“penetration testing has become one of the most important concepts to identify and assess possible risks”
“I already knew what they’d find ... completely failed .... waste of money .... now, what do I do?”
Overview

1. Types of testing
2. Security testing process
3. Secrets of success
   - Elevate testing to executives
   - Open the kimono
   - NO limitations
   - Realistic testing
   - Purple-team approach
   - Defined responsibility
01. Types of Testing
Types of Security Tests

1. Uncredentialed vulnerability scan
2. Credentialed vulnerability scan
3. Penetration testing (with/without adversary emulation)
4. Post-compromise assessment
5. Red team assessment
6. Purple team assessment

Invasiveness
Vulnerability Assessments

- Relies largely on automated scanning
- Common tool set
- Lots of false positive results, unless manually verified
- Authenticated vs unauthenticated
- Client is passive ... “there’s my network – scan it”
- Value of the tester is explaining results, minimizing unnecessary work
Penetration Test

Builds on results from a vulnerability scan
Interactive – additional techniques (physical attacks, social engineering, phishing)
Focus is on proving vulnerabilities by demonstrating exploits
But ... you don’t have to demonstrate all the vulnerabilities that exist
Penetration Test

Phase I
Intelligence Gathering
Gather detailed information about internal or external environment

Phase II
Threat Modeling
Identify attack scenarios and associated risks based on environment information

Phase III
Vulnerability Analysis
Systematically identify weaknesses in environment

Phase IV
Exploitation
Conduct proof of concept exploitation of identified weaknesses

Phase V
Post-Exploitation
Identify and exploit privilege escalation vulnerabilities and pivot to other systems

Phase VI
Reporting
Provide detailed reporting on findings along with risk rating, business impact, escalation and prioritized remediation recommendations
Penetration Test
Vulnerability Scan vs. Penetration Testing
Scoping with “Box Perspective”

White box = full-knowledge of network, configuration; access to IT
Black box = no knowledge
What’s best?
What Testing Methodology is Best?
02. Security Testing Process
Before Beginning, Ask:

What is a “penetration test”, and why do I want one?
Guiding Questions – Client-Side

- Budget! (Before, after)
- Who supports and endorses the testing?
- Who will do the testing? (internal / external)
- Who signs the contract? (Lawyer!)
- Who will manage the testing process?
- What will be done with the results?
- Will there be a re-test?
- How will you address the root cause(s) of any findings?
- How will you learn from testing?
Before beginning, does client approve the output and documentation?
Does client have an information security policy, similar guidance?
Previous testing? Review results
What are the risks to testing?
What does the client value?
What is a win?
Testing Process

1. Scoping
2. Statement of Work, SOW
3. Acceptance and kick-off meeting
4. Delivery
5. Documentation
6. Follow-up
1. Scoping

- Network – cloud architecture, wired, wireless, VoIP, industrial control systems (ICS / SCADA), “Internet of Things”, IOT
- Hardware – embedded operating systems, medical devices
- Applications – remote access technology, identity and access management including Active Directory, ERM (SAP, Baan), web services, mobile applications, source code review
- Social engineering – access card cloning, leave-behind devices, physical access, phishing tests
2. Statement of Work, SOW

- Contract governing the engagement
- Used for internal or external testers
- Grants tester permission to test, reduces liability
- Signed by lawyer
- Defines test parameters
  - What / when / how
- Payment terms – fixed price, phased or complete pricing
3. Acceptance and Kick-Off Meeting

- Client meeting with testing team
- Determine dates for testing
- Review methodology with technology owners
- Make revisions or changes
- Determine escalation path to be used during testing
- Agree to format for final deliverable / documentation
4. Delivery

- Defined and consistent methodology (PTES, MITRE ATT&CK)
5. Documentation

- Format determined in consultation with client at kick-off
- Deliverable: executive summary and technical report
  - Executive summary: overview, high-level findings, strategic and tactical findings
  - Technical report: overview, findings – description, impact, proof, remediation steps
- Presented as draft for comments
- Final deliverable incorporates original draft + client comments
6. Follow-Up

- Knowledge transfer
- Tools, techniques used during testing
- Retest following mediation
- Post-test contact
- Identification of new vulnerabilities
- Identification of new remediation technologies
03.
Secrets of Success
Elevate Testing to Executives

- No longer an “IT issue” – partners, third parties involved
- Board members, executives are liable for network security
- Visibility to current and required network states
- Supports funding requests
- Security awareness training for executives
- Metrics for IT security management
“Open the kimono”
NO limitations
Realistic Testing
Train As You Fight, Fight as You Train
Every Engagement a “Purple Team”

- Defender is “blue”; attacker is “red” - train them together (“purple”)
- If you don’t, you’ve lost ½ the value of the security test
- Validate people, automatic security controls
Defined Responsibility

- Goal: security testing is a managed “change control” process
- Assigned, competent manager
- Assigned responsibility for patching, mediation
- May require 3<sup>rd</sup> parties, contractors
- Mediation schedule
- Part of initial budget
More Questions / Copy of Pres

Robert Beggs
Penetration testing and incident response / data forensics leader
Canada · 500+ connections · Contact info

About
Robert Beggs is the founder and CEO of Digital Defence, a Canadian-focused company that specializes in preventing and responding to information security incidents. Robert is a security practitioner with more than 15 years of experience. He has been responsible for the technical leadership and project management of more than 300 consulting engagements.

Phone: +1-800-385-1632
robert.beggs@digitaldefence.ca
linkedin.com/in/robertbeggs/

https://www.linkedin.com/groups/3666591/