BY NADIA SCHUTZ

PENETRATION TESTING

BEGINNER

OSCP/KALI/LINUX COMMAND LINE

DISCLAMER:

Nadia Schutz is not affiliated with anyone or any products mentioned in this course.
The course is made for educational purposes only. Please be cautious and follow the law.

Who should become a pen tester?

3 Ingredients to be successful in this field:

1. Natural curiosity
2. Discipline
3. Integrity

✓

- love to study and continuously improve your skills
- love puzzles
- love taking things apart and creating new things
- want to protect the community and spread awareness
- being humble and helpful

✗

- to get the experience of a “bad guy”
- hacking is just simply cool
- to learn hacking to spy on your GF/BF
- to learn hacking to revenge on your enemies
- black hat hackers are more superior/knowledgeable than white hat hackers
- to hack NASA using HTML

OSCP Certification

PEN-200: Penetration Testing with Kali Linux
https://www.offsec.com/courses/pen-200/

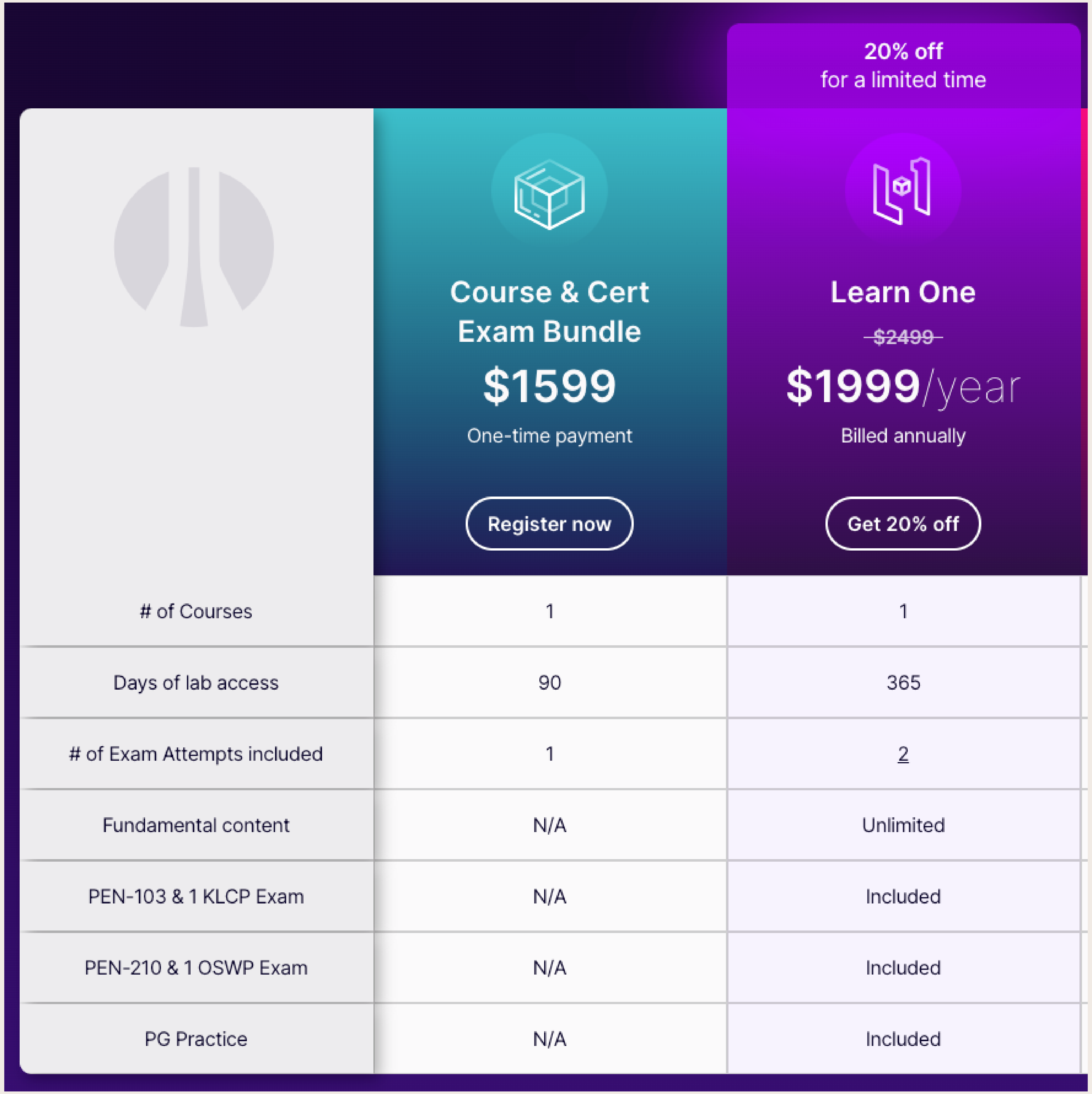
- practical exam which proves your actual practical ethical hacking skills (6 machines over 24 hrs + report)
- great labs (PWK + PG)
- tons of exercises

1-year subscription

- new to pen-testing
- new to cybersecurity
- finished a few HTB labs or some other labs
- finished A+/Network+/Network+

3-months subscription

- a year or more of pen-testing experience
- finished over 100 HTB labs



20% off
for a limited time

	Course & Cert Exam Bundle $1599 One-time payment Register now	Learn One ~~$2499~~ $1999/year Billed annually Get 20% off
# of Courses	1	1
Days of lab access	90	365
# of Exam Attempts included	1	2
Fundamental content	N/A	Unlimited
PEN-103 & 1 KLCP Exam	N/A	Included
PEN-210 & 1 OSWP Exam	N/A	Included
PG Practice	N/A	Included

OSCP Certification

- it’s ok if you don’t pass on your first attempt
- don’t rush, take your time
- use this opportunity to learn as much as you can instead of trying to pass the exam ASAP
- practice and discipline will take you far on your journey!

1. Pen-100
2. TJNULL: HTB list
3. TJNULL: PG list
4. Pen-200
5. PWK labs (75)

TJNULL boxes list
https://docs.google.com/spreadsheets/u/0/d/1dwSMIAPIam0PuRBkCiDI88pU3yzrqqHkDtBngUHNCw8/htmlview?pli=1#

Installing VirtualBox

Download VirtualBox from this link:
https://www.virtualbox.org/wiki/Downloads

Click on the downloaded file, and after a few following prompts, VirtualBox will be installed on your host machine.

Detailed installation documentation:
https://www.virtualbox.org/manual/ch02.html

Network settings:
https://www.virtualbox.org/manual/ch06.html
https://www.nakivo.com/blog/virtualbox-network-setting-guide/

Installing Kali

Download Kali from this link:
https://www.kali.org/get-kali/#kali-platforms

Click on the downloaded file and after a few following prompts it will be installed.

Detailed installation documentation:
https://www.kali.org/docs/virtualization/install-virtualbox-guest-vm/

Free Kali course by OffSec
https://portal.offsec.com/courses/pen-103

Linux commands

to change the root password:

sudo -s (enter "kali" for password)

passwd root (change password)

passwd kali (change password)

Update and upgrade the Kali distribution:

apt-get update && apt-get upgrade

Change the hostname of your device:

nano /etc/hostname [change “kali” to anything you want]

nano /etc/hosts [change “kali” to anything you want]

Then reboot:

reboot

whoami - what user

sudo su - switch to root

ls - Lists a directory’s content

pwd - Shows the current working directory’s path

cd - Changes the working directory

mkdir - Creates a new directory

rm - Deletes a file

cp - Copies files and directories, including their content

mv - Moves or renames files and directories

touch - Creates a new empty file

file - Checks a file’s type

zip and **unzip** - Creates and extracts a ZIP archive

tar - Archives files without compression in a TAR format

nano, **vi**, and **jed** - Edits a file with a text editor

cat - Lists, combines, and writes a file’s content as a standard output

grep - Searches a string within a file

sed - Finds, replaces, or deletes patterns in a file

head - Displays a file’s first ten lines

tail - Prints a file’s last ten lines

awk - Finds and manipulates patterns in a file

sort - Reorders a file’s content

Linux commands

cut - Sections and prints lines from a file

diff - Compares two files' content and their differences

tee - Prints command outputs in Terminal and a file

locate - Finds files in a system's database

find - Outputs a file or folder's location

sudo - Runs a command as a superuser

su - Runs programs in the current shell as another user

chmod - Modifies a file's read, write, and execute permissions

chown - Changes a file, directory, or symbolic link's ownership

useradd and **userdel** - Creates and removes a user account

df - Displays the system's overall disk space usage

du - Checks a file or directory's storage consumption

top - Displays running processes and the system's resource usage

htop - Works like top but with an interactive user interface

ps - Creates a snapshot of all running processes

uname -Prints information about your machine's kernel, name, and hardware

hostname - Shows your system's hostname

systemctl - Manages system services

watch - Runs another command continuously

jobs - Displays a shell's running processes with their statuses

kill - Terminates a running process

shutdown - Turns off or restarts the system

ping - Checks the system's network connectivity

wget - Downloads files from a URL

curl - Transmits data between servers using URLs

scp - Securely copies files or directories to another system

rsync - Synchronizes content between directories or machines

Ifconfig - Displays the system's network interfaces and their configurations

netstat - Shows the system's network information, like routing and sockets

traceroute - Tracks a packet's hops to its destination

nslookup - Queries a domain's IP address and vice versa

dig - Displays DNS information, including record types

history - Lists previously run commands

man - Shows a command's manual

echo - Prints a message as a standard output

ln - Links files or directories

alias and **unalias** - Sets and removes an alias for a file or command

apt-get - Manages Debian-based distros package libraries

Pen-testing phases

PHASE 1: INFO GATHERING/RECON

a. discover network hosts
b. enumerate listening services
c. discover vuln attack holes

PHASE 2: FOCUSED PENETRATION

a. compromise vuln hosts(level1)
a.1. exploit missing software patches
a.2. deploy custom executable payloads
a.3. access remote management interfaces(RMI)

PHASE 3: POST-EXPLOIT AND PRIV ESC

a. establish reliable re-entry
b. harvest credentials
c. move to layer 2
c.1. identify privileged user accounts
c.2. elevate to domain admin

PHASE 4: DOCUMENTATION

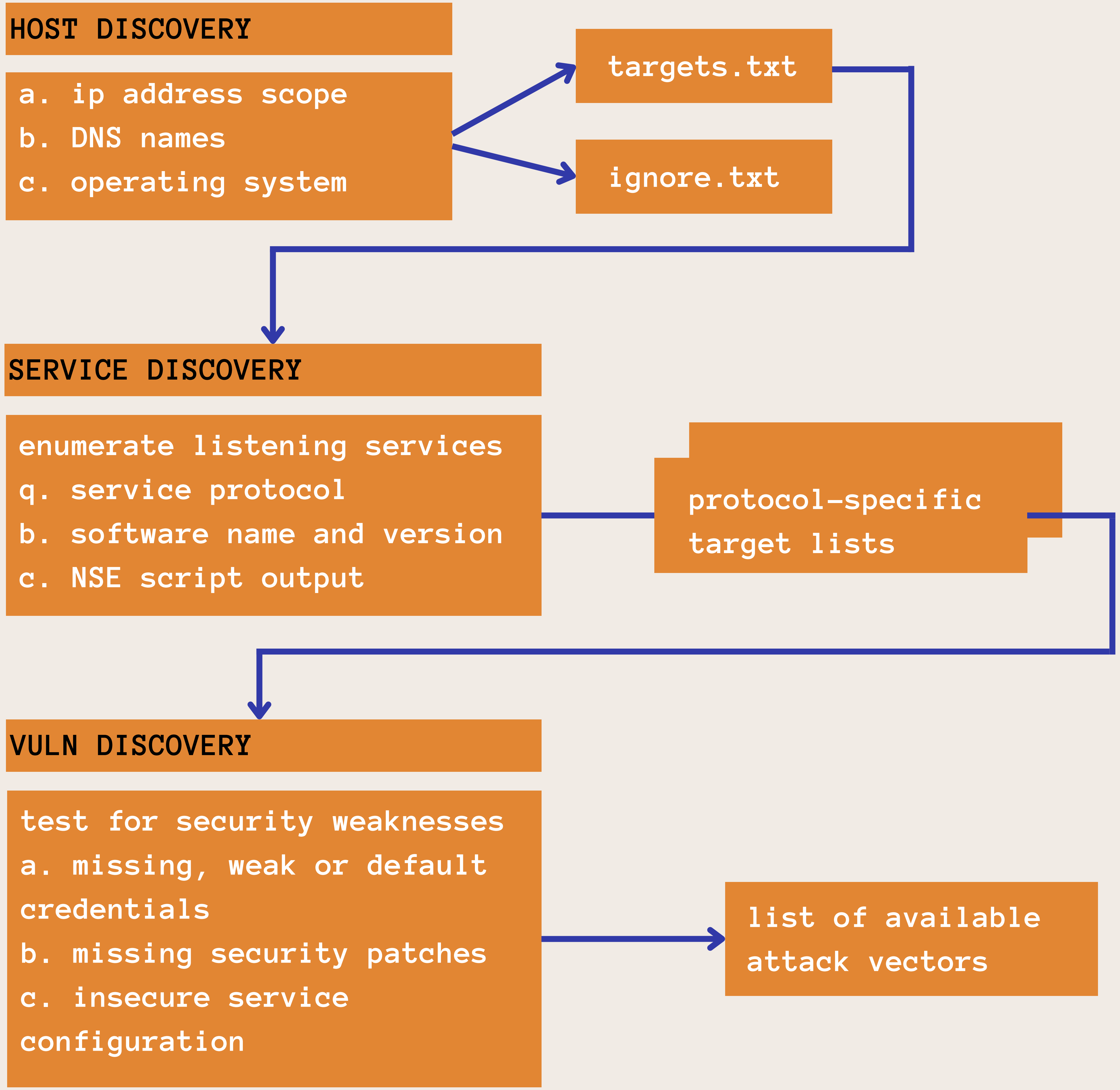
a. gather evidence/screenshots
b. create linear attack narratives-
c. create a final deliverable doc

PHASE 5: CLEAN UP

remove all payloads, fix credentials, fix firewalls to the previous settings and etc

Pen-testing phases

PHASE 1



HOST DISCOVERY

a. ip address scope

b. DNS names

c. operating system

targets.txt

ignore.txt

SERVICE DISCOVERY

enumerate listening services

q. service protocol

b. software name and version

c. NSE script output

protocol-specific target lists

VULN DISCOVERY

test for security weaknesses

a. missing, weak or default credentials

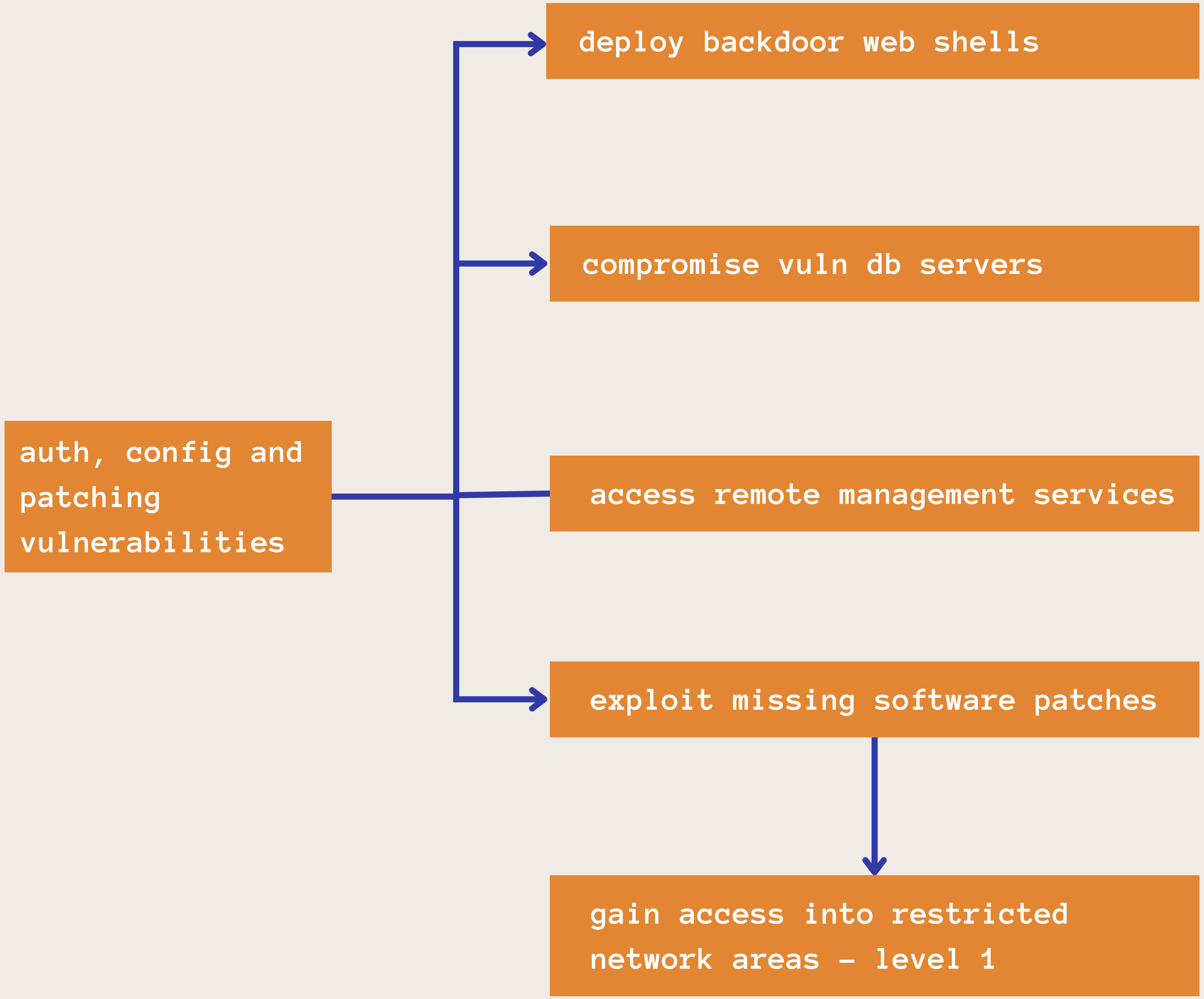
b. missing security patches

c. insecure service configuration

list of available attack vectors

Pen-testing phases

PHASE 2



auth, config and patching vulnerabilities

deploy backdoor web shells

compromise vuln db servers

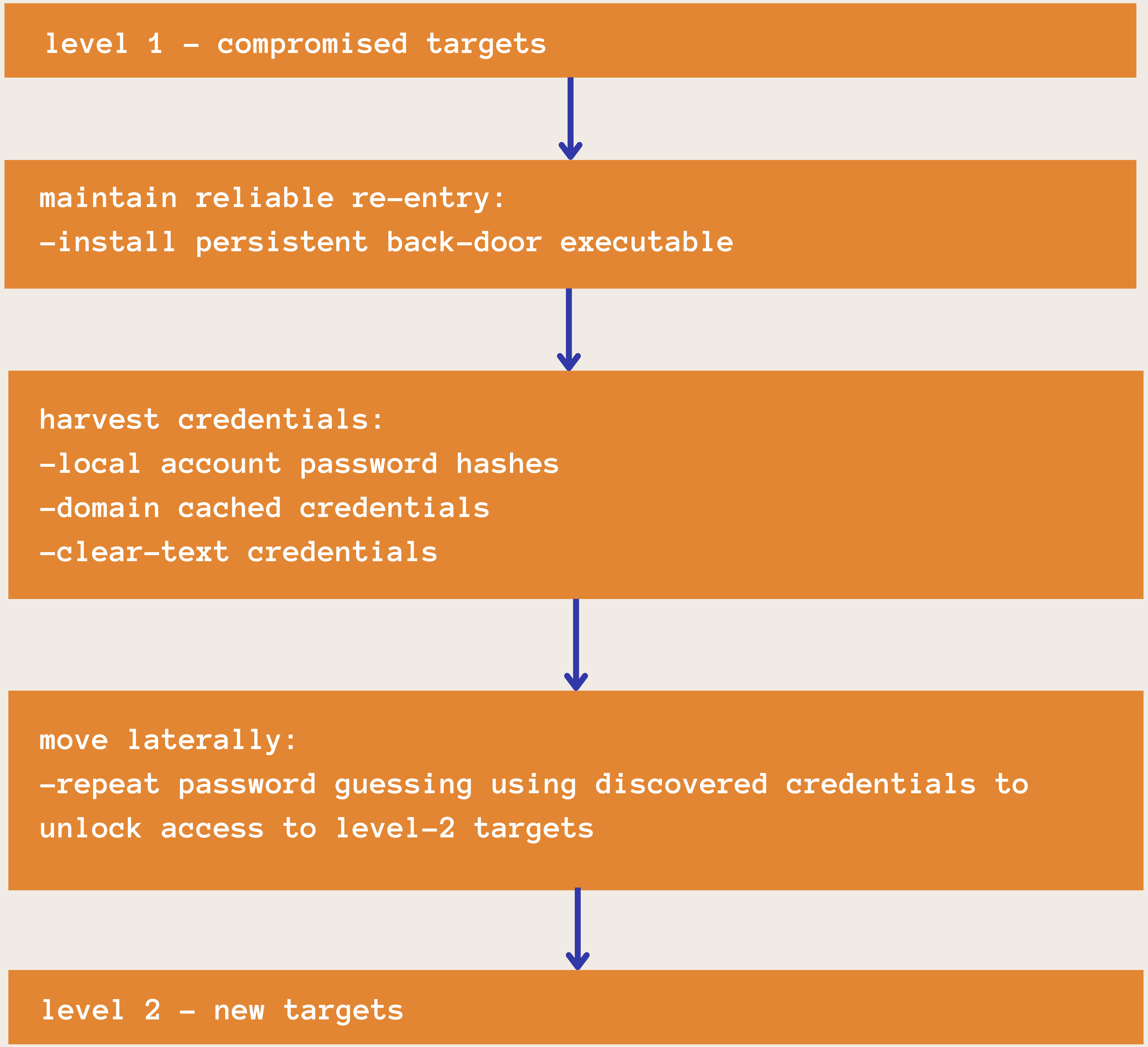
access remote management services

exploit missing software patches

gain access into restricted network areas – level 1

Pen-testing phases

PHASE 3



level 1 – compromised targets

maintain reliable re-entry:
-install persistent back-door executable

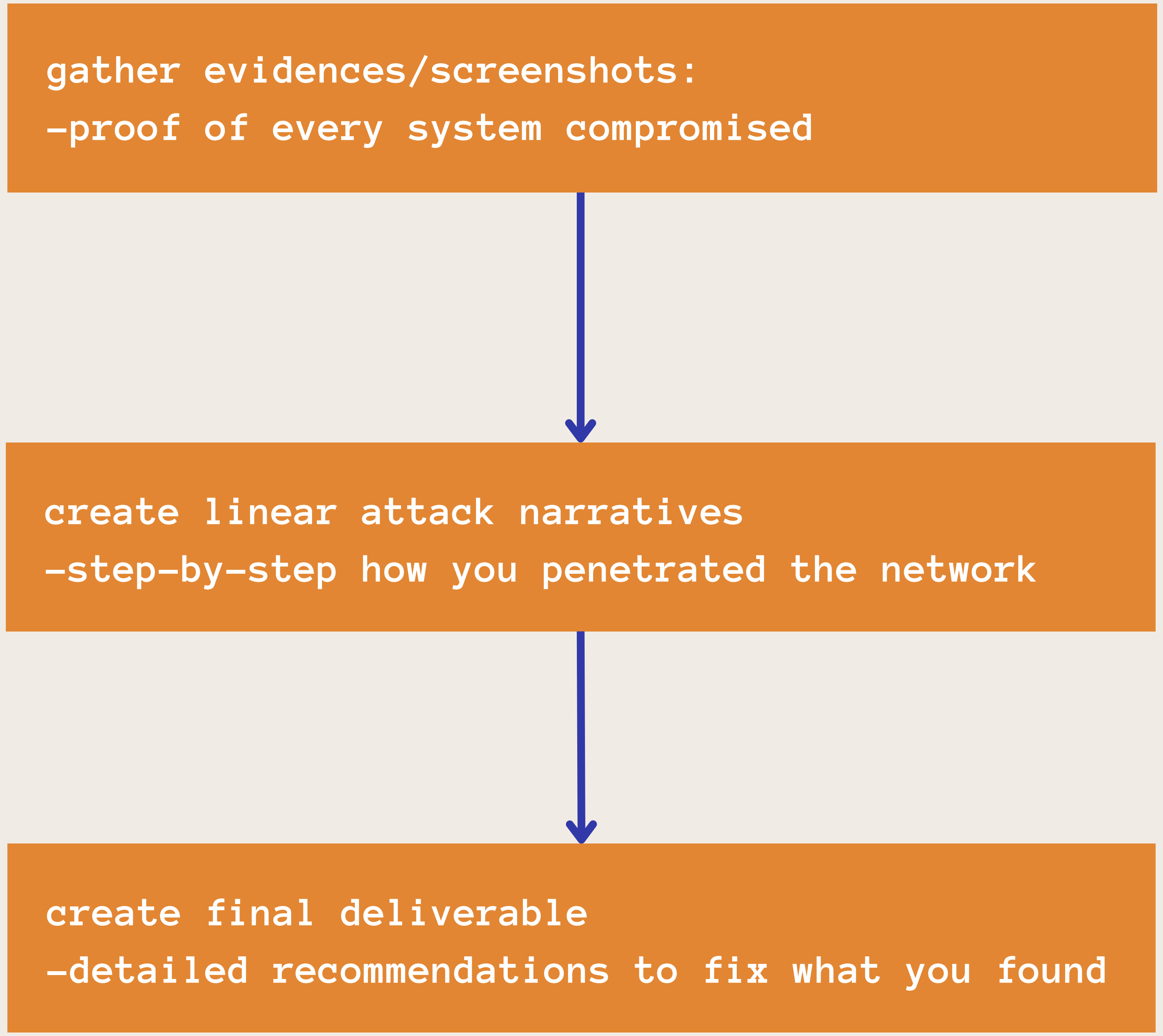
harvest credentials:
-local account password hashes
-domain cached credentials
-clear-text credentials

move laterally:
-repeat password guessing using discovered credentials to unlock access to level-2 targets

level 2 – new targets

Pen-testing phases

PHASE 4



gather evidences/screenshots:
-proof of every system compromised

create linear attack narratives
-step-by-step how you penetrated the network

create final deliverable
-detailed recommendations to fix what you found

HOMEWORK

brush up on bash scripting