

[Home](#) [Posts](#) [Tools](#) [Twitter](#) [GitHub](#) [@](#)

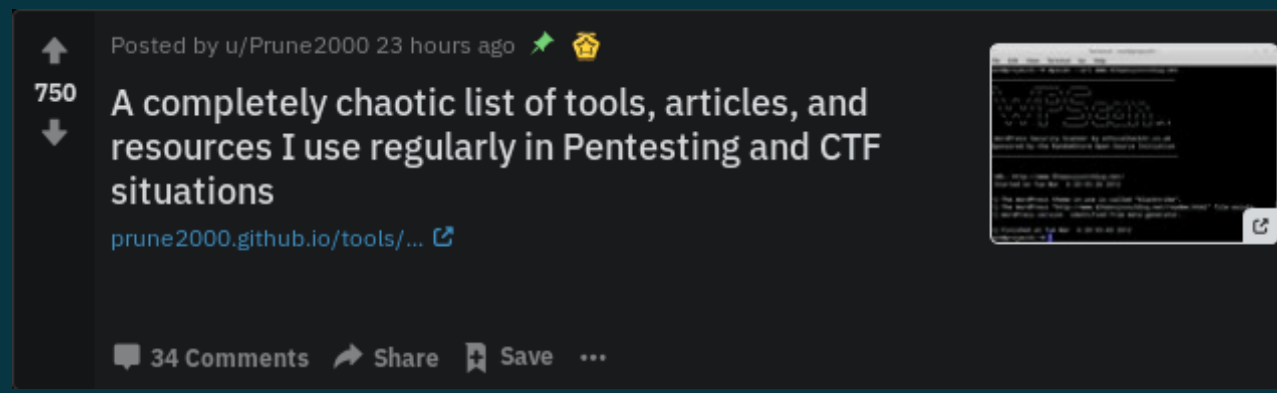
Pentesting tools

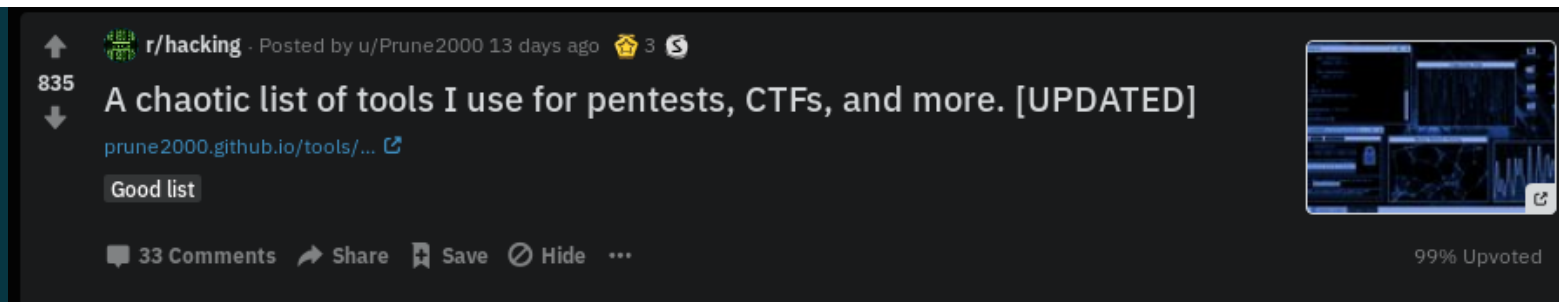
=====

This page will be a completely chaotic list of tools, articles, and resources I use regularly in Pentesting and CTF situations. My goal is to update this list as often as possible with examples, articles, and useful tips. It will serve as a reference for myself when I forget things and hopefully help other to discover tools that they haven't used. If you know of more tools or find a mistake, please contact me on Twitter or by email (links above).

(last edited: 29th of September 2019)

Was pinned on /r/hacking (even more tools suggested there):





Hydra

```
hydra options $user/$passOptions $ip/$url serviceOptions
```

Example I used during a CTF to find valid usernames:

```
hydra -L usernames.txt -p password -f -s 5001 35.227.x.x http-post-form  
"/hash/login:username=^USER^&password=^PASS^:Invalid username" -t 64
```

John the Ripper

Another bruteforcing tool, for password hashes this time. I explain how to add a new rule in [this post](#).

```
john --wordlist=password.lst --rules mypasswd
```

hashcat

hashcat is the world's fastest and most advanced password recovery utility, supporting five unique modes of attack for over 200 highly-optimized hashing algorithms. hashcat currently supports CPUs, GPUs, and other hardware accelerators on Linux, Windows, and macOS, and has facilities to help enable distributed password cracking.

Important note: a VM won't have access to your hardware so you'll need to do modifications to make it work as it will try to use GPU.

SQLMap

I use this tool a lot for SQL injections. For more information, check [this tutorial](#).

```
sqlmap -u $url options
```

Very useful option:

```
--forms: Parse and test forms
```

WPScan

WPScan is a free, for non-commercial use, black box WordPress vulnerability scanner written for security professionals and blog maintainers to test the security of their sites.

```
wpscan --url myblog.com
```

If a more stealthy approach is required, then
`wpscan --stealthy --url myblog.com` can be used.

When using the `--enumerate` option, don't forget to set the `--plugins-detection` accordingly, as its default is 'passive'.

Pentestmonkey Reverse Shell

The PHP reverse shell I use the most, you'll find it on [this page](#) with a tutorial on how to use it. Explore the rest of the Pentestmonkey website, it's great.

SecLists

SecLists is the security tester's companion. It's a collection of multiple types of lists used during security assessments, collected in one place. List types include usernames, passwords, URLs, sensitive data patterns, fuzzing payloads, web shells, and many more.

NMAP

No need to introduce this extremely useful tool, but here my usual command if it interests you:

```
nmap -sV -sC -oN myscan.txt $ip
```

- -sV: Version/Service info
- -sC: Run default scripts
- -oN: Normal output

Or the shorter version which combines sV and sC:

```
nmap -A -oN myscan.txt $ip
```

And if you do not need to be discreet (for certain CTFs without firewall f.ex.), you can add T5 which is the insane mode. T0 being the paranoid mode and will be a very slow scan.

```
nmap -A -T5 -oN myscan.txt $ip
```

Useful one-liner to look all the scripts that nmap can provide:

```
locate -r '\.nse$' | xargs grep categories | grep 'default\|version'
```

Let's say you're looking for SMB scripts:

```
locate -r '\.nse$' | xargs grep categories | grep 'default\|version' | grep  
smb
```

[Masscan](#)

I started using this tool as an addition to NMAP. It is a great port scanner and effective to grab banner information, but it can also scan the entire Internet in under 6 minutes!!

Command example for a simple port scan:

```
masscan -p80,8000-8100 10.0.0.0/8
```

And for banner checking:

```
masscan 10.0.0.0/8 -p80 --banners --source-ip 192.168.1.200
```

Wfuzz

Extremely useful for enumeration, Wfuzz is a tool designed for bruteforcing Web Applications, it can be used for finding resources not linked (directories, servlets, scripts, etc), bruteforce GET and POST parameters for checking different kind of injections (SQL, XSS, LDAP, etc), bruteforce Forms parameters (User/Password), Fuzzing, etc.

```
wfuzz -c -z file,/usr/share/wfuzz/wordlist/general/common.txt --hc 404  
http://192.168.1.202/FUZZ
```

Dirb

Another enumeration tool I use a lot.

```
dirb http://$ip/ /usr/share/wordlists/dirb/common.txt
```

DirBuster

Never enough enumeration tools! One more. This one as a GUI, so just type the command 'dirbuster' and it will launch the program.

Nikto

Did I say enumeration again? Nikto is the last enumeration tool I use. Never underestimate an effective enumeration during the recon phase.

```
nikto -Display 1234EP -o report.html -Format htm -Tuning 123bde -host $ip
```

Gobuster

I know, I know: more enumeration. But trust me having different tools to enumerate directories often helped me during CTFs in the recon phase. Just choose the ones that will do the job.

```
gobuster dir -u $url -w $wordlist
```

Sublist3r

Sublist3r is a python tool designed to enumerate subdomains of websites using OSINT. Sublist3r enumerates subdomains using many search engines such as Google, Yahoo, Bing, Baidu, and Ask. Sublist3r also enumerates subdomains using Netcraft, Virustotal, ThreatCrowd, DNSdumpster, and ReverseDNS.

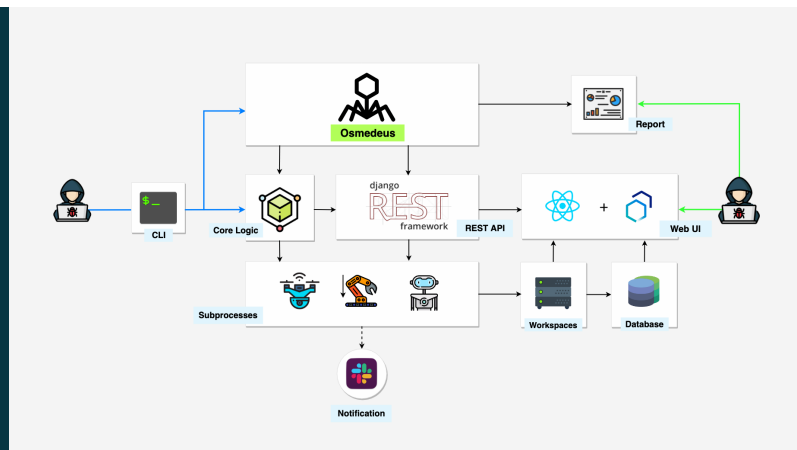
```
python sublist3r.py -d example.com
```

The Awesome Red Teaming

List of Awesome Red Team / Red Teaming Resources. This list is for anyone wishing to learn about Red Teaming but do not have a starting point.

Osmedeus


Osmedeus allows you automated run the collection of awesome tools to reconnaissance and vulnerability scanning against the target. Even has a slack bot to send notifications!



```
./osmedeus.py -t example.com
```

XSS Hunter

XSS Hunter allows you to find all kinds of cross-site scripting vulnerabilities, including the often-missed blind XSS. The service works by hosting specialized XSS probes which, upon firing, scan the page and send information about the vulnerable page to the XSS Hunter service.

XSS Payload Fires			
Thumbnail	Victim IP	Vulnerable Page URI	Options
	50.184.1.1	http://www.insecurelabs.org/Talk/Details/1?RemoveWarning=1	View Full Report Resend Email Report Delete

Upon signing up you will create a special xss.ht short domain such as yoursubdomain.xss.ht which identifies your XSS vulnerabilities and hosts your payload. You then use this subdomain in your XSS testing and XSS Hunter will automatically serve up XSS probes and collect the resulting information when they fire.

pspy

pspy is a command line tool designed to snoop on processes without need for root permissions. It allows you to see commands run by other users, cron jobs, etc. as they execute. Great for enumeration of Linux systems in CTFs. Also great to demonstrate your colleagues why passing secrets as arguments on the command line is a bad idea.

I explain [in this post](#) how to upload enumeration tools to a server.

LinEnum

Scripted Local Linux Enumeration & Privilege Escalation Checks.

I explain [in this post](#) how to upload enumeration tools to a server.

GTF0Bins

GTF0Bins is a curated list of Unix binaries that can be exploited by an attacker to bypass local security restrictions.

[LOLBAS](#)

The goal of the LOLBAS project is to document every binary, script, and library that can be used for [Living Off The Land techniques](#).

[TCM Security Sample Pentest Report](#)

This is a template for a pentest report kindly given by [the Cyber Mentor](#) (subscribe to his channel, awesome content), and in his own words:

"I am frequently asked what an actual pentest report looks like. I am providing a barebones demo report for "demo company" that consisted of an external penetration test. The report only includes one finding and is meant to be a starter template for others to use. Please feel free to download and make this your own."

[Cyber Chef](#)



A simple, intuitive web app for analysing and decoding data without having to deal with complex tools or programming languages. CyberChef encourages both technical and non-technical people to explore data formats, encryption and compression.

Extremely usefull to quickly decrypt simple hashes. Highly recommend.

exiftool

ExifTool is a platform-independent Perl library plus a command-line application for reading, writing and editing meta information in a wide variety of files.

For example, I explain how I extracted hidden information in images in this post.

Wireshark

Wireshark is the world's foremost and widely-used network protocol analyzer. It lets you see what's happening on your network at a microscopic level and is the standard.

In many forensic CTF challenges, you might have a pcap (Packet Capture Data) to analyze and Wireshark is more than often the best tool to do that. Check out [my write-up of the first exercise from Malware Traffic Analysis' exercise list](#). Planning to do many more in the future.

[Rawsec's CyberSecurity Inventory](#)

A much bigger inventory of tools and resources about CyberSecurity than mine here. Highly recommend if you want to scroll around and look at all the awesome tools that we have to play with.

[explainshell](#)

explainshell is a tool (with a web interface) capable of parsing man pages, extracting options and explain a given command-line by matching each argument to the relevant help text in the man page.

Tool recommended for this list by [@n1cfury](#)

[PayloadsAllTheThings](#)

A list of useful payloads and bypasses for Web Application Security.

You can contribute through pull requests, beers IRL or with buymeacoffee.com

PadBuster

PadBuster is a Perl script for automating Padding Oracle Attacks. PadBuster provides the capability to decrypt arbitrary ciphertext, encrypt arbitrary plaintext, and perform automated response analysis to determine whether a request is vulnerable to padding oracle attacks.

If you find a website that uses only cookies for authentication, it's a good idea to give PadBuster a try.

Command example to decrypt:

```
padbuster http://url.com/profile.php
4Ax3gr6sdNiBYo7LIkJUavx89eauhggdrMICdOvdWmDMM60o%2BHiXmg%3D%3D 8 -cookies
"Cookie: PHPSESSID=bn22u9fe085pkut4nsnrrckm96;
auth=4Ax3gr6sdNiBYo7LIkJUavx89eauhggdrMICdOvdWmDMM60o%2BHiXmg%3D%3D"
For example, this could result in {"user":"test","role":"user"}
```

So now, we can encrypt a new cookie with a different role:

```
padbuster http://url.com/profile.php
4Ax3gr6sdNiBYo7LIkJUavx89eauhggdrMICdOvdWmDMM60o%2BHiXmg%3D%3D 8 -cookies
"Cookie: PHPSESSID=bn22u9fe085pkut4nsnrrckm96;
auth=4Ax3gr6sdNiBYo7LIkJUavx89eauhggdrMICdOvdWmDMM60o%2BHiXmg%3D%3D" -
```

```
plaintext "{\"user\":\"test\",\"role\":\"admin\"}"
```

Which will give us a new encrypted cookie.

Malware Traffic Analysis

If you're interested in forensic and malware traffic analysis, this is THE website. It contains a lot of great articles, but also a very long list of exercises to practice your Wireshark skills! And of course following [@malware_traffic](#) on twitter is a must.

Check out [my write-up of the first exercise](#). Planning to do many more in the future.

Discover

Just started using Discover recently and I love it. It is used to automate various penetration testing tasks including recon, scanning, parsing, and creating malicious payloads and listeners with Metasploit. It will create a webpage for the report, really well done.

Give it a try with the passive recon!

CTF Time

CTF Time has all the past, present, and future CTF competitions. You can create an account, join a team, and start participating to competitions to climb the world ranks! Really useful to be motivated and never miss a good CTF to sharpen your skills.