



 /dmuhackers

 @dmuhackers



Pentesting/CTF Tools

Overview

- Mass automation scripts
- Privilege Escalation
- Windows Resources
- Big ol' resource lists
- IppSec
- Web resources
- Miscellaneous extras



Mass Automation Scripts



AutoRecon

- Multi-threaded, automated recon tool
- Combines functionality of Reconnoitre, ReconScan, and bscan.
- Designed for use in OSCP – no automated exploitation
- Highly customisable
- Uses results from port/service scans to run further enumeration scans, e.g. Nikto for port 80 etc.

```
ddos@DESKTOP-HIGB3FF: ~/AutoRecon

AutoRecon

# Code written by @agrawalsmart7

Target:- google.com

[+]Checking DNS Zone transfer leakage:- No

[+]Checking of Virtual hosting of target:- Found. (will save the result in output file)

[-] The target is not using CSP. Hence skipping this step

[!] Spidering Target to see if any parameter is Vulnerable to XSS. (will print if any)

[!] Checking for any s3 buckets

List of buckets found
```

```
[*] Found ftp on tcp/21 on target 192.168.200.129
[*] Found ssh on tcp/22 on target 192.168.200.129
[*] Found telnet on tcp/23 on target 192.168.200.129
[*] Found smtp on tcp/25 on target 192.168.200.129
[*] Found domain on tcp/53 on target 192.168.200.129
[*] Found http on tcp/80 on target 192.168.200.129
[*] Found rpcbind on tcp/111 on target 192.168.200.129
[*] Found netbios-ssm on tcp/139 on target 192.168.200.129
[!] [tcp/139/nbtscan] Scan cannot be run against tcp port 139. Skipping.
[*] Found netbios-ssm on tcp/445 on target 192.168.200.129
[!] [tcp/445/enumfileux on 192.168.200.129] Scan should only be run once and it appears to have already been queued. Skipping.
[!] [tcp/445/nbtscan] Scan cannot be run against tcp port 445. Skipping.
[!] [tcp/445/enumclinet on 192.168.200.129] Scan should only be run once and it appears to have already been queued. Skipping.
[*] Found exec on tcp/512 on target 192.168.200.129
[*] Found login on tcp/513 on target 192.168.200.129
[*] Found tcpwrapped on tcp/514 on target 192.168.200.129
[*] Found java-rmi on tcp/1099 on target 192.168.200.129
[*] Found hlsdshell on tcp/1324 on target 192.168.200.129
[*] Found nfs on tcp/2049 on target 192.168.200.129
[*] Found ftp on tcp/2121 on target 192.168.200.129
[*] Found mysql on tcp/3306 on target 192.168.200.129
[*] Found postgresql on tcp/5432 on target 192.168.200.129
```



Lazy Script

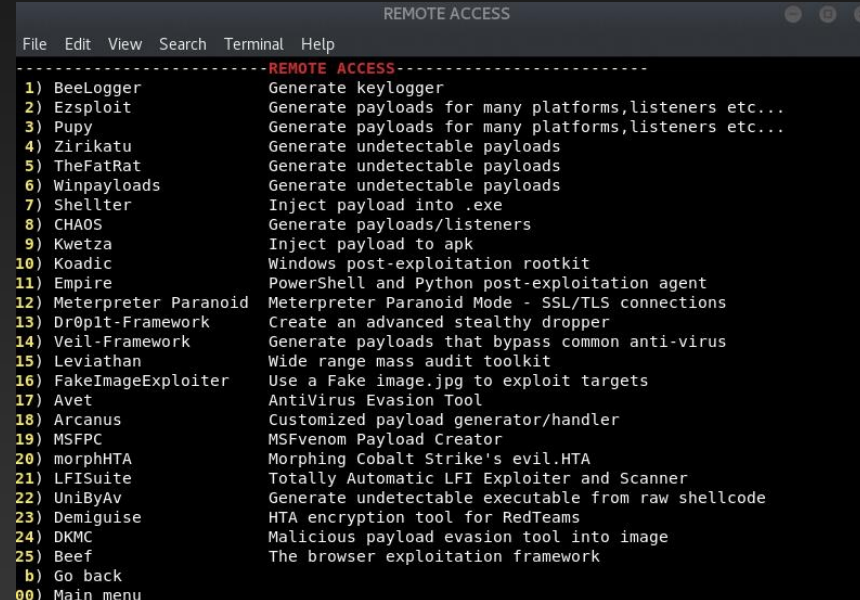
- Automate many tasks within Kali
- Wifi Hacking
- Recon
- SQLMap
- Metasploit
- Tonnes more...



The LAZY script v2.1.3 by ARIS MELACHROINOS

The LAZY script

if) Ifconfig	l) Local IPs & gateways	scan) Arp-scan network
1) Enable wlan0	d1) Disable wlan0	start) Start monitor mode
2) Enable wlan0mon	d2) Disable wlan0mon	stop) Stop monitor mode
3) Change MAC	d3) Restore original MAC	update) Check for updates
4) Enable anonym8	d4) Disable anonym8	errors) Fix some errors
5) Enable anonsurf	d5) Disable anonsurf	ks) Keyboard shortcuts
6) Anonsurf's status	d6) Restart anonsurf	d) Buy me a coffee
7) View public IP		s) Go to settings menu
8) View MAC		
9) TOOLS	15) Spoof EMAIL	
10) Handshake	16) Ngrok port forward	
11) Find WPS pin	17) Ask (Howdoi tool)	
12) WEP hacking	18) Auto-exploit browser	
13) MITM	19) Geolocate an IP	
14) Metasploit		
0) EXIT		



REMOTE ACCESS

-----REMOTE ACCESS-----

1) BeeLogger	Generate keylogger
2) Ezsploit	Generate payloads for many platforms,listeners etc...
3) Pupy	Generate payloads for many platforms,listeners etc...
4) Zirikatu	Generate undetectable payloads
5) TheFatRat	Generate undetectable payloads
6) Winpayloads	Generate undetectable payloads
7) Shellter	Inject payload into .exe
8) CHAOS	Generate payloads/listeners
9) Kwetza	Inject payload to apk
10) Koadic	Windows post-exploitation toolkit
11) Empire	PowerShell and Python post-exploitation agent
12) Meterpreter Paranoid	Meterpreter Paranoid Mode - SSL/TLS connections
13) Dr0pit-Framework	Create an advanced stealthy dropper
14) Veil-Framework	Generate payloads that bypass common anti-virus
15) Leviathan	Wide range mass audit toolkit
16) FakeImageExploiter	Use a Fake image.jpg to exploit targets
17) Avet	AntiVirus Evasion Tool
18) Arcanus	Customized payload generator/handler
19) MSFPC	MSFvenom Payload Creator
20) morphHTA	Morphing Cobalt Strike's evil.HTA
21) LFISuite	Totally Automatic LFI Exploiter and Scanner
22) UniByAv	Generate undetectable executable from raw shellcode
23) Demiguise	HTA encryption tool for RedTeams
24) DKMC	Malicious payload evasion tool into image
25) Beef	The browser exploitation framework
b) Go back	
00) Main menu	



Reverse Shell Info

So you gain access to a box. Now what?

Reverse shells allow you to create a connection back to your attack box in order to execute different commands.

There are numerous methods of doing this depending on the box.

- [Pentest Monkey Reverse Shell Cheatsheet](#)
- [msfvenom cheatsheet](#)
- [Rapid7 - How to use msfvenom](#)
- [Web Shell Cheatsheet](#)



Privilege Escalation

- [LinEnum](#) - Local enumeration and privesc checker (linux)
- [pspy](#) - Monitor processes running, cron jobs etc. (linux)
- [GTFOBins](#) - Searchable database of binaries useful in privesc (linux)
- [SUDO KILLER](#) - A tool to identify and exploit sudo rules' misconfigurations and vulnerabilities within sudo (linux)
- [PrivEsc Workshop](#) - Practical slides and exercises for practicing privesc. (windows and linux)
- [PEASS](#) - PrivEsc Awesome Script Suite. Local enumeration/privesc checking scripts (windows and linux)
- [Windows Exploit Suggester](#) - automated tool that checks windows version with known CVEs, Metasploit modules etc.
- [Windows Kernel exploits](#) - Selection of kernel exploits for known CVEs



Windows Resources

- [Red Team Cheatsheet](#) - Powershell one liners to download and execute various programs
- [Kerberos Attack Cheatsheet](#) - Cheatsheet for everything Kerberos related
- [PowerShell Cheatsheet](#) - Basic PowerShell commands
- [Bloodhound Cheatsheet](#) - A guide to bloodhound queries
- [LOLBAS](#) - Guide to built in Windows binaries and scripts useful for living off the land techniques



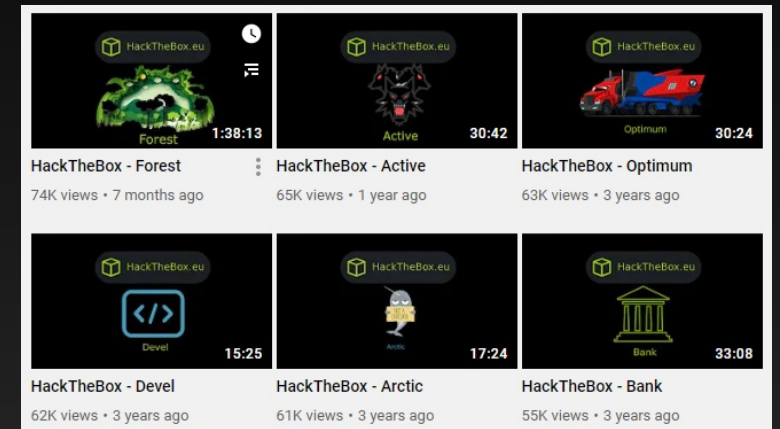
Resource lists

- [Payloads All The Things](#) - Collection of payloads for web app testing / pentests
- [CTF Katana](#) - Commands/tools useful for CTFs
- [Red-Teaming Toolkit](#) - Tools to aid in red team engagements
- [Red Team](#) - Scripts useful in red team engagements
- [Awesome Red-Teaming](#) - List of Awesome Red Team / Red Teaming Resources
- [Awesome Hacking](#) - A collection of various awesome lists for hackers, pentesters and security researchers
- [CTF-Tools](#) - Collection of CTF tools/cheatsheets
- [The Book Of Secret Knowledge](#) - A collection of inspiring lists, manuals, cheatsheets, blogs, hacks, one-liners, cli/web tools and more.
- [CYBOK](#) - Written by the NCSC, covers literally everything cyber security related



Ippsec

- Infosec professional with a large catalogue of HackTheBox walkthroughs
- [IppSec on Youtube](#)
- [Ippsec.rocks](#)
 - Site to search for specific techniques from his walkthroughs



IPPSEC	
Twitter • Patreon • Youtube	
sql	
Video	Description
Admirer	Bypassing adminer authentication by creating a MySQL Database
Multimaster	Using unicode to bypass the bad character list, then launching a super slow SQLMap that never finishes
Multimaster	While SQLMap runs, lets manually exploit this
Script now makes it easy to run UNION	



Web Resource

- Web application security testing software that comes with Kali
 - [Web Security Academy](#) - Sign up for free labs

- [DVWA \(Damn Vulnerable Web App\)](#)



- [OWASP Juice Shop](#)



Miscellaneous Extras

- Steg - [stegoVeritas](#) - has presets for image files
- Wi-Fi - [Fluxion](#) - Suite of wifi tools for automated MITM, hash attacks etc.
- Linux - [explain shell](#) - dissects any linux command showing you what each part does
- Hardware - [The Hardware Hacking Toolkit](#) - The best hacker's gadgets for Red Team pentesters and security researchers.
- [Google Dorks](#)
- OSINT - [OSINT Framework](#) - collection of sites useful for OSINT

