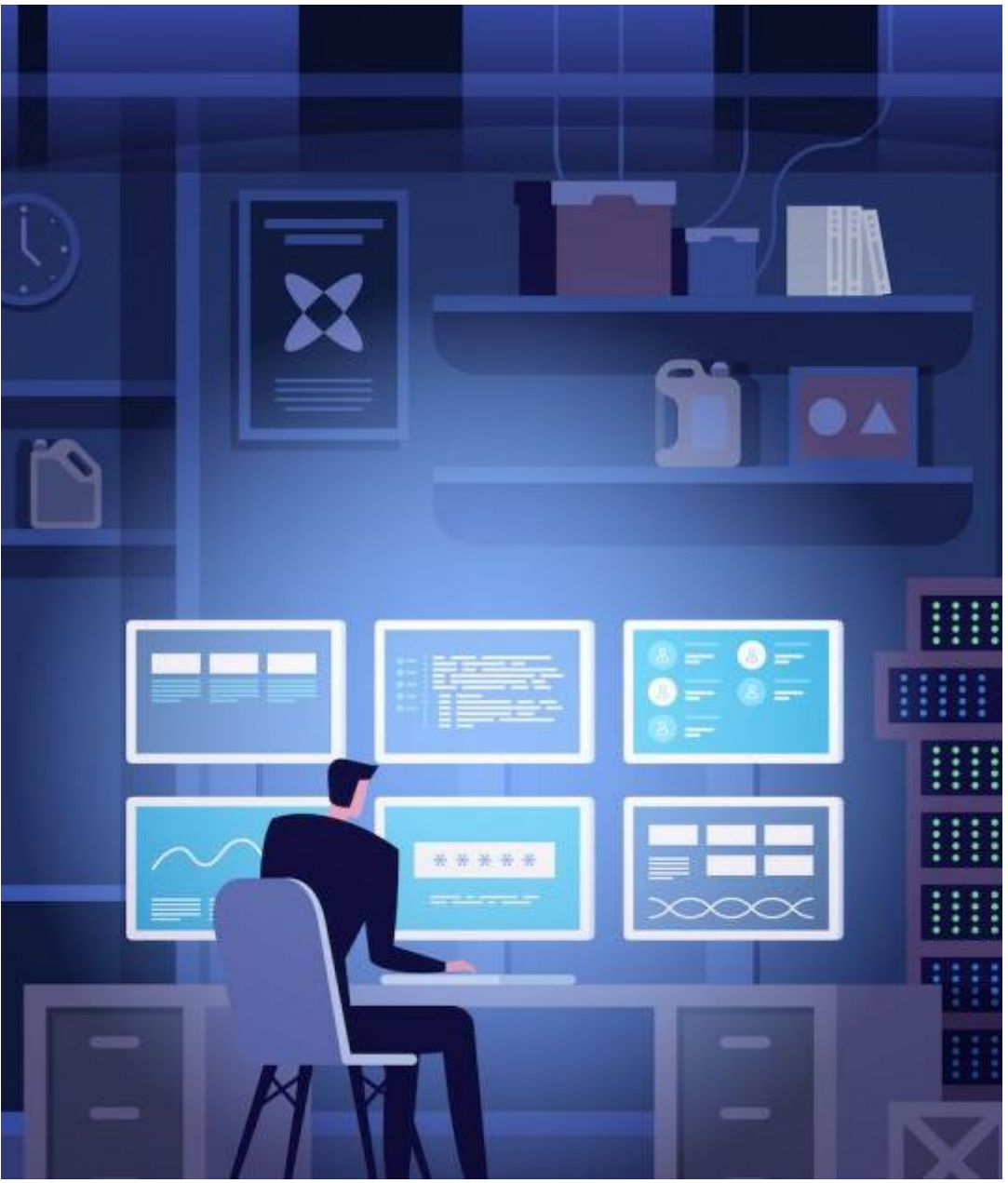


What to Expect from a Penetration Test

MICHAEL VIEAU, CISSP, CEH

PENETRATION TESTER

MSOE UNIVERSITY

whoami

- Full-time managing consultant at Sikich LLP on the penetration testing team
- Adjunct associate professor at MSOE
- Author and coordinator for CS4920 Information Security class at MSOE
- Over 20 years in the Information Technology field
- Last eight years as a penetration tester

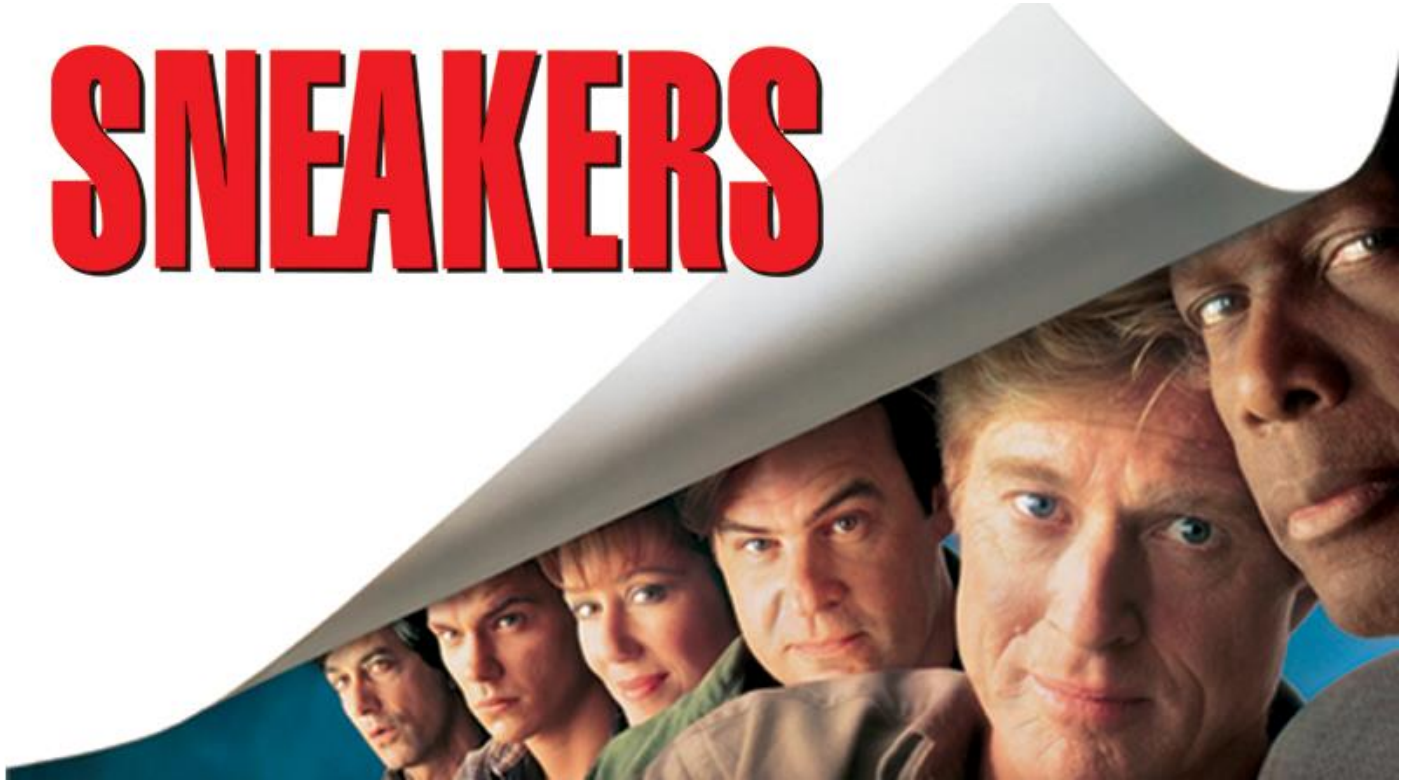
First things first

- This is not a sales pitch
- Yes, I work for a penetration testing firm, but I am not trying to sell you a penetration test (I'm not in sales)
- The goal is to walk through a typical penetration test so you can determine what type of testing you might need and what to expect during the engagement

- Bank Secretary: “So, people hire you to break into their places… to make sure no one can break into their places?”

- Bishop: “It's a living.”

- Bank Secretary: “Not a very good one.”



Agenda

I like to have discussions not just lectures
(this means I will be asking you questions too)

- Overview
- Setting up a penetration test
- The flow of a penetration test
- The output from a penetration test
- Key take-a-ways

Please ask questions anytime, no need to wait until the end

Overview

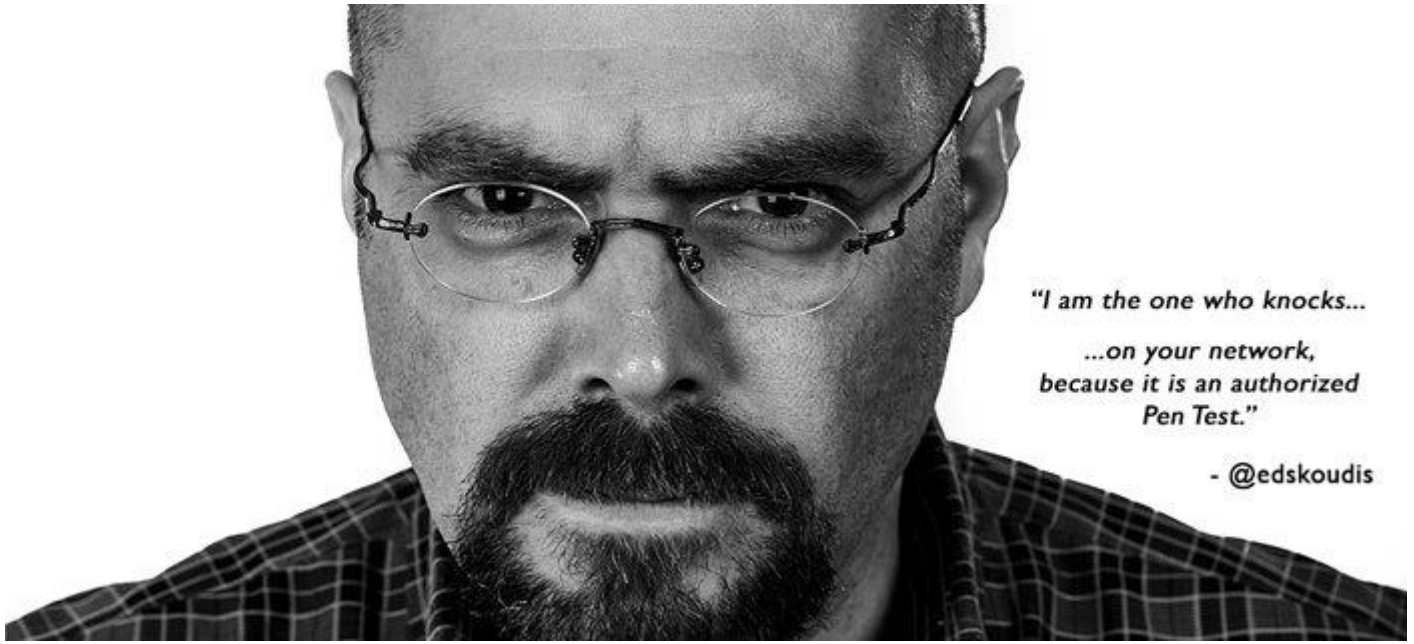
Question for you…

What do you think a penetration test is

What a penetration test is

A **penetration test** is a way for an organization to validate the security of their systems through manual or automated testing. Penetration tests typically will look for and exploit vulnerabilities within target systems.

Penetration tester is an individual or a team that has specific training and authorization to conduct penetration tests against a given organization.



Question for you…

What should not be done during a penetration test

What shouldn’t happen

- Your penetration tester should not attempt to break into systems you have not listed as “in scope” for the test
- The penetration tester should not perform actions that go against your wishes of the test
- Sensitive information should not be removed from your environment and posted online

So, you need a penetration test

DETERMINE WHAT PENETRATION TEST IS RIGHT FOR YOU

Types of penetration tests

- Covert (Sneaky)
- Overt (Out in the open)
- White box (All information is provided)
  - Normally used for compliance style testing
- Gray box (Some information is provided)
  - Normally used to test select sections of an organization
- Black box (No/little information is provided)
  - Normally used to test internal IT teams and controls

Defining the scope Q1

- Why are you looking to have a penetration test performed?
  - A compliance need such as PCI-DSS, HIPAA, SOC, GDPR
  - There has been a data breach
  - A new system was installed and have an upcoming go-live
  - You just love security and want to protect your systems

Defining the scope Q2

- What systems or technology should be tested?
  - Host exposed to the Internet such as firewalls, web servers, email servers, etc.
  - Web applications that are accessible from the Internet
  - Host on your internal network
  - Mobile applications
  - Physical locations
  - Embedded devices

Note: Don’t forget to test critical systems that are older

Defining the scope Q3

- What systems or technology should **NOT** be tested?
  - If the test is for compliance, the scope can be limited to only what is required to meet the compliance needs
  - Limit testing to a given network range
  - Exclude links to other partners and vendors
- Consider realistic testing (this is what a real attacker will do)

What is your timeframe?

- Knowing how soon you need to have the test completed is an important factor to take into consideration before starting
- Try to plan in advance to give the penetration test adequate time

What is your budget?

- Each penetration testing firm will charge different rates depending on the type of test you are looking for
- It is a good idea to know why you are looking to have a penetration test performed and what your budget is

Finding a penetration tester

- Google
- Word of mouth
- Check compliance sites

Penetration test risks

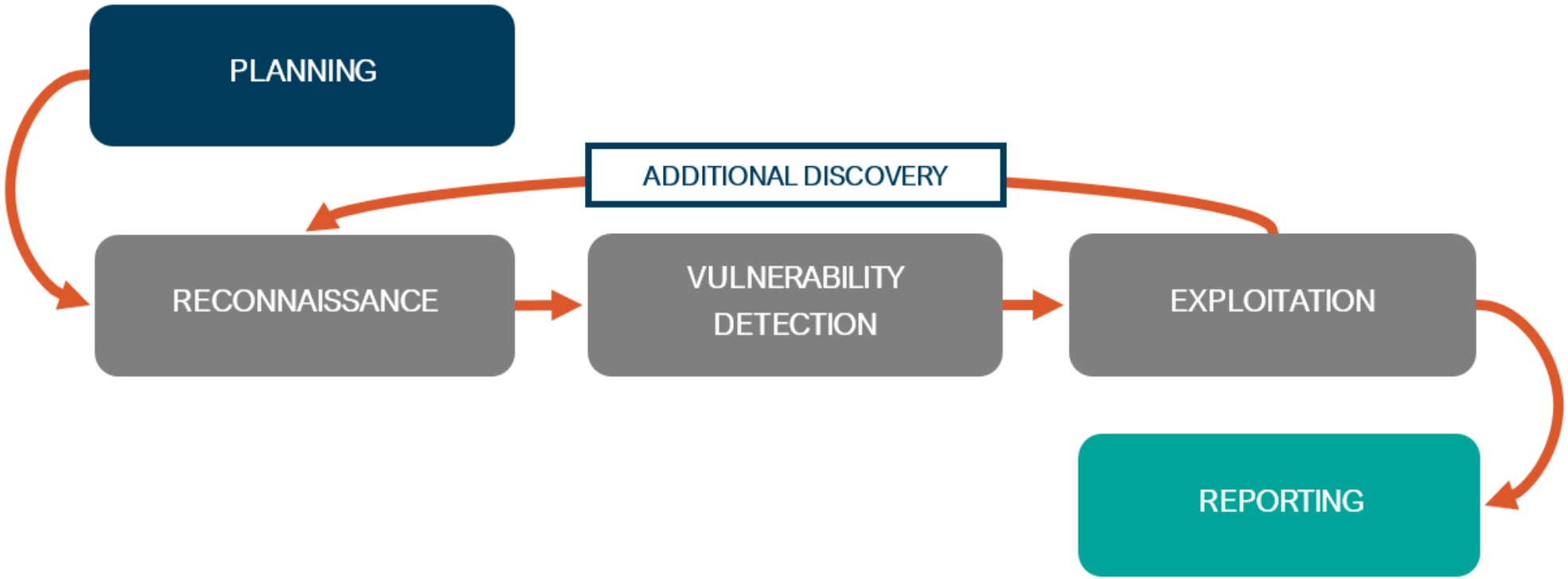
- There is always a risk that a penetration test will take down a system
- A penetration test is designed to find and take advantage of vulnerabilities within a system

Categorizing vulnerabilities

- Commonly, vulnerabilities are categorized based on the Common Vulnerability Scoring System (CVSS)
- The CVSS scale is from 0.0 to 10.0 and is broken into the Base Score, Temporal Score, and Environmental Score sections
- For general vulnerability categorization only the Base Score is considered
- The categories are typically High, Medium and Low (sometimes Critical)

The flow of a penetration project

Pentest methodology



Planning (Kick-off call)

- Now that you have determined the scope for the penetration test, there should be a call with the penetration testing team to discuss the scope and how testing will be performed
- Confirm what will be tested
- Confirm when testing will take place
- Confirm who will be notified of testing

Reconnaissance

- Look for company information on the Internet
  - LinkedIn
  - Data dumps
  - Dark web
- Examine targets for open ports and listening services
- Research unknown ports or services that have been identified

Vulnerability detection

- Use automated tools to look for known vulnerabilities
- Use manual testing to confirm automated tool findings
- Use manual testing to locate potentially unknown vulnerabilities

Exploitation

- This is a way to confirm the vulnerability exists and is truly a risk
- Determine if it is safe to attempt an exploit
  - If not, contact the client
- Attempt the exploit and record results
- If/when access is gained, go back to reconnaissance step

Reporting

- Review information gathered during testing
- Write a narrative (story) of how the attack was performed
- Detail out the technical information needed to correct any issues
- Make recommendations on other testing that could be beneficial
- Summarize the report at an executive level

Draft report delivery

- The report should contain information related to the observed vulnerabilities

Retesting

- Not a FULL retest
- Going back to review the findings that have been corrected

Final report delivery

- Review and incorporate any feedback from the client
- Updates are made to the draft report to reflect what has been corrected

Key take-a-ways

Things to remember

- Have a rules of engagement in writing
- Clearly define the scope you want to have tested
- Remember, you get what you pay for

Questions to ask

- What methodology do you use for testing?
- What is the proposed timeframe to conduct the test?
- What certifications do your penetration testers have?
- Do your testers have experience in our industry?
- What type of report can I expect in the end?
- Do you offer retesting?
- What happens if we go over the budget?

Questions?

Michael Vieau

MSOE

Vieau@msoe.edu

Michael.Vieau@sikich.com

https://michaelvieau.com

Twitter: @michael_vieau