

Lecture 7 - Penetration Testing

Networks and System Security

Learning Objectives

1. Understanding penetration testing fundamentals
2. Purpose and limitations of pen testing
3. Types of penetration tests
4. Planning and scoping test engagements
5. Managing test processes and outcomes
6. Follow-up and remediation strategies

What is Penetration Testing?

NCSC Definition

"A method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the same tools and techniques as an adversary might."

Penetration testing is a powerful tool but must be:

- Properly commissioned
- Correctly scoped
- Integrated with routine security measures
- Used as part of a comprehensive security strategy

Purpose of Penetration Testing

Primary Function

Quality Assurance for Security Processes

- Method for gaining assurance in vulnerability assessment and management processes

Lecture 7 - Penetration Testing

- NOT a primary method for identifying vulnerabilities
- Think of it as verification, not discovery

The Financial Audit Analogy

Finance Side:

- Finance team → tracks daily expenditure/income
- External audit → ensures internal processes are sufficient

Security Equivalent:

- Internal security team → manages daily vulnerability assessment
- Penetration test → verifies internal processes are working

Ideal Scenario

You should know what the penetration testers are going to find **BEFORE** they find it

This means:

- Good understanding of existing vulnerabilities
- Effective internal assessment processes
- Using third-party tests for verification only

Expected Outcomes

✓ Confirmation of known issues ✓ Verification of remediation efforts ✓ Occasional discovery of subtle issues

The Exception, Not the Rule: Highly experienced testers finding completely unknown vulnerabilities

Goal: Use findings to improve internal processes

Lecture 7 - Penetration Testing

What Penetration Tests Identify

Typically identifies:

1. Technical risk levels from software vulnerabilities
2. Hardware vulnerability exposure
3. Configuration compliance with good practices
4. Known vulnerabilities in tested components

Important: Results are valid only at the time of testing

Types of Penetration Tests

Variables in Testing

Tests can vary in:

- **Techniques used:** tools and methods employed
- **Allowed targets:** scope of systems tested
- **Knowledge provided:** information given to testers beforehand
- **System administrator awareness:** level of notification

Test Basis (Information Level)

1. Opaque (Black Box) Testing

- Testers have minimal prior knowledge
- Simulates external attacker perspective
- Tests what an outsider could discover
- Reveals external security posture
- **Advantage:** Most realistic external threat simulation

2. Transparent (White Box) Testing

- Testers have full system knowledge
- Access to architecture, code, credentials

Lecture 7 - Penetration Testing

- Can test more thoroughly
- More efficient use of testing time
- **Advantage:** More comprehensive coverage of potential issues

Test Type (What is Being Tested)

1. Application Testing

- **Focus:** Vulnerability identification in custom/niche software
- **Most Common:** Web applications
- **Critical Requirement:** Provide feedback to developers on:
 - Secure coding practices
 - How to avoid identified vulnerability categories
 - Prevention strategies for future development

2. Scenario Testing

- **Purpose:** Explore specific scenarios to discover defense vulnerabilities
- **Example Scenarios:**
 - Lost laptop with company credentials
 - Unauthorized device connected to internal network
 - Compromised DMZ host
 - Insider threat simulation
- **Key:** Choose scenarios based on organization's risk profile and previous incidents

3. Red Teaming

- **Enhanced Scenario Testing:** Tests both vulnerabilities AND organizational response capabilities
- **Evaluates:**
 - Detection capability effectiveness
 - Response process efficiency
 - Coverage of security controls

Lecture 7 - Penetration Testing

- Incident handling procedures
- **Note:** Active area of NCSC development

4. Bespoke Testing

- For scenarios requiring additional assurance
- Specifically targeted penetration tests
- Custom scoped assessments
- Specialized threat simulations
- **Getting Help:** Qualified teams can guide scenario selection and proper scoping

What Pen Testing Is Suitable For

✓ SUITABLE

- Specific operational systems
- Multi-vendor product environments
- In-house developed systems and applications
- Live production environments

X NOT SUITABLE

- Product-specific testing (use other methods)

Limitations of Penetration Testing

Critical Time Limitation

- **Tests only validate security on the day of testing**
- **Common Reality:**
 - 12+ months between tests
 - Vulnerabilities can exist for extended periods
 - New threats emerge constantly

Lecture 7 - Penetration Testing

- Systems change and evolve
- **Solution:** Continuous security monitoring and assessment

Penetration Testing Does NOT Replace Regular Security

Must Continue:

- Functional testing of security controls
- Regular vulnerability assessments
- Security control validation
- Continuous monitoring

Principle: Penetration testing supplements, not replaces, routine security

Functional Testing vs Penetration Testing

Security Controls Must Be Functionally Tested

Positive Tests (should work):

- "The logon box appears when attempting to log in"
- "Authentication process initiates correctly"
- "Security controls activate as designed"

Negative Tests (should fail):

- "Cannot log in without correct password"
- "Unauthorized access attempts are blocked"
- "Invalid inputs are rejected"

When NOT to Use Pen Testing

NOT valuable for:

- Assessing if defined security controls are functioning
- Basic functional testing
- Routine verification tasks

Lecture 7 - Penetration Testing

Best used for:

- Complex vulnerability discovery
- Real-world attack simulation
- Validation of security posture
- Finding subtle, complex issues

Requirements for Effective Testing

Qualified and Experienced Staff

- Tests cannot be entirely procedural
- No exhaustive test case list exists
- Quality directly linked to tester abilities
- Expertise determines what gets discovered

NCSC Recommendation: CHECK Scheme

For HMG (Her Majesty's Government) Organizations:

- Verified qualifications
- Standardized methodologies
- Quality assurance
- Government-approved testing standards

The Penetration Testing Process

Five Critical Phases

1. Initial Engagement → selecting the team

↓

2. Scoping → defining the test

Lecture 7 - Penetration Testing

↓

3. Testing → conducting the assessment

↓

4. Reporting → documenting findings

↓

5. Follow-up → remediation and improvement

Model Assumptions

- You want to understand impact of exploited vulnerabilities
- You want to know likelihood of exploitation
- You have an internal vulnerability assessment process
- You're seeking external validation of internal processes

Phase 1: Initial Engagement (Selecting the Team)

Ensure the External Team Has

- Relevant qualifications (CHECK, CREST, etc.)
- Appropriate skills for your IT estate
- Experience with your system types

Highlight During Bidding

- Unusual systems (mainframes, legacy systems)
- Uncommon networking protocols
- Bespoke hardware
- Specialized requirements

Lecture 7 - Penetration Testing

Phase 2: Scoping

Importance

- **Poor scoping = Poor results**
- Invest time in getting this right

What Scoping Determines

- What systems will be tested
- What methods will be used
- What access will be provided
- What the success criteria are
- What constraints exist

Key Questions to Answer

1. What are the test objectives?
2. Which systems are in scope?
3. What level of access is appropriate?
4. What knowledge should testers have?
5. What are the time constraints?
6. What are the business impact limits?
7. Who needs to be notified?

Phase 3: Testing

During Active Testing

- Testers attempt to breach system security

Lecture 7 - Penetration Testing

- Multiple tools and techniques are employed
- Various attack vectors are explored
- Findings are documented in real-time
- Critical issues may be reported immediately

Your Role

- Monitor progress
- Respond to queries
- Maintain communication
- Stay vigilant (testing can impact systems)

Communication Requirements

- Designated contact person
- Clear escalation procedures
- Rapid response to critical findings
- Regular progress updates
- Immediate notification of any issues

Phase 4: Reporting

Comprehensive Report Should Include

- Executive summary
- Methodology description
- Detailed findings
- Risk ratings for each issue
- Reproduction steps
- Recommended remediation
- Supporting evidence

Lecture 7 - Penetration Testing

Each Finding Should Have

- Severity level (Critical, High, Medium, Low)
- Likelihood of exploitation
- Impact if exploited
- CVSS score (where applicable)
- Business risk assessment

Note: Ratings may differ from your internal assessment - this is normal

Typical Rating Factors

- Ease of exploitation
- Required attacker skill level
- Available exploits
- Potential damage
- Affected systems
- Compensating controls

Remember: External ratings are a starting point, not the final word

Phase 5: Follow-up and Remediation

Step 1: Internal Review

Your vulnerability management group should:

- Assess the report thoroughly
- Compare findings to internal assessments
- Evaluate proposed solutions
- Consider business context
- Determine actual risk levels

Critical Principle: Risk assessment and fix decisions are YOUR responsibility

Lecture 7 - Penetration Testing

Why Testers May Rate Differently

- Limited business context
- Incomplete system knowledge
- Standard methodology constraints
- Different risk perspectives

Your job: Contextualize findings for your organization

When Testers Find Unknown Issues

Special Attention Required - Ask yourself:

1. Why didn't we find this?
2. What process gaps exist?
3. How can we spot similar issues?
4. What do we need to change?

Goal: Improve internal processes to catch these in future

Remediation Options

Proposed Solutions Are Not Always the Only Solutions

Tester Suggestion: "Patch this software"

Consider alternatives:

1. Uninstall if not required
2. Implement additional controls
3. Increase monitoring
4. Accept the risk with justification
5. Compensating controls
6. Remove functionality
7. Network segmentation
8. Enhanced monitoring
9. Access controls

Lecture 7 - Penetration Testing

10. WAF rules

Consult: Your technical staff and suppliers

Business Process, Not Just Technical

Key Understanding: Vulnerability risk assessment and mitigation is a BUSINESS PROCESS

Should NOT Be:

- Wholly outsourced to test team
- Treated as purely technical
- Isolated from business context
- Decided without stakeholder input

Include: Business owners, technical staff, risk managers, compliance team

Integration with Broader Security

Pen Testing Must Integrate With

- Continuous vulnerability scanning
- Security monitoring
- Incident response
- Patch management
- Security awareness training
- Threat intelligence

It's one component of defense in depth

Use Pen Test Results To

1. Validate internal processes
2. Identify process gaps
3. Improve detection capabilities

Lecture 7 - Penetration Testing

4. Enhance security controls
5. Train security staff
6. Update security procedures

Each test should make you stronger

Best Practices Summary

DO

1. Use qualified testers (CHECK scheme recommended)
2. Invest time in proper scoping
3. Maintain internal vulnerability processes
4. Communicate clearly throughout
5. Assess findings in business context
6. Use results to improve processes
7. Schedule tests appropriately
8. Plan remediation before testing

DON'T

- Treat pen testing as a one-time compliance checkbox
- Ignore findings that contradict your assumptions
- Automatically accept tester risk ratings
- Delay remediation indefinitely
- Forget about findings after initial review
- Use pen testing as substitute for regular security

Penetration Testing Methodology

The Six Phases of Attack

Lecture 7 - Penetration Testing

1. Reconnaissance

↓

2. Scanning & Enumeration

↓

3. Vulnerability Assessment

↓

4. Exploitation

↓

5. Post-Exploitation

↓

6. Reporting

1. Reconnaissance

Gathering information about the target organization

Passive Information Gathering

- **Definition:** Collecting data without directly interacting with target system
- **Goal:** Remain undetected while learning about target
- **Techniques:**
 - WHOIS lookups
 - DNS queries
 - Public website analysis
 - Social media profiling
 - Google dorking
- **Advantages:** Low risk of detection, useful for early-stage recon
- **Limitations:** May not reveal internal or real-time system details

Active Information Gathering

- **Definition:** Directly interacting with target system to extract information

Lecture 7 - Penetration Testing

- **Goal:** Obtain detailed, often technical data
- **Techniques:**
 - Port scanning (e.g., Nmap)
 - Banner grabbing
 - Vulnerability scanning
 - Network sniffing
- **Advantages:** Provides deeper insights into system configuration and vulnerabilities
- **Limitations:** Higher risk of detection, may trigger security alerts

2. Scanning & Enumeration

Identifying live hosts, ports, and services

3. Vulnerability Assessment

Detecting weaknesses in systems and applications

4. Exploitation

Attempting to compromise identified vulnerabilities

5. Post-Exploitation

Maintaining access and expanding control

6. Reporting

Documenting findings and remediation recommendations

Penetration Testing Tools

Key Principles

- Tools automate and enhance testing efficiency across different attack phases
- Categories include reconnaissance, scanning, exploitation, and post-exploitation

Lecture 7 - Penetration Testing

- Proper tool selection depends on scope, target, and testing objectives
- **Always obtain written authorization before conducting any penetration test**

Passive Reconnaissance Tools

- **Google Dorking:** Advanced search operators to find exposed information
- **Shodan:** Search engine for internet-connected devices and services
- **theHarvester:** Collects emails, subdomains, IPs from public sources
- **Maltego:** Visual link analysis and data mining platform
- **WHOIS/DNS tools:** Domain registration and DNS record enumeration

Active Reconnaissance Tools

- **Nmap:** Network discovery and port scanning
- **DNSRecon:** Active DNS enumeration including zone transfers
- **Sublist3r:** Subdomain enumeration using multiple search engines
- **Fierce:** DNS reconnaissance and subdomain brute-forcing

Nmap (Network Mapper)

- Industry-standard network scanner for host and service discovery
- Supports multiple scan types: SYN, TCP connect, UDP, ACK, and more
- Service version detection and OS fingerprinting capabilities
- NSE (Nmap Scripting Engine) extends functionality with custom scripts
- **Essential syntax:** `nmap -sV -sC -oA output target`

Vulnerability Assessment Tools

- **Nessus:** Commercial vulnerability scanner with extensive plugin library
- **OpenVAS:** Open-source vulnerability assessment system
- **Nikto:** Web server scanner identifying common vulnerabilities
- **OWASP ZAP:** Web application security scanner and proxy

Exploitation Frameworks

Lecture 7 - Penetration Testing

- **Metasploit Framework:** Comprehensive exploitation and post-exploitation platform
 - Contains hundreds of exploit modules for various vulnerabilities
 - Payload generation, encoding, and delivery mechanisms
 - Integrates with scanning tools for automated exploitation
 - **Caution:** Only use against authorized targets with proper scope

Web Application Testing Tools

- **Burp Suite:** Intercepting proxy for manual web app testing
- **SQLmap:** Automated SQL injection detection and exploitation
- **XSSStrike:** Cross-site scripting vulnerability scanner
- **Gobuster/Dirb:** Directory and file brute-forcing tools
- **WPScan:** WordPress-specific vulnerability scanner

Wireless Testing Tools

- **Aircrack-ng suite:** Wireless packet capture and WEP/WPA cracking
- **Kismet:** Wireless network detector and packet sniffer
- **Reaver:** WPS (Wi-Fi Protected Setup) brute-force tool
- **Wifite:** Automated wireless attack tool
- **Requires:** Compatible wireless adapters supporting monitor mode

Password Cracking Tools

- **John the Ripper:** Fast password hash cracking with multiple attack modes
- **Hashcat:** GPU-accelerated password recovery supporting many hash types
- **Hydra:** Network login cracker for various protocols (SSH, FTP, HTTP, etc.)
- **CeWL:** Custom wordlist generator from website content
- **Attack strategies:** Dictionary, brute-force, and rule-based

Post-Exploitation Tools

- **Mimikatz:** Windows credential extraction from memory

Lecture 7 - Penetration Testing

- **BloodHound:** Active Directory attack path mapping
- **PowerSploit:** PowerShell-based post-exploitation framework
- **Empire/Starkiller:** Post-exploitation agent and C2 framework

Social Engineering Tools

- **Social Engineering Toolkit (SET):** Framework for social engineering attacks
- **GoPhish:** Phishing campaign management and tracking
- **King Phisher:** Phishing campaign toolkit with analytics
- **Features:** Email templates, credential harvesting, and reporting

Network Analysis Tools

- **Wireshark:** Industry-standard packet capture and analysis tool
- **tcpdump:** Command-line packet analyzer for quick captures
- **Bro/Zeek:** Network security monitoring framework
- **NetworkMiner:** Network forensics analysis tool

Scripting Languages

- **Python:** Dominant language for security tool development
- **Bash scripting:** Automation of command-line tools and workflows
- **PowerShell:** Windows automation and Active Directory enumeration
- **Ruby:** Language behind Metasploit modules

Operating Systems for Pen Testing

- **Kali Linux:** Most popular distribution with 600+ pre-installed tools
- **Parrot Security OS:** Alternative with focus on privacy and development
- **BlackArch:** Arch-based distribution with 2800+ tools
- **Benefits:** Pre-configured environments reduce setup time and tool conflicts
- **Isolation:** Virtual machines and containers provide isolated testing environments

Cloud Security Tools

Lecture 7 - Penetration Testing

- **ScoutSuite:** Multi-cloud security auditing tool (AWS, Azure, GCP)
- **Prowler:** AWS security assessment and compliance tool
- **Cloud Custodian:** Cloud security, compliance, and governance
- **Pacu:** AWS exploitation framework for penetration testers

Reporting & Documentation Tools

- **Dradis Framework:** Centralized reporting and collaboration platform
 - **Faraday:** Collaborative penetration testing IDE
 - **KeepNote/CherryTree:** Note-taking applications for pentesters
 - **Markdown/LaTeX:** Professional report formatting
-

Legal and Ethical Considerations

Mandatory Requirements

- **Written authorization** (scope, targets, timeframes) is mandatory before testing
- Respect rules of engagement and escalation procedures
- Bug bounty programs provide legal testing opportunities
- **Data protection:** handle discovered sensitive information responsibly

Operational Best Practices

- Match tools to engagement objectives and scope limitations
- Understand tool capabilities and limitations—avoid blind reliance
- Verify automated findings manually to reduce false positives
- Document tool versions and commands for reproducibility
- Maintain updated toolkits addressing latest vulnerabilities
- Consider operational security and tool artifacts left on target systems

Lecture 7 - Penetration Testing

Future Trends in Penetration Testing

- AI/ML integration for intelligent vulnerability analysis
- Container and Kubernetes security testing tools
- IoT and embedded device penetration testing frameworks
- Purple teaming tools bridging offensive and defensive operations
- Continuous security validation and breach-and-attack simulation
- Emphasis on developer security training and secure coding practices

Key Takeaways

1. **Pen testing validates security processes** - it's quality assurance, not primary vulnerability discovery
2. **Results are time-limited** - valid only at the time of testing
3. **You own the risk decisions** - testers provide input, you make final calls
4. **Proper scoping is critical** - poor scoping = poor results
5. **Integration is essential** - must work with broader security program
6. **Continuous improvement** - use findings to strengthen internal processes
7. **Qualified testers matter** - expertise directly impacts what gets discovered
8. **Written authorization required** - always obtain legal permission before testing
9. **Business context matters** - technical findings must be assessed in organizational context