Chapter 1: Planning and Scoping

Ethical Hacking and CompTIA PenTest+ Exam Prep (PT0-001)

1

Episode 0 - Introduction

2

ABOUT THE EXAM

- The CompTIA PenTest+ exam will certify the successful candidate has the knowledge and skills required to:
  - Plan and scope an assessment
  - Understand legal and compliance requirements
  - Perform vulnerability scanning and penetration testing using appropriate tools and techniques
  - Analyze the results
- In addition, the candidate will be able to:
  - Produce a written report containing proposed remediation techniques
  - Effectively communicate results to management

3

EXAM DETAILS

Required exam	PT0-001
Number of questions	Maximum of 80
Type of questions	Multiple choice and performance-based
Length	165 minutes
Recommended experience	3-4 years of hands-on experience performing penetration tests, vulnerability assessments, and vulnerability management
Passing score	750 (on a scale of 100-900)

4

TARGET AUDIENCE

- Recommended experience
  - 3 to 4 yrs in penetration testing or equivalent
- Cybersecurity professionals with intermediate skill level
  - Active in hands-on penetration testing

5

Planning a Pen Test

Episode 1

6

PENTEST+ EXAM OBJECTIVES

DOMAIN	PERCENTAGE OF EXAM
1.0 Planning and Scoping	15%
2.0 Information Gathering and Vulnerability Identification	22%
3.0 Attacks and Exploits	30%
4.0 Penetration Testing Tools	17%
5.0 Reporting and Communication	16%
TOTAL	**100%**

7

1.0 PLANNING AND SCOPING

- Get permission
- Know how much work you have to do
  - Don’t do more than that
- Watch out for scope creep

8

PLANNING A PEN TEST

- Penetration Testing Execution Standard
  - http://www.pentest-standard.org/index.php/Main_Page
  - Defines seven sections of a penetration test
- Pen test sections
  - Pre-engagement interactions
  - Intelligence Gathering
  - Threat Modeling
  - Vulnerability Analysis
  - Exploitation
  - Post Exploitation
  - Reporting

9

THE IMPORTANCE OF PLANNING

- Each section of a pen test is important
  - Attackers generally skip the first step and last two steps
- Each step is important
- Don’t skip steps
  - You might miss an exploit
  - You might scope the test improperly
- Lots of options in each section
- Easy to waste time and effort
  - Experience helps avoid this
- Project management skills are important here

10

Rules of Engagement

Episode 2

11

TARGET AUDIENCE AND ROE

- Know your target audience
  - Who is sponsoring the pen test?
  - What is the purpose for the test?
- Rules of engagement – governs the pen tester's activities
  - Schedule - start, stop, temporal restrictions
  - Team composition, location, access
- Test scope
  - Technical/physical/personnel
  - Target limits (inclusion, invasiveness, etc.)

12

TARGET AUDIENCE AND ROE

- Test scope
  - Technical/physical/ personnel
  - Target limits (inclusion, invasiveness, etc.)

13

COMMUNICATION ESCALATION PATH

- Risks of pen testing
  - Crashing devices, services, whole servers
  - Corrupting data
  - Degrading performance
  - Terms of Service (TOS)/regulation/legislation violation
- Communication escalation path
  - Who to contact if things go wrong
  - Communication expectations (content, trigger, frequency)

14

Resources and Budgets

Episode 3

15

RESOURCES AND REQUIREMENTS

- What does each party provide?
- At what point does the engagement begin?
- Confidentiality of findings
- Known vs. unknown
  - Is the test a secret?

16

BUDGET

- How much will each section of the test cost?
- Every task in the test should have a value
  - Want to add more tests? It'll cost more
- One of the most important factors
  - Directly impacts available resources and time

17

Impact and Constraints

Episode 4

18

IMPACT AND DISCLAIMERS

- Impact analysis and remediation timelines
  - The result of testing
  - Report vulnerabilities
  - Report expectations to stakeholders
  - Estimate of time required to complete remediation recommendations
    - How should client respond?
- Disclaimers
  - Point-in-time assessment – only valid now
  - Comprehensiveness – enterprise/division/department, etc.

19

SET EXPECTATIONS

- Disclaimers
  - Point-in-time assessment
    - Only valid now
  - Comprehensiveness
    - Enterprise/division/ department, etc.

20

TECHNICAL CONSTRAINTS

- Any technical limitations that reduce test scope
- Production (live) components
- Out-of-service devices
- Can’t access
  - Physical/geographic access limitations
  - Legal/regulatory/out of scope

21

Support Resources

Episode 5

22

SUPPORT RESOURCES

- Black box testers generally don't have access
- WSDL/WADL
  - Web services/application description language
  - XML file with lots of info about web service/application and its interface requirements
    - Input/output specs

SUPPORT RESOURCES, cont'd

- SOAP project file
  - Simple Object Access Protocol – used to exchange info for web services
  - Project file provides low level web service interface details (input/output/server info)
  - Not exposed to public
  - Used by developers in development environment

SUPPORT RESOURCES, cont'd

- SDK documentation
  - Software Development Kit docs help provide info on tools used to develop software
  - Reveals software libraries in use
- Swagger document
  - Popular open source framework for developing REST services
  - Document can provide internal info on REST services exposed to clients
- XSD
  - XML Schema Definition – defines XML document content

25

SUPPORT RESOURCES, cont'd

- Sample application requests
  - Well-formed requests, generally to web services
  - Useful when testing web services/applications of all types
- Architectural diagrams
  - Diagrams of networks and connected devices
  - Helpful when determining targets to attack
    - May provide physical info too

Legal Groundwork

Episode 6

27

LEGAL CONCEPTS

- Explain key legal concepts
- Contracts
  - Statement of Work (SOW)
    - Clearly states what tasks are to be accomplished during an engagement
  - Master Service Agreement (MSA)
    - High level contract between a service provider and a client that specifies details of the business arrangement
  - Non-Disclosure Agreement (NDA)
    - Agreement that defines confidential material and restrictions on use and sharing sensitive information with other parties

28

ENVIRONMENTAL DIFFERENCES

- Export restrictions – restrictions on shipments, transfer of technology, or services outside the U.S.
  - See U.S. State Department resource - https://www.state.gov/strategictrade/overview/
- National or local restrictions
  - Differ among countries
  - Local customs differ
- Corporate policies
  - Differ between most organizations

29

WRITTEN AUTHORIZATION

- Obtain signature from proper signing authority
  - "Get out of jail free" card
  - Pen tests can reveal sensitive or confidential information
  - Activities may be illegal without proper permission
  - Signed permission makes you a white hat pen tester
- Third-party authorization when necessary
  - Ex: from a Cloud service provider
  - Get permission for any outside resources used
    - Cloud, Internet (ISP usage), etc

30

Scope Considerations

Episode 7

31

SCOPING THE ENGAGEMENT

- Types of assessment
  - Goals-based
    - Goals set up front, testers work to fulfill goals
  - Objective-based
    - Define a resource to attack
    - Tests use all angles to attack protected objectives
  - Compliance-based
    - Mandated by standard, regulation, or legislation
      - Ex: PCI-DSS
- Red team
  - Typically internal
  - A single compromise is success
  - Ongoing
- Blue team
  - Defense against the red team

32

SPECIAL SCOPING CONSIDERATIONS

- Premerger
  - Part of due diligence prior to mergers
  - Used to harmonize security efforts
- Supply chain
  - Partners often provide software and/or hardware to interface with an organization
  - Weaknesses in interfaces can provide unauthorized access
    - Especially from trusted vendors

33

TARGET SELECTION

- Targets
  - Internal (on-site vs. off-site)
  - External
  - First-party vs. third-party hosted
  - Physical
  - Users
  - SSIDs
  - Applications

Lab Environment Setup

Episode 8

35

Demo

- Introduction to class environment

36

Project Strategy and Risk

Episode 9

37

CONSIDERATIONS

- White-listed
  - No one can access resources unless specifically granted
- Black-listed
  - Everyone can access unless specifically blocked
- Security exceptions
  - IPS (Intrusion Prevention System)/WAF (Web application firewall) whitelist
  - NAC (Network Access Control)
  - Certificate pinning (public key pinning)
  - Company's policies
- Explore company policies to learn about security considerations

38

STRATEGY

- Black box
  - Zero prior information
  - Most similar to real attacker
  - Test is generally a surprise to all internal personnel
- White box
  - Full access to internal information
  - Simulates insider attack
- Gray box
  - Some internal information available
  - Consistent with an insider attack with limited access

39

RISK ACCEPTANCE

- Pen tests can be risky
  - Service can be interrupted
  - Devices/servers can become unresponsive
- How much risk is the client willing to accept?
  - Client has identified risks
  - Acceptance: willing to accept risks, based on likelihood and impact
- Tolerance to impact
  - If risk is realized, what is client's tolerance to the result?
  - How much disruption is tolerable?

40

Scope Vulnerabilities

Episode 10

41

SCHEDULING AND SCOPE CREEP

- Scheduling
  - When can/should test be run?
  - Who should be notified?
  - When must tests be completed?
- Scope creep – common in nearly all projects
  - Client requests additional tasks after SOW is signed
  - Many may seem “doable”
  - Takes resources away from core SOW tasks
  - Must get authorization for any SOW modifications

THREAT ACTORS

- Adversary tier – what role should the pen tester assume?
  - APT (Advanced Persistent Threat)
  - Script kiddies
  - Hacktivist
  - Insider threat
- Capabilities
  - What resources does the attacker(s) have?
  - Organized and sponsored attackers have more equipment and sophistication

43

THREAT ACTORS, cont'd

- Intent
  - Power/revenge
  - Status/validation
  - Monetary gain
  - Ideology
- Threat model
  - Gather information and identify assets
  - Rank pertinent threats
  - Map threats to assets

44

Compliance-Based Assessments

Episode 11

45

COMPLIANCE-BASED ASSESSMENT

- Rules to complete assessment
- Password policies
- Data isolation
- Key management
- Limitations
- Clearly defined objectives based on regulations

46