Penetration Testing

UH ITMA & HATS

March 28, 2018

Table of Contents

1. Course Details

Title: UH Penetration Testing Course

Synopsis: During this three-day course, the student will learn how to conduct penetration testing. On the first day, the practitioner will learn how to use industry-standard tools like Metasploit, NMap, and Burp Suite to identify vulnerabilities and exploit them. How do companies put these skills to good use without breaking the law? We will discuss this topic, along with other legal and ethical issues relating to the use of your newly-acquired skills.

The second day will be an actual penetration test where the student will be allowed to interact with a lab consisting of a set of hosts. Following the penetration test, the student will compose and submit their findings as a **Penetration Test Formal Report**. The final report will be graded (details of the grading process will be discussed in section __ of this document).

The third day will be the conclusion of the course. This day will consist of the award and commencement ceremony. Awards will be granted to students who have scored the highest in the **Penetration Test Formal Report** followed by the discussion of the solutions to the vulnerable servers.

Table 1 – Additional Course Information

Additional Course Details	
Suggested Level Experience	Beginner to Intermediate
How this benefits you	All training participants will learn offensive security and penetration testing tactics that is found in the industry.
Course Duration	March 28th through the 30th (two consecutive 8-hour days and a half-day)
Number of Seats	39

Table 2 – Required Materials

Required Materials

Kali Linux Installed	Either a laptop or VM hosting a full installation of the Kali Linux distribution. It will be preferred to use the image provided via the URLs in the salutation email. o Kali Linux credentials: ▪ Username: root ▪ Password: toor
Vulnerable Servers	Vulnerable servers will be provided by the instructor for the students to use during the March 28th, 2018 course. • Students will be required to download two vulnerable server images o A windows XP with a vulnerable application ▪ Username: Administrator ▪ Password: password o A metasploitable server. ▪ Username: msfadmin ▪ Password: msfadmin • The images will be used for educational purposes • The links will be provided in the corresponding salutation email
Discord App with a Working Account	Students will need a discord application (preferably installed on a compatible smart phone) with a working account

2. Instructor Information

Orlando Galindo, OSCP, CISSP, PMP

Address:
Honolulu, HI 96816
Email: orlando.galindo.edu@gmail.com
Phone: (808) 561-6882

Orlando is an Operation Administrator for KPMG, a global network of professional firms providing Audit, Tax, Advisory, and Cyber-Security Services operating in 152 countries with over 189,000 employees. He is a subject matter expert in Software as a Service (SaaS) solutions and has over 10 years of Information Technology experience. Orlando earned his Bachelor's in Business Administration in Management Information Systems, graduating Magnum Cum Laude from the Shidler College of Business at the University of Hawai'i at Manoa.

He is an Information Technology Management Association (ITMA) and Golden Key International Honour Society Alumni. His certifications include Offensive Security Certified Professional (OSCP), Project Management Professional (PMP), Microsoft Certified Solutions Expert (MCSE): Cloud Platform and Infrastructure, Microsoft Certified IT Professional Enterprise Administrator, Windows Server 2008 Applications Infrastructure, Microsoft Certified Professional Developer, Microsoft Certified Technology Specialist, Microsoft Certified Professional, CompTIA A+, and ServiceNow Certified System Administrator. Orlando has held a Cisco Certified Network Associate certification, has provisionally passed the Certified Information Systems Security Professional (CISSP), and is currently pursuing the Certificate of Cloud Security Knowledge (CCSK) and the CISSP Information Systems Security Engineering Professional (CISSP-ISSEP).

Teaching Experience:

Instructor
Shakacon IX, Honolulu, Hawaii, 2017
Taught Introduction to Kali Penetration Testing with the Raspberry Pi. It was an ethical hacking course that used the Raspberry Pi as the primary device. The course covered the follow, but not limited to:

- Assistance in assembling the Raspberry Pi
- The installation of Kali Linux for the Raspberry Pi
- Configurations and customizations of Kali
- The use of popular pentesting tools
- Conducted a mock penetration testing against Metasploitable (a purposely-vulnerable Linux server) and a Windows XP system.

3. Class Agenda

Total Course Duration: 20 hours

Day 1, March 28th, 2018, 9 AM – 5 PM HST:

1. Introduction (15 minutes)
2. Legal/Ethics/Disclaimers (15 minutes)
3. Tools (90 minutes)
4. Overview of Penetration Testing Part I (60 minutes)
5. Lunch (60 minutes)
6. Overview of Penetration Testing Part II (220 minutes)
7. Documentation and Reporting (15 minutes)
8. Conclusion (5 minutes)

Day 2, March 29th, 2018, 9 AM – 5 PM HST:

1. Lab Introduction and Instructions given (15 minutes)
2. Questions and Answers - Q & A (15 minutes)
3. Penetration Testing (150 minutes)
4. Lunch (60 minutes)
5. Penetration Testing cont. (220 minutes)
6. Review of Submission of Documentation and Reporting (15 minutes)
7. Conclusion (5 minutes)

Day 3, March 30th, 2018, 9 AM – 12 PM HST:

1. Introduction (15 minutes)
2. Review of Lab Solutions, Report Feedback, and Q & A (120 minutes)
3. Award and Commencement Ceremony (30 minutes)

4. Conclusion (15 minutes)

4. Lab/Competition Details

This section explains the objectives of the Penetration Testing Lab Competition. Section 1 describes the requirements for the penetration test and Section 2 provides instructions for the post penetration test formal report submissions.

Section 1: Penetration Test Requirements

- The Lab will consist of four target machines that must be compromised
    - The IP addresses, pre-scanned NMap results, as well as the point values of the target hosts will be supplied to each individual on the day of the exam
    - Only the targets' IP addresses are to be exploited
    - Alteration or reconfiguration of the targets' system/.conf files that would render the target unusable, inoperable, and/or cause a denial of service for other individuals is strictly prohibited
- Each machine has a low-level and root or administrator accounts
    - Each low-level and root or administrator accounts has a medal.txt and trophy.txt respectively
    - The medal.txt and trophy.txt will have a hashed value (i.e. 9RVEiS1z7E6Lpg5JjBqZ) that needs to be recorded and submitted with the final **Penetration Test Formal Report**
- Some machines will require multiple exploitation techniques
- The use of vulnerability scanners are prohibited in the competition i.e. Nessus, OpenVas, NMap vulnerability scripts, etc.
- Use of Metasploit is restricted during the competition
    - Metasploit may only be used once against a single machine of choice
        - Only use **Auxiliary**, **Exploit**, **Post**, and **Meterpreter payload**, on that one target machine
        - Metasploit may be ran as many times as needed on the one machine of choice
        - If Metasploit fails after execution on that one machine, it may not be used on another

- The use of multi handler, msfvenom, pattern_create.rb, and pattern_offset.rb may be used on all targets

- Metasploit cannot be used to test for vulnerabilities

Section 2: Penetration Test Formal Report Requirements

- A professional comprehensive **Penetration Test Formal Report** will be required at the end of the Lab/Competition to qualify for rewards that are based on a grading system

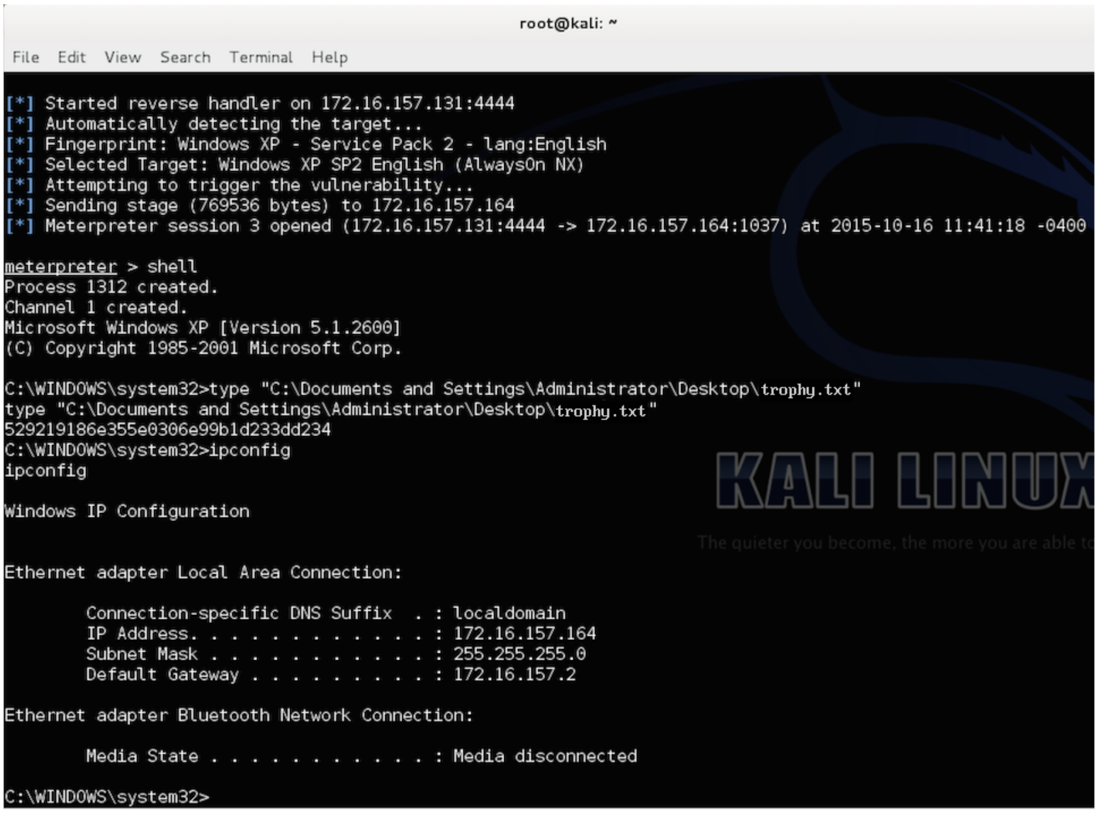
- The report will include the hash raw text values of all medal.txt and trophy.txt retrieved

- Screenshot requirements:

  - Corresponding screenshots of the medals and trophies must be included in the **Penetration Test Formal Report** via **type**, **cat**, or a **gui** window i.e. notepad, vim, etc.

  - Show the current user by running **echo %USERDOMAIN%\%USERNAME%**, **whoami**, etc.

  - Screenshots must include an **ifconfig** or **ipconfig** output i.e.


root@kali: ~
File Edit View Search Terminal Help
KALI LINUX
The quieter you become, the more you are able t

```
[*] Started reverse handler on 172.16.157.131:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (769536 bytes) to 172.16.157.164
[*] Meterpreter session 3 opened (172.16.157.131:4444 -> 172.16.157.164:1037) at 2015-10-16 11:41:18 -0400

meterpreter > shell
Process 1312 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>type "C:\Documents and Settings\Administrator\Desktop\trophy.txt"
type "C:\Documents and Settings\Administrator\Desktop\trophy.txt"
529219186e355e0306e99b1d233dd234
C:\WINDOWS\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : localdomain
        IP Address. . . . . . . . . . . . : 172.16.157.164
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 172.16.157.2

Ethernet adapter Bluetooth Network Connection:

        Media State . . . . . . . . . . . : Media disconnected

C:\WINDOWS\system32>
```

- Format of the report must be consistent and treated as quality material that can be submitted as a project deliverable to a client

- The organization of the **Penetration Test Formal Report** must be similar to the templated provided below:
  - https://drive.google.com/open?id=1S0C_pP_NzrgAWlxnIdBMOXBuLvK9GvZ4
- Total points for the competition and **Penetration Test Formal Report** is 330 pts
- Breakdown of the grading system is as follows:
  - Medals and Trophy point values for each vulnerable target will be listed on the NMap scan handouts on the day of the competition
  - There are four medals in the lab totaling a possible 60 pts.
    - There are three medals worth 10 pts. each and one worth 30 pts.
  - There are four trophies in the lab totaling a possible 140 pts.
    - There are three trophies worth 30 pts. each and one worth 50 pts.
  - Report will be graded as follows:
    - Name/username/ID/contact info = 3 pts.
    - Grammar = 15 pts.
    - Formatting = 10 pts.
    - Introduction = 5 pts.
    - Overview = 5 pts.
    - Requirements = 5 pts.
    - Information gathering = 5 pts.
    - Service enumeration = 5 pts.
    - Penetration = 40 pts.
    - Maintaining access = 10 pts.
    - House cleaning = 5 pts.
    - Additional items = 15 pts.
    - Presentation/visualization = 10 pts.
- The **Penetration Test Formal Report** will be due on March 29th, 2018 at 11 PM HST, no exceptions

- Once the **Penetration Test Formal Report** is submitted, the submission is final

For more information, contact us:

Orlando Galindo
Advisory, Customer Operations
Information System Security and Solution Architect
noob.elite.hacker@gmail.com

Stacy Lee
Advisory, Customer Operations
Business Analyst
stacylee@kpmg.com