PREPARATIONS

Introduction to
Penetration Testing

ORG REQUIREMENTS

- Properly understand the client's requirements.
  - To assess overall current security posture.
  - To meet regulatory requirements.
  - To test specific systems, applications, and scenarios.
- Demonstrate impact of findings in relation to the business.
  - Monetary loss
  - Loss of intellectual property
  - Brand damage

ORG REQUIREMENTS

Scoping

- Questionnaires
  - Determine the type of testing.
  - Ask about the criticality of the systems.
  - Identify fragile systems.
  - How many IP addresses will be tested?
  - How many web applications will be tested?
- Dealing with third party vendors.
  - Agree on the testing window.
  - Supply them with the IP addresses where the test will be conducted from.

ORG REQUIREMENTS

Scoping

- Verify IP address range
  - Ensure that all of the IP addresses belong to the customer.
- Rules of engagement
  - Determine what kind of techniques are allowed:
    - Client-side exploitation.
    - Social engineering.
    - Denial of service.

ORG REQUIREMENTS

Scoping

- Agree on a realistic time frame for testing.
  - Start date and end date of testing.
  - Daily time window for testing.
- Agree on the frequency of status updates.
- Evidence handling.
  - How is the data gathered from the test protected?

PERSONNEL REQUIREMENTS

- Project manager.
  - Coordinating meetings
  - Project scheduling
  - Status updates
  - Scoping
- Team leader.
  - Coordinates the actual penetration test.
  - Finalizes findings and report.

PERSONNEL REQUIREMENTS

- Penetration tester(s).
  - Does the actual penetration testing.
  - Verifies findings.
  - Assess impact.
  - Collects evidence.
  - Writes exploits and devises proof-of-concept.
  - Recommendations for remediation.

PERSONNEL REQUIREMENTS

- Client point of contact.
  - Liaises with the penetration team's project manager.
  - Provides legal documents.
  - Coordinates revalidation of findings after remediation.
- Client technical point of contact.
  - Required for escalation path.
  - Reviews technical report and formulates remediation plan.

TECHNICAL REQUIREMENTS

- No criminal record.
- A deep understanding of technical IT knowledge.
  - Networking.
  - Experience with multiple operating systems and applications.
  - Programming and scripting skills.

TECHNICAL REQUIREMENTS

- Experience and understanding of different types of attack vectors.
  - Host based vulnerabilities
    - Buffer overflow
    - Format string
    - Race condition
    - Denial of service / Distributed denial of service

TECHNICAL REQUIREMENTS

- Experience and understanding of different types of attack vectors.
  - Web based vulnerabilities
    - SQL injection
    - Cross-site scripting
    - File inclusion exploitation
    - LDAP injection
    - Null byte poisoning
    - Cross-site request forgery
    - Command injection

TECHNICAL REQUIREMENTS

- Experience and understanding of different types of attack vectors.
  - Network based vulnerabilities
    - ARP spoofing
    - Sniffing
    - VLAN hopping
    - Denial of service / Distributed denial of service
    - IP address / MAC address spoofing

TECHNICAL REQUIREMENTS

- Experience and understanding of different types of attack vectors.
  - Client-side attacks
    - Browser based exploits
    - Malicious documents
  - Social engineering
    - Obtain information by exploiting trust
    - Spoofing emails
    - Phishing

TECHNICAL REQUIREMENTS

- Experience and understanding of different types of attack vectors.
  - Database attacks
    - Identifying database type
    - Abusing permissions
    - Command execution
    - Common misconfigurations

TECHNICAL REQUIREMENTS

- Ensure that you have all of the needed tools
  - Update your tools!
  - Familiarize yourself with the tools.
  - Have sandboxes for testing exploits and tools.
- Creative and able to think outside of the box.
- Have actual hacking experience.
  - Participate in Capture the flag & hacking competitions.

LEGAL ISSUES

- Legal action taken due to negligence.
  - Penetration tester accidentally spreads malware.
  - Accidentally deletes data on servers.
- Legal action taken due to improper scoping.
  - Hacking the wrong targets.

LEGAL ISSUES

- Unexpected down time that causes monetary losses.
  - Accidentally crashing a server or application impacting the business financially.
- Data leakage.
  - Untested public exploit quietly installs a backdoor.
  - Unencrypted data stored in penetration tester's laptop.
  - Revealing penetration test findings to external parties.

LEGAL ISSUES

- Check with local cyber law, http://nitc.mosti.gov.my/nitc_beta/index.php/national-ict-policies/cyberlaws-in-malaysia
- Ensure that you have proper legal documents to protect yourself.

ETHICAL ISSUES

- Collecting trophies.
  - Database dumps.
  - Confidential files and documents.
  - Cracked usernames and passwords.
- Maintaining access.
  - Maintaining backdoors.
  - Keeping newly created accounts.
- Unauthorized sharing of penetration test report.

STANDARDS AND GUIDELINES

- NIST SP 800-115
  - Target identification
    - Network discovery
    - Vulnerability scanning
    - Wireless scanning
  - Target vulnerability validation
    - Password cracking
    - Exploitation
    - Social engineering

STANDARDS AND GUIDELINES

- NIST SP 800-115
  - Security assessment planning
    - Planning assessment policy
    - Selecting & customizing techniques
    - Legal considerations
  - Security assessment execution
    - Coordination
    - Assessing & analysis
    - Data handling

STANDARDS AND GUIDELINES

- NIST SP 800-115
    - Post testing activities
        - Mitigation recommendations
        - Reporting

STANDARDS AND GUIDELINES

- Open Source Security Testing Methodology (OSSTM)
  - Scope & rules of engagement
  - Common test types
  - Security analysis
  - Operational security metrics
  - Human security testing
  - Physical security testing
  - Wireless security testing

STANDARDS AND GUIDELINES

- OWASP Security Testing Guide
  - Information gathering
  - Configuration & deployment testing
  - Authentication testing
  - Session management testing
  - Authorization testing
  - Business logic testing
  - Data validation testing
  - Data encryption testing
  - Web service testing
  - Client-side testing

STANDARDS AND GUIDELINES

- NIST SP 800-115
  - http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf
- Open Source Security Testing Methodology (OSSTM)
  - http://www.isecom.org/mirror/OSSTMM.3.pdf
- OWASP Security Testing Guide
  - https://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf (v4 at point of writing is still in Beta)