Practical Ethical Hacking – Frequently Asked Questions

The purpose of this document is to provide students with the most frequently asked questions we have received and the solutions to those questions. **Please note:** If you do not see your question listed here, please utilize the Discord channel or Udemy Q&A (in that preferred order) for further troubleshooting.

Commonly Reported Issues (sorted by video appearance):

Location: Section 5, video "Installing Kali Linux"
Question: I installed a version of Kali > 2019.4. The credentials of root:toor no longer work. What are the correct credentials?
Resolution:

The correct credentials, as of 2020.1, are kali:kali

Location: Section 6, video "Installing and Updating Tools"
Question: I cannot install pip. What gives?
Resolution:

Run the following command: `curl https://bootstrap.pypa.io/get-pip.py -o get-pip.py; python get-pip.py`

Alternatively, you can run "sudo apt install python3-pip" and then "pip3 install ."

Location: Section 6, video "Scripting with Bash"
Question: My bash script is producing an error with "seq". How do I resolve?
Resolution:

Ensure use of backtick (`) instead of using single quote ('). Alternatively, use $(seq 1 254) instead of seq

Location: Section 7, video "Building a Port Scanner"
Question: My Python script is giving a socket.gaierror
Resolution:

This error means the script cannon resolve the hostname via DNS. It is later taken care of when we write out the exception in the script. However, you can safely ignore it or try an actual website, such as google.com.

Location: Section 10, video “Scanning with Nmap”
Question: I cannot discover the Kioptrix machine with netdiscover on VirtualBox/Mac. How do I resolve?
Resolution:

1. Create a NAT network for Kali and Kioptrix VMs
2. Enable promiscuous mode for both VMs in the Network Settings in VirtualBox
3. Ensure config file is changed from "bridged" to "nat"
4. Reboot both machines

Additionally, let netdiscover run for a few minutes after it says finished. It will continue to passively scan for hosts and may take a minute or two to find the host

If all else fails, please follow this guide and attempt again:
https://vivirytech.blogspot.com/2018/01/oscp-journey-001-vm-prep-for-kioptrix.html

Location: Section 10, video “Enumerating SMB”
Question: My enum4linux and/or smbclient are not working. I am receiving "Protocol negotiation failed: NT_STATUS_IO_TIMEOUT". How do I resolve?
Resolution:

On Kali, edit /etc/samba/smb.conf

Add the following under global:
client min protocol = CORE
client max protocol = SMB3

Location: Section 14, video “Fuzzing”
Question: My script is crashing at 100 bytes?
Resolution: Use the following script below, which utilizes payload.encode

```
#!/usr/bin/python

import sys, socket
from time import sleep

buffer = "A" * 100

while True:
    try:
        payload = "TRUN /.:/" + buffer

        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        s.connect(('192.168.1.35',9999))
        print ("[+] Sending the payload...\n" + str(len(buffer)))
        s.send((payload.encode()))
        s.close()
        sleep(1)
        buffer = buffer + "A"*100
    except:
        print ("The fuzzing crashed at %s bytes" % str(len(buffer)))
        sys.exit()
```

Location: Section 17, video “SMB Relay Attacks”
Question: My SMB relay is not working. How do I resolve?
Resolution:

> There have been reports that SMB is failing to relay for some users in their labs. If this is happening, attempt to navigate to the attacker’s IP address from a web browser (such as \\192.168.10.1) instead of the SMB event. You should trigger a relay.

Location: Section 17, video “IPv6 DNS Takeover via mitm6”
Question: My ntlmrelayx is giving an error during the attack. How can I resolve?
Resolution:

Impacket versions > 0.9.19 are unstable and causing issues for students and pentesters alike. Try purging impacket completely and downloading 0.9.19 from here: https://github.com/SecureAuthCorp/impacket/releases.

Location: Section 21, video “Installing Go”
Question: My Go is not working. How do I resolve?
Resolution:

Edit your ~/.bashrc and add:

```
export GOPATH=$HOME/go
export GOROOT=/usr/local/go
export PATH=$PATH:$GOROOT/bin:$GOPATH/bin
```

Save and type “source ~/.bashrc”

Frequently Asked Questions not directly related to material:

Q: Will this course prepare me for a certification (e.g. OSCP, CEH, etc.)?

A: In terms of certifications, this course is not geared towards helping students pass any specific certification courses. Each certification has slightly different curriculum and most focus on a lot of tools and methods that aren't truly practical in penetration testing. A lot of what you'll learn will absolutely help ease the burden on these courses, but the course should be used as a supplement vs. a complete replacement.

Q: Will I be employment ready after this course?

A: Yes and no. You will have an understanding of most of the topics asked in an interview as well as how to exploit them. However, it is recommended to supplement with other items and practice to boost your resume, skills, and confidence. This could be adding a certification like the OSCP to your repertoire, spending some time attacking Hack The Box or Virtual Hacking Labs machines, and/or starting a blog, YouTube, etc. to improve your skillset. TLDR; it's a great start, but practice makes perfect.