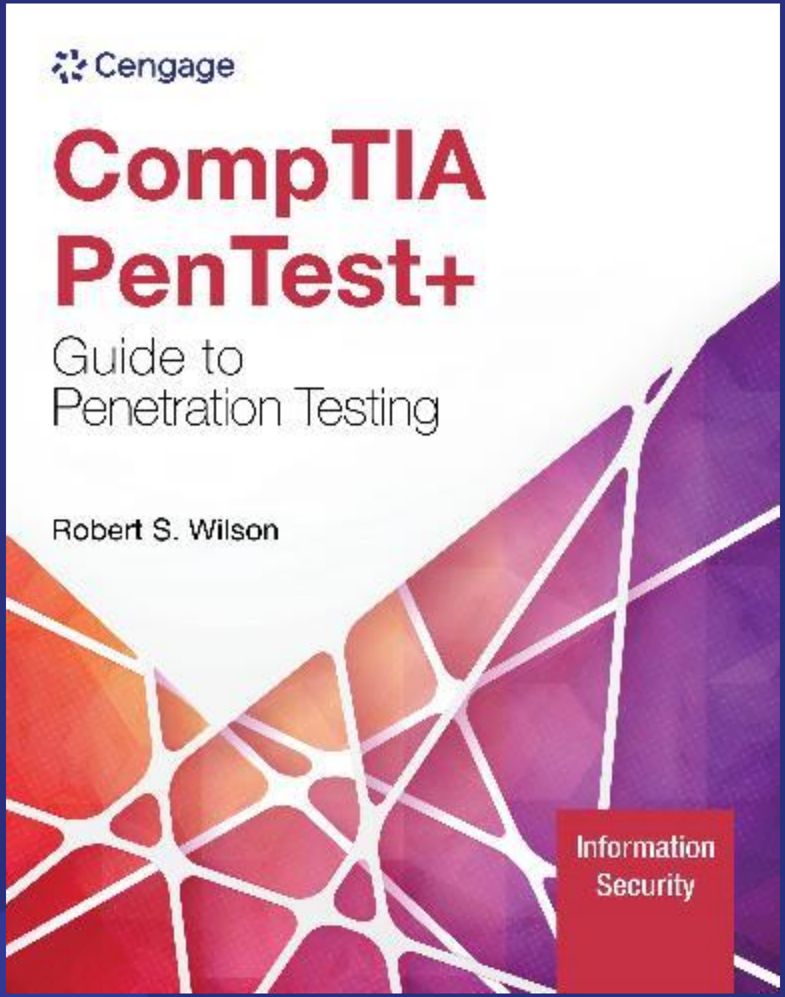


CompTIA PenTest+ Guide to Penetration Testing, 1e

Module 1: Introduction to Penetration Testing

Icebreaker: Interview Simulation

1. The class will be broken up into pairs of students.
2. Each pair of students will interview each other to discover interesting or unusual facts.
3. Then, each pair will introduce each other to the class.
4. As you are interviewed, think about connecting a story from your personal experiences to topics that are relevant to this course.

Module Objectives

By the end of this module, you should be able to:

1. Describe the penetration testing process and its phases, activities, and team members
2. Describe the CIA and DAD triads
3. Describe the ethical hacking mindset
4. Describe some of the tools used in penetration testing

What, Why, When, How, and Who? (1 of 6)

What Is Penetration Testing?

- Commonly called “pen testing” or “ethical hacking”
- Authorized security tests on targets to discover vulnerabilities
  - Targets include computing devices, applications, physical resources and personnel
  - Vulnerabilities include flaws in software, hardware, operational procedure
- *Exploit* – software, data, or commands taking advantage of vulnerabilities to cause unintended behavior in target system

What, Why, When, How, and Who? (2 of 6)

National Institute of Standards and Technology (NIST)

Special Publication 800-115 Technical Guide to Information Security Testing and Assessment

Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability.

What, Why, When, How, and Who? (3 of 6)

Why Do Security Professionals Pen Test?

- To discover vulnerabilities in targets before a threat actor does
  - Vulnerabilities can then be eliminated or mitigated
  - Finding and eliminating vulnerabilities improves overall security

What, Why, When, How, and Who? (4 of 6)

When Do Security Professionals Conduct Pen Tests?

- When a major change in computing environment occurs
- According to schedule for compliance requirements
  - Payment Card Industry Data Security Standard (PCI DSS)
  - PCI DSS v 4.0 Requirement 11
  - “Test security systems and processes regularly”
- At other strategic times and as necessary determined by organization

What, Why, When, How, and Who? (5 of 6)

How Do Security Professionals Pen Test?

- Several established penetration testing methodologies are used
- Pen test methodologies provide standardized guidance and process to conduct a pen test
- The type of target tested or the compliance requirement can drive methodology choice

What, Why, When, How, and Who? (6 of 6)

Who Performs Pen Tests?

- An authorized attacker performs pen tests
  - Known trusted entity
  - Member of organization IT Department
  - Outside third party hired to perform test

CIA, DAD, and the Hacker Mindset (1 of 5)

CIA Triad – Confidentiality, Integrity, Availability

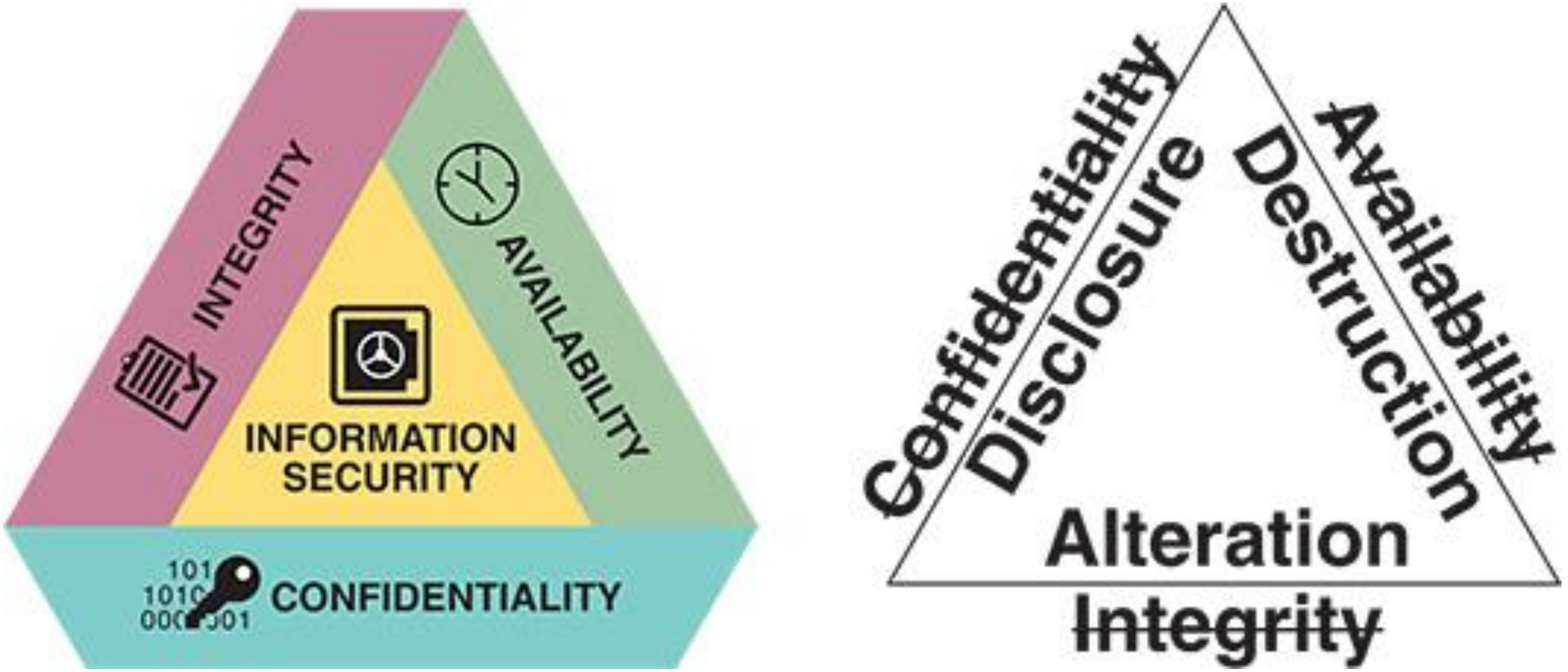
- One of the most well-known concepts and models in cybersecurity
- The three CIA concepts link together to provide security
  - Confidentiality: achieved using technology such as authentication, access control, and encryption
  - Integrity: achieved using authentication, access control, and digital signatures
  - Availability: objects and services are accessible when required by those authorized

CIA, DAD, and the Hacker Mindset (2 of 5)

DAD Triad – Disclosure, Alteration, Destruction

- Antithesis or opposite of the CIA triad
- Hacker’s ultimate goal
  - Disclosure of confidential information
  - Alteration or corruption of integrity of information
  - Destruction or denial of availability of access to resources

CIA, DAD, and the Hacker Mindset (3 of 5)



CIA triad versus DAD triad

CIA, DAD, and the Hacker Mindset (4 of 5)

The Hacker Mindset and Ethical Hacking

If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.

—Source: Sun Tzu/The Art of War

CIA, DAD, and the Hacker Mindset (5 of 5)

Ethical Hacking Guidelines – For Penetration Testers

- Background checks for pen testers; no unethical behavior
- Pen testers must:
  - adhere to the specific scope of engagement
  - report evidence of criminal activity or breaches immediately
  - choose and limit tools and use wisely
  - limit invasiveness to meet the scope of engagement
- Confidentiality must always be maintained

Discussion Activity 1-1

The CIA triad has long been used as an example and model for information security services and systems.

In small groups, create an updated version of the triad, considering what additional qualities or characteristics are important in an information security program.

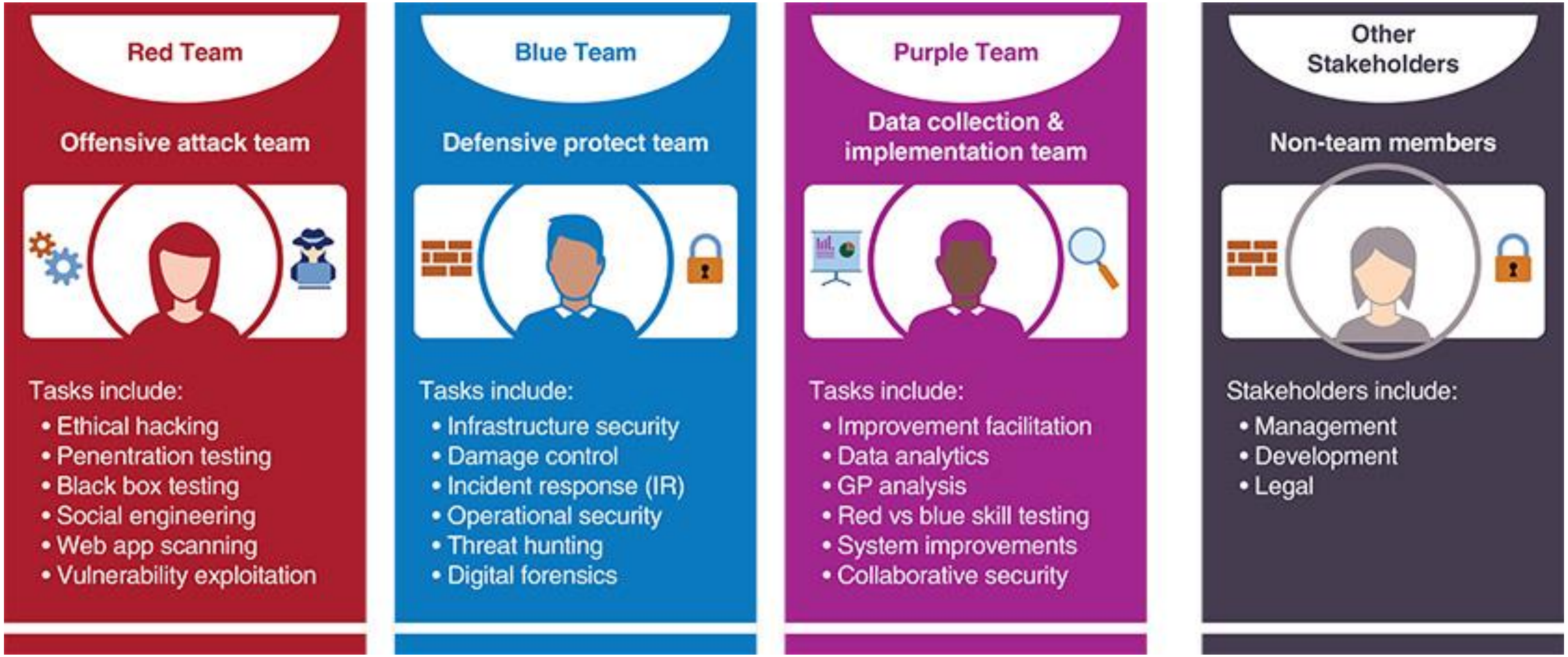
- Is a triangle still an effective model, or are there additional facets of information security to be considered?
- Could a visual model be created to encompass ethical hacking and pen testing? What would it look like and what would the important components be?

The Pen-Test Teams and Other Stakeholders (1 of 5)

Key Participants in Penetration Tests

- Red Team – performs the security and pen testing
- Blue Team – attempts to detect or prevent red team activities
- Purple Team – data collection, analytics, facilitation of teams
- Other Stakeholders
    - IT Department
    - Management
    - Legal Department

The Pen-Test Teams and Other Stakeholders (2 of 5)



Red Team

Offensive attack team

Tasks include:

- Ethical hacking
- Penentration testing
- Black box testing
- Social engineering
- Web app scanning
- Vulnerability exploitation

Blue Team

Defensive protect team

Tasks include:

- Infrastructure security
- Damage control
- Incident response (IR)
- Operational security
- Threat hunting
- Digital forensics

Purple Team

Data collection & implementation team

Tasks include:

- Improvement facilitation
- Data analytics
- GP analysis
- Red vs blue skill testing
- System improvements
- Collaborative security

Other Stakeholders

Non-team members

Stakeholders include:

- Management
- Development
- Legal

Pen-test teams

The Pen-Test Teams and Other Stakeholders (3 of 5)

Red Team

- Consists of pen-test team members
- May contain target organization team members such as IT Department
- Often has members with their own specialized skill sets
  - Team leaders and project managers
  - Programmers and scripters
  - Social engineers
  - Network and wireless engineers
  - Server and operating system administrators

The Pen-Test Teams and Other Stakeholders (4 of 5)

Blue Team

- Blue team may not always exist in pen-test engagements
- May consist of IT team members or contracted security services
- Blue team is responsible for:
  - Preparation
  - Detection
  - Identification
  - Containment
  - Recovery
  - Lessons learned
  - Implementation

The Pen-Test Teams and Other Stakeholders (5 of 5)

Purple Team

- Observes red and blue teams and guides them to a more effective test
- Understands the “big picture” and provides oversight
  - Gathers results
  - Performs analysis
  - Reports results

The Pen-Test Teams and Other Stakeholders

Other Stakeholders

- Management
  - Provides authorization and permission for pen test
- Development
  - Guides and oversees tests on custom software and applications
  - May provide attack guidance to red team
- Legal
  - Creates necessary documents to assure safe pen test
  - Create legal documents such as nondisclosure agreements

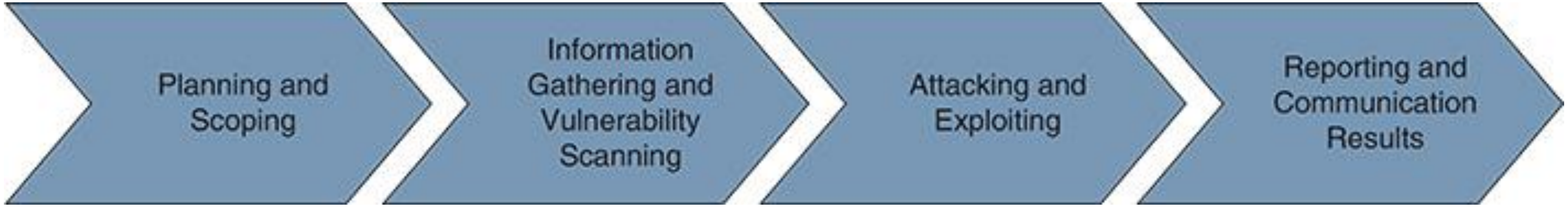
Discussion Activity 1-2

Module 1 details several stakeholders who may be involved in the planning and scoping of the penetration test. Each penetration test is unique, and each pen testing team and client seeking a pen test is also unique. Think about stakeholders, and discuss the questions below:

1. What other stakeholders might be required to appropriately plan a penetration test?
2. How might the industry of the client organization affect stakeholder participation?
3. Are there specific types of organizations such as government, military, or global corporations that might have stakeholders outside those discussed?

The Pen-Test Process (1 of 6)

CompTIA Pen-Test Process


Planning and Scoping
Information Gathering and Vulnerability Scanning
Attacking and Exploiting
Reporting and Communication Results

CompTIA Pen-Test Process

The Pen-Test Process (2 of 6)

Planning and Scoping

- First step in a penetration test
- Specifies which computers, applications, and network device are targeted
- Identifies logistics, teams, stakeholders, and expectations
- Defines Rules Of Engagement (ROE)

The Pen-Test Process (3 of 6)

Planning and Scoping – Rules of Engagement

- How is sensitive information handled?
- How will project updates be communicated?
- Who are the emergency contacts?
- Which targets are in the scope?
- Are target personnel aware of the test activities?
- What should be done if previous compromises are discovered?

The Pen-Test Process (4 of 6)

Information Gathering and Vulnerability Scanning

- Red team goal is finding useful information about the target
- Initial goal is broad discovery and narrowing the focus as the test continues
- Other goals include:
  - Active reconnaissance
  - Vulnerability scanning and analysis
  - Social engineering

The Pen-Test Process (5 of 6)

Attacking and Exploiting

- Details are gathered in previous phase drive attacks
- Target configuration and status determine which attacks are used
  - Password cracking
  - SQL injection
  - Circumventing security settings
  - Physical attacks
  - Many other attacks, dependent on information gathered on targets

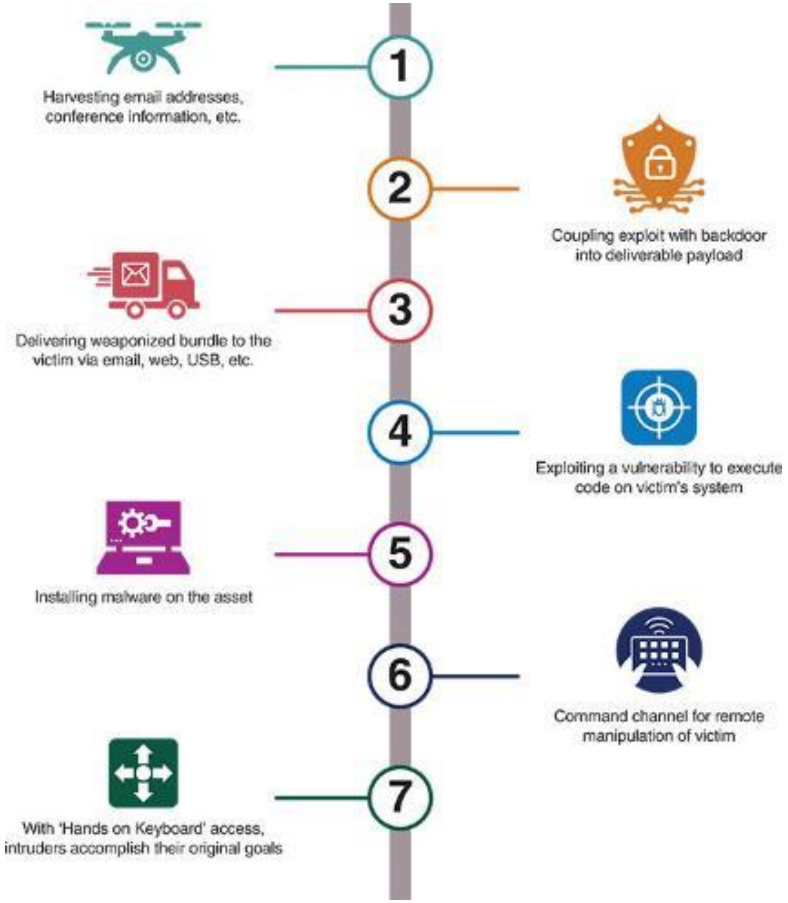
The Pen-Test Process (6 of 6)

Reporting and Communicating Results

- Information gathered up to this point is organized
- Report is created with specific problems found and actionable items identified
  - Vulnerabilities are uncovered
  - Successful attacks are identified
  - Fixes or remediation steps for vulnerabilities are outlined
- During this phase, a “clean up” of pen test occurs
- Proper reporting and communication covered in Module 12

The Cyber Kill Chain

- Model created by Lockheed Martin
- Seven stages
- Guides defenders in efforts to “kill” cyber attack


1
Harvesting email addresses, conference information, etc.
2
Coupling exploit with backdoor into deliverable payload
3
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
Exploiting a vulnerability to execute code on victim's system
5
Installing malware on the asset
6
Command channel for remote manipulation of victim
7
With 'Hands on Keyboard' access, intruders accomplish their original goals

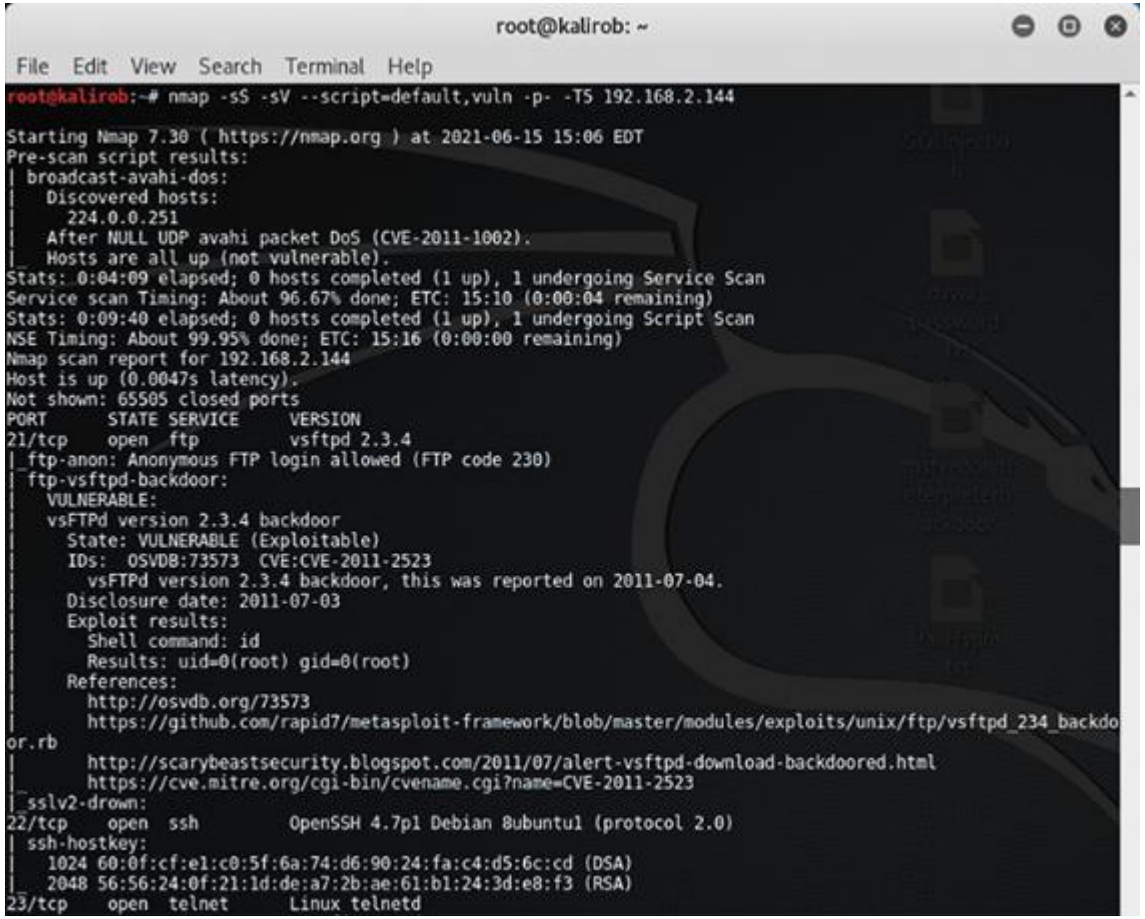
Cyber kill chain

The Pen-Test Toolkit (1 of 5)

Common Software Types Used in Pen-Test

- Scanners
- Credential Testing Tools
- Debuggers
- Open Source Intelligence (OSINT)
- Wireless Tools
- Web Application Tools
- Social Engineering Tools
- Remote Access Tools
- Network Tools
- Steganography Tools
- Cloud Tools

The Pen-Test Toolkit (2 of 5)

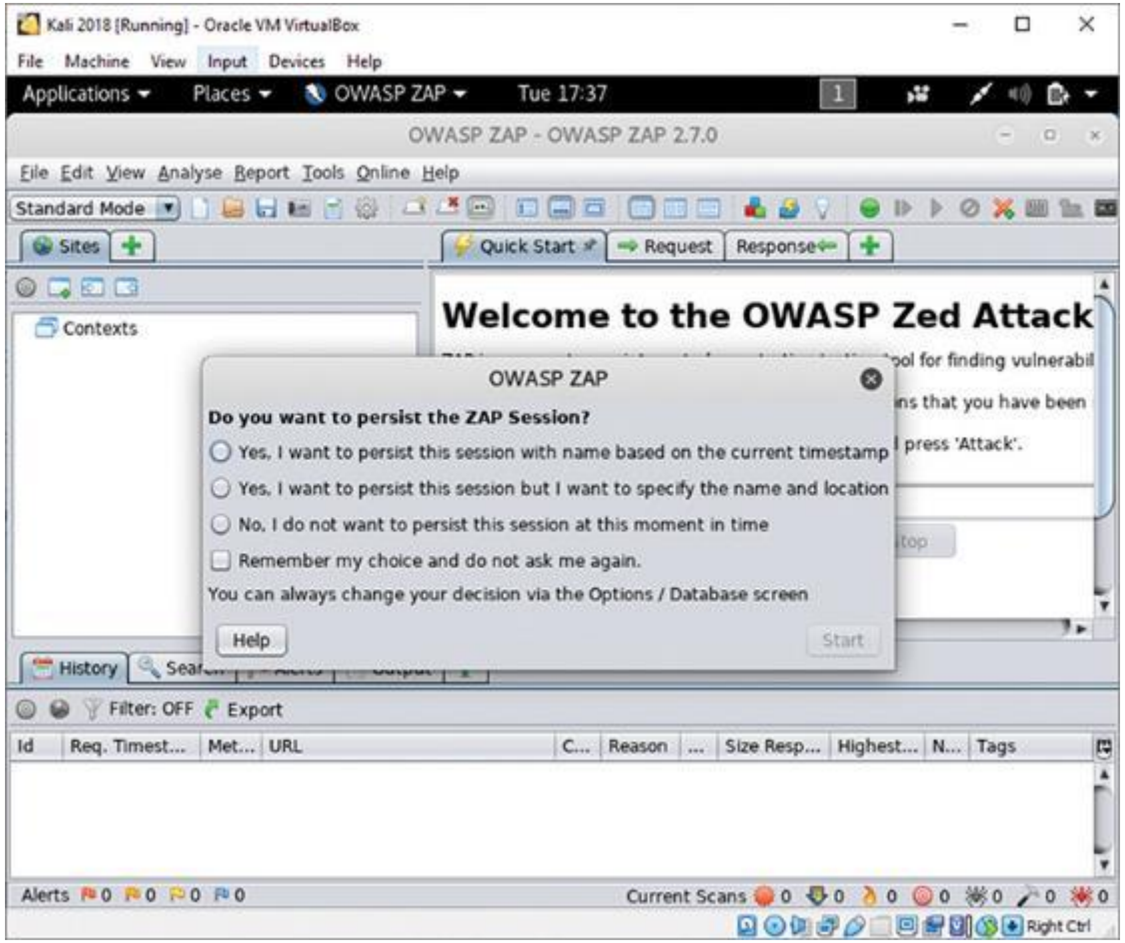


```
root@kalirob:~# nmap -sS -sV --script=default,vuln -p- -T5 192.168.2.144

Starting Nmap 7.30 ( https://nmap.org ) at 2021-06-15 15:06 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Stats: 0:04:09 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 15:10 (0:00:04 remaining)
Stats: 0:09:40 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.95% done; ETC: 15:16 (0:00:00 remaining)
Nmap scan report for 192.168.2.144
Host is up (0.0047s latency).
Not shown: 65505 closed ports
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  OSVDB:73573  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       http://osvdb.org/73573
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdo
or.rb
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_sslv2-drown:
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet      Linux telnetd
```

Nmap scanning tool

The Pen-Test Toolkit (3 of 5)



Kali 2018 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications ▾ Places ▾ OWASP ZAP ▾ Tue 17:37
OWASP ZAP - OWASP ZAP 2.7.0
File Edit View Analyse Report Tools Online Help
Standard Mode
Sites
Quick Start
Request
Response
Contexts
History
Search
Filter: OFF
Export
Id
Req. Timest...
Met...
URL
C...
Reason
...
Size Resp...
Highest...
N...
Tags
Alerts 0 0 0 0
Current Scans 0 0 0 0 0 0 0
Right Ctrl

Welcome to the OWASP Zed Attack

ool for finding vulnerabil

ns that you have been

press 'Attack'.

OWASP ZAP

Do you want to persist the ZAP Session?

○ Yes, I want to persist this session with name based on the current timestamp

○ Yes, I want to persist this session but I want to specify the name and location

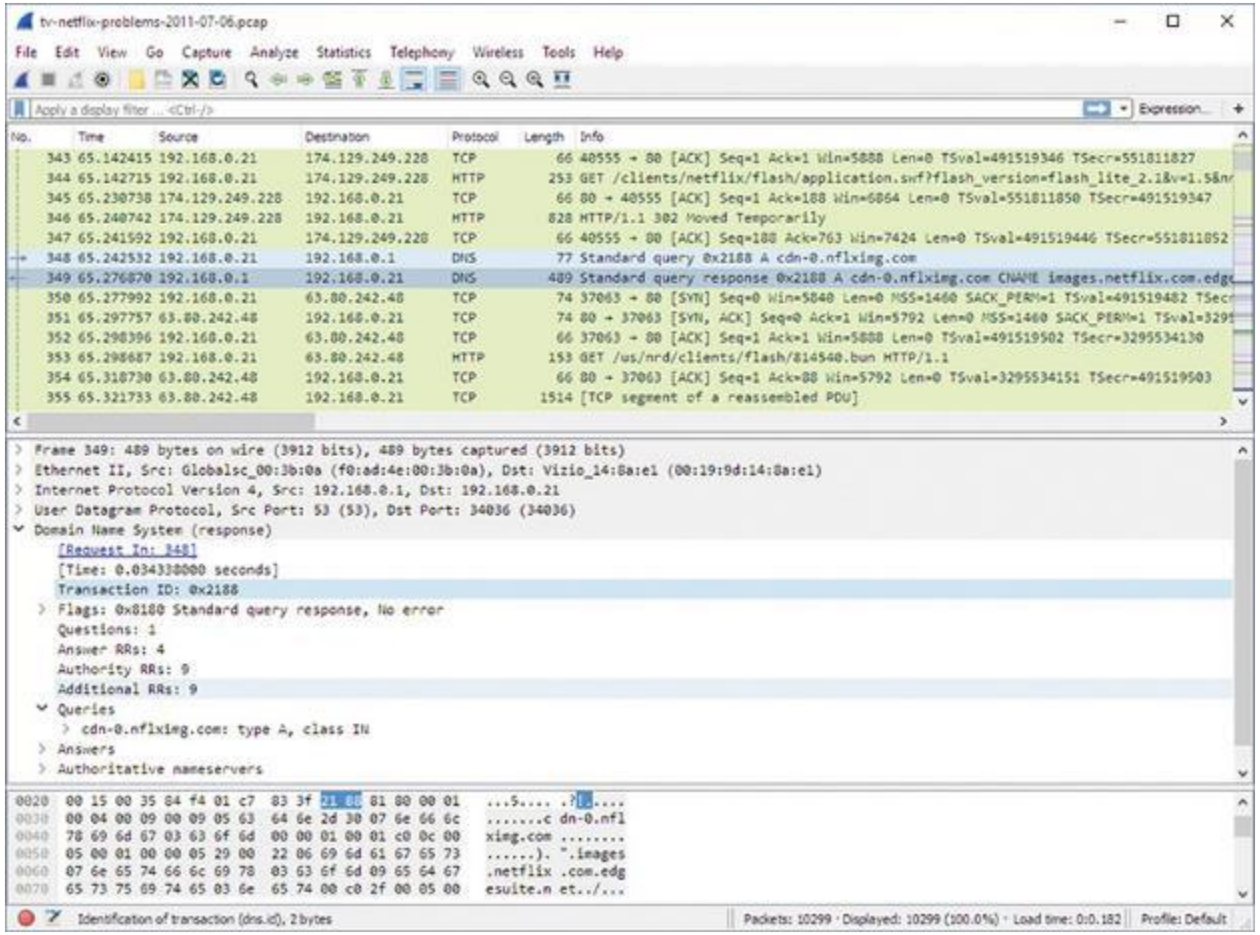
○ No, I do not want to persist this session at this moment in time

□ Remember my choice and do not ask me again.

You can always change your decision via the Options / Database screen

OWASP ZAP

The Pen-Test Toolkit (4 of 5)



```
No.   Time      Source          Destination     Protocol Length Info
  343 65.142415 192.168.0.21    174.129.249.228 TCP        66 40555 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519346 TSecr=551811827
  344 65.142715 192.168.0.21    174.129.249.228 HTTP      253 GET /clients/netflix/flash/application.swf?flash_version=flash_lite_2.1&v=1.5&nr
  345 65.230738 174.129.249.228 192.168.0.21    TCP        66 80 → 40555 [ACK] Seq=1 Ack=188 Win=6864 Len=0 TSval=551811850 TSecr=491519347
  346 65.240742 174.129.249.228 192.168.0.21    HTTP      828 HTTP/1.1 302 Moved Temporarily
  347 65.241592 192.168.0.21    174.129.249.228 TCP        66 40555 → 80 [ACK] Seq=188 Ack=763 Win=7424 Len=0 TSval=491519446 TSecr=551811852
  348 65.242532 192.168.0.21    192.168.0.1     DNS        77 Standard query 0x2188 A cdn-0.nflximg.com
  349 65.276870 192.168.0.1     192.168.0.21    DNS       489 Standard query response 0x2188 A cdn-0.nflximg.com CNAME images.netflix.com.edge
  350 65.277992 192.168.0.21    63.80.242.48    TCP        74 37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSecr
  351 65.297757 63.80.242.48    192.168.0.21    TCP        74 80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3295
  352 65.298396 192.168.0.21    63.80.242.48    TCP        66 37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=3295534130
  353 65.298687 192.168.0.21    63.80.242.48    HTTP      153 GET /us/nrd/clients/flash/814540.bun HTTP/1.1
  354 65.318730 63.80.242.48    192.168.0.21    TCP        66 80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=3295534151 TSecr=491519503
  355 65.321733 63.80.242.48    192.168.0.21    TCP      1514 [TCP segment of a reassembled PDU]
```

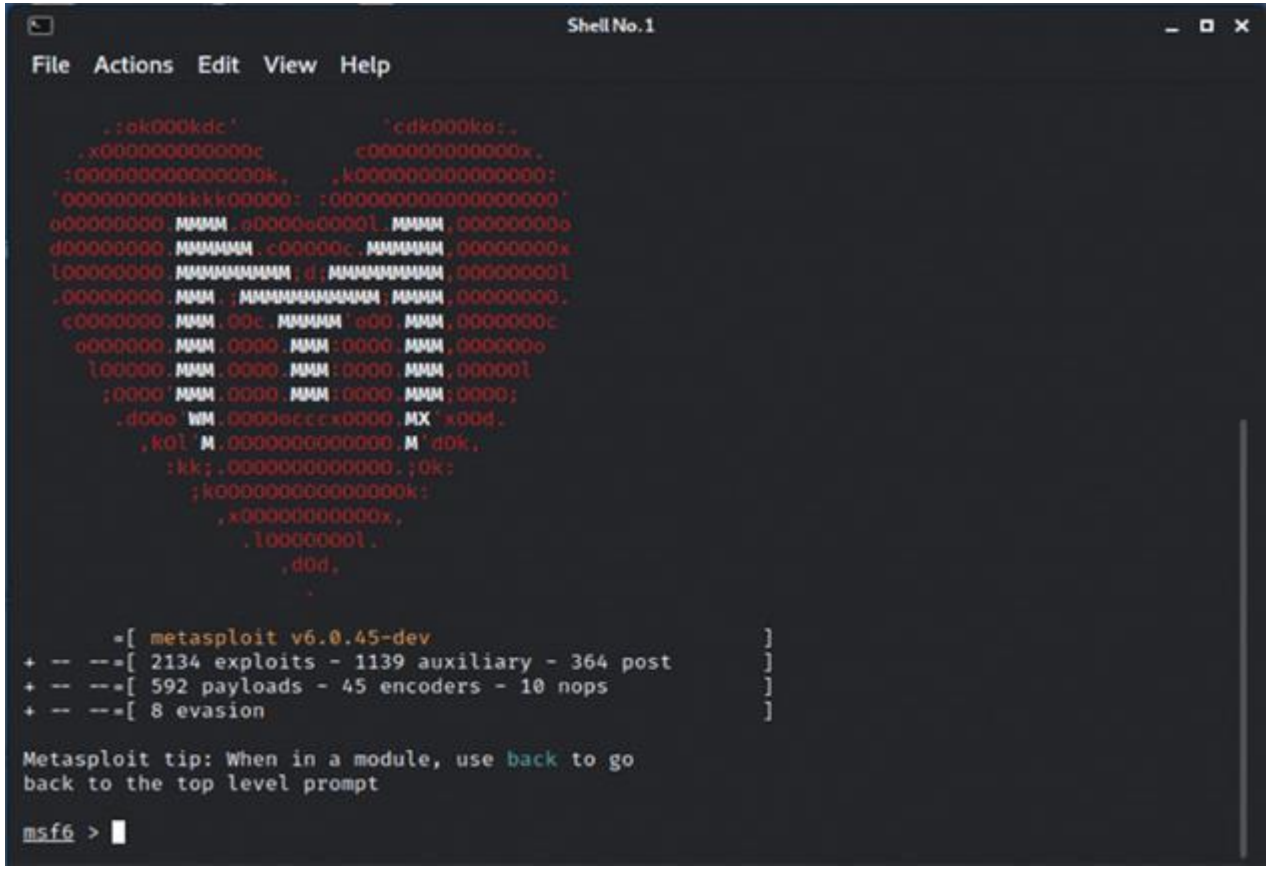
```
> Frame 349: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
> Ethernet II, Src: Globalsc_00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Vizio_14:8a:e1 (00:19:9d:14:8a:e1)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21
> User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)
v Domain Name System (response)
    [Request In: 348]
    [Time: 0.034338000 seconds]
    Transaction ID: 0x2188
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 9
    Additional RRs: 9
  v Queries
    > cdn-0.nflximg.com: type A, class IN
  > Answers
  > Authoritative nameservers
```

```
0020  00 15 00 35 84 f4 01 c7  83 3f 21 88 81 80 00 01   ...5.... .?!.....
0030  00 04 00 09 00 09 05 63  64 6e 2d 30 07 6e 66 6c   .......c dn-0.nfl
0040  78 69 6d 67 03 63 6f 6d  00 00 01 00 01 c0 0c 00   ximg.com ........
0050  05 00 01 00 00 05 29 00  22 06 69 6d 61 67 65 73   ......). ".images
0060  07 6e 65 74 66 6c 69 78  03 63 6f 6d 09 65 64 67   .netflix .com.edg
0070  65 73 75 69 74 65 03 6e  65 74 00 c0 2f 00 05 00   esuite.n et../...
```

Identification of transaction (dns.id), 2 bytes | Packets: 10299 · Displayed: 10299 (100.0%) · Load time: 0:0.182 | Profile: Default

Wireshark

The Pen-Test Toolkit (5 of 5)



```
       =[ metasploit v6.0.45-dev                          ]
+ -- --=[ 2134 exploits - 1139 auxiliary - 364 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 8 evasion                                       ]

Metasploit tip: When in a module, use back to go
back to the top level prompt

msf6 >
```

Metasploit Framework

Self-Assessment

What traits or background might make an ethical hacker successful?

Why is it important for pen testers to understand and use software pen-testing tools that can be used in malicious or illicit circumstances?

Summary

Now that the lesson has ended, you should be able to:

1. Describe the penetration testing process and its phases, activities, and team members
2. Describe the CIA and DAD triads
3. Describe the ethical hacking mindset
4. Describe some of the tools used in penetration testing