Penetration Testing

Version Date: 24 SEP 2018

Student Guide Printable Format

Skills and Objectives

Table of Contents

Facilitation: Penetration Test Overview

Outcome:

- Identify the phases of a Penetration Test
- Plan and scope a Penetration Test at an "entry level"
- Write a formal report

Phases and Methodology of a Penetration Test

Introduction

There is an easily overlooked force multiplier in the world of Cybersecurity whether you perform duties within the OCO or DCO mission. History. As time goes on and more missions are completed, the historical record of those missions can be one of the most valuable resources to an ever changing force with new personnel coming, going, and missions changing potentially every day. The documentation becomes a pass down of lore, much like the written history of our ancestors so that many others may learn from the direct experiences of one.

Phase 1: Mission Definition

- Define mission goals and targets.
- Determine scope of mission.
- What networks are valid targets?
- What machines are valid targets?
- What attacks or exploits are authorized/appropriate?
- Define RoE.

Phase 2: Recon

- Information gathering about the target through public sources.
- Websites, job postings, search engines, etc.
- Done without touching the target.

Phase 3: Footprinting

- Accumulate data through scanning and/or interation with the target/target resources.
- Use a variety of scanning and fingerprinting to determine information about target networks and devices.

Phase 4: Exploitation/Initial Access

- Gain intial foothold into target network
- There is a more in-depth discussion that is done in exploitation research lesson

Phase 5: Post-exploitation

- Establish persistence
- escalate priveleges
- obfuscate
- cover your tracks
- exfiltrate target data

Phase 6: Document Mission

- Document and report mission details.

Write a Formal Report

Opnotes

- Technical details recorded while on mission
- Feeds into finished reports and products

Formalized Report

- **Executive Summary**
  The lead in for the report, and would also be the place for your bottom line up front (BLUF) recommendation based on the results. It provides the following layout for operations and penetration testing.
  - **mission**
  - **scope**
  - **parameters**
- **Technical Summary**
  The nuts and bolts of the Who, What, When, Where, Why, and How the penetration test was conducted. It should document actions at a technical level which would allow the test to be directly repeated for similar results. It should thoroughly reinforce the given recommendation in the executive summary.

Why should you create a Report

There are plenty of reasons as to why taking careful notes for any mission is important, Including historical data, evidence handling, operation hand off, repeatability, repudiation, Lessons learned, AARs, Covering your tracks, TTP and or SOP creation.

Continuity of Operations

- So you can pick up where you left off
- So someone else can pick up where you left off

Accounting of Actions Taken

- Documentation may be a legal requirement
- Prevent repudiation issues if you need to prove actions taken

Ability to Repeat Exact Actions

- Documenting what did work so it can be repeated

Troubleshooting and lessons Learned

- Documenting what didn't work

Operational Concerns

OFFENSIVE:
Primarily concerning ourselves with taking a careful record of everything that occurred, mostly so we can undo changes, or look for evidence of second and third tier effects resulting from our actions. Should something happen preventing us from being able to properly cover our tracks, the recorded notes will remind us of the things we'll need to take care of as soon as we're able to.

DEFENSIVE:
It's important to record the detailed notes on our investigation as a complex investigation can take many turns as clues are uncovered and require additional exploration and analysis. Thorough and detailed notes can help keep you on track so that you don't lose your place. It can also be important regarding evidence handling that the techniques, tools, and procedures used resulted in accurate information without possibly manipulating or altering the information leading to a faulty conclusion.

What should be included

Tools Used:
Along with the specific options, it's important to record exactly what tools were used and how

Timestamps:
It's important to know exactly when certain actions took place for purposes of deconflicting events outside of the given pentest. As an example, if during the pentest a real world attack also took place, you'd want to be able to differentiate which logs were explicitly caused by the pentesting team.

Success:
Noting what things worked and to what extent they were successful can be important when trying to reproduce your results

Failure:
Recording the things that didn't work become equally important when trying to make an overall security assessment. Depending on the purpose behind the mission, recording what did not work and when may be important when it comes to being able to cover your tracks.

Analytic Conclusions:
If you have to make any assessments or generate any courses of action that differed from the originally planned mission, you'll want to record those in your report as well. Showing the detailed result of when you made certain decisions based on what information you had available to you at the time is important when trying to walk somebody through your report and explaining your actions.

Unexpected Results:
When it comes to a Black Box pentest, there isn't a whole lot of information provided up front, if any at all. The ability to plan an operation relies heavily on what's found at each stage and

continuing accordingly. There will still likely be expected results along the way as you use tried and true exploitation techniques against uncovered vulnerabilities. When those expected results don't go the way you expect them to, it needs to be recorded so that they can be looked into. It could have failed as a result of another security product you were unaware of, or a recent signature update that you weren't aware of. Either way, it's something you want to record so it can be further tested and looked into for future tests. If you just lost a capability, future team is going to want to know about that.

Overall Impact

When detailing the technical summary SCREEN CAPTURES can be a helpful way to convey a large amount of information in a relatively concise and complete way. Be careful not to include too much in your captures. Extraneous information will take away from your graphic. Highlight or otherwise call-out relevant areas of the graphic if it's impossible to filter or trim it down first. Lastly, always CAPTION your screen captures so that there's no question for the reader as to what you're trying to show.

On the other hand, don't overly saturate your report with graphics that don't show anything of value. As an example, we all know what a desktop looks like. So unless you specifically need to show something ON the desktop of the compromised system, and it can't be easily conveyed through words, it might be better to leave that generic snapshot out of the report as it provides little value.