

Forum: [Hack Forums](#)

Thread: [pentester halp](#)

the_x - July 30, 2025, 7:11 pm

trying to get better at pentesting and wondering where you seasoned pentesters keep up to date with tools, vulns, news?

i try and keep busy with thm with walkthroughs and some CTF boxes

htb occasionally

searching cs news sites like bleepingcomputer

watching lots of yt from david bombal, john hammond, network chuck, cyber news, hackersploit, the cyber mentor, nahamsec

not great on keeping up with chats on discord or forums like this place but looking to get better at it

working a lot in AD directories, playing around with password cracking and some wifi hacking like rogue APs, seeing whats good with bettercap/ettercap, and osint tools like social media, people lookup, breach lookups

just wondering if anyone had some good sources for sites, blogs, forums, discord chats.....

really into work by jim browning, scammer payback, and what ryan montgomery goes would be interesting to work with a group on that sorta stuff or help anyone out

DramaKing - July 30, 2025, 7:45 pm

You're on a good track; maybe get some professional training/certifications.

Err0rX - July 30, 2025, 9:33 pm

(Jul 30, 2025 07:11 PM)the_x Wrote: [CITE](#) trying to get better at pentesting and wondering where you seasoned pentesters keep up to date with tools, vulns, news?

i try and keep busy with thm with walkthroughs and some CTF boxes

htb occasionally

searching cs news sites like bleepingcomputer

watching lots of yt from david bombal, john hammond, network chuck, cyber news, hackersploit, the cyber mentor, nahamsec

not great on keeping up with chats on discord or forums like this place but looking to get better at it

working a lot in AD directories, playing around with password cracking and some wifi hacking like rogue APs, seeing whats good with bettercap/ettercap, and osint tools like social media, people lookup, breach lookups

just wondering if anyone had some good sources for sites, blogs, forums, discord chats.....

really into work by jim browning, scammer payback, and what ryan montgomery goes would be interesting to work with a group on that sorta stuff or help anyone out

If you want to seriously level up your pentesting game and keep up with the latest tools, vulnerabilities, and news, check out these tried-and-true resources:

Cybersecurity News & Research [BleepingComputer](#) – Packed with breaking cybersecurity news, malware breakdowns, and vulnerability reports.

[Exploit Database](#) – Public archive of recent exploits and software weakness disclosures.

[National Vulnerability Database \(NVD\)](#) – Official, government-backed repository of detailed vulnerability data.

[HackerOne Blog](#) – Deep-dive write-ups from top bug bounty hunters.

[ThreatPost](#) – Fast, concise coverage on emerging threats and security research.

YouTube Channels for Pentesting & Security [NetworkChuck](#) – Super digestible cybersecurity concepts with real demos. (My personal top pick.)

[The Cyber Mentor](#) – Hands-on ethical hacking tutorials and OSCP prep.

[NahamSec](#) – Live hacking streams, bounty tips, and CTF walkthroughs.

[Hackersploit](#) – In-depth red-teaming and pentesting tool guides.

[Scammer Payback \(Jim Browning\)](#) – Real-world scam investigations and social engineering exposés.

Training Platforms & Labs [TryHackMe](#) – Beginner-friendly, interactive labs with guided challenges.

[Hack The Box](#) – Realistic CTF-style environments to test your skills.

[PentesterLab](#) – Web-app security exercises with practical tutorials.

[VulnHub](#) – Download vulnerable VMs for offline practice.

Essential Tools & Resources Bettercap & Ettercap – Network sniffing, spoofing, and MITM frameworks.

[CrackStation](#) & [Hashcat](#) – Brute-force and dictionary-based password cracking.

[OSINT Framework](#) – Curated directory of open-source intelligence tools.

[Maltego](#) – Uses “Transforms” to pull data (WHOIS, DNS, social media) and visualize relationships on interactive graphs.

Nmap, Metasploit & Burp Suite – The core triad every pentester needs in their toolkit.

How to Install Core Tools on Debian/Ubuntu

Code `sudo apt update`

```
[h1]Install Bettercap[/h1]
sudo apt install bettercap
```

```
[h1]Install Ettercap (GUI version)[/h1]
sudo apt install ettercap-graphical
```

```
[h1]Install Hashcat[/h1]
sudo apt install hashcat
```

```
[h1]Install Nmap[/h1]
sudo apt install nmap
```

```
[h1]Install Metasploit Framework[/h1]
curl https://raw.githubusercontent.com/rapid7/metasploit-framework/master/msfupdate | sudo bash
For Burp Suite & Maltego:
Download the official installers from their websites and run the setup.
```

CrackStation & OSINT Framework:
Browser-based tools—no installation required.

Master these resources, keep practicing, and you'll build a rock-solid foundation in pentesting and cybersecurity.

If any link in this post is broken or removed, let me know so I can fix it.

??????????? - July 31, 2025, 3:25 am

(Jul 30, 2025 09:33 PM)Err0rX Wrote: [CITE](#) If you want to seriously level up your pentesting game and keep up with the latest tools, vulnerabilities, and news, check out these tried-and-true resources:

Cybersecurity News & Research [BleepingComputer](#) – Packed with breaking cybersecurity news, malware breakdowns, and vulnerability reports.

[Exploit Database](#) – Public archive of recent exploits and software weakness disclosures.

[National Vulnerability Database \(NVD\)](#) – Official, government-backed repository of detailed vulnerability data.

[HackerOne Blog](#) – Deep-dive write-ups from top bug bounty hunters.

[ThreatPost](#) – Fast, concise coverage on emerging threats and security research.

YouTube Channels for Pentesting & Security [NetworkChuck](#) – Super digestible cybersecurity concepts with real demos. (My personal top pick.)

[The Cyber Mentor](#) – Hands-on ethical hacking tutorials and OSCP prep.

[NahamSec](#) – Live hacking streams, bounty tips, and CTF walkthroughs.

[Hackersploit](#) – In-depth red-teaming and pentesting tool guides.

[Scammer Payback \(Jim Browning\)](#) – Real-world scam investigations and social engineering exposés.

Training Platforms & Labs [TryHackMe](#) – Beginner-friendly, interactive labs with guided challenges.

[Hack The Box](#) – Realistic CTF-style environments to test your skills.

[PentesterLab](#) – Web-app security exercises with practical tutorials.

[VulnHub](#) – Download vulnerable VMs for offline practice.

Essential Tools & Resources Bettercap & Ettercap – Network sniffing, spoofing, and MITM frameworks.

[CrackStation](#) & [Hashcat](#) – Brute-force and dictionary-based password cracking.

[OSINT Framework](#) – Curated directory of open-source intelligence tools.

[Maltego](#) – Uses “Transforms” to pull data (WHOIS, DNS, social media) and visualize relationships on interactive graphs.

Nmap, Metasploit & Burp Suite – The core triad every pentester needs in their toolkit.

How to Install Core Tools on Debian/Ubuntu

Code sudo apt update

[h1]Install Bettercap[/h1]

sudo apt install bettercap

[h1]Install Ettercap (GUI version)[/h1]

sudo apt install ettercap-graphical

[h1]Install Hashcat[/h1]

sudo apt install hashcat

[h1]Install Nmap[/h1]
sudo apt install nmap

[h1]Install Metasploit Framework[/h1]
curl https://raw.githubusercontent.com/rapid7/metasploit-framework/master/msfupdate | sudo bash
For Burp Suite & Maltego:
Download the official installers from their websites and run the setup.

CrackStation & OSINT Framework:
Browser-based tools—no installation required.

Master these resources, keep practicing, and you'll build a rock-solid foundation in pentesting and cybersecurity.

If any link in this post is broken or removed, let me know so I can fix it.

good post and a lot of info/intel. Some mf will say it is AI, ignore it bro.

Err0rX - July 31, 2025, 3:28 am

(Jul 31, 2025 03:25 AM)??????? Wrote: [\[CITE\]](#) good post and a lot of info/intel. Some mf will say it is AI, ignore it bro.

Thanks bro, but I only use AI for minor formatting. As for the sources, I gather them myself. And if you test the content on any detection site, it'll instantly flag phrases like "If any link in this post is broken or removed, let me know so I can fix it." as AI-generated — that's why those tools aren't exactly accurate.

???????????? - July 31, 2025, 3:34 am

(Jul 31, 2025 03:28 AM)Err0rX Wrote: [\[CITE\]](#) Thanks bro, but I only use AI for minor formatting. As for the sources, I gather them myself. And if you test the content on any detection site, it'll instantly flag phrases like "If any link in this post is broken or removed, let me know so I can fix it." as AI-generated — that's why those tools aren't exactly accurate.

I use those tools to help with formatting since English isn't my first language and to make my replies more presentable. Please disregard any noise and keep contributing.

Err0rX - July 31, 2025, 3:48 am

(Jul 31, 2025 03:34 AM)??????? Wrote: [\[CITE\]](#) I use those tools to help with formatting since English isn't my first language and to make my replies more presentable. Please disregard any noise and keep contributing.

Same case here — Russian is my main language, so I let AI shape the format a bit
That's why any AI detector will only show a low score if you test it.

???????????? - July 31, 2025, 3:49 am

(Jul 31, 2025 03:48 AM)Err0rX Wrote: [\[CITE\]](#) Same case here — Russian is my main language, so I let AI shape the format a bit

That's why any AI detector will only show a low score if you test it.
Bingo we are on the same track. Wanna meetup in St Petersburg?

Err0rX - July 31, 2025, 3:52 am

(Jul 31, 2025 03:49 AM)??????? Wrote: [\[CITE\]](#) Bingo we are on the same track. Wanna meetup in St Petersburg?

If I was still in Russia, I wouldn't even hesitate — but I'm far out right now

??????????? - July 31, 2025, 4:10 am

(Jul 31, 2025 03:52 AM)Err0rX Wrote: [\[CITE\]](#) If I was still in Russia, I wouldn't even hesitate — but I'm far out right now

No worries, we will meet sometime in future.

Err0rX - July 31, 2025, 4:12 am

(Jul 31, 2025 04:10 AM)??????? Wrote: [\[CITE\]](#) No worries, we will meet sometime in future.

Haha, I hope so too, my friend

the_x - July 31, 2025, 9:52 am

woof ?

lots of good stuff. i do appreciate the help but i actually do have a lot of that under my belt already even if i should probably play around with the tools a lot more

also looking to make some friends here to get into some stuff or start something fun up. not looking to get in trouble but i like tinkering

not great on the web app or programming side but we all have our specialties ?

??????????? - July 31, 2025, 9:57 am

(Jul 31, 2025 09:52 AM)the_x Wrote: [\[CITE\]](#) woof ?

lots of good stuff. i do appreciate the help but i actually do have a lot of that under my belt already even if i should probably play around with the tools a lot more

also looking to make some friends here to get into some stuff or start something fun up. not looking to get in trouble but i like tinkering

not great on the web app or programming side but we all have our specialties ?

Which part are you good with?

the_x - August 1, 2025, 7:37 am

id say networking side, physical or lower end of the OSI model

haven't really determined what i wanna be l33t at but hey, i have plenty of time

??????????? - August 2, 2025, 7:26 am

(Aug 1, 2025 07:37 AM)the_x Wrote: [\[CITE\]](#) id say networking side, physical or lower end of the OSI model

haven't really determined what i wanna be l33t at but hey, i have plenty of time

Start working on linux basics.

the_x - September 3, 2025, 8:11 pm

i hope im past the basics

just looking to levl up and get into some real world stuff

chasing certs gets old but i guess i can start looking into red team stuff since thats seems more 'hands on'