# Project-0: Penetration Testing

Kulesh Shanmugasundaram  
kulesh@isis.poly.edu  

Vikram Padman  
vikram@computer.org  

Posted: October 23rd  
Checkpoint-0 due: October 30th  
Checkpoint-1 due: November 6th

This is a two-week long assignment to evaluate the security of “The Bunker.” During the first week, your team (Tiger Team) will do an external penetration testing on a live network. In the following week, you will be given access to one of the machines (henceforth referred to as a host) in the network to do an internal penetration testing and you will augment additional results to your report from the new vantage point. Moreover, you will also do a penetration testing on the host itself. This assignment is broken into two segments therefore at the end of each week there will be a report due. Please have your reports in PS or PDF format and email the reports to me and Vikram on or before the due date.

---

## 1 Penetration Testing

There are no hard-and-fastened rules on how to do penetration testing. Over the years experience and trial-and-error have lead to several “methodologies.” Following is one such methodology. Reports should clearly indicate each section described below and explain the what, who, when, where, and how’s. Since you will be dealing with a live network be prepared to fend off any false accusations. Keep a comprehensive record (logs, audit trails) of what you are doing just in case someone brings up a complaint against you. (Rest assured that someone will!)

1. **Rules of Engagement.** Unlike assignments you have done in the past, this one requires that you pentest live networks. People depend on the reliability and integrity of the networks you test for their daily routines and do not appreciate any interruption or down time. Therefore, you must be extremely careful when testing these networks. Your immediate step is to identify the point of contact (POC) for the network (person who can authorize a pentest) and get a written permission from the POC on exactly what you will be doing and when. For details on what should be included in your request for authorization see [1]. You must explain what kind of attacks or tests you will be performing, how their network components may react to these tests, during what time you will be performing these tests and most importantly how to contact you in case of emergencies.

2. **Footprinting.** Once you have the authorization, gather as much information as you can about the network and its components. By the end of footprinting you should have a comprehensive map of the target network’s electronic perimeter. Following is an incomplete list of items that might be of interest:

   - MAC addresses, IP addresses, DNS names, WHOIS names, DNS servers, gateways, routers, switches, hubs, etc.
3. **Vulnerability Analysis.** Use information obtained during footprinting to formulate various strategies to exploit the network. Identify vulnerabilities and describe how to exploit them. If a component is not vulnerable give reasons why it is not vulnerable or under what circumstances it will be vulnerable. (For the report: for each service you find on the network, if the current configuration is not vulnerable name the previous vulnerable version and list at least five vulnerabilities.) Following is an incomplete list of items you might want to investigate:

- Clearly identify vulnerable services
- Identify scenarios for exploitation
- Augment a risk-factor for each vulnerability and list the targets in order of risk
- Develop a plan of attack (POA)

4. **Verification.** Carry out the POA developed during vulnerability analysis to verify that your hypothesis is in fact correct. For each successful attack, you must provide the following information:

- Victim/target
- The vulnerability
- How it was exploited, tools used, logs, audit record of exploit etc.
- Why it was exploitable
- Proof of exploitation
- Extensiveness of damages

5. **Risk Analysis.** With information you obtained during the verification phase refine the risks factored earlier during vulnerability analysis. During risk analysis you are identifying the risks posed by vulnerabilities to The Bunker. Describe each vulnerability found (in the order of risk, highest first) in detail and for each vulnerability describe the following list of (incomplete) items:

- What are the consequence of exploiting the vulnerability (downtime, DoS, loss of trade secrets etc.)
- What is the risk to the business due to vulnerability
- How to minimize the risk
- Recommendations on how to minimize the type of vulnerability in future

6. **Reporting.** Finally you will have to put all the information you gathered through out the pentest in a readable form. The report you submit to the POC of the The Bunker should include at least the following list of items:

- Executive Summary (Rate the overall security of the network and what the document is about)
- Footprinting & Vulnerability Analysis (What you found on the network and how vulnerable they are)
- Risk Analysis & Mitigation (Rate the overall security of the network, clearly state the risks, and how to minimize the risks, be specific)
- Risk Mitigation (give recommendations on policy, procedures, processes, and products)
- Conclusion (What should be done to keep the network safe(r) in future)
2 Handins

You will submit three reports in total for this assignment. One for the POC of the network, describing the outcome of the pentest at the end of the second week. Report for the POC is written for the management of The Bunker so tune it accordingly. Two additional reports for the graders. By the end of the first week the team will submit a report on the first three phases of pentest. At the end of the second week the team will refine the first report and add information about rest of the pentest. These reports should clearly indicate the tools used, how they were used, why, and the outcomes. For these reports, spare no detail.

References