JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Planning and Scoping

CompTIA Pentest+

Domain 1
Planning and Scoping

- Planning an engagement
- Key legal concepts
- Scoping an engagement
- Compliance-based assessments

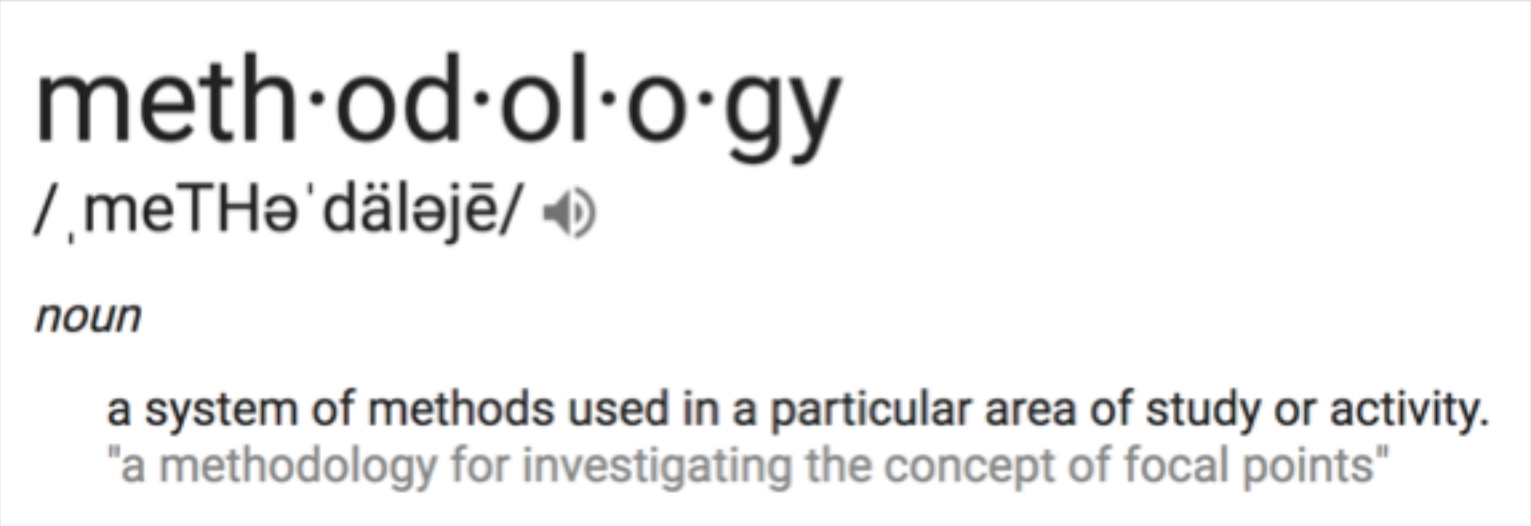
What kinds of questions can I expect on test day?

- All objectives for Domain 1 are listed as “explain” only by CompTIA
- Therefore, no simulations will come from this domain…

Penetration Testing Methodology

CompTIA Pentest+

Methodology



meth·od·ol·o·gy

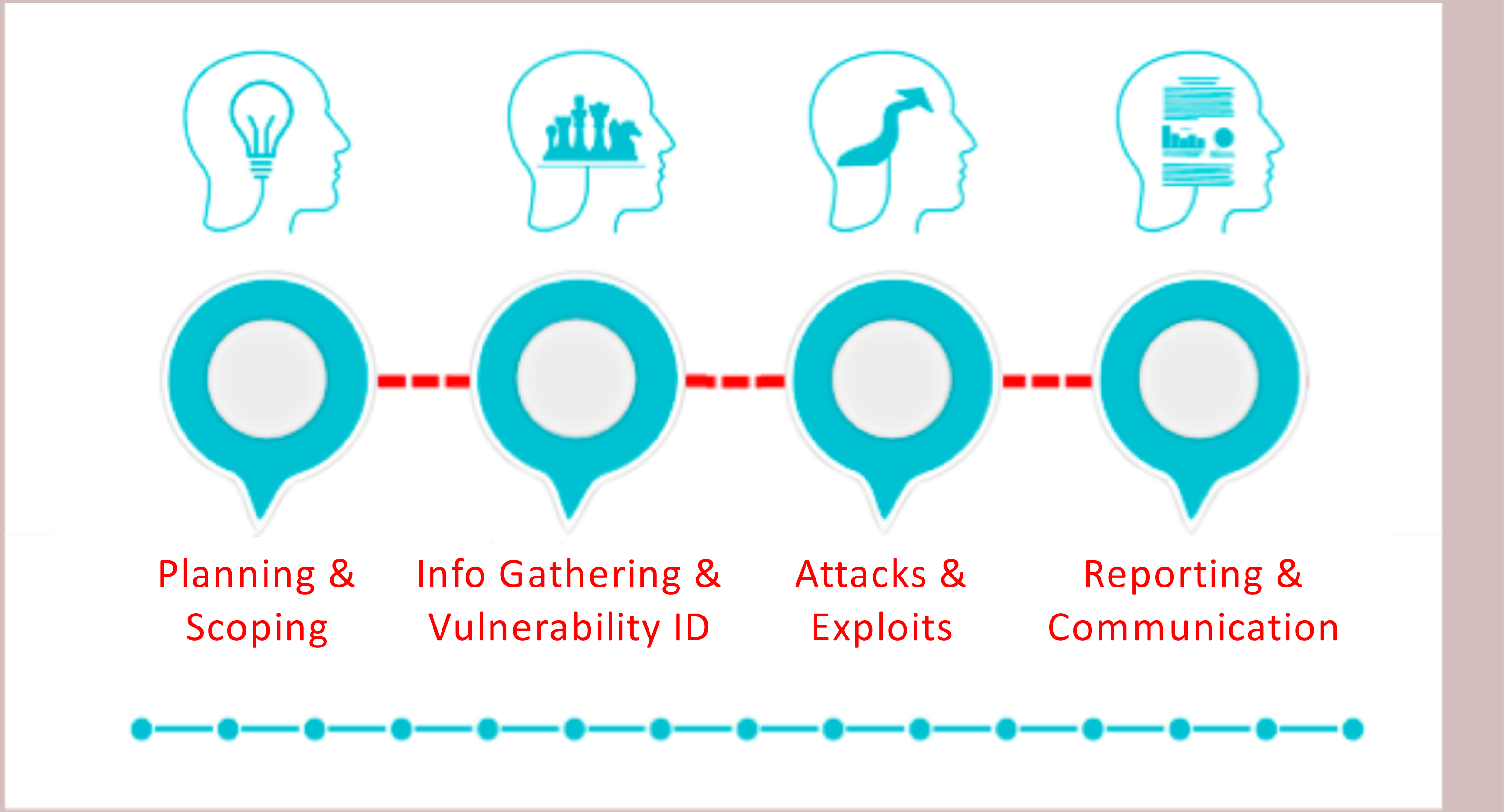
/ˌmeTHəˈdäləjē/

noun

a system of methods used in a particular area of study or activity.

"a methodology for investigating the concept of focal points"

Pentest Methodology



Planning & Scoping

Info Gathering & Vulnerability ID

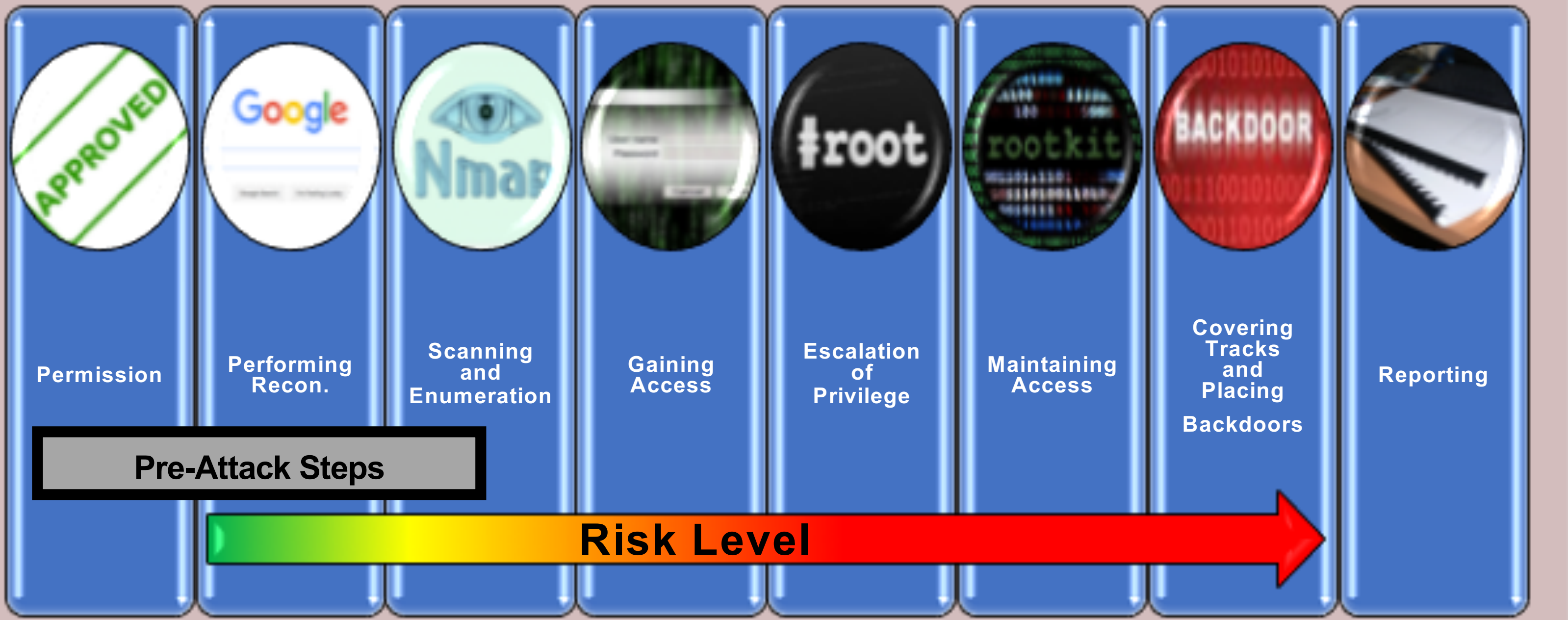
Attacks & Exploits

Reporting & Communication

Ethical Hacker's Methodology

JASON DION

TRAINING THE CYBER SECURITY WORKFORCE



Permission

Performing Recon.

Scanning and Enumeration

Gaining Access

Escalation of Privilege

Maintaining Access

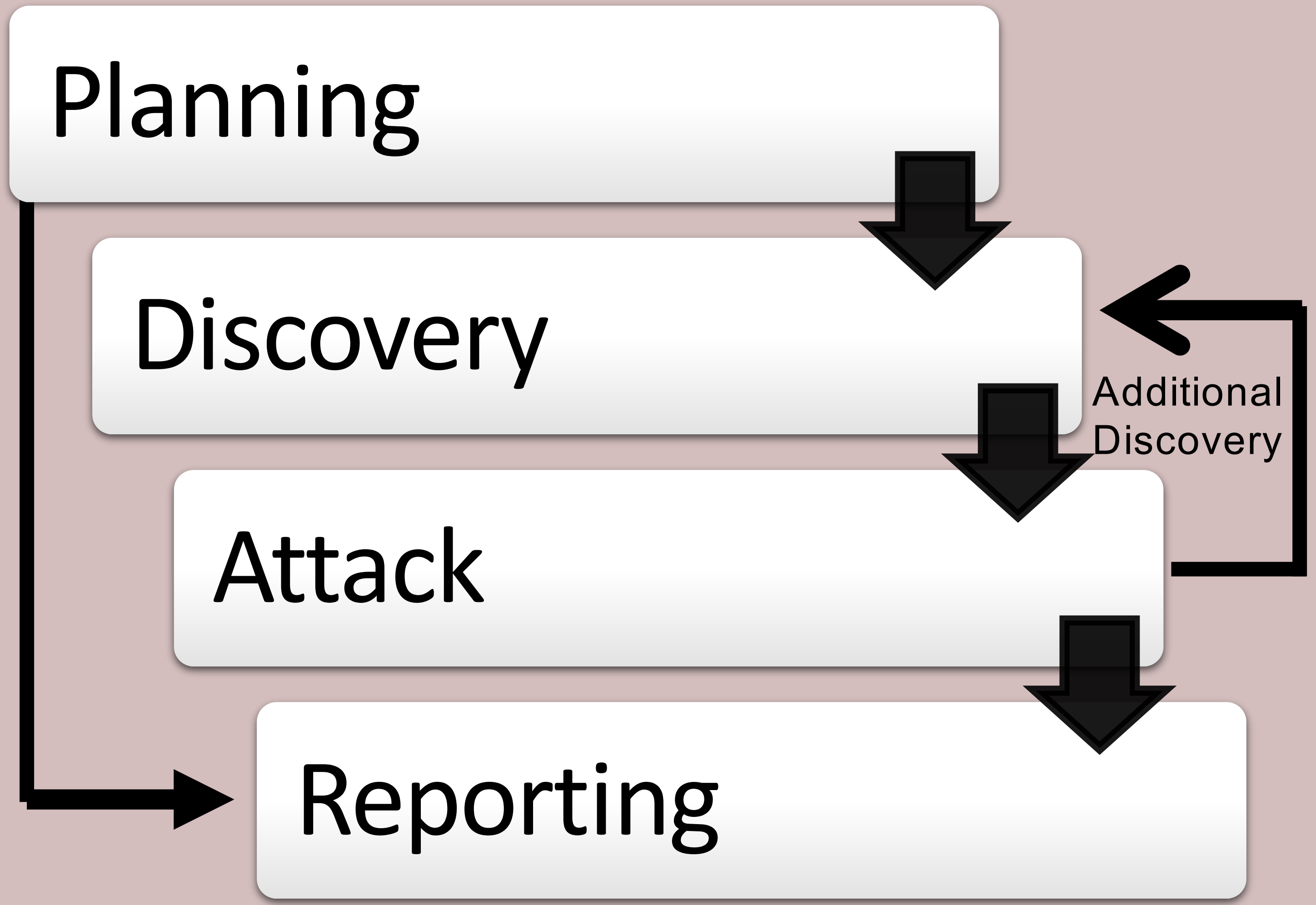
Covering Tracks and Placing Backdoors

Reporting

Pre-Attack Steps

Risk Level

NIST SP 800-115 Methodology



Planning

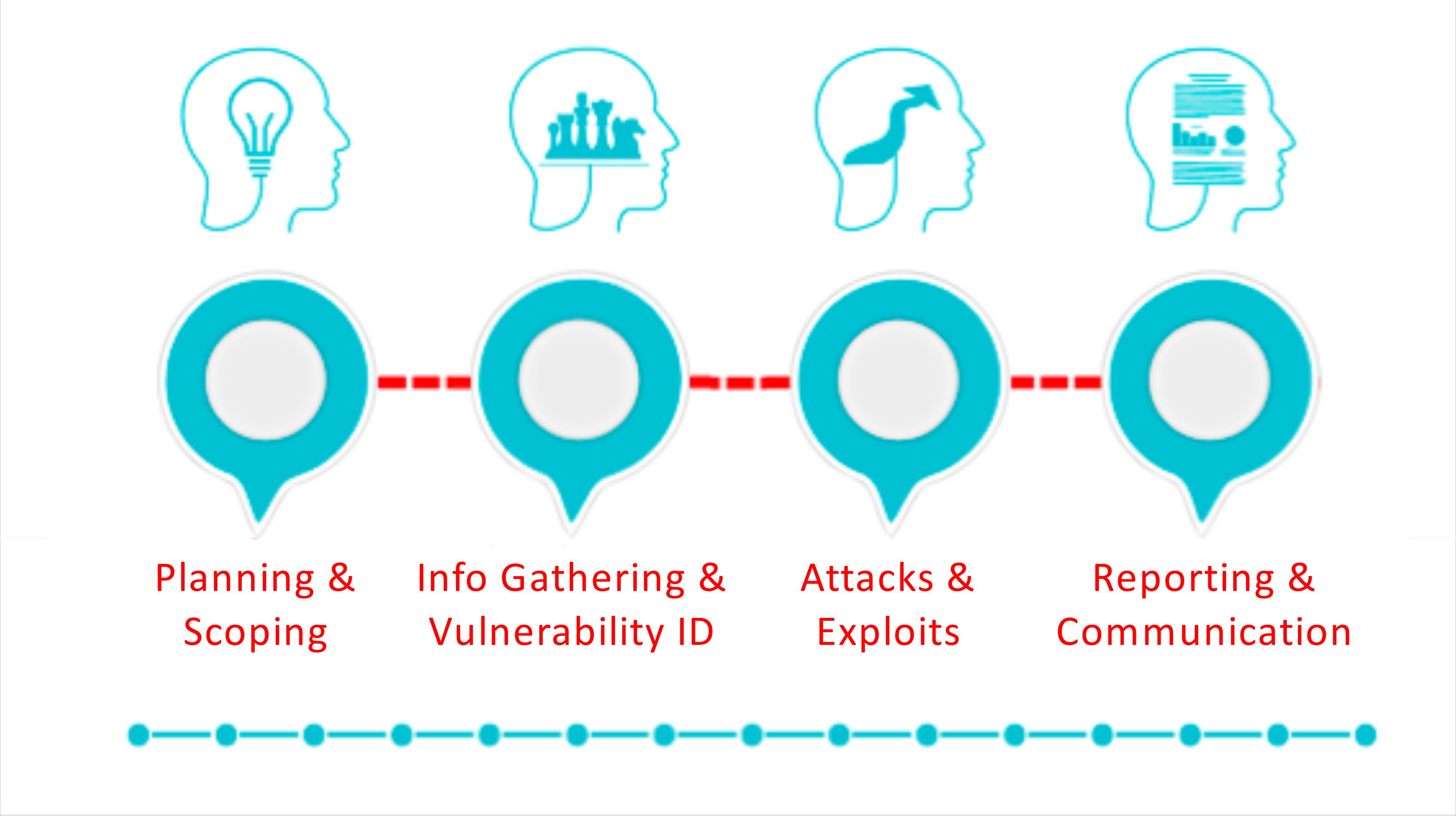
Discovery

Additional Discovery

Attack

Reporting

Pentest Methodology



Planning & Scoping

Info Gathering & Vulnerability ID

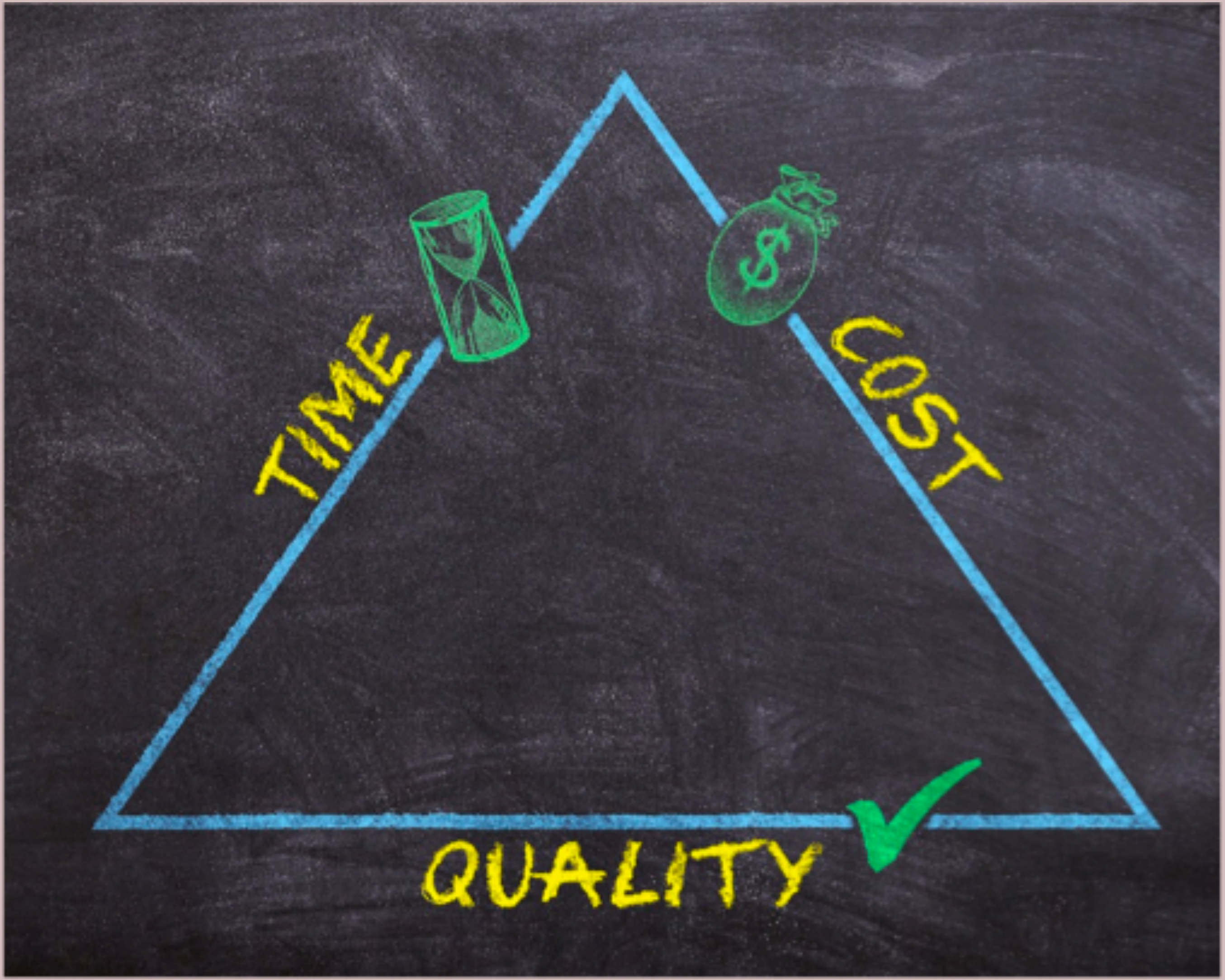
Attacks & Exploits

Reporting & Communication

Planning a Penetration Test

CompTIA Pentest+

Why Is Planning Important?



Who is the Target Audience?

- Need to know to properly plan the pentest
- What does the business do?
- What are their objectives?

Small Retailer

Multinational Bank

Budgeting

- Controls many factors in a test
- If you have a large budget, you can perform a more in-depth test
  - Increased timeline for testing
  - Increased scope
  - Increased resources (people, tech, etc.)

Resources and Requirements

- What resources will the assessment require?
- What requirements will be met in the testing?
  - Confidentiality of findings
  - Known vs. unknown vulnerabilities
  - Compliance-based assessment

We will discuss these more when we get to scoping the assessment

Communication Paths

- Who do we communicate with about the test?
- What info will be communicated and when?
- Who is a trusted agent if testing goes wrong?

What is the End State?

- What kind of report will be provided after test?

- Will you provide an estimate of how long remediations would take?

Technical Constraints

- What constraints limited your ability to test?

- Provide the status in your report
  - Tested
  - Not Tested
  - Can't Be Tested

Disclaimers

- Point-in-Time Assessment
  - Results were accurate when the pentest occurred
- Comprehensiveness
  - How complete was the test?
  - Did you test the entire organization or only specific objectives?

Rules of Engagement

CompTIA Pentest+

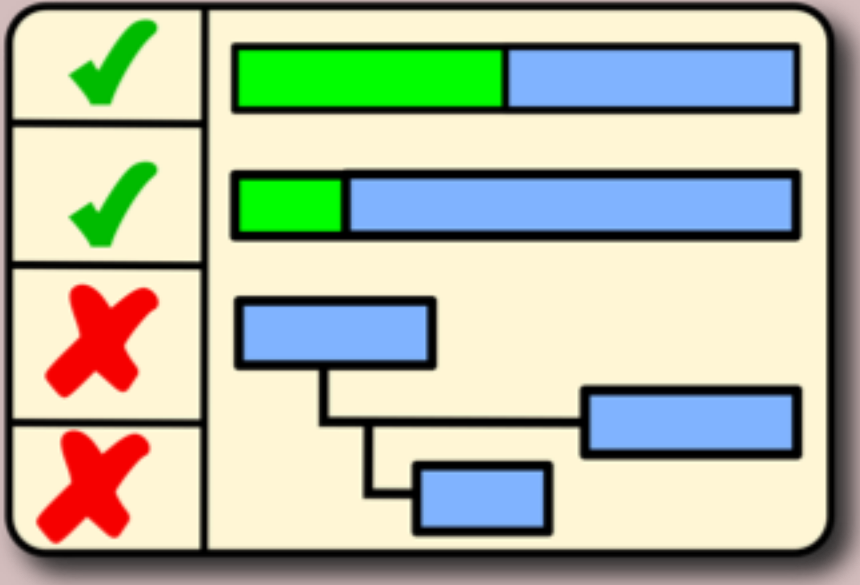
Rules of Engagement (RoE)

- Timeline
- Locations
- Time restrictions
- Transparency
- Test boundaries

RoE: Timeline

- How long will the test be conducted?
  - A week, a month, a year

- What tasks will be performed and how long will each be planned for?



RoE: Locations

- Where will the testers be located?
  - On-site or remote location
- Does organization have numerous locations?
- Does it cross international borders?

RoE: Time Restrictions

- Are there certain times that aren't authorized?
- What about days of the week?
- What about holidays?

RoE: Transparency

- Who will know about the pentest?
- Will the organization provide resources to the testers (white box test)?

CONFIDENTIAL

RoE: Boundaries

- What will be tested?
- Is social engineering allowed to be used?
- What about physical security testing?
- How invasive can the pentest be?

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Legal Concepts

CompTIA Pentest+

Local and National Restrictions

- Laws and regulations regarding cybercrime vary from country to country, check the local laws before conducting an assessment

Consult your attorney before performing any penetration testing work to ensure you are within the legal bounds for the countries laws where you are operating

CRIME AND CRIMINAL PROCEDURE

- Hacking is covered under United States Code, Title 18, Chapter 47, Sections 1029 and 1030 (*Crimes and Criminal Procedure*)

- **§ 1029 Fraud & related activity w/ access devices**
  - Prosecute those who knowingly and with intent to defraud produce, use, or traffic in one or more counterfeit access devices.
  - Access devices can be an application or hardware that is created specifically to generate any type of access credentials

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

CRIME AND CRIMINAL PROCEDURE

- Hacking is covered under United States Code, Title 18, Chapter 47, Sections 1029 and 1030 (*Crimes and Criminal Procedure*)

- **§ 1030 Fraud and related activity with computers**
  - Covers just about any computer or device connected to a network
  - Mandates penalties for anyone who accesses a computer in an unauthorized manner or exceeds one's access rights
  - Can be used to prosecute employees using capability and accesses provided by their company to conduct fraudulent activity

Obtain Written Authorization

- White hat hackers always get permission
- *This is your get our of jail free card…*

- Penetration tests can expose confidential information so permission must be granted

Third-Party Authorization

- If servers and services are hosted in the cloud, you must request permission from the provider prior to conducting a penetration test

Contracts

- Statement of Work (SOW)
  - Formal document stating scope of what will be performed during a penetration test
- Master Service Agreement (MSA)
  - Contract where parties agree to most of the terms that will govern future actions
- Non-Disclosure Agreement (NDA)
  - Legal contract outlining confidential material or information that will be shared during the assessment and what restrictions are placed on it

Corporate Policies

- What do corporate policies allow you to do?
- Have employees waived their privacy?
- What policies should be tested?
  - Password strength/reuse
  - Bring Your Own Device (BYOD)
  - Encryption
  - Update frequency

Export Restrictions

- Wassenaar Agreement precludes the transfer of technologies considered ”dual-use”
- Strong encryption falls under this restriction
- Penetration testing tools could be considered surveillance tools and fall under these rules

Testing Strategies

CompTIA Pentest+

Penetration Testing Strategies

Black Box

Gray Box

White Box

Black Box
(No Knowledge Test)

- No prior knowledge of target or network
- Simulates an outsider attack
- Only focuses on what external attacks see and ignores the insider threat
- Takes more time and is much more expensive

White Box
(Full Knowledge Test)

- Full knowledge of network, systems, and the infrastructure

- Spend more time probing vulnerabilities and less time gathering information

- Tester is given support resources from the organization

Support resources will be covered in more detail in a different lesson

Gray Box
(Partial Knowledge Test)

- Partial knowledge of target

- Can be used as an internal test to simulate an insider attack with minimal knowledge
- Can also be used to decrease the information gathering stage so more time can be spent on identifying vulnerabilities
- Examples
  - IP ranges provided
  - Company emails to create phishing campaigns

White Box Support Resources

CompTIA Pentest+

Support Resources

- Generally provided only for a white box penetration test
  - Architectural diagrams
  - Sample application requests
  - SDK documentation
  - SOAP project files
  - Swagger document
  - WSDL/WADL
  - XSD

Architectural Diagrams

- Network diagrams, software flow charts, physical maps of organizational facilities

- Assists the tester in mapping out network topologies, location of switch closets, and where key information systems are located

Sample Application Requests

- Generally used for testing web applications or other applications developed by organization

```
    content: '';
    content: none;
}
table {
    border-collapse: collapse;
    border-spacing: 0;
}
button, input, select, textarea { margin: 0 }
:focus { outline: 0 }
a:link { -webkit-tap-highlight-color: #FF5E99 }
img, video, object, embed {
    max-width: 100%;
    height: auto!important;
}
iframe { max-width: 100% }
blockquote {
    font-style: italic;
    font-weight: normal;
    font-family: Georgia,Serif;
    font-size: 15px;
    padding: 0 10px 20px 27px;
    position: relative;
    margin-top: 25px;
}
blockquote:after {
    position: absolute;
    content: '”';
```

```
blockquote p { margin-bottom: 10px }
strong, b { font-weight: bold }
em, i, cite {
    font-style: normal;
    font-family: arial;
}
small { font-size: 100% }
figure { margin: 10px 0 }
code, pre {
    font-family: monospace,consolas,sans-serif;
    font-weight: normal;
    font-style: normal;
}
pre {
    margin: 5px 0 20px 0;
    line-height: 1.3em;
    padding: 8px 10px;
    overflow: auto;
}
    {
    ng: 0 8px;
    eight: 1.5;

    : 1px 6px;
    0 2px;
    lack;
```

SDK Documentation

- Software Developer's Kit (SDK) provides a set of tools, libraries, documentation, code samples, processes, or guides to allow faster development of a new app on a platform

- SDK provides code libraries for use

```
        input;
    nt iLength, iN;
    double dblTemp;
    bool again = true;

    while (again) {
        iN = -1;
        again = false;
        getline(cin, sInput);
        system("cls");
        stringstream(sInput) >> dblTemp;
        iLength = sInput.length();
        if (iLength < 4) {
            again = true;
            continue;
        } else if (sInput[iLength - 3] != '.') {
            again = true;
            continue;
        } while (++iN < iLength) {
            if (isdigit(sInput[iN])) {
                continue;
            else if (iN == (iLength - 3) ) {
                inue;
```

SOAP Project File

- Simple Objective Access Protocol (SOAP) is a messaging protocol specification for exchanging structured information in the implementation of web services
- SOAP project files are created from WSDL files or a single service call

Swagger Document

- Open-source framework with a large system of tools to help design, build, document, test, and standardize REST Web Services

- Representational State Transfer (REST) has been replacing SOAP in most web applications in recent years

- REST is a web application architectural style based on HTTP

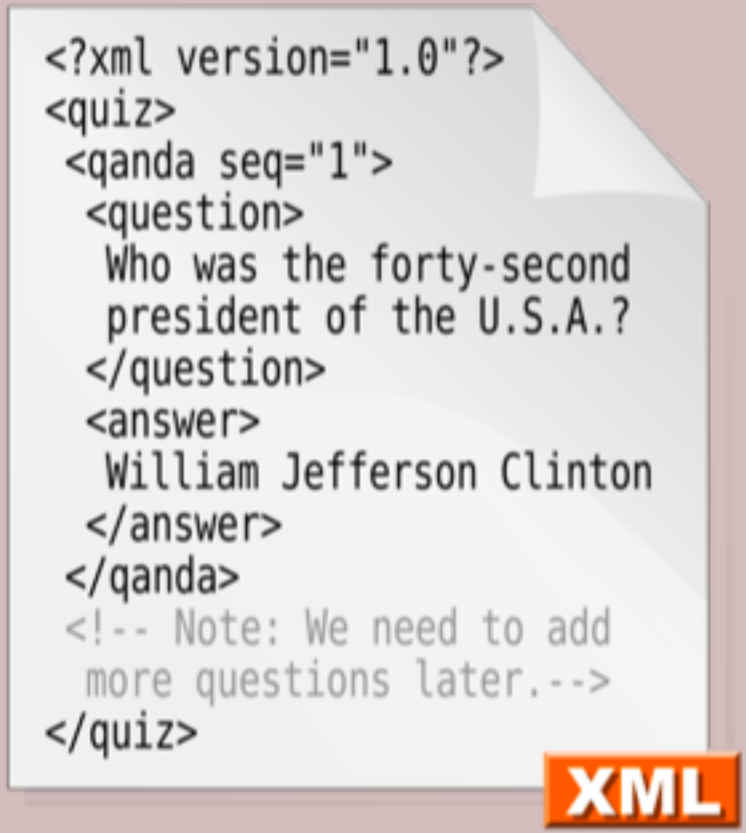
WSDL and WADL

- Web Services Description Language
  - XML-based interface definition language used for describing the functionality offered by a web service such as a SOAP server
  - Flexible and allows binding options
  - Not useful for REST services with WSDL 1.1

- Web Application Description Language
  - XML-based machine readable description of HTTP-based web services
  - Easier to write than WSDL but not as flexible
  - Typically used for REST services

XML Schema Definition (XSD)

- World Wide Web Consortium (W3C) recommendation that specifies how to formally describe elements in an Extensible Markup Language (XML) document



```
<?xml version="1.0"?>
<quiz>
 <qanda seq="1">
  <question>
   Who was the forty-second
   president of the U.S.A.?
  </question>
  <answer>
   William Jefferson Clinton
  </answer>
 </qanda>
 <!-- Note: We need to add
  more questions later.-->
</quiz>
```

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Types of Assessments

CompTIA Pentest+

Goal-based Pentests

- Specific goals are defined before testing starts
- Pentester may attempt to find many unique methods to achieve the specific goals

Objective-based

- Objective-based pentests seek to ensure the information remains secure
- Testing occurs using all methods and more accurately simulates a real attack

Compliance-based

- Risk-based compliance assessment that is required to ensure policies or regulations are being followed properly
- Regulations and policies provide checklists, for example the PCI-DSS compliance assessment
- Objectives are clearly defined
- Focus is on password policies, data isolation, limited network/storage access, and key management

Premerger

- Before two companies perform a merger it is common to conduct penetration tests on them to identify weaknesses being inherited

- Can be a part of the due diligence efforts

Supply Chain

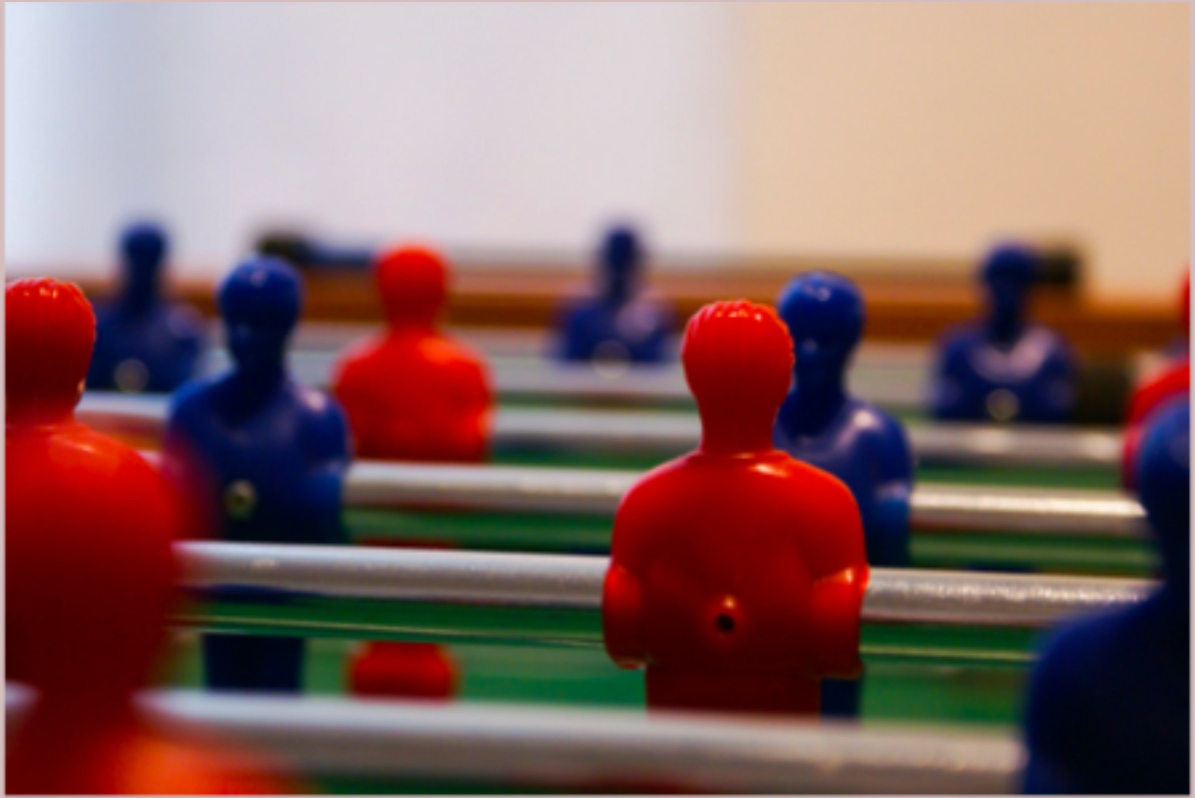
- Pentest may be required of your suppliers to ensure they are meeting their cybersecurity requirements

- Can be required prior to allowing an interconnection between the supplier’s systems and your organization’s systems

- Minimize risk by purchasing only from trusted vendors

Red Team

- Penetration test conducted by internal pentesters of an organization during security exercise to ensure defenders (blue team) can perform their jobs adequately



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Threat Actors

CompTIA Pentest+

Tiers of Adversaries

- Not all threat actors are created equal
- Some are structered, some are unstructured
- Some are more skilled than others

Advanced Persistent Threat (APT)

- Group with great capability and intent to hack a particular network or system
- Target organizations for business or political motives and usually funded by nation states
- Conduct highly covert hacks over long periods of time

Hacktivist

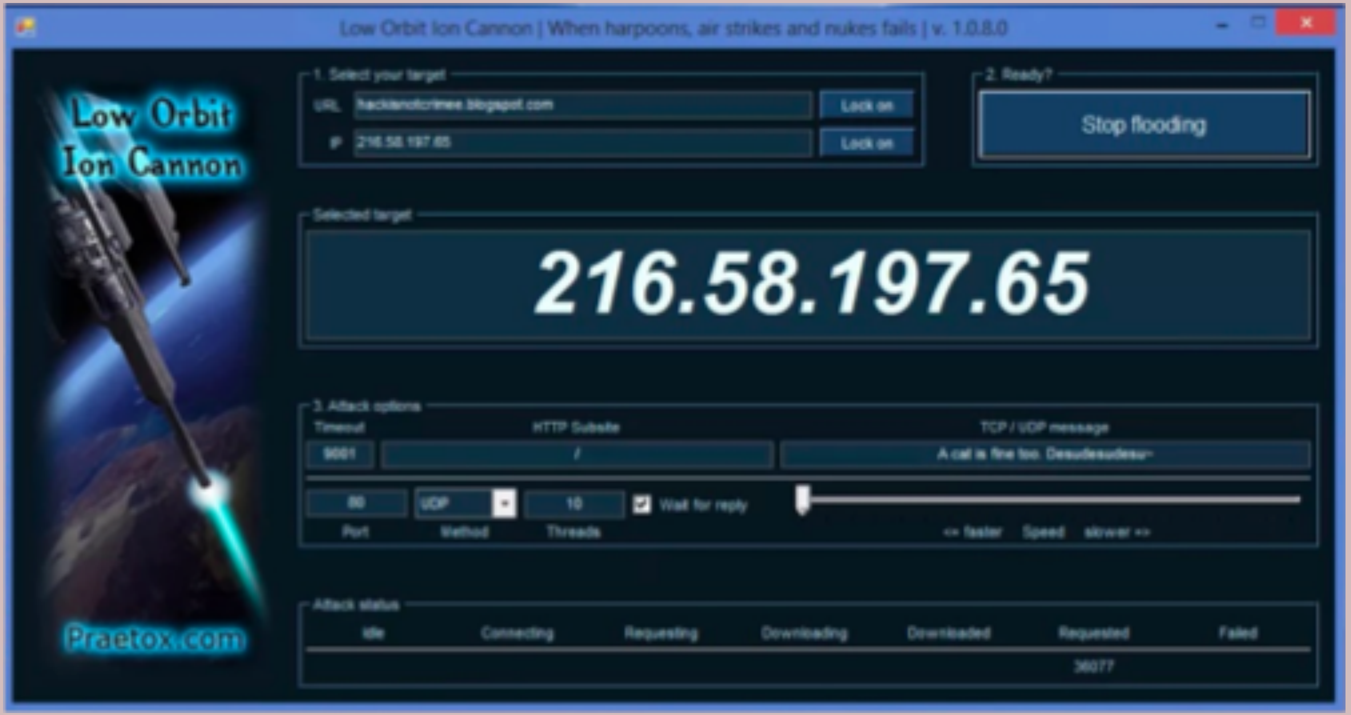
- Conduct activities against governments, corporations, or individuals
- Can be an individual or member of a group

Insider Threat

- Already have authorized user access to the networks, making them extremely dangerous
- May be a skilled or unskilled attacker
- Might be a former or current employee

Script Kiddies

- Low-skilled attackers who use other’s tools
- Use freely available vulnerability assessment and hacking tools to conduct attacks



Low Orbit Ion Cannon | When harpoons, air strikes and nukes fails | v. 1.0.8.0

1. Select your target

URL: hackianotcrimee.blogspot.com [Lock on]

IP: 216.58.197.65 [Lock on]

2. Ready? [Stop flooding]

Selected target: 216.58.197.65

3. Attack options

Timeout: 9001

HTTP Subsite: /

TCP / UDP message: A cat is fine too. Desudesudesu~

Port: 80

Method: UDP

Threads: 10

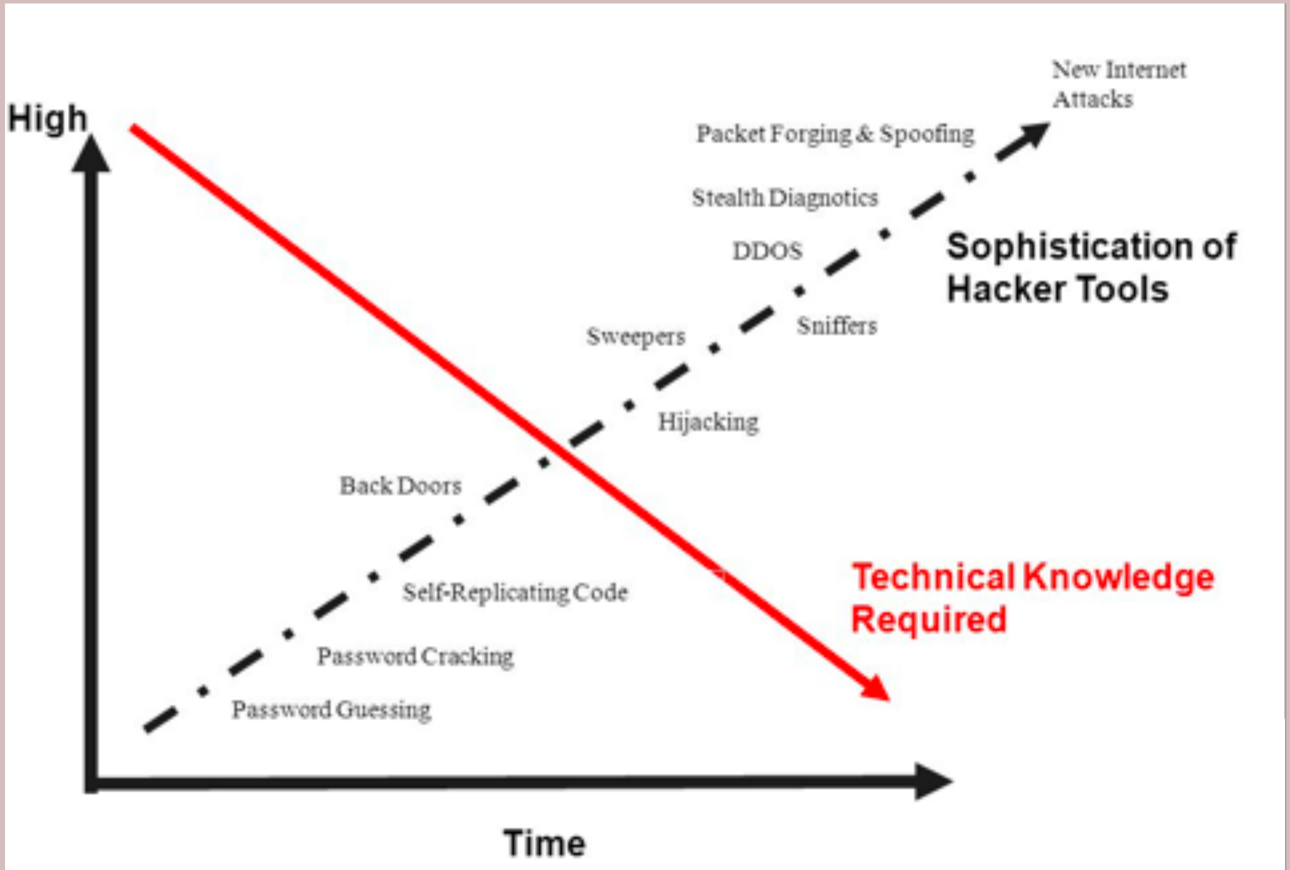
☑ Wait for reply

<< faster Speed slower >>

Attack status

Idle	Connecting	Requesting	Downloading	Downloaded	Requested	Failed
					36077	

Capabilities



Less technical knowledge is required to perform attacks because of the increased sophistication of hacking tools

What is the Intent?

- Greed or monetary gain
- Power, revenge, or blackmail
- Thrills, reputation, or recognition
- Espionage or political motivation

Threat Modeling

- What threat are you trying to emulate?
- Will you use open-source and openly available tools like a script kiddie, or create custom hacks like a Advanced Persistent Threat?
- Will you be given insider knowledge or perform a white box penetration test?

Tiers of Adversaries

Tier	Description
I	Little money and rely on off-the-shelf tools and known exploits
II	Little money and invest in own tools against known vulnerabilities
III	Invest lots of money to find unknown vulnerabilities in order to steal data to sell for profit (criminal hackers)
IV	Organized, highly technical, proficient, well-funded hackers working in teams to develop new exploits
V	Nation states investing tons of money creating vulnerabilities/exploits
VI	Nation states investing tons of money to carry out cyber, military, and intelligence operations to achieve political, military, or economic goals

Target Selection

CompTIA Pentest+

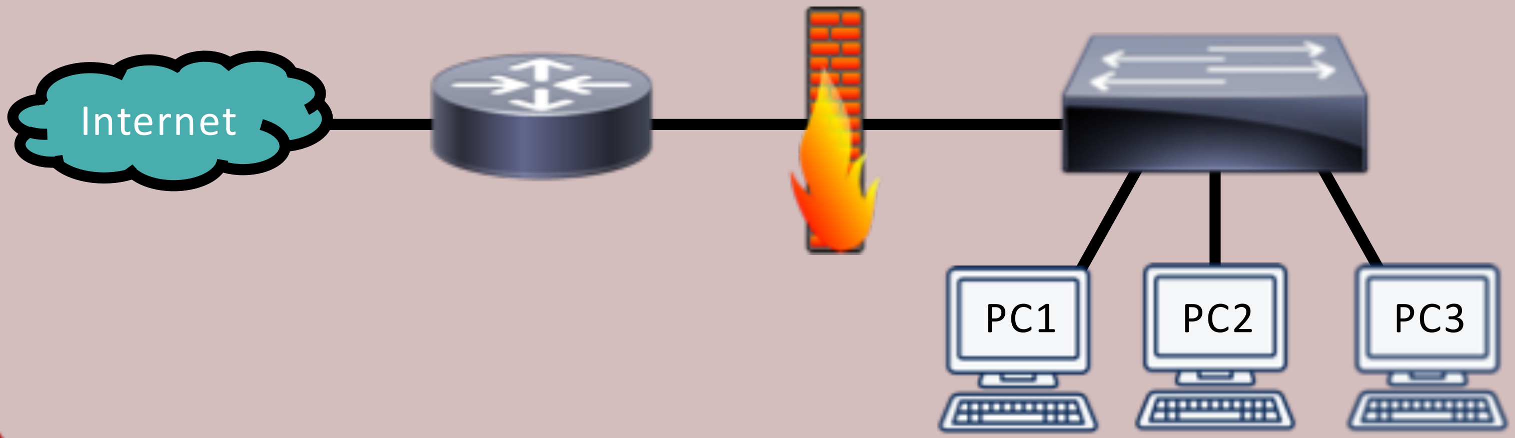
Target Selection

- Internal or External
- First-party or Third-party hosted
- Physical
- Users
- SSIDs
- Applications

Internal or External

- Internal focuses on targets inside the firewall
  - Can be on-site or off-site
  - Logically internal

- External focuses on publicly facing targets
  - Webservers in the DMZ
  - Outside the protected LAN



First-party or Third-party

- Are the targets hosted by the organization or by a third-party service provider?
- DionTraining.com is hosted by Thinkific and might be outside the penetration test scope

Physical

- Are we contracted to test physical security?

- Should we attempt to break into the facility?

Users

- Is social engineering authorized?
- Are particular users being targeted or not considered part of the assessment?

Wireless and SSIDs

- Is wireless pentesting being conducted?
- Are any SSID's out of scope?
  - Guest or public networks

Applications

- Are we focused on a particular application?
- Is a particular application mission critical and cannot be targeted?
  - Credit card processing system
  - Health care systems

Other Scoping Considerations

CompTIA Pentest+

Whitelist vs Blacklist

- Will your pentest systems be put on a list?
- Whitelist will allow you access, but blacklist will prevent your system from connecting

Security Exceptions

- Intrusion Prevention System (IPS)
- Web Application Firewall (WAF)
- Network Access Control
- Certificate Pinning
  - Required if the organization relies on digital certificates as part of their security
- Company policies

Risk

- What is the risk tolerance of the organization?

- Avoidance
  - Actions taken to eliminate risk completely

- Transference
  - Risk is moved to another entity

- Mitigation
  - Controls and countermeasures are put into place

- Acceptance
  - Risk is identified, analyzed, and within limits

Tolerance to Impact

- What is the impact to operations going to be?
- Balance the assessment needs with the operational needs of the organization by placing things in or out of scope

In Scope	Out of Scope
Network storage	Email servers
Web servers	Ecommerce servers
Intranet	Database servers
Physical security	Public Wifi

Schedule

- Will the timing of the penetration test be known by the organization’s defenders?
- Will it be performed during peak or off-peak hours?
- What about holidays?

List of events

Date and time restrictions

Client stakeholder notifications

Scope Creep

- Condition when a client requests additional services after the SOW and project scope have been agreed to and signed
- How will scope be contained?
- Document any changes to the scope of test
- Recommend signing a change order to SOW

More devices = More time = More resources