o banco de dados SQLite e Google Earth / arquivos KML para gráficos

Sintaxe:

giskismet [Opções]

Opções: Arquivo de Entrada

--csv <csv-file>	analisar entrada a partir Kismet- devel CSV
-x --xml <xml-file>	analisar entrada a partir Kismet-anthropologicus NETXML

Opções: Filtros de Entrada

--bssid file | list	lista de filtro baseado em BSSID
--essid file | list	lista de filtro baseado em ESSID
--encryption file| list	lista de filtro baseado em criptografia (Encryption)
--channel file|list	lista de filtro baseado no Canal(Channel)
file | list	(lista = lista separado por vírgula (necessário aspas)

Opções Kismet-anthropologicus:

-a --ap	Inserir apenas os APs

Opções: Consulta

-q --query [sql]	consulta SQL
-m --manual [csv]	saida manual em CSV da consulta SQL
-o --output [file]	arquivo de saída
-n --name [str]	Nome do KML layer

--desc [str] Descrição do KML layer

Opções Gerais:

-d --debug [num] Mostra informações de depuração

-s --silent Sem saída silenciosa ao adicionar APs

-v --version versão

-h --help ajuda

Observação: nenhuma

Exemplo:

http://my-trac.assembla.com/giskismet/wiki/GISKismetExamples

Airpwn http://airpwn.sourcef
orge.net/Airpwn.html

Localização: Path

Descrição: é um framework para redes sem fio 802.11 para injeção de pacotes. Airpwn escuta a entrada de pacotes wireless e se os dados correspondem a um padrão especificado nos arquivos de configuração, o conteúdo personalizado é injectado e "falsificado" do Access Point Wireless. Do ponto de vista do cliente sem fio, airpwn se torna o servidor.

Sintaxe:

airpwn -c <conf file> -d <driver name> [interface options] [options]

Opções:

<conf file> : arquivo de configuração

<driver name> : nome do driver wireless suportados

Observação:

Opções de Interface:

Você pode usar parâmetro -i para definir todas as 3 interfaces de uma só vez, ou usar as outras opções para configurar cada interface individualmente.

-i <iface> : define a ouvir (listen)/controlar/injetar interface

-M <iface> : define a ouvir (listen) monitor interface

-C <iface> : define a interface de controle

-I <iface> : define a interface de injeção

Argumentos opcionais:

-l <logfile> : log detalhado de dados para um arquivo

-f <filter> : filtro bpf para libpcap

-F :	não assumem valores de FCS a partir da interface monitorada
-m <max> :	Especifica o tamanho de bloco de dados máxima (MTU - headers)
-k <WEP key>:	chave para a utilização descriptografar / criptografar pacotes WEP. Você pode usar essa opção várias vezes para especificar várias chaves WEP
-v :	aumentar a verbosidade (pode ser usado várias vezes)
-h	ajuda

Drivers suportados são: wlan-ng hostap airjack prism54 madwifing madwifiold rtl8180 rt2570 rt2500 rt73 rt61 zd1211rw bcm43xx mac80211

Exemplo: nenhum

BrAA http://linux.softpedia.com/get/System/Networking/braa-14436.shtml

Localização: Path

Descrição: Sobregrava com segurança o espaço de swap. O padrão é o modo de segurança (38 gravações).

Sintaxe:

braa [opções] [quesito1] [quesito2] ...

Opções:

-h ajuda

-2 propoem ser um agente SNMP2C

-v resumo depois de fazer todas as consultas

-x hexdump octet-strings

-t <s> esperar <s> segundos para respostas

-d <s> esperar <s> microsegundos depois de enviar each packet

-p <s> esperar <s> millisegundos entre subsequent passes

-f <file> carregar queries do arquivos <file> (linha por linha)

-a <time> sair depois de <time> segundos, independente do que acontecer

-r <rc> contagem de repetição (padrão 3)

Formato de consulta:

GET [community@]iprange[:port]:oid[/id]
WALK [community@]iprange[:port]:oid.*[/id]
SET [community@]iprange[:port]:oid=value[/id]

Observação: nenhuma

Exemplo:

Exemplos:
public@10.253.101.1:161:.1.3.6.*
10.253.101.1-10.253.101.255:.1.3.6.1.2.1.1.4.0=sme
10.253.101.1:.1.3.6.1.2.1.1.1.0/description

Também é possível especificar várias consultas de uma vez:

10.253.101.1-10.253.101.255:.1.3.6.1.2.1.1.4.0=sme,.1.3.6.*
Will set .1.3.6.1.2.1.1.4.0 to 'me' and do a walk starting from .
1.3.6

Valores de consultas SET têm que ser precedidas por um caractere que especifica o tipo de valor:

i INTEGER
a IP ADDRESS
s OCTET STRING
o OBJECT IDENTIFIER

Se o especificador do tipo estiver em falta, o tipo de valor é auto-detectado.

Exemplo:
brAA public@192.168.1.1-192.168.1.254: 161: .1.3.6 .*

Xgps http://gpsd.berlios.de

Localização: Path

Descrição: é um cliente de teste simples para witn gpsd witn com uma interface X. Ele exibe a posição atual do GPS/tempo/velocidade de informação e (para GPSs que suportam o recurso) as localizações dos satélites acessíveis. xgps requer o serviço [http://gpsd.berlios.de/gpsd] para ser executado. gpsd exige [hardware compatível http://gpsd.berlios.de/hardware.html] - especificamente uma antena GPS.

Sintaxe:

gpsd [-f GPS-devicename] [-F control-socket] [-S listener-port] [-b] [-n] [-N] [-h] [-P pidfile] [-D debuglevel] [-V] [[source-name]...]

xgps [X-options] [-h] [-j] [-V] [-speedunits {mph | kph | knots}] [-altunits {feet | meters}] [-l [d | m | s]] [-s smoothing] [server [:port [:device]]]

xgpsspeed [-rv] [X-options] [-h] [-V] [-nc X-color] [-speedunits {mph | kph | knots}] [server [:port [:device]]]

cgps [-h] [-j] [-V] [-speedunits {mph | kph | knots}] [-altunits {feet | meters}] [-l [d | m | s]] [server [:port [:device]]]

gpxlogger [logfile]

cgpxlogger [-s gpsd-server] [-p gpsd-port] [-i poll-interval] [-h]

Opções: nenhuma

Observação: nenhuma

Exemplo:

http://www.4x4falcon.com/gpsdrive/howtos/HOWTO_Ubuntu_Gpsdrive_Full_manual_install.php

Jmeter http://jakarta.apache.org/jmeter/

Localização: /pentest/web/jakarta-jmeter

Descrição: Apache JMeter é uma aplicação 100% puro Java desktop projetado para carregar o cliente de teste/software de servidor (como uma aplicação web). Ele pode ser usado para testar o desempenho tanto em recursos estáticos e dinâmicos, como arquivos estáticos, Java Servlets, CGI scripts, objetos Java, bancos de dados, servidores de FTP e muito mais. JMeter pode ser usado para simular uma carga pesada em um servidor, rede ou objeto para testar a sua força ou para analisar o desempenho global no âmbito de diferentes tipos. Além disso, JMeter pode ajudá-lo a teste de regressão da sua aplicação, permitindo que você criar scripts de teste para validar com as afirmações de que sua aplicação está retornando no resultado esperado. Para uma flexibilidade máxima, JMeter permite criar estas afirmações usando expressões regulares. Mas, por favor, note que JMeter não é um navegador.

Sintaxe: nenhuma

Opções: nenhuma

Observação:

http://jakarta.apache.org/jmeter/usermanual/index.html
http://jakarta.apache.org/jmeter/usermanual/jmeter_distributed_testing_step_by_step.pdf
http://jakarta.apache.org/jmeter/usermanual/jmeter_proxy_step_by_step.pdf
http://jakarta.apache.org/jmeter/usermanual/junitsampler_tutorial.pdf
http://jakarta.apache.org/jmeter/usermanual/jmeter_accesslog_sampler_step_by_step.pdf
http://jakarta.apache.org/jmeter/extending/jmeter_tutorial.pdf

Exemplo: nenhuma

Macchanger http://alobbs.com/macchanger/

Localização: Path

Descrição: A ferramenta GNU / Linux para visualizar / manipular o endereço MAC de interfaces de rede

Sintaxe:

macchanger [opções] dispositivo

Opções:

-h	ajuda
-V	versão
-s	mostra o endereço MAC
-e	não altere os bytes do vendedor
-a	MAC do fabricante aleatório do mesmo tipo
-A	MAC do fabricante aleatório do mesmo tipo ou de qualquer tipo e fabricante
-r	MAC do fabricante aleatório totalmente aleatório
-l	exibi os fabricantes conhecidos
-m	inserir manualmente um endereço MAC

Observação: nenhuma

Exemplo:

macchanger -s eth0