

Last Edited: 6 January

# DOLOS HONEYPOT

## THE COMPLETE INSTALLATION GUIDE AND CONFIGURATION

VALLIE JOSEPH  
MARIST COLLEGE  
IBM JOINT STUDY



## Table of Contents

<b>TABLE OF CONTENTS.....</b>	<b>1</b>
<b>CONFIGURATION AND INSTALLATION .....</b>	<b>3</b>
SYSTEM REQUIREMENTS: .....	4
VERSION INFORMATION.....	4
(BACKGROUND SECTION TO GO HERE- SUMMARY OF OTHER HONEYPOTS).....	<b>ERROR! BOOKMARK NOT DEFINED.</b>
PACKAGES TO INSTALL.....	7
<i>Apache2 Modules</i> .....	7
<i>Ubuntu Packages</i> .....	7
<b>INSTALLATION GUIDE .....</b>	<b>7</b>
MOD_SECURITY .....	7
MOD_REWRITE.....	8
.HTACCESS .....	8
SYSLOG-NG AND SYSLOG-NG-CORE .....	9
<b>LOGIN PAGE.....</b>	<b>10</b>
ODL HONEYPOT LOGIN.....	10
DISPLAYING THE ERROR MESSAGE .....	11
HTML.....	11
<i>Ng-app and ng-Controller:</i> .....	11
<i>Ng-Bind:</i> .....	11
Angular: .....	11
<i>Scope.name</i> .....	11
THE COMMON APPROACH: ISSUES AND SOLUTIONS.....	12
<i>The Issue: Redirecting</i> .....	12
<i>The Solution: AJAX</i> .....	12
Detailed Solution .....	13
AJAX/jQuery .....	13
<i>Issue: Difference in Page Calls</i> .....	13
<i>Solution: Page Masking with Symbolic Links</i> .....	14
Symbolic Link Configuration.....	14
Symbolic Links .....	14
Mod_rewrite Configuration .....	14
.htaccess .....	14
Break down of the .htaccess configuration .....	15
<i>Issue: Server honeypot is on differs from the server the honeypot is mimicking</i> .....	16
Headers: .....	16
<i>Solution: Mod Security</i> .....	17
Configuring Mod Security.....	17
<b>GATHERING AND PARSING ATTACKER INFORMATION.....</b>	<b>19</b>
<b>PARSING ATTACKER INFORMATION.....</b>	<b>20</b>
PASSING VARIABLES FROM LOGIN TO SERVER .....	20
Optional: Database Backup .....	20
MySQL Connect to Remote Server .....	21
Syslog-ng: Pushing to Syslog.....	21
What is Syslog-ng?.....	21

Installing Syslog-ng .....	22
Configuring Syslog-ng (Client-Host) .....	22
Configuring Syslog-ng (Host-Server) .....	23
Optional: Sending Logs to Multiple Destinations .....	24
Host-Server .....	24
<i>Client-Server</i> .....	24
Testing .....	34
<b>FINAL SCANS .....</b>	<b>35</b>
ZENMAP .....	35
NIKTO .....	74
UNISCAN .....	75
MASSCAN .....	78
DnsTRACER .....	79
DOTDOTPWN .....	87
ENUM4LINUX .....	90
AMAP .....	92
<b>TROUBLESHOOTING .....</b>	<b>94</b>
COMMON ERRORS: .....	94
<i>ModSecurity</i> : .....	94
Mod_security is not installing .....	94
I am unable to verify mod_security (receiving an error like: apachectl: command not found) .....	94
<i>ModRewrite</i> : .....	95
While installing Mod_rewrite, I receive a the following sudo error: 'a2enmod: command not found' .....	95
<i>Syslog/ Syslog-ng</i> : .....	95
Syslog-ng "Error binding socket; addr='AF_INET(\$CLIENT)', error ='Cannot assign requested address (99)' Error initializing message pipeline.....	95
Error resolving reference; content='source', name='s_network', location='/etc/syslog-ng/syslog-ng.conf:135:21' <b>or</b> Error resolving reference content='string', name='string', location ='/etc/syslog-ng.conf:line#:column#' (where string is anything within the single quotes) .....	96
WARNING: Your configuration file uses an obsoleted keyword, please update your configuration; keyword='log_prefix', change='program_override' .....	96
My packets aren't sending .....	96
<b>HELPFUL LINKS AND RESOURCES: .....</b>	<b>100</b>
LEARN REGEX: .....	100
MOD REWRITE: .....	100
MOD SECURITY: .....	100
APACHE: .....	100
AJAX AND ANGULAR HELP: .....	100
SYSLOG-NG: .....	100
<b>WORKS CITED .....</b>	<b>101</b>

## Background

### Abstract:

Over the past few years, the internet has experienced some of the most massive attacks than ever before. With attack types such as DDoS (distributed denial of service), brute force, the use of botnets and malware attacks, it becomes increasingly difficult to rely on only one layer of defense. Both hackers and their equipment are adapting quickly to new cyber security initiatives, cracking their defenses sometimes in a matter of days. So how do we go about remedying this issue? While it may be impossible to fully secure a network, system administrators can deploy as many layers of defense as their systems are capable of. This document focuses on a single layer: the honeypot.

### Introduction: Meet Dolos

Sans defines a cyber-security honeypot as “decoy servers or systems setup to gather information regarding an attacker or intruder into your system”.<sup>1</sup> While honeypots are not a stand-alone method of security, they can be very powerful aids analyzing attacker’s specific to your system, which will ultimately allow the system administrators to deploy adaptive defense mechanisms. In our case, the honeypot we’ve created for an SDN controller (OpenDaylight) which has been given the name Dolos, mimics the exact look and feel of the real controller, although it has a few very important differences. With each login attempt the attacker makes, Dolos will crawl their browser, operating system, username, password and port information, the logistics of which will explained in greater detail within this document. For example, Example Law Firm™ may notice that botnets from China tend to attempt a DDoS attack on specific days or specific times. The honeypot will crawl the information of the attackers, parse it into a format that can be understood by a cyber-security initiative named Longtail, which organizes the information in user-friendly graphs and attack patterns that will help the company modify its defenses as necessary. Longtail “a program that analyzes ssh brute force attacks and statistically quantifies them based on IP addresses used, Accounts, passwords, AND account/password pairs, and (what nobody else is doing at the moment) analyzing attack patterns for commonality and number of times used.”. This document explains how this was made to be possible, along with general instructions concerning the creation of your own custom honeypot.

---

<sup>1</sup> (Even 2000)

## Configuration and Installation

### System Requirements:

<b>OS:</b>	<b>Debian-Based Linux Distro</b>
<b>PHP:</b>	5.5 or Greater
<b>MySQL:</b>	5.5 or Greater
<b>Apache2</b>	2.4.0 or Greater

### Version Information

<b>syslog-ng</b>	<b>3.5.3</b>
<b>Installer-Version:</b>	3.5.3
<b>Revision:</b>	3.5.3-1 [@9695e81] (Ubuntu/14.04)
<b>Compile-Date:</b>	Dec 25 2013 23:13:11
<b>Available-Modules:</b>	afsql,afsocket-tls,afsocket,confgen,linux-kmsg-format,afmongodb,cryptofuncs,afamqp,dbparser,csvparser,afuser,afsocket-notls,redis,affile,syslogformat,afsmtp,basicfuncs,afstomp,json-plugin,tfgeoip,system-source,afprog
<b>Enable-Debug:</b>	off
<b>Enable-GProf:</b>	off
<b>Enable-Memtrace:</b>	off
<b>Enable-IPv6:</b>	on
<b>Enable-Spoof-Source:</b>	on
<b>Enable-TCP-Wrapper:</b>	on
<b>Enable-Linux-Caps:</b>	on
<b>Enable-Pcre:</b>	on

<b>PHP</b>	<b>5.5.9</b>	<b>1ubuntu4.17 (cli)</b>
<b>Copyright (c)</b>	<b>1997</b>	2014 The PHP Group
<b>Zend Engine</b>	<b>v2.5.0, Copyright (c) 1998</b>	2014 Zend Technologies with Zend OPcache v7.0.3, Copyright (c) 1999 2014, by Zend Technologies

<b>mysql Ver</b>	<b>14.14 Distrib 5.5.49, for debian-linux-gnu (x86_64) using readline 6.3</b>
------------------	---

<b>Server version:</b>	<b>Apache/2.4.7 (Ubuntu)</b>
<b>Distributor ID:</b>	Ubuntu
<b>Description:</b>	Ubuntu 14.04.3 LTS
<b>Release:</b>	14.04

Codename: `trusty`

## OpenDaylight Distribution

## Lithium

Zenmap	7.12
Nikto	2.1.6
LibWhisker	2.5
db_404_strings	2.003
db_content_search	2.000
nary	1.0
db_drupal	1.00
db_embedded	2.004
db_favicon	2.010
db_headers	2.008
db_httptoptions	2.002
db_multiple_index	2.005
db_outdated	2.017
db_parked_strings	2.001
db_realms	2.002
db_server_msgs	2.006
db_subdomains	2.006
db_tests	2.021
db_variables	2.004
nikto_apache_expect_xss.plugin	2.04
nikto_apacheusers.plugin	2.06
nikto_auth.plugin	2.04
nikto_cgi.plugin	2.06
nikto_clientaccesspolicy.plugin	1.00
nikto_content_search.plugin	2.05
nikto_cookies.plugin	2.05
nikto_core.plugin	2.1.5
nikto_dictionary_attack.plugin	2.04
nikto_drupal.plugin	1.00
nikto_embedded.plugin	2.07
nikto_favicon.plugin	2.09
nikto_fileops.plugin	1.00
nikto_headers.plugin	2.11
nikto_httptoptions.plugin	2.10
nikto_ms10_070.plugin	1.00
nikto_msgs.plugin	2.07
nikto_multiple_index.plugin	2.03
nikto_negotiate.plugin	2.00
nikto_outdated.plugin	2.09
nikto_parked.plugin	2.00

nikto_paths.plugin	2.00
nikto_put_del_test.plugin	2.04
nikto_report_csv.plugin	2.07
nikto_report_html.plugin	2.05
nikto_report_nbe.plugin	2.02
nikto_report_sqlg.plugin	2.00
nikto_report_text.plugin	2.05
nikto_report_xml.plugin	2.05
nikto_robots.plugin	2.06
nikto_shellshock.plugin	2.01
nikto_siebel.plugin	1.00
nikto_sitefiles.plugin	2.00
nikto_ssl.plugin	2.01
nikto_subdomain.plugin	2.01
nikto_tests.plugin	2.04

**Uniscan****6.3****Masscan**

**version 1.0.3 (**  
<https://github.com/robertdavidgraham/masscan>  
**)**

<b>Compiled on:</b>	Mar 5 2016 18:46:21
<b>Compiler:</b>	gcc 5.3.1 20160224
<b>OS:</b>	Linux
<b>CPU:</b>	unknown (64 bits)
<b>GIT version:</b>	unknown

**DNSTracer****1.8.1****DotDotPwn****3.0****Enum4Linux****0.8.9****Amap****5.4.1**

## Packages to Install

The installation of the following packages are recommended for the purpose of this honeypot configuration:

### Apache2 Modules

- Mod\_security
- Mode\_rewrite
- Mod\_headers

### Ubuntu Packages

- Syslog-ng / Syslog-ng-core
- LAMP Stack (Linux Apache MySQL PHP)
- Postgresql

## Installation Guide

Before installing any of the following packages, ensure that your system's minimum configurations at least match the system that is used in this tutorial. You can find these specifications within the System Specs section located in System Requirements.

### LAMP Stack

In this instance of Dolos, a majority of our code is written in PHP. Dolos also relies heavily on Apache specific modules. That begin said, it would be wise to install the LAMP stack in our environment. The following steps will walk you through the LAMP stack installation:

To make sure you are running the latest instance of Ubuntu (or the distribution of your choice) , run the following command

```
sudo apt-get update
```

Then, install Apache

```
sudo apt-get install apache2
```

Then, install PHP5 or the most current version of PHP alongside MySQL

```
sudo apt-get install mysql-server libapache2-mod-auth-mysql php5-mysql
```

```
sudo apt-get install php5 libapache2-mod-php5 php5-mcrypt
```

### Mod\_Security

To install mod security, follow these steps:

In the terminal, enter the following commands:

```
sudo apt-get install libxml2 libxml2-dev libxml2-utils
```



```
sudo apt-get install libaprutil1 libaprutil1-dev
```

Then, to ensure the module loaded, enter the next command:

```
sudo apachectl -M | grep --color security2
```

You should receive a result that resembles the following (Note, if you see a warning like the one below, ignore it):

```
openflow@OpenDayLight-Lithium:~$ sudo apachectl -M | grep --color security
[Thu Jun 09 09:02:41.147102 2016] [so:warn] [pid 32652] AH01574: module php5_module is already loaded, skipping
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 10.11.17.133. Set the 'ServerName' directive globally to suppress this message
security2 module (shared)
```

After a package-module is installed or configured, apache must be restarted. The following command will be used frequently when configuring your system for the honeypot:

```
sudo service apache2 restart
```

[Mod\\_Rewrite – or maybe tell them to activate it here. ldk bro](#)

The rewrite module will require no actual installation, so long as the user has apache2 installed and configured on their machine. If this is the case, they will only need to enable the module.

To activate the rewrite module, use the following command and restart apache2:

```
sudo a2enmod rewrite2
```

In order to use mod\_rewrite, however, you will need to configure apache2's as well as create an .htaccess file.

[.htaccess \(to do: troubleshoot not being able to create file –as su or root, make alternative touch step\)](#)

The htaccess will hold the configuration settings for Mod\_Rewrite, as well as any redirect rules. Follow the instructions below to create your htaccess file:

Navigate to the directory your html files are stored (i.e. /var/www/html) and create a file with the name “.htaccess”

```
cat > .htaccess
```

Restart apache to make sure that it is still operational To check to see if your htaccess file was created successfully, check the folder you placed the file in with the list all command. You should see something akin to the below image:

```
root@OpenDayLight-Lithium:/var/www/html# ls -a
. .. assets .htaccess index-2.html index.html index.html# restconf src testing vendor
root@OpenDayLight-Lithium:/var/www/html#
```

---

<sup>2</sup> (Sverdolv 2012)

Syslog-ng is a system log manager. It allows clients to send their syslogs to remote hosts in an effective, easy to set up method. In this case, syslog will be used to manage logs sent by the honeypot into the syslog server.<sup>3</sup>

```
sudo apt-get install syslog-ng-core
```

(more details in Syslog Section Below)

[illegible]

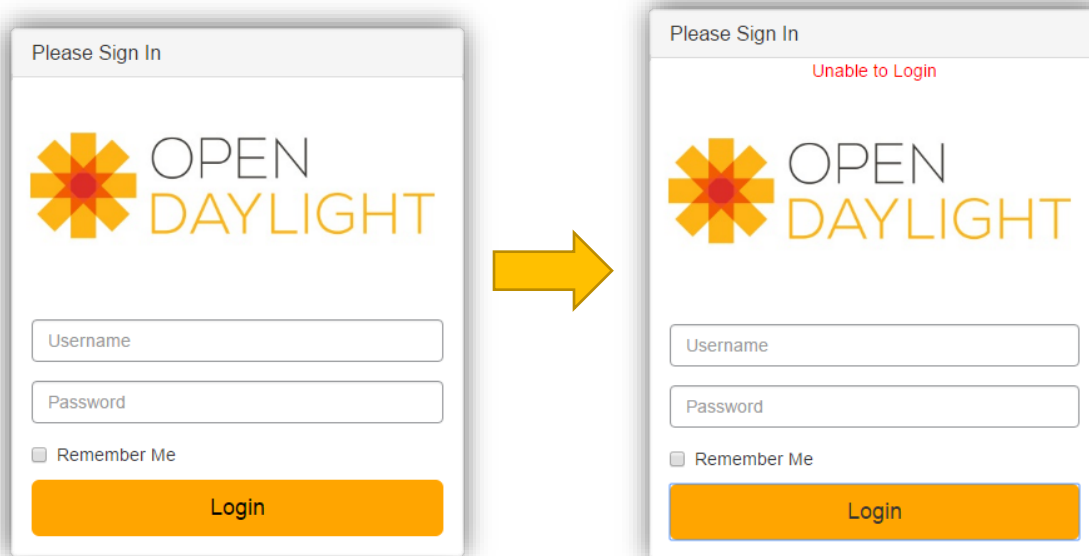
<sup>4</sup> (Syslog-ng, Chapter 4. The syslog-ng OSE quick-start guide 2015)

## Login Page

### ODL Honeypot Login

The OpenDaylight SDN Controller Honeypot was designed to mimic the look and feel of the real controller.

It utilizes the same HML elements/divs that the real controller, going so far as to even display the login error message using the real controller's methods.



## Displaying the Error Message

HTML<sup>5</sup>

```
<div ng-app="myApp" ng-controller="myCtrl">
    <p style="color: red; text-align:center;" ng-bind="name"></p>
```

The above code can be broken into the following interactions:

### Ng-app and ng-Controller:

Required for AngularJS to locate and interact in a specific area of the page.

### Ng-Bind:

Used by AngularJS to 'bind' the login error string. The app communicates with the controller who then delivers the information to the bind directive

### Angular:

```
var app = angular.module('myApp', []);
    app.controller('myCtrl', function($scope) {
        $scope.name;
        $scope.sendLogin = function() {
            $scope.name = "Unable to Login";
        }
    });
```

### Scope.name

Here, the scope is being initialized to allow for later input by a function called "sendLogin." This function is defined using the ng-click directive within the submission button.

```
<button ng-click="sendLogin()" class="btn btn-lg btn-orange btn-block">Login</a>
```

The click directive tells AngularJS to call the function within the appropriate controller scope, which places the message within the top of the login form.

---

<sup>5</sup> (W3Schools 2016)

Please Sign In

Unable to Login

## The Common Approach: Issues and Solutions

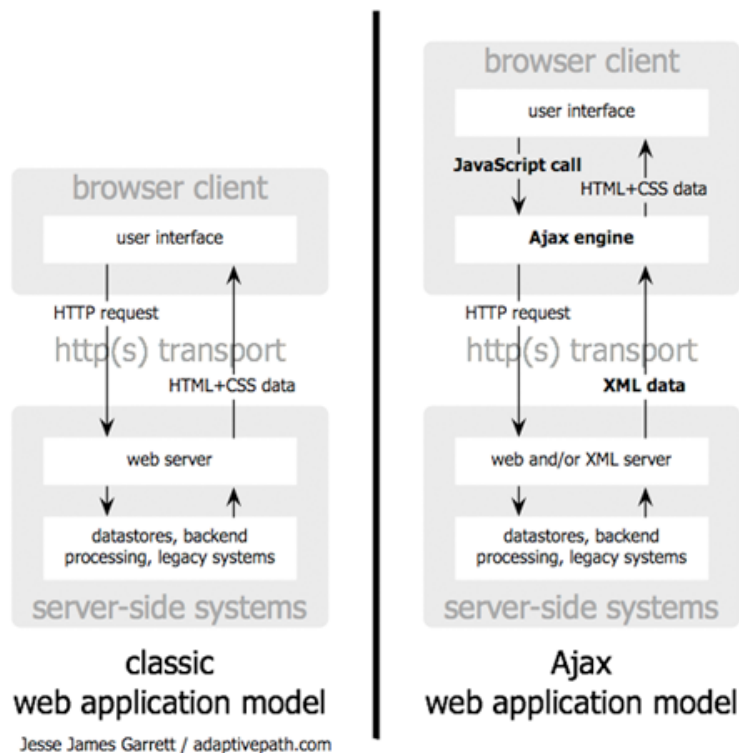
### The Issue: Redirecting

Using the common form approach (form action='url\_goes\_here' method='post/get') will ultimately redirect the user to the PHP page where their information is parsed and stored. To an attacker, this will make the program an obvious decoy which they will then stop attacking, this would be unfavorable in this instance.

### The Solution: AJAX

We will therefore need to employ a technique named AJAX, which stands for Asynchronous JavaScript and XML

Here is a diagram to provide a quick understanding of how AJAX works:<sup>6</sup>



<sup>6</sup> (Garret n.d.)

### Detailed Solution

#### AJAX/jQuery

```
$('.btn-block').click(function () {  
    var usernames = $("input[name = 'usernames']").val();  
    var passwords = $("input[name = 'passwords']").val();  
    var dataString = '&usernames=' + usernames + '&passwords=' + passwords  
    $.ajax({  
        type: "POST"  
        , url: "restconf/modules"  
        , data: dataString  
        , success: function () {  
            //Testing if variables are going through, uncomment to test  
            //console.log(usernames);  
            //console.log(passwords);  
            //console.log('success');  
        }  
    });  
});
```

In this solution, AJAX is initiated and parsed through jQuery. After the attacker inputs their attempted username and password combination, jQuery will take the value of the associate input fields:

```
var usernames = $("input[name = 'usernames']").val();
```

After all of the variable values are created, they are stored within a variable named 'dataString'. This variable works something like an associated array, where the values are prefaced with their names:

```
var dataString = '&usernames=' + usernames + '&passwords=' + passwords
```

Datastring is then used to call upon our previously stored values and push them to our PHP page, which leads us to our next potential problem.

#### Issue: Difference in Page Calls

When the attacker spider crawls the website, they will be able to see all pages that have been called through the page. Although the page is no longer being redirected or refreshed, when browsing the network tab in the most recent versions of Google Chrome, Mozilla Firefox, and Microsoft Internet Explorer, and Microsoft Edge all display the presence of the PHP page. Since the real controller has no page of the PHP variety, an attacker may interpret this difference and discontinue their use of the honeypot.

### Solution: Page Masking with Symbolic Links

The most effective solution in this case would be to rewrite the page as something that would appear on the real controller. When browsing through the real ODL controller, after the user submits their credentials, a file named “modules” within the “restconf” directory is called. Typically, this file is used to display virtual router data. However, since the honeypot does not actually connect to any of our software, there is no need to install and configure the virtual routers for the sake of spoofing the honeypots authenticity. Instead, a combination of linux’s symbolic links (also known as symlink or softlink) and apache2’s `mod_rewrite`.

### Symbolic Link Configuration

The following instructions will depict the method in which `mod_rewrite` is used to rename and hide a page’s title and extension:

#### Symbolic Links

```
root@OpenDayLight-Lithium:/var/www# find . -type l -ls
692799 0 lrwxrwxrwx 1 root root 31 Jun 1 13:08 ./html/testing/restconf/modules2 -> /var/www/html/src/checkUser.php
692801 0 lrwxrwxrwx 1 root root 31 Jun 1 13:08 ./html/testing/restconf/modules4 -> /var/www/html/src/checkUser.php
692816 0 lrwxrwxrwx 1 root root 31 Jun 1 13:08 ./html/testing/restconf/modules.php -> /var/www/html/src/checkUser.php
656262 0 lrwxrwxrwx 1 root root 32 Jun 2 13:04 ./html/restconf/modules -> /var/www/html/src/checkUser2.php
root@OpenDayLight-Lithium:/var/www#
```

- Symbolic links are simply user-defined references that can be created to refer to a directory or file by a name other than what it was originally created with.
- In this case, a symbolic link is needed to hide our php page as something else (a file within the “restconf” directory named “modules” in this instance)
- To create a symbolic link, follow the below syntax:

```
ln -s /the/link/that/you/want/to/display/ /the/real/file/you/are/referencing
```

- Syntax used:

```
ln -s /var/www/html/src/checkUser2.php /html/testing/restconf/modules
```

- Although this masks the page as an extensionless mask, it will still appear within each browser’s network tab. This issue will resolve itself once the rewrite module is applied correctly.

### Mod\_rewrite Configuration

The following instructions will depict the method in which `mod_rewrite` is used to rename and hide a page’s title and extension:

Before continuing on with the `mod_rewrite` configuration, make sure that you have `mod_rewrite` enabled. To enable the module, use the following command:

```
sudo a2enmod mod-security
```

#### .htaccess

- Navigate to the .htaccess file
- In the file, insert the following configurations:

```
Options +FollowSymLinks -Multiviews
```

```
RewriteRule ^restconf/modules$ src/checkUser2.php [L]
```

#### Break down of the .htaccess configuration

```
Options +FollowSymLinks -Multiviews
```

- “Options” in the case is a directive of apache. Within .htaccess, “options” dictates the rules of what is allowed or enabled within the server.
- With this in mind, the “FollowSymLinks” option refers to whether or not the following of symbolic links is allowed. Using either the “+” or “-” will determine whether or not the option is allowed
- “MultiViews” will determine how the file-look will be handled. For the purpose of the honeypot, “multiviews” needs to be disabled.

```
RewriteRule ^restconf/modules$ src/checkUser2.php [L]
```

- Mod\_rewrite’s rewrite rules give the apache server directions on how to handle specific pages. Alternatively, if there are multiple pages that require the rule to be used (giving that they all follow the same pattern), rewrite condition (RewriteCond) can be used alongside it.
- Both RewriteRule and RewriteCond use RegEx or RegularExpressions syntax to determine what page or pattern the rule will be applied to.
  - Note: To better understand RegEx syntax, there is a link within the helpful resources section of this documentation

After it’s finished, .htaccess should look something like the following:

```
Options +FollowSymLinks -Multiviews
RewriteEngine On
#RewriteRule ^/?index.html$ test.php [L]
#RewriteRule "^/index\.html$" "/index.html#/login" [R]

#Working Test
RewriteRule ^restconf/modules$ src/checkUser2.php [L]

#RewriteRule ^restconf/modules$ restconf/checkUser2.php [L]

#RewriteRule ^checkUser\.php$ checkUser.js [L]
#RewriteRule ^/?testing/([a-z/.]+)$ testing/restconf/modules/$1 [R=301,L]
```

The commented lines are purely for testing purposes. Should the uncommented line prove unsuccessful, attempt to use the different formats that are commented out.




## Issue: Server Honeypot Is on Differs from the Server the Honeypot is Mimicking

The final step in masking all differences from the attacker is to mask the server headers. Typically, a webpage will have three separate header categories. The header section can be found under any browser's 'Network' tab within the developer tools.

### Headers:

#### ▼ General

**Request URL:** http://10.11.17.135:8080/index.html  
**Request Method:** GET  
**Status Code:**  200 OK  
**Remote Address:** 10.11.17.135:8080

General usually displays the URL in which the page was requested from, the method in which the page was requested with, the page's status code and finally it's remote address.

#### ▼ Response Headers [view source](#)

**Accept-Ranges:** bytes  
**Connection:** Keep-Alive  
**Content-Encoding:** gzip  
**Content-Length:** 2034  
**Content-Type:** text/html  
**Date:** Thu, 16 Jun 2016 12:41:15 GMT  
**ETag:** "1856-534f066243e80-gzip"  
**Keep-Alive:** timeout=5, max=100  
**Last-Modified:** Fri, 10 Jun 2016 18:06:34 GMT  
**Server:** Jetty(8.1.15.v20140411)  
**Vary:** Accept-Encoding

The next category, 'Response Header', holds more specific information such as cache validation and managing (cache-control), content details, server names and the status of said server. These are the items the server gives in response to the request, hence it's name.<sup>7</sup>

---

<sup>7</sup> (Grigorik 2016)

The last category, 'Request Header' is what the page is requesting of the server. It holds information such as the location of the page, host information, the type of browser being used, how cookies are stored and other items of that nature. <sup>8</sup>

---

▼ Request Headers [view source](#)

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8
Cache-Control: max-age=0
Connection: keep-alive
Host: 10.11.17.135:8080
If-Modified-Since: Fri, 10 Jun 2016 18:06:34 GMT
If-None-Match: "1856-534f066243e80-gzip"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.84 Safari/537.36
```

### Solution: Mod Security

You may notice that the above server section within the header response tells the user the server is Jetty, a java serverlet container, although the server this honeypot utilizes is an Apache server. This is made possible through mod\_security. The relatively straight-forward process can be found below:

### Configuring Mod Security

Navigate to the configuration files of mod security (typically located in /etc/apache2/conf.d/security, however also check /etc/apache2/conf-enabled/security.conf if you are unable to locate the file)

```
openflow@OpenDayLight-Lithium:/etc/apache2/conf-enabled$ ls
charset.conf  javascript-common.conf  localized-error-pages.conf  other-vhosts-access-log.conf  security.conf  serve-cgi-bin.conf
```

---

<sup>8</sup> (Guzel 2009)

After opening the file, something akin to the image to the right should be displayed.

Search within the file for a line that begins 'ServerTokens' right below 'ServerTokens OS'. It will most likely be turned off, however it needs to be set to 'Full'. Adjust the line to the below configuration:

```
ServerTokens Full
```

Next, locate SecServerSignature which should be directly below 'ServerSignature' and adjust it to match the following configuration:

```
SecServerSignature Your_Server_Name_Here
```

Should you find a need to edit any other server response or request headers, this is most likely the location to do so.<sup>9</sup>

```
# Disable access to the entire file system except for the directories that
# are explicitly allowed later.
#
# This currently breaks the configurations that come with some web application
# Debian packages.
#
#<Directory />
#   AllowOverride None
#   Order Deny,Allow
#   Deny from all
#</Directory>
#
# Changing the following options will not really affect the security of the
# server, but might make attacks slightly more difficult in some cases.
#
ServerTokens ProductOnly
# This directive configures what you return as the Server HTTP response
# Header. The default is 'Full' which sends information about the OS-Type
# and compiled in modules.
# Set to one of: Full | OS | Minimal | Minor | Major | Prod
# where Full conveys the most information, and Prod the least.
#ServerTokens Minimal
ServerTokens OS
ServerTokens Full
#
# Optionally add a line containing the server version and virtual host
# name to server-generated pages (internal error documents, FTP directory
# listings, mod_status and mod_info output etc., but not CGI generated
# documents or custom error documents).
# Set to "EMail" to also include a mailto: link to the ServerAdmin.
# Set to one of: On | Off | EMail
#ServerSignature Off
ServerSignature Off
#
SecServerSignature Jetty(8.1.15.v20140411)
# Allow TRACE method
#
# Set to "extended" to also reflect the request body (only for testing and
# diagnostic purposes).
#
# Set to one of: On | Off | extended
TraceEnable Off
#TraceEnable On
```

---

<sup>9</sup> (Farmad unknown)

## Gathering and Parsing Attacker Information

In order to gather the attack information discreetly, there are a variety of actions that must be done. The attacker will first access the login screen and most likely attempt to brute force their way into the system. As the honeypot is not actually connected to the ODL controller, the attacker will be unable to successfully complete a login.

The attacker will, however, send their inputted information as well as have their browser and IP information crawled to be later inserted into the Syslog Server. Below, you will see a diagram detailing the process:

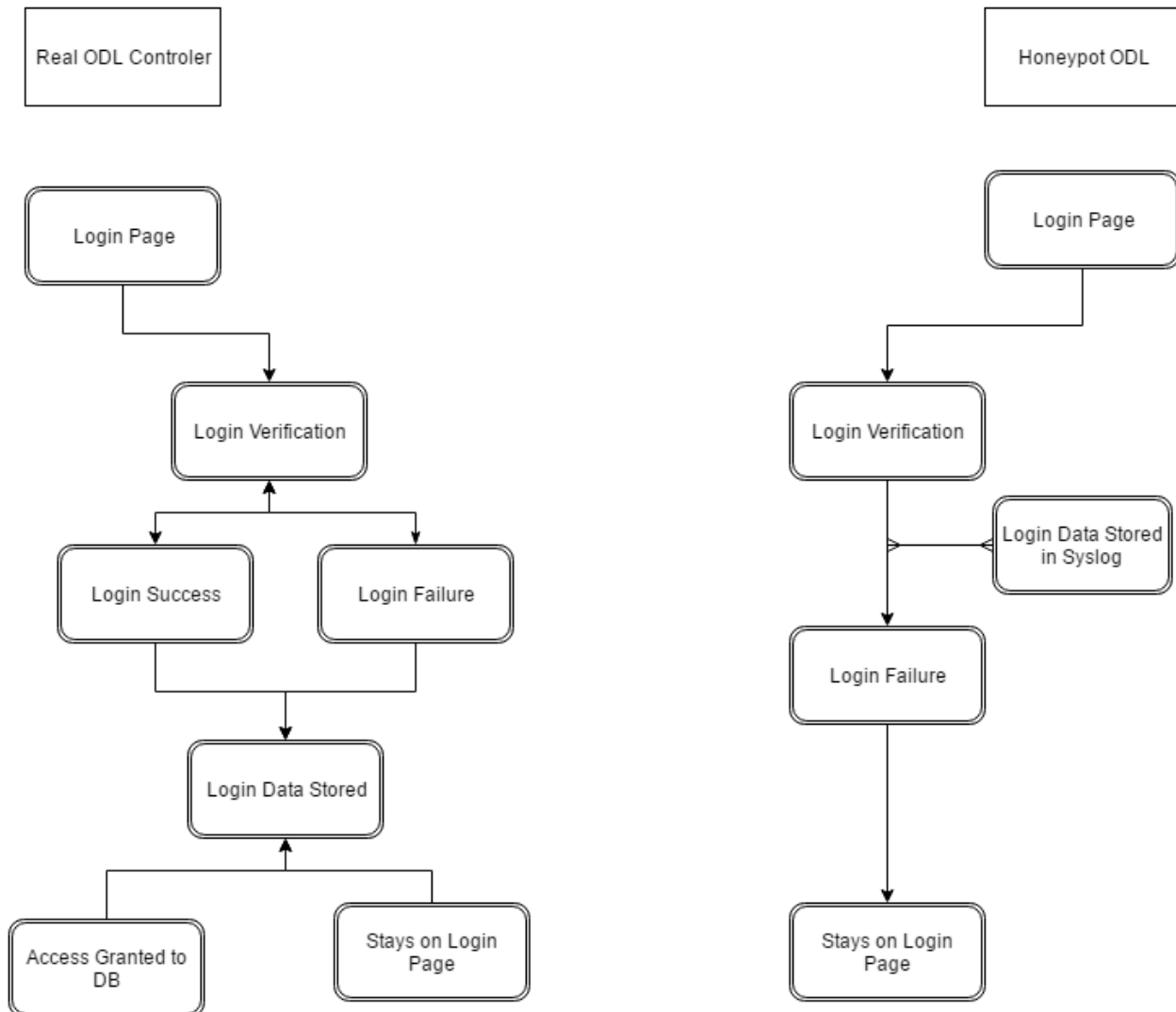


Figure 1 Honeypot Diagram

## Parsing Attacker Information

Now that the attacker no longer has the ability to notice our PHP script, we can set it up so that it grabs specific information from the attacker.

There are three items that need to be completed in order to correctly send information to the server:

- Passing variables from the HTML login to be prepared to send to the server
- Grabbing the IP address of the attacker
- Send data to both database and syslog server

```
Success: A proper connection to MySQL was made! The my_db database is great.
Host information: 10.11.17.218 via TCP/IP
```

```
Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.84 Safari/537.36
```

```
2016-06-10T02:06:57 -04:00
```

```
Success: A proper connection to MySQL was made! The my_db database is great.
```

```
Host information: 10.11.17.218 via TCP/IP
```

```
There is no match for test in the database.
```

```
Creating an entry for test.
```

```
test was created successfully
```

```
test was created successfully
```

## Passing Variables from Login to Server

After we collect our variables using the aforementioned AJAX/jQuery method, we need to parse the attacker inputted data.

```
syslog(LOG_INFO, "$timestamps opendaylight sshd22[6033]: IP: $ip PassLog:Username: $username Password: $password");
```

In order to send data to the database and syslog servers, the PHP page must be able to connect with a remote server. This script requires the PHP connection file to run before anything else on the page.

PHP has a built-in method for sending data to syslog servers ,here is an example:

```
bool syslog ( int $priority , string $message )
```

It is recommend that this line be placed after you submit the data to the database (if you choose to back up the data) of your choosing.

### Optional: Database Backup

#### Mysql

However, in order for the page to connect to a remote server, there are a few configuration changes that need to be made to the server's access permissions:

```
mysql> GRANT ALL ON database_name.* TO root@'1.2.3.4' IDENTIFIED BY 'password';
```

Once the command is run, it is highly recommended to test the connection on your client-server, or the server you wish to send information from. Use the following command to connect to the mysql database

#### MySQL Connect to Remote Server

```
Mysql -u root -p -h xxx.xxx.xxx.xxx
```

Where 'x' is the server you are attempting to connect to.

#### Postgresql

To set up a postgresql database, simply run the following command:

```
apt-get install php5-pgsql
```

After this package installs, restart apache and you should then be able to create a database and connect it with a basic connection script.

#### Syslog-ng: Pushing to Syslog

##### What is Syslog-ng?

Syslog-ng is a system log manager. It allows clients to send their syslogs to remote hosts in an effective, easy to set up method. In this case, syslog will be used to manage logs sent by the honeypot into the longtail syslog server.<sup>10</sup>

Once working properly, syslog-ng works something like the diagram below:



11

<sup>10</sup> (Syslog-ng, Chapter 1. Introduction to syslog-ng 2015)

<sup>11</sup> (Joseph, Syslog-Explanation n.d.)

Essentially, after syslog-ng is properly configured, the client will be allowed access to place its syslog information into the host's syslog.

### Installing Syslog-ng

There are two locations syslog-ng must be installed in, both the client-host and the server-host. Syslog-ng has received a major update since 3.0, so the install is a bit different (at least for Ubuntu). Run the following commands on both your client-host (the server where you want the syslog information to come from) as well as your host-server (the server where you want the syslog information to go to).<sup>12</sup>

```
sudo apt-get install syslog-ng-core
```

```
sudo apt-get install syslog-ng
```

### Configuring Syslog-ng (Client-Host)

To configure the client-host (where the syslog messages will originate from) follow these instructions:

1. Open the syslog-ng.conf

- a. `sudo nano-c /etc/syslog-ng/syslog-ng.conf`<sup>13</sup>

2. In that file, edit the following areas:

- a. Sources

- i. After

```
source s_src {  
    system();  
    internal();  
};
```

- ii. Add the following configuration

```
source s_myfilesources {  
    file("/var/log/log-test.log" follow-  
    freq(1)); };
```

- b. Destinations

- i. After

```
destination d_local {file"/var/log/messages.log"}; ;
```

- ii. Add

```
destination d_network { syslog("10.11.17.231"  
    transport("tcp")); };
```

- c. Logs

- i. After

---

<sup>12</sup> (Syslog-ng, Chapter 4. The syslog-ng OSE quick-start guide 2015)

<sup>13</sup> **Invalid source specified.**

```
log { source(s_src); filter(f_uucp); destination(d_uucp); };
```

- ii. Add

```
log { source(s_src); destination(d_network); };
```

3. After you have updated the configuration files, syslog-ng needs to be restarted in order for your changes to take effect. To restart syslog-ng, use the following command:

```
sudo /etc/init.d/syslog-ng restart
```

4. You should then receive the following messages:

```
* Stopping system logging syslog-ng      [OK ]
* Starting system logging syslog-ng      [OK ]
```

If you receive an error message, refer to the troubleshooting section for assistance.

### Configuring Syslog-ng (Host-Server)

To configure the host-server (the syslog destination server) follow these instructions:

1. Open the syslog-ng.conf

```
sudo nano-c /etc/syslog-ng/syslog-ng.conf
```

2. In that file, edit the following areas:

- a. Sources

- i. After

```
source s_src {
    system();
    internal();
};
```

- ii. Add the following configuration

```
source s_network { syslog(ip(10.11.17.231)
transport("tcp")); };14
```

- b. Destinations

- i. In the host-server, there is actually no need to edit the destinations section any differently than the client server so long as you wish for the external syslog message information to merge with your current syslog messages. For example, if a client host who resides at 10.11.17.11 sends to the host server at 10.11.17.12, the host server will have both 10.11.17.11 and 10.11.17.12 syslog files stored in /var/logs/messages.

```
destination d_local {file("/var/log/messages");};
```

- ii. However, if you wish to separate the files, add the following beneath any destination configuration:

```
destination d_local { file("/var/log/messages_${HOST}");};
```

<sup>14</sup> (Syslog-ng, 4.2 Configuring syslog-ng on server hosts 2015)



## c. Logs

## i. After

```
log { source(s_src); filter(f_uucp); destination(d_uucp); };
```

## i. Add the following configuration

```
log { source(s_src); source(s_network); destination(d_local);
};
```

5. After you have updated the configuration files, syslog-ng needs to be restarted in order for your changes to take effect. To restart syslog-ng, use the following command:

```
sudo /etc/init.d/syslog-ng restart15
```

6. You should then receive the following messages:

```
* Stopping system logging syslog-ng      [OK ]
* Starting system logging syslog-ng      [OK ]
```

If you receive an error message, refer to the troubleshooting section for assistance.

#### Optional: Sending Logs to Multiple Destinations

If need be, syslog-ng also has the ability to send the log to multiple servers. In order to configure this option, simply follow these steps:

##### Host-Server

1. Navigate to the host-server's configuration file
2. Find the destination section and place your cursor just beneath the last syslog statement:
  - a. Ex: 

```
destination d_network { syslog("10.11.17.218"
transport("tcp")); };
```
3. After that line, create a new destination
  - a. 

```
destination d_loghost2 { syslog("10.10.7.72"
transport("tcp")); };
```
4. Then, locate the log section of the configuration file and place your cursor just underneath the first destination's configuraton:
  - a. 

```
log { source(s_src); destination(d_network); };
```
5. Now, add a new log statement that uses the same naming conventions as your new destination
  - a. 

```
log {source(s_src); destination(d_loghost2); };
```

##### Client-Server

1. Navigate to the client-server's configuration file
2. Find the source section and place your cursor just beneath the source s\_local statement:
  - a. 

```
source s_local {
system();
internal();
};
```
3. After that line, create a source network:

<sup>15</sup> (Mewbies 2010)

```
a. source s_network {  
    (ip(10.10.7.72) transport("tcp"));  
};
```

4. Then, create a destination for the source network syslog information to dump to:

```
a. destination d_local {  
    file("/var/log/messages/sdn-messages.log");  
};
```

5. Finally, locate your log section and mirror the following configuration:

```
a. log {  
    source(s_local);  
    # uncomment this line to open port 514 to receive messages  
    source(s_network);  
    destination(d_local);  
};
```

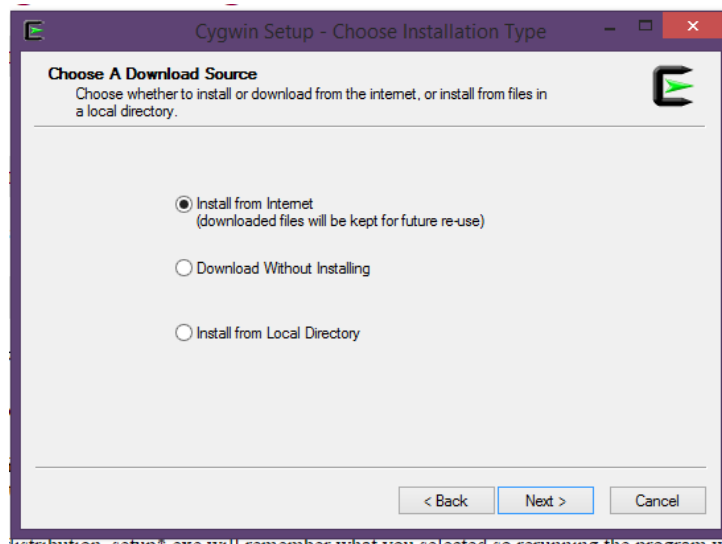
#### *Extra Optional: Sending Syslog to Remote Syslog on a Different OS (Windows)*

In order to send syslog data to a remote server located on a different OS, in this case, a Windows machine, you may need to install other programs such as CYGWIN or any other Linux-like environment shell. This documentation will only assist in the installation and use within the Windows Machine, however, users on Macintosh should be able to easily follow along.

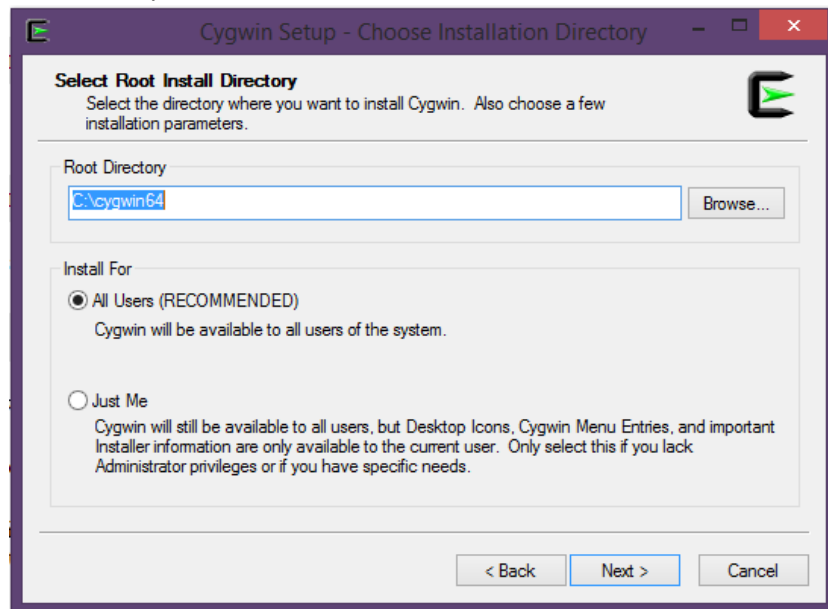
#### Method 1: CYGWIN-Syslog

1. Install CYGWIN

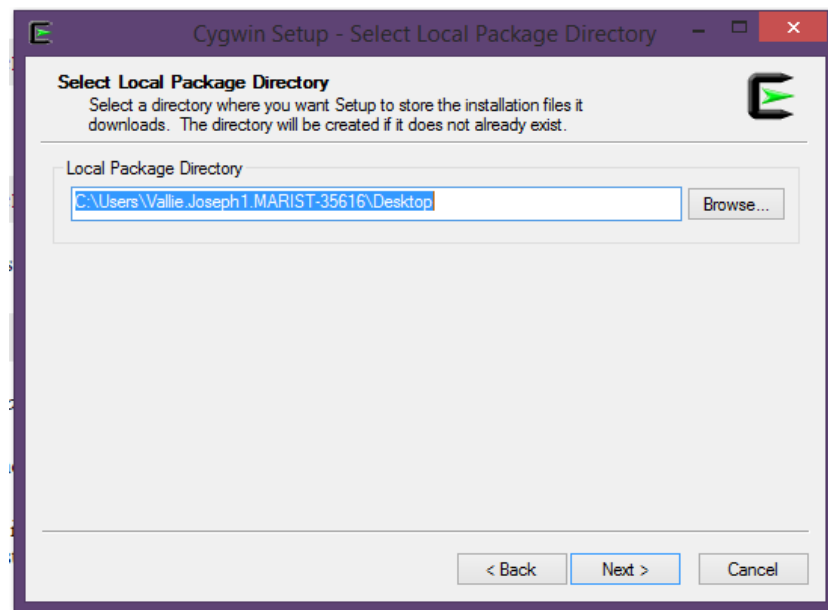
- a. Navigate to: <https://cygwin.com/install.html>
- b. Click and download the "setup-x86.exe" link or the "set-upx86\_64.exe"
- i. You will be presented with a basic install gui, select the following options when prompted:
  1. "Install from Internet"



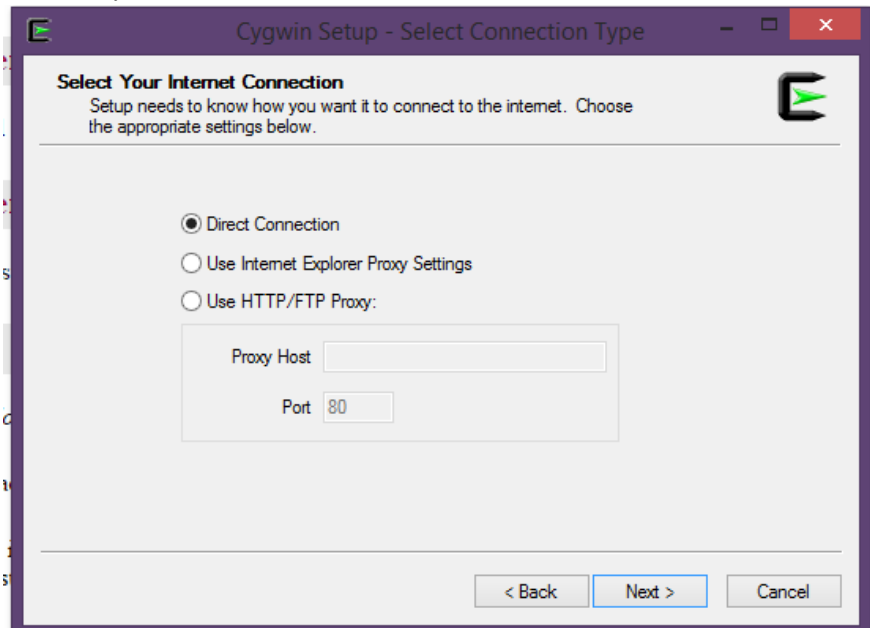
2. Set directory as main drive, set users as “all users”



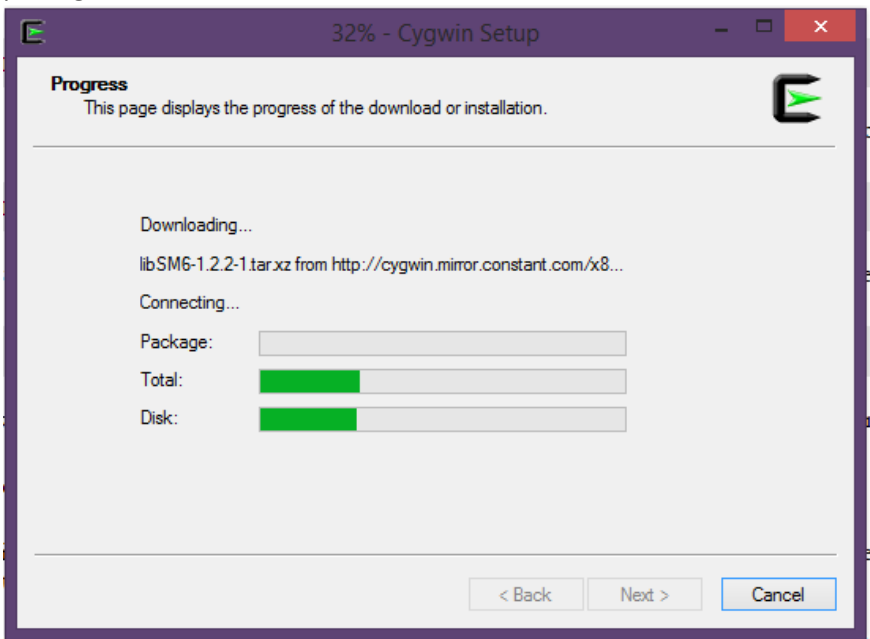
3. Default location



4. Select any site to download from

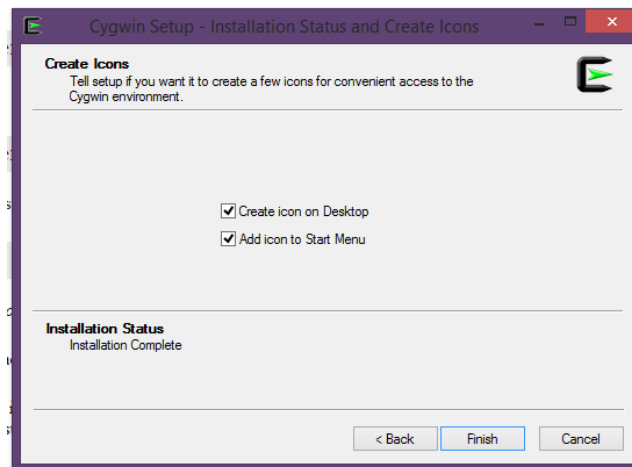


5. Install the syslog, Admin/cygrunsrv, editors/VIM, and Gnome/glib packages





## 6. Finish



2. After CYGWIN is installed, open the program and you should see the command shell
3. Now, navigate to the service file for syslog:
  - a. `./bin/syslog-ng-config`
4. You will be asked if you want to install syslog-ng as a service, enter yes and syslog will install

```
./syslog-ng-config
creating default syslog-ng configuration files in /etc/syslog-ng

Warning: The following function requires administrator privileges!

Do you want to install syslog-ng as service?
(Say "no" if it's already installed as service) (yes/no) yes
cygrunsrv: Error installing a service: OpenSCManager: Win32 error 5:
Access is denied.

Configuration finished. Have fun!
```

5. Syslog should now be installed on your windows machine. Now, navigate to the syslog config file
  - a. Vi (text editor here) `/etc/syslog-ng/syslog-ng.conf`

6. When the file opens, you should see something like the following:

```
# Default syslog-ng.conf file which collects all local logs into a
# single file called /var/log/messages.
#

@version: 3.2
@include "scl.conf"

source s_local {
    system();
    internal();
};

source s_network {
    udp();
};

destination d_local {
    file("/var/log/messages");
};

log {
    source(s_local);

    | # uncomment this line to open port 514 to receive messages
    #source(s_network);
    destination(d_local);
};
```

7. After this, you should be able to use the above configuration to grab syslog data from a remote server, effectively making a secondary host server.

#### Method 2: Samba-Syslog

First, install the **Samba** packages:

```
Sudo apt-get install samba samba-common system-config-samba
```

#### *Creating Users*

Then, create a user with a password to access your shared drive:

```
sudo smbpassword -a [username_here]
```

Samba will then prompt you to create a password, enter your chosen password once at the prompt, and then again at the re-type prompt.

#### *Configuring Samba:*

Next, open the configuration file:

```
sudo /etc/samba/smb.conf
```

Once the file is opened, you should be able to see something like the following:

```

# Sample configuration file for the Samba suite for Debian GNU/Linux.
#
# This is the main Samba configuration file. You should read the
# smb.conf(5) manual page in order to understand the options listed
# here. Samba has a huge number of configurable options most of which
# are not shown in this example
#
# Some options that are often worth tuning have been included as
# commented-out examples in this file:
# - When such options are commented with ";", the proposed setting
#   differs from the default Samba behaviour
# - When commented with "!", the proposed setting is the default
#   behaviour of Samba but the option is considered important
#   enough to be mentioned here
#
# NOTE: Whenever you modify this file you should run the command
# "testparm" to check that you have not made any basic syntactic
# errors.

===== Global Settings =====

[global]

## Browsing/Identification ###

# Change this to the workgroup/NT-domain name your Samba server will part of
workgroup = WORKGROUP

# server string is the equivalent of the NT Description field
server string = %b server (Samba, Ubuntu)

# Windows Internet Name Serving Support Section:
# WINS Support - Tells the NMBD component of Samba to enable its WINS Server
# wins support = no

# WINS Server - Tells the NMBD components of Samba to be a WINS Client
# Note: Samba can be either a WINS Server, or a WINS Client, but NOT both
# wins server = w.x.y.z

# This will prevent nmbd to search for NetBIOS names through DNS.
dns proxy = no

#### Networking ####

# The specific set of interfaces / networks to bind to
# This can be either the interface name or an IP address/netmask:
# interface names are normally preferred
# interfaces = 127.0.0.0/8 eth0

# Only bind to the named interfaces and/or networks: you must use the
# 'interfaces' option above to use this.
# It is recommended that you enable this feature if your Samba machine is
# not protected by a firewall or is a firewall itself. However, this
# option cannot handle dynamic or non-broadcast interfaces correctly.
# bind interfaces only = yes

#### Debugging/Accounting ####

```

Scroll down until you see a line that says '[homes]'.

This is your shared drive name, for example, usually when connecting to a shared mapped drive, you'd map it as:

[\\server\sharedname](#)

In this case, '[homes]' is your shared name. Rename it to anything of your choosing. For our purposes, it will be 'dolos\_shares'. Each shared drive will be defined as a shared block, and will be placed directly under your shared drive name. Under your custom shared drive name, edit your configuration so that it looks like the following:

```

===== Share Definitions =====

# Un-comment the following (and tweak the other settings below to suit)
# to enable the default home directory shares. This will share each
# user's home directory as \\server\username

[dolos_shares]
    comment = testing the shared drive
    path = /home/openflow/Shares
    browsable = yes
    read only = no
    guest ok = no
    force user = openflow

# By default, the home directories are exported read-only. Change the
# next parameter to 'no' if you want to be able to write to them.

```



You may notice a force user field. This is where you will place the username you created earlier.

Scroll down a bit more until you see a line that is commented out reading 'valid users = %S'

Edit your configuration so that your username is listed as a valid user:

```
# By default, \\server\username shares can be connected to by anyone
# with access to the samba server.
# Un-comment the following parameter to make sure that only "username"
# can connect to \\server\username
# This might need tweaking when using external authentication schemes
valid users = openflow
```

Finally, make sure that your shared drive has linux reading and writing permissions

```
Cmod 777 /path/to/folder/here
```

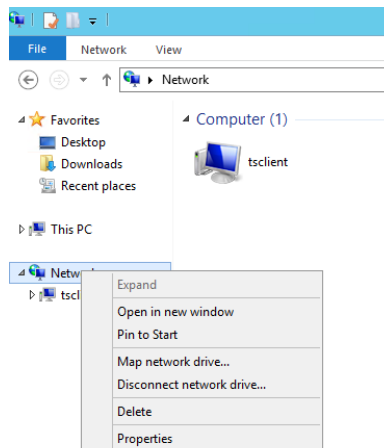
```
openflow@OpenDayLight-Lithium:~/Shares$ pwd
/home/openflow/Shares
openflow@OpenDayLight-Lithium:~/Shares$ sudo chmod 777 /home/openflow/Shares
openflow@OpenDayLight-Lithium:~/Shares$ sudo nano -c /etc/samba/smb.conf
openflow@OpenDayLight-Lithium:~/Shares$ sudo service smbd restart
```

*Do not forget to restart your smbd service, if you do not, the configuration will not apply*

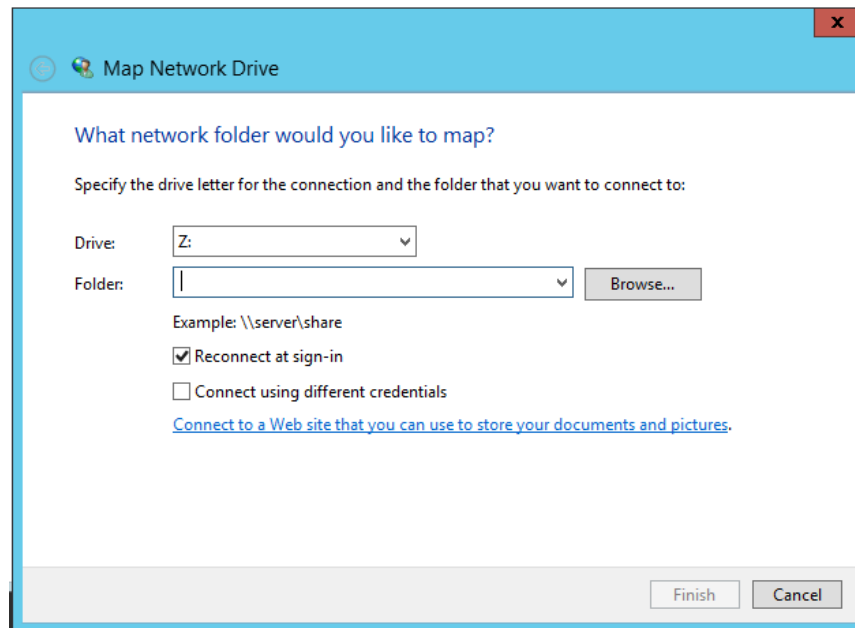
Mapping the Drive

After all of the above configuration, you should be able to map your drive on your windows machine:

First, go to your library and right click the 'Network' drive



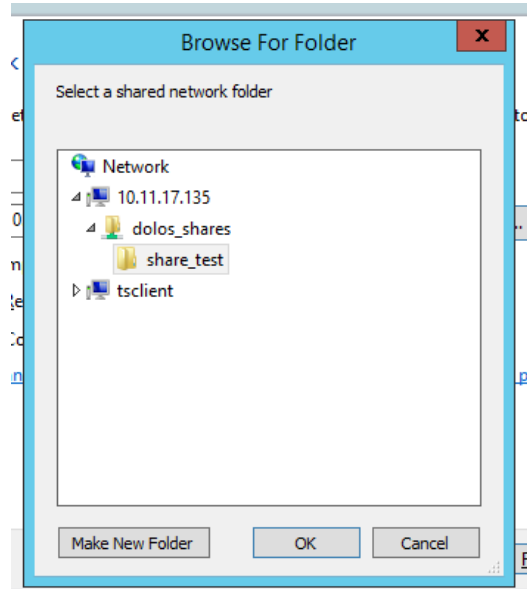
Then, select 'Map network drive...'



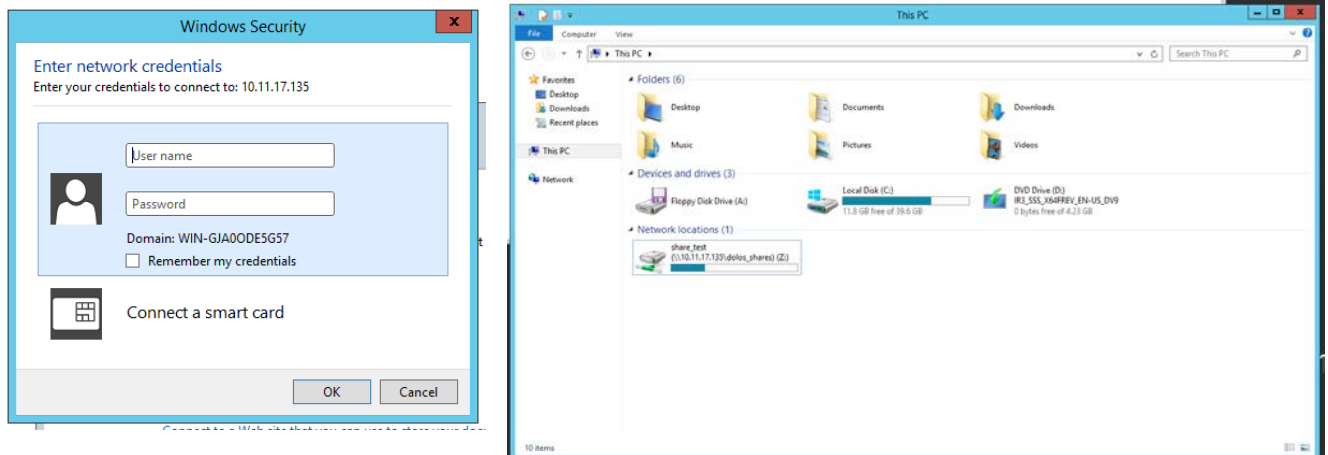
A dialog box like the one above should prompt you to enter a folder name. To write it in manually, use the following format:

[\\server\shared drive name\shared folder](#)

Alternatively, feel free to use the browse option located just to the right to search through the directory:



After the file is selected, Windows will prompt you for the username and password created with Samba. Enter your credentials and you should be able to connect your drive.



### Testing

After following the above configurations, test your syslog to ensure that it is being sent to the host-server.

Here is a brief php script that will do the job:

```
<?php

//Optional --> opensyslog("honeypotsyslog", LOG);

$timestamp= date('Y-m-d');

$timestamp2=date('h:m:s P');

$timestamps = $timestamp."T".$timestamp2;

syslog(LOG_INFO, "$timestamps opendaylight sshd-22[6033]: IP: $ip PassLog:
Username: $username Password: $password");

?>
```

And now view the tail end of both syslog files:

```
tail -f /var/log/messages
```

Passing Variables from Login to Server Client-Server

The tails should update automatically, and you should now see syslog messages passing through both the client-server and host-server

```

Sun 7 14:00:21 TrustedSC sudo: pam_unix(session): session opened for user root by opendaylight(uid=0)
/v:/usr/local/sbin:
Sun 7 14:00:21 TrustedSC sudo: pam_unix(session): session opened for user root by opendaylight(uid=0)
Sun 7 14:00:43 10.11.17.135 spachev: 2016-06-07T01:06:43+0400 opendaylight sshd-22[6093]: IP: 10.128.236.123
PassLog: Username: thalysayalmogtest Password: testingsayalogs
Sun 7 14:00:23 Opndaylight-Lithium syslog-ng[6093]: Initialising destination file writer: template="/var/log/syslog", filename="/var/log/syslog/"
Sun 7 14:00:23 Opndaylight-Lithium syslog-ng[6093]: Initialising destination file writer: template="/var/log/messages", filename="/var/log/messages/"
Sun 7 14:00:43 Opndaylight-Lithium spachev: 2016-06-07T01:06:43+0400 opendaylight sshd-22[6093]: IP: 10.128.236.123 PassLog: Username: thalysayalmogtest Password: testingsayalogs

```

(include other scanning tools check previous documentation )

## Final Scans

After completing all of the above configurations, here are the final scans that compare the honeypot server to the one it was attempting to mimic. The honeypot is on the right while the original server is on the left.

## Zenmap

<pre>1&lt;?xml version="1.0" encoding="iso-8859-1"??&gt;</pre>	<pre>1&lt;?xml version="1.0" encoding="iso-8859-1"??&gt;</pre>
<pre>&lt;?xml-stylesheet href="file:///usr/bin/../../share/nmap/nmap.xsl" type="text/xsl"?&gt;&lt;nmaprun start="1470002473" profile_name="Slow comprehensive scan" xmloutputversion="1.04" scanner="nmap" version="7.12" startstr="Sun Jul 31 18:01:13 2016" args='nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)" 10.11.17.133'&gt;&lt;scaninfo services="1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,113,119,125,135,139,143-144,146,161,163,179,199,211-212,222,254-256,259,264,280,301,306,311,340,366,389,406-407,416-417,425,427,443-445,458,464-465,481,497,500,512-515,524,541,543-545,548,554-555,563,587,593,616-617,625,631,636,646,648,666-668,683,687,691,700,705,711,714,720,722,726,749,765,777,783,787,800-801,808,843,873,880,888,898,900-903,911-912,981,987,990,992-</pre>	<pre>&lt;?xml-stylesheet href="file:///usr/bin/../../share/nmap/nmap.xsl" type="text/xsl"?&gt;&lt;nmaprun start="1470000415" profile_name="Slow comprehensive scan" xmloutputversion="1.04" scanner="nmap" version="7.12" startstr="Sun Jul 31 17:26:55 2016" args='nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)" 10.11.17.135'&gt;&lt;scaninfo services="1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,113,119,125,135,139,143-144,146,161,163,179,199,211-212,222,254-256,259,264,280,301,306,311,340,366,389,406-407,416-417,425,427,443-445,458,464-465,481,497,500,512-515,524,541,543-545,548,554-555,563,587,593,616-617,625,631,636,646,648,666-668,683,687,691,700,705,711,714,720,722,726,749,765,777,783,787,800-801,808,843,873,880,888,898,900-903,911-912,981,987,990,992-</pre>

993,995,999-1002,1007,1009-  
 1011,1021-1100,1102,1104-  
 1108,1110-1114,1117,1119,1121-  
 1124,1126,1130-1132,1137-  
 1138,1141,1145,1147-1149,1151-  
 1152,1154,1163-1166,1169,1174-  
 1175,1183,1185-1187,1192,1198-  
 1199,1201,1213,1216-1218,1233-  
 1234,1236,1244,1247-  
 1248,1259,1271-  
 1272,1277,1287,1296,1300-  
 1301,1309-  
 1311,1322,1328,1334,1352,1417,1433  
 -1434,1443,1455,1461,1494,1500-  
 1501,1503,1521,1524,1533,1556,1580  
 ,1583,1594,1600,1641,1658,1666,168  
 7-1688,1700,1717-  
 1721,1723,1755,1761,1782-  
 1783,1801,1805,1812,1839-  
 1840,1862-  
 1864,1875,1900,1914,1935,1947,1971  
 -1972,1974,1984,1998-  
 2010,2013,2020-2022,2030,2033-  
 2035,2038,2040-2043,2045-  
 2049,2065,2068,2099-  
 2100,2103,2105-  
 2107,2111,2119,2121,2126,2135,2144  
 ,2160-2161,2170,2179,2190-  
 2191,2196,2200,2222,2251,2260,2288  
 ,2301,2323,2366,2381-2383,2393-  
 2394,2399,2401,2492,2500,2522,2525  
 ,2557,2601-2602,2604-2605,2607-  
 2608,2638,2701-2702,2710,2717-  
 2718,2725,2800,2809,2811,2869,2875  
 ,2909-2910,2920,2967-  
 2968,2998,3000-3001,3003,3005-  
 3007,3011,3013,3017,3030-  
 3031,3052,3071,3077,3128,3168,3211  
 ,3221,3260-3261,3268-  
 3269,3283,3300-3301,3306,3322-  
 3325,3333,3351,3367,3369-  
 3372,3389-  
 3390,3404,3476,3493,3517,3527,3546  
 ,3551,3580,3659,3689-  
 3690,3703,3737,3766,3784,3800-  
 3801,3809,3814,3826-  
 3828,3851,3869,3871,3878,3880,3889  
 ,3905,3914,3918,3920,3945,3971,398  
 6,3995,3998,4000-  
 4006,4045,4111,4125-  
 4126,4129,4224,4242,4279,4321,4343

993,995,999-1002,1007,1009-  
 1011,1021-1100,1102,1104-  
 1108,1110-1114,1117,1119,1121-  
 1124,1126,1130-1132,1137-  
 1138,1141,1145,1147-1149,1151-  
 1152,1154,1163-1166,1169,1174-  
 1175,1183,1185-1187,1192,1198-  
 1199,1201,1213,1216-1218,1233-  
 1234,1236,1244,1247-  
 1248,1259,1271-  
 1272,1277,1287,1296,1300-  
 1301,1309-  
 1311,1322,1328,1334,1352,1417,1433  
 -1434,1443,1455,1461,1494,1500-  
 1501,1503,1521,1524,1533,1556,1580  
 ,1583,1594,1600,1641,1658,1666,168  
 7-1688,1700,1717-  
 1721,1723,1755,1761,1782-  
 1783,1801,1805,1812,1839-  
 1840,1862-  
 1864,1875,1900,1914,1935,1947,1971  
 -1972,1974,1984,1998-  
 2010,2013,2020-2022,2030,2033-  
 2035,2038,2040-2043,2045-  
 2049,2065,2068,2099-  
 2100,2103,2105-  
 2107,2111,2119,2121,2126,2135,2144  
 ,2160-2161,2170,2179,2190-  
 2191,2196,2200,2222,2251,2260,2288  
 ,2301,2323,2366,2381-2383,2393-  
 2394,2399,2401,2492,2500,2522,2525  
 ,2557,2601-2602,2604-2605,2607-  
 2608,2638,2701-2702,2710,2717-  
 2718,2725,2800,2809,2811,2869,2875  
 ,2909-2910,2920,2967-  
 2968,2998,3000-3001,3003,3005-  
 3007,3011,3013,3017,3030-  
 3031,3052,3071,3077,3128,3168,3211  
 ,3221,3260-3261,3268-  
 3269,3283,3300-3301,3306,3322-  
 3325,3333,3351,3367,3369-  
 3372,3389-  
 3390,3404,3476,3493,3517,3527,3546  
 ,3551,3580,3659,3689-  
 3690,3703,3737,3766,3784,3800-  
 3801,3809,3814,3826-  
 3828,3851,3869,3871,3878,3880,3889  
 ,3905,3914,3918,3920,3945,3971,398  
 6,3995,3998,4000-  
 4006,4045,4111,4125-  
 4126,4129,4224,4242,4279,4321,4343

,4443-  
 4446,4449,4550,4567,4662,4848,4899  
 -4900,4998,5000-  
 5004,5009,5030,5033,5050-  
 5051,5054,5060-  
 5061,5080,5087,5100-  
 5102,5120,5190,5200,5214,5221-  
 5222,5225-  
 5226,5269,5280,5298,5357,5405,5414  
 ,5431-  
 5432,5440,5500,5510,5544,5550,5555  
 ,5560,5566,5631,5633,5666,5678-  
 5679,5718,5730,5800-5802,5810-  
 5811,5815,5822,5825,5850,5859,5862  
 ,5877,5900-5904,5906-5907,5910-  
 5911,5915,5922,5925,5950,5952,5959  
 -5963,5987-5989,5998-  
 6007,6009,6025,6059,6100-  
 6101,6106,6112,6123,6129,6156,6346  
 ,6389,6502,6510,6543,6547,6565-  
 6567,6580,6646,6666-  
 6669,6689,6692,6699,6779,6788-  
 6789,6792,6839,6881,6901,6969,7000  
 -  
 7002,7004,7007,7019,7025,7070,7100  
 ,7103,7106,7200-  
 7201,7402,7435,7443,7496,7512,7625  
 ,7627,7676,7741,7777-  
 7778,7800,7911,7920-7921,7937-  
 7938,7999-8002,8007-8011,8021-  
 8022,8031,8042,8045,8080-  
 8090,8093,8099-8100,8180-  
 8181,8192-  
 8194,8200,8222,8254,8290-  
 8292,8300,8333,8383,8400,8402,8443  
 ,8500,8600,8649,8651-  
 8652,8654,8701,8800,8873,8888,8899  
 ,8994,9000-9003,9009-  
 9011,9040,9050,9071,9080-  
 9081,9090-9091,9099-9103,9110-  
 9111,9200,9207,9220,9290,9415,9418  
 ,9485,9500,9502-  
 9503,9535,9575,9593-  
 9595,9618,9666,9876-  
 9878,9898,9900,9917,9929,9943-  
 9944,9968,9998-10004,10009-  
 10010,10012,10024-  
 10025,10082,10180,10215,10243,1056  
 6,10616-10617,10621,10626,10628-  
 10629,10778,11110-  
 11111,11967,12000,12174,12265,1234

,4443-  
 4446,4449,4550,4567,4662,4848,4899  
 -4900,4998,5000-  
 5004,5009,5030,5033,5050-  
 5051,5054,5060-  
 5061,5080,5087,5100-  
 5102,5120,5190,5200,5214,5221-  
 5222,5225-  
 5226,5269,5280,5298,5357,5405,5414  
 ,5431-  
 5432,5440,5500,5510,5544,5550,5555  
 ,5560,5566,5631,5633,5666,5678-  
 5679,5718,5730,5800-5802,5810-  
 5811,5815,5822,5825,5850,5859,5862  
 ,5877,5900-5904,5906-5907,5910-  
 5911,5915,5922,5925,5950,5952,5959  
 -5963,5987-5989,5998-  
 6007,6009,6025,6059,6100-  
 6101,6106,6112,6123,6129,6156,6346  
 ,6389,6502,6510,6543,6547,6565-  
 6567,6580,6646,6666-  
 6669,6689,6692,6699,6779,6788-  
 6789,6792,6839,6881,6901,6969,7000  
 -  
 7002,7004,7007,7019,7025,7070,7100  
 ,7103,7106,7200-  
 7201,7402,7435,7443,7496,7512,7625  
 ,7627,7676,7741,7777-  
 7778,7800,7911,7920-7921,7937-  
 7938,7999-8002,8007-8011,8021-  
 8022,8031,8042,8045,8080-  
 8090,8093,8099-8100,8180-  
 8181,8192-  
 8194,8200,8222,8254,8290-  
 8292,8300,8333,8383,8400,8402,8443  
 ,8500,8600,8649,8651-  
 8652,8654,8701,8800,8873,8888,8899  
 ,8994,9000-9003,9009-  
 9011,9040,9050,9071,9080-  
 9081,9090-9091,9099-9103,9110-  
 9111,9200,9207,9220,9290,9415,9418  
 ,9485,9500,9502-  
 9503,9535,9575,9593-  
 9595,9618,9666,9876-  
 9878,9898,9900,9917,9929,9943-  
 9944,9968,9998-10004,10009-  
 10010,10012,10024-  
 10025,10082,10180,10215,10243,1056  
 6,10616-10617,10621,10626,10628-  
 10629,10778,11110-  
 11111,11967,12000,12174,12265,1234

```

5,13456,13722,13782-
13783,14000,14238,14441-
14442,15000,15002-
15004,15660,15742,16000-
16001,16012,16016,16018,16080,1611
3,16992-
16993,17877,17988,18040,18101,1898
8,19101,19283,19315,19350,19780,19
801,19842,20000,20005,20031,20221-
20222,20828,21571,22939,23502,2444
4,24800,25734-
25735,26214,27000,27352-
27353,27355-
27356,27715,28201,30000,30718,3095
1,31038,31337,32768-
32785,33354,33899,34571-
34573,35500,38292,40193,40911,4151
1,42510,44176,44442-
44443,44501,45100,48080,49152-
49161,49163,49165,49167,49175-
49176,49400,49999-
50003,50006,50300,50389,50500,5063
6,50800,51103,51493,52673,52822,52
848,52869,54045,54328,55055-
55056,55555,55600,56737-
56738,57294,57797,58080,60020,6044
3,61532,61900,62078,63331,64623,64
680,65000,65129,65389"
protocol="tcp" numservices="1000"
type="syn"></scaninfo><scaninfo
services="2-3,7,9,13,17,19-23,37-
38,42,49,53,67-69,80,88,111-
113,120,123,135-139,158,161-
162,177,192,199,207,217,363,389,40
2,407,427,434,443,445,464,497,500,
502,512-515,517-
518,520,539,559,593,623,626,631,63
9,643,657,664,682-689,764,767,772-
776,780-
782,786,789,800,814,826,829,838,90
2-903,944,959,965,983,989-990,996-
1001,1007-1008,1012-1014,1019-
1051,1053-1060,1064-
1070,1072,1080-1081,1087-
1088,1090,1100-
1101,1105,1124,1200,1214,1234,1346
,1419,1433-1434,1455,1457,1484-
1485,1524,1645-1646,1701,1718-
1719,1761,1782,1804,1812-
1813,1885-1886,1900-
1901,1993,2000,2002,2048-

```

```

5,13456,13722,13782-
13783,14000,14238,14441-
14442,15000,15002-
15004,15660,15742,16000-
16001,16012,16016,16018,16080,1611
3,16992-
16993,17877,17988,18040,18101,1898
8,19101,19283,19315,19350,19780,19
801,19842,20000,20005,20031,20221-
20222,20828,21571,22939,23502,2444
4,24800,25734-
25735,26214,27000,27352-
27353,27355-
27356,27715,28201,30000,30718,3095
1,31038,31337,32768-
32785,33354,33899,34571-
34573,35500,38292,40193,40911,4151
1,42510,44176,44442-
44443,44501,45100,48080,49152-
49161,49163,49165,49167,49175-
49176,49400,49999-
50003,50006,50300,50389,50500,5063
6,50800,51103,51493,52673,52822,52
848,52869,54045,54328,55055-
55056,55555,55600,56737-
56738,57294,57797,58080,60020,6044
3,61532,61900,62078,63331,64623,64
680,65000,65129,65389"
protocol="tcp" numservices="1000"
type="syn"></scaninfo><scaninfo
services="2-3,7,9,13,17,19-23,37-
38,42,49,53,67-69,80,88,111-
113,120,123,135-139,158,161-
162,177,192,199,207,217,363,389,40
2,407,427,434,443,445,464,497,500,
502,512-515,517-
518,520,539,559,593,623,626,631,63
9,643,657,664,682-689,764,767,772-
776,780-
782,786,789,800,814,826,829,838,90
2-903,944,959,965,983,989-990,996-
1001,1007-1008,1012-1014,1019-
1051,1053-1060,1064-
1070,1072,1080-1081,1087-
1088,1090,1100-
1101,1105,1124,1200,1214,1234,1346
,1419,1433-1434,1455,1457,1484-
1485,1524,1645-1646,1701,1718-
1719,1761,1782,1804,1812-
1813,1885-1886,1900-
1901,1993,2000,2002,2048-

```

2049,2051,2148,2160-2161,2222-  
 2223,2343,2345,2362,2967,3052,3130  
 ,3283,3296,3343,3389,3401,3456-  
 3457,3659,3664,3702-  
 3703,4000,4008,4045,4444,4500,4666  
 ,4672,5000-  
 5003,5010,5050,5060,5093,5351,5353  
 ,5355,5500,5555,5632,6000-  
 6002,6004,6050,6346-6347,6970-  
 6971,7000,7938,8000-  
 8001,8010,8181,8193,8900,9000-  
 9001,9020,9103,9199-  
 9200,9370,9876-  
 9877,9950,10000,10080,11487,16086,  
 16402,16420,16430,16433,16449,1649  
 8,16503,16545,16548,16573,16674,16  
 680,16697,16700,16708,16711,16739,  
 16766,16779,16786,16816,16829,1683  
 2,16838-  
 16839,16862,16896,16912,16918-  
 16919,16938-16939,16947-  
 16948,16970,16972,16974,17006,1701  
 8,17077,17091,17101,17146,17184-  
 17185,17205,17207,17219,17236-  
 17237,17282,17302,17321,17331-  
 17332,17338,17359,17417,17423-  
 17424,17455,17459,17468,17487,1749  
 0,17494,17505,17533,17549,17573,17  
 580,17585,17592,17605,17615-  
 17616,17629,17638,17663,17673-  
 17674,17683,17726,17754,17762,1778  
 7,17814,17823-  
 17824,17836,17845,17888,17939,1794  
 6,17989,18004,18081,18113,18134,18  
 156,18228,18234,18250,18255,18258,  
 18319,18331,18360,18373,18449,1848  
 5,18543,18582,18605,18617,18666,18  
 669,18676,18683,18807,18818,18821,  
 18830,18832,18835,18869,18883,1888  
 8,18958,18980,18985,18987,18991,18  
 994,18996,19017,19022,19039,19047,  
 19075,19096,19120,19130,19140-  
 19141,19154,19161,19165,19181,1919  
 3,19197,19222,19227,19273,19283,19  
 294,19315,19322,19332,19374,19415,  
 19482,19489,19500,19503-  
 19504,19541,19600,19605,19616,1962  
 4-  
 19625,19632,19639,19647,19650,1966  
 0,19662-19663,19682-  
 19683,19687,19695,19707,19717-

2049,2051,2148,2160-2161,2222-  
 2223,2343,2345,2362,2967,3052,3130  
 ,3283,3296,3343,3389,3401,3456-  
 3457,3659,3664,3702-  
 3703,4000,4008,4045,4444,4500,4666  
 ,4672,5000-  
 5003,5010,5050,5060,5093,5351,5353  
 ,5355,5500,5555,5632,6000-  
 6002,6004,6050,6346-6347,6970-  
 6971,7000,7938,8000-  
 8001,8010,8181,8193,8900,9000-  
 9001,9020,9103,9199-  
 9200,9370,9876-  
 9877,9950,10000,10080,11487,16086,  
 16402,16420,16430,16433,16449,1649  
 8,16503,16545,16548,16573,16674,16  
 680,16697,16700,16708,16711,16739,  
 16766,16779,16786,16816,16829,1683  
 2,16838-  
 16839,16862,16896,16912,16918-  
 16919,16938-16939,16947-  
 16948,16970,16972,16974,17006,1701  
 8,17077,17091,17101,17146,17184-  
 17185,17205,17207,17219,17236-  
 17237,17282,17302,17321,17331-  
 17332,17338,17359,17417,17423-  
 17424,17455,17459,17468,17487,1749  
 0,17494,17505,17533,17549,17573,17  
 580,17585,17592,17605,17615-  
 17616,17629,17638,17663,17673-  
 17674,17683,17726,17754,17762,1778  
 7,17814,17823-  
 17824,17836,17845,17888,17939,1794  
 6,17989,18004,18081,18113,18134,18  
 156,18228,18234,18250,18255,18258,  
 18319,18331,18360,18373,18449,1848  
 5,18543,18582,18605,18617,18666,18  
 669,18676,18683,18807,18818,18821,  
 18830,18832,18835,18869,18883,1888  
 8,18958,18980,18985,18987,18991,18  
 994,18996,19017,19022,19039,19047,  
 19075,19096,19120,19130,19140-  
 19141,19154,19161,19165,19181,1919  
 3,19197,19222,19227,19273,19283,19  
 294,19315,19322,19332,19374,19415,  
 19482,19489,19500,19503-  
 19504,19541,19600,19605,19616,1962  
 4-  
 19625,19632,19639,19647,19650,1966  
 0,19662-19663,19682-  
 19683,19687,19695,19707,19717-



19719,19722,19728,19789,19792,19933,19935-  
 19936,19956,19995,19998,20003-  
 20004,20019,20031,20082,20117,20120,20126,20129,20146,20154,20164,20206,20217,20249,20262,20279,20288,20309,20313,20326,20359-  
 20360,20366,20380,20389,20409,20411,20423-20425,20445,20449,20464-  
 20465,20518,20522,20525,20540,20560,20665,20678-  
 20679,20710,20717,20742,20752,20762,20791,20817,20842,20848,20851,20865,20872,20876,20884,20919,21000,21016,21060,21083,21104,21111,21131,21167,21186,21206-  
 21207,21212,21247,21261,21282,21298,21303,21318,21320,21333,21344,21354,21358,21360,21364,21366,21383,21405,21454,21468,21476,21514,21524-  
 21525,21556,21566,21568,21576,21609,21621,21625,21644,21649,21655,21663,21674,21698,21702,21710,21742,21780,21784,21800,21803,21834,21842,21847,21868,21898,21902,21923,21948,21967,22029,22043,22045,22053,22055,22105,22109,22123-  
 22124,22341,22692,22695,22739,22799,22846,22914,22986,22996,23040,23176,23354,23531,23557,23608,23679,23781,23965,23980,24007,24279,24511,24594,24606,24644,24854,24910,25003,25157,25240,25280,25337,25375,25462,25541,25546,25709,25931,26407,26415,26720,26872,26966,27015,27195,27444,27473,27482,27707,27892,27899,28122,28369,28465,28493,28543,28547,28641,28840,28973,29078,29243,29256,29810,29823,29977,30263,30303,30365,30544,30656,30697,30704,30718,30975,31059,31073,31109,31189,31195,31335,31337,31365,31625,31681,31731,31891,32345,32385,32528,32768-  
 32780,32798,32815,32818,32931,33030,33249,33281,33354-  
 33355,33459,33717,33744,33866,33872,34038,34079,34125,34358,34422,34433,34555,34570,34577-  
 34580,34758,34796,34855,34861-

19719,19722,19728,19789,19792,19933,19935-  
 19936,19956,19995,19998,20003-  
 20004,20019,20031,20082,20117,20120,20126,20129,20146,20154,20164,20206,20217,20249,20262,20279,20288,20309,20313,20326,20359-  
 20360,20366,20380,20389,20409,20411,20423-20425,20445,20449,20464-  
 20465,20518,20522,20525,20540,20560,20665,20678-  
 20679,20710,20717,20742,20752,20762,20791,20817,20842,20848,20851,20865,20872,20876,20884,20919,21000,21016,21060,21083,21104,21111,21131,21167,21186,21206-  
 21207,21212,21247,21261,21282,21298,21303,21318,21320,21333,21344,21354,21358,21360,21364,21366,21383,21405,21454,21468,21476,21514,21524-  
 21525,21556,21566,21568,21576,21609,21621,21625,21644,21649,21655,21663,21674,21698,21702,21710,21742,21780,21784,21800,21803,21834,21842,21847,21868,21898,21902,21923,21948,21967,22029,22043,22045,22053,22055,22105,22109,22123-  
 22124,22341,22692,22695,22739,22799,22846,22914,22986,22996,23040,23176,23354,23531,23557,23608,23679,23781,23965,23980,24007,24279,24511,24594,24606,24644,24854,24910,25003,25157,25240,25280,25337,25375,25462,25541,25546,25709,25931,26407,26415,26720,26872,26966,27015,27195,27444,27473,27482,27707,27892,27899,28122,28369,28465,28493,28543,28547,28641,28840,28973,29078,29243,29256,29810,29823,29977,30263,30303,30365,30544,30656,30697,30704,30718,30975,31059,31073,31109,31189,31195,31335,31337,31365,31625,31681,31731,31891,32345,32385,32528,32768-  
 32780,32798,32815,32818,32931,33030,33249,33281,33354-  
 33355,33459,33717,33744,33866,33872,34038,34079,34125,34358,34422,34433,34555,34570,34577-  
 34580,34758,34796,34855,34861-

<pre> 34862,34892,35438,35702,35777,3579 4,36108,36206,36384,36458,36489,36 669,36778,36893,36945,37144,37212, 37393,37444,37602,37761,37783,3781 3,37843,38037,38063,38293,38412,38 498,38615,39213,39217,39632,39683, 39714,39723,39888,40019,40116,4044 1,40539,40622,40708,40711,40724,40 732,40805,40847,40866,40915,41058, 41081,41308,41370,41446,41524,4163 8,41702,41774,41896,41967,41971,42 056,42172,42313,42431,42434,42508, 42557,42577,42627,42639,43094,4319 5,43370,43514,43686,43824,43967,44 101,44160,44179,44185,44190,44253, 44334,44508,44923,44946,44968,4524 7,45380,45441,45685,45722,45818,45 928,46093,46532,46836,47624,47765, 47772,47808,47915,47981,48078,4818 9,48255,48455,48489,48761,49152- 49163,49165-49182,49184- 49202,49204-49205,49207- 49216,49220,49222,49226,49259,4926 2,49306,49350,49360,49393,49396,49 503,49640,49968,50099,50164,50497, 50612,50708,50919,51255,51456,5155 4,51586,51690,51717,51905,51972,52 144,52225,52503,53006,53037,53571, 53589,53838,54094,54114,54281,5432 1,54711,54807,54925,55043,55544,55 587,56141,57172,57409- 57410,57813,57843,57958,57977,5800 2,58075,58178,58419,58631,58640,58 797,59193,59207,59765,59846,60172, 60381,60423,61024,61142,61319,6132 2,61370,61412,61481,61550,61685,61 961,62154,62287,62575,62677,62699, 62958,63420,63555,64080,64481,6451 3,64590,64727,65024" protocol="udp" numservices="1000" type="udp"&gt;&lt;/scaninfo&gt;&lt;verbose level="1"&gt;&lt;/verbose&gt;&lt;debugging level="0"&gt;&lt;/debugging&gt;&lt;output type="interactive"&gt; </pre>	<pre> 34862,34892,35438,35702,35777,3579 4,36108,36206,36384,36458,36489,36 669,36778,36893,36945,37144,37212, 37393,37444,37602,37761,37783,3781 3,37843,38037,38063,38293,38412,38 498,38615,39213,39217,39632,39683, 39714,39723,39888,40019,40116,4044 1,40539,40622,40708,40711,40724,40 732,40805,40847,40866,40915,41058, 41081,41308,41370,41446,41524,4163 8,41702,41774,41896,41967,41971,42 056,42172,42313,42431,42434,42508, 42557,42577,42627,42639,43094,4319 5,43370,43514,43686,43824,43967,44 101,44160,44179,44185,44190,44253, 44334,44508,44923,44946,44968,4524 7,45380,45441,45685,45722,45818,45 928,46093,46532,46836,47624,47765, 47772,47808,47915,47981,48078,4818 9,48255,48455,48489,48761,49152- 49163,49165-49182,49184- 49202,49204-49205,49207- 49216,49220,49222,49226,49259,4926 2,49306,49350,49360,49393,49396,49 503,49640,49968,50099,50164,50497, 50612,50708,50919,51255,51456,5155 4,51586,51690,51717,51905,51972,52 144,52225,52503,53006,53037,53571, 53589,53838,54094,54114,54281,5432 1,54711,54807,54925,55043,55544,55 587,56141,57172,57409- 57410,57813,57843,57958,57977,5800 2,58075,58178,58419,58631,58640,58 797,59193,59207,59765,59846,60172, 60381,60423,61024,61142,61319,6132 2,61370,61412,61481,61550,61685,61 961,62154,62287,62575,62677,62699, 62958,63420,63555,64080,64481,6451 3,64590,64727,65024" protocol="udp" numservices="1000" type="udp"&gt;&lt;/scaninfo&gt;&lt;verbose level="1"&gt;&lt;/verbose&gt;&lt;debugging level="0"&gt;&lt;/debugging&gt;&lt;output type="interactive"&gt; </pre>
<pre> 3 Starting Nmap 7.12 ( <a href="https://nmap.org">https://nmap.org</a> ) at 2016-07-31 18:01 EDT </pre>	<pre> 3 Starting Nmap 7.12 ( <a href="https://nmap.org">https://nmap.org</a> ) at 2016-07-31 17:26 EDT </pre>
<pre> 4NSE: Loaded 262 scripts for scanning. </pre>	<pre> 4NSE: Loaded 262 scripts for scanning. </pre>

5 NSE: Script Pre-scanning.	5 NSE: Script Pre-scanning.
6 Initiating NSE at 18:01	6 Initiating NSE at 17:26
	7 NSE: [mtrace] A source IP must be provided through fromip argument.
7 NSE: [shodan-api] Error: Please specify your ShodanAPI key with the shodan-api.apikey argument	8 NSE: [shodan-api] Error: Please specify your ShodanAPI key with the shodan-api.apikey argument
8 NSE: [mtrace] A source IP must be provided through fromip argument.	
9 Completed NSE at 18:01, 10.05s elapsed	9 Completed NSE at 17:27, 10.13s elapsed
10 Initiating NSE at 18:01	10 Initiating NSE at 17:27
11 Completed NSE at 18:01, 0.00s elapsed	11 Completed NSE at 17:27, 0.00s elapsed
12 Initiating NSE at 18:01	12 Initiating NSE at 17:27
13 Completed NSE at 18:01, 0.00s elapsed	13 Completed NSE at 17:27, 0.00s elapsed
14 Pre-scan script results:	14 Pre-scan script results:
15   broadcast-igmp-discovery:	15   broadcast-igmp-discovery:
16   10.11.17.145	16   10.11.17.238
17   Interface: eth0	17   Interface: eth0
18   Version: 2	18   Version: 2
19   Group: 224.0.0.252	19   Group: 224.0.0.252

2   Description: Link-local (Multicast Name Resolution (rfc4795)	2   Description: Link-local (Multicast Name Resolution (rfc4795)
2   10.11.17.9 1	2   10.11.17.9 1
2   Interface: eth0 2	2   Interface: eth0 2
2   Version: 2 3	2   Version: 2 3
2   Group: 239.255.255.253 4	2   Group: 239.255.255.253 4
2   Description: Organization- 5 Local Scope (rfc2365)	2   Description: Organization- 5 Local Scope (rfc2365)
2   10.11.17.50 6	2   10.11.17.145 6
	2   Interface: eth0 7
	2   Version: 2 8
	2   Group: 239.255.255.250 9
	3   Description: Organization- 0 Local Scope (rfc2365)
	3   10.11.17.212 1
2   Interface: eth0 7	3   Interface: eth0 2
2   Version: 2 8	3   Version: 2 3
2   Group: 239.255.255.250 9	3   Group: 239.255.255.250 4
3   Description: Organization- (Local Scope (rfc2365)	3   Description: Organization- 5 Local Scope (rfc2365)

3   10.11.17.224	3   10.11.17.224
2   Interface: eth0	3   Interface: eth0
3   Version: 2	3   Version: 2
4   Group: 239.255.255.250	3   Group: 239.255.255.250
3   Description: Organization- 5 Local Scope (rfc2365)	4   Description: Organization- C Local Scope (rfc2365)
3   10.11.17.238	4   10.11.17.238
3   Interface: eth0	4   Interface: eth0
3   Version: 2	4   Version: 2
3   Group: 239.255.255.250	4   Group: 239.255.255.250
4   Description: Organization- C Local Scope (rfc2365)	4   Description: Organization- 5 Local Scope (rfc2365)
4   _ Use the newtargets script-arg 1 to add the results as targets	4   _ Use the newtargets script-arg 6 to add the results as targets
4   broadcast-ping:	4   broadcast-ping:
	4   IP: 10.11.17.3 MAC: 4 00:a0:98:11:d3:9c
	4   IP: 10.11.17.6 MAC: 9 00:a0:98:24:16:b4
	5   IP: 10.11.17.12 MAC: C 34:40:b5:40:b8:fe
	5   IP: 10.11.17.171 MAC: 1 00:23:8a:e9:7a:b0
4   IP: 10.11.17.13 MAC: 3 34:40:b5:3c:19:fe	5   IP: 10.11.17.13 MAC: 2 34:40:b5:3c:19:fe

4   IP: 10.11.17.6 MAC: 00:a0:98:24:16:b4	
4   IP: 10.11.17.171 MAC: 00:23:8a:e9:7a:b0	
4   IP: 10.11.17.3 MAC: 00:a0:98:11:d3:9c	
4   IP: 10.11.17.11 MAC: 34:40:b5:3c:18:fe	5   IP: 10.11.17.11 MAC: 34:40:b5:3c:18:fe
4   IP: 10.11.17.170 MAC: 00:23:8a:e9:80:40	5   IP: 10.11.17.170 MAC: 00:23:8a:e9:80:40
4   IP: 10.11.17.12 MAC: 34:40:b5:40:b8:fe	
5   _ Use --script-args=newtargets 0 to add the results as targets	5   _ Use --script-args=newtargets 5 to add the results as targets
5   targets-asn: 1	5   targets-asn: 6
5   _ targets-asn.asn is a mandatory 2 parameter	5   _ targets-asn.asn is a mandatory 7 parameter
5   Initiating ARP Ping Scan at 18:01	5   Initiating ARP Ping Scan at 17:27
5   Scanning 10.11.17.133 [1 port]	5   Scanning 10.11.17.135 [1 port]
5   Completed ARP Ping Scan at 18:01, 5 0.03s elapsed (1 total hosts)	6   Completed ARP Ping Scan at 17:27, 0 0.02s elapsed (1 total hosts)
5   Initiating Parallel DNS resolution 6 of 1 host. at 18:01	6   Initiating Parallel DNS resolution 1 of 1 host. at 17:27
5   Completed Parallel DNS resolution 7 of 1 host. at 18:01, 0.00s elapsed	6   Completed Parallel DNS resolution 2 of 1 host. at 17:27, 0.00s elapsed
5   Initiating SYN Stealth Scan at 8 18:01	6   Initiating SYN Stealth Scan at 3 17:27
5   Scanning 10.11.17.133 [1000 ports]	6   Scanning 10.11.17.135 [1000 ports]

6 Discovered open port 22/tcp on 0 10.11.17.133	
6 Discovered open port 8080/tcp on 1 10.11.17.133	6 Discovered open port 8080/tcp on 5 10.11.17.135
	6 Discovered open port 22/tcp on 6 10.11.17.135
6 Discovered open port 8181/tcp on 2 10.11.17.133	6 Discovered open port 8181/tcp on 7 10.11.17.135
6 Discovered open port 1099/tcp on 3 10.11.17.133	
6 Completed SYN Stealth Scan at 4 18:01, 0.07s elapsed (1000 total ports)	6 Completed SYN Stealth Scan at 8 17:27, 0.05s elapsed (1000 total ports)
6 Initiating UDP Scan at 18:01 5	6 Initiating UDP Scan at 17:27 9
6 Scanning 10.11.17.133 [1000 ports] 6	7 Scanning 10.11.17.135 [1000 ports] 0
6 Increasing send delay for 7 10.11.17.133 from 0 to 50 due to max_successful_tryno increase to 5	7 Increasing send delay for 1 10.11.17.135 from 0 to 50 due to max_successful_tryno increase to 5
6 Increasing send delay for 8 10.11.17.133 from 50 to 100 due to 11 out of 12 dropped probes since last increase.	7 Increasing send delay for 2 10.11.17.135 from 50 to 100 due to 11 out of 12 dropped probes since last increase.
6 Increasing send delay for 9 10.11.17.133 from 100 to 200 due to 11 out of 11 dropped probes since last increase.	7 Increasing send delay for 3 10.11.17.135 from 100 to 200 due to 11 out of 11 dropped probes since last increase.
7 UDP Scan Timing: About 9.00% done; 0 ETC: 18:07 (0:05:13 remaining)	7 UDP Scan Timing: About 9.04% done; 4 ETC: 17:32 (0:05:12 remaining)
7 Increasing send delay for 1 10.11.17.133 from 200 to 400 due to 11 out of 11 dropped probes since last increase.	7 Increasing send delay for 5 10.11.17.135 from 200 to 400 due to 11 out of 11 dropped probes since last increase.
7 Increasing send delay for 2 10.11.17.133 from 400 to 800 due to 11 out of 11 dropped probes since last increase.	7 Increasing send delay for 6 10.11.17.135 from 400 to 800 due to 11 out of 11 dropped probes since last increase.

UDP Scan Timing: About 12.87% done; ETC: 18:09 (0:06:53 remaining)	UDP Scan Timing: About 12.87% done; ETC: 17:35 (0:06:53 remaining)
UDP Scan Timing: About 15.84% done; ETC: 18:10 (0:08:03 remaining)	UDP Scan Timing: About 15.86% done; ETC: 17:36 (0:08:03 remaining)
UDP Scan Timing: About 19.01% done; ETC: 18:12 (0:08:35 remaining)	UDP Scan Timing: About 19.01% done; ETC: 17:37 (0:08:35 remaining)
UDP Scan Timing: About 41.33% done; ETC: 18:15 (0:08:03 remaining)	UDP Scan Timing: About 41.13% done; ETC: 17:40 (0:08:02 remaining)
UDP Scan Timing: About 47.87% done; ETC: 18:15 (0:07:19 remaining)	UDP Scan Timing: About 47.57% done; ETC: 17:41 (0:07:21 remaining)
UDP Scan Timing: About 54.01% done; ETC: 18:15 (0:06:34 remaining)	UDP Scan Timing: About 53.61% done; ETC: 17:41 (0:06:38 remaining)
UDP Scan Timing: About 59.76% done; ETC: 18:15 (0:05:50 remaining)	UDP Scan Timing: About 59.24% done; ETC: 17:41 (0:05:54 remaining)
UDP Scan Timing: About 65.29% done; ETC: 18:16 (0:05:05 remaining)	UDP Scan Timing: About 64.67% done; ETC: 17:41 (0:05:10 remaining)
UDP Scan Timing: About 70.60% done; ETC: 18:16 (0:04:20 remaining)	UDP Scan Timing: About 69.99% done; ETC: 17:41 (0:04:25 remaining)
UDP Scan Timing: About 76.03% done; ETC: 18:16 (0:03:34 remaining)	UDP Scan Timing: About 75.21% done; ETC: 17:41 (0:03:41 remaining)
UDP Scan Timing: About 81.34% done; ETC: 18:16 (0:02:47 remaining)	UDP Scan Timing: About 80.43% done; ETC: 17:42 (0:02:55 remaining)
UDP Scan Timing: About 86.57% done; ETC: 18:16 (0:02:01 remaining)	UDP Scan Timing: About 85.96% done; ETC: 17:42 (0:02:07 remaining)
	UDP Scan Timing: About 91.17% done; ETC: 17:42 (0:01:20 remaining)



8 5 UDP Scan Timing: About 92.00% done; ETC: 18:16 (0:01:13 remaining)	9 0 UDP Scan Timing: About 96.40% done; ETC: 17:42 (0:00:33 remaining)
8 6 Completed UDP Scan at 18:17, 950.11s elapsed (1000 total ports)	9 1 Completed UDP Scan at 17:42, 1950.09s elapsed (1000 total ports)
8 7 Initiating Service scan at 18:17	9 2 Initiating Service scan at 17:42
8 8 Scanning 48 services on 10.11.17.133	9 3 Scanning 47 services on 10.11.17.135
	9 4 Service scan Timing: About 8.51% done; ETC: 17:53 (0:09:51 remaining)
8 9 Service scan Timing: About 10.42% done; ETC: 18:25 (0:07:44 remaining)	9 5 Service scan Timing: About 68.09% done; ETC: 17:45 (0:00:41 remaining)
9 0 Service scan Timing: About 72.92% done; ETC: 18:19 (0:00:32 remaining)	9 6 Service scan Timing: About 80.85% done; ETC: 17:45 (0:00:31 remaining)
9 1 Service scan Timing: About 79.17% done; ETC: 18:19 (0:00:32 remaining)	
9 2 Completed Service scan at 18:19, 145.06s elapsed (48 services on 1 host)	9 7 Completed Service scan at 17:45, 145.07s elapsed (47 services on 1 host)
9 3 Initiating OS detection (try #1) against 10.11.17.133	9 8 Initiating OS detection (try #1) against 10.11.17.135
9 4 NSE: Script scanning 10.11.17.133.	9 9 NSE: Script scanning 10.11.17.135.
9 5 Initiating NSE at 18:19	1 0 Initiating NSE at 17:45
9 6 Completed NSE at 18:20, 18.99s elapsed	1 1 Completed NSE at 17:45, 18.84s elapsed
9 7 Initiating NSE at 18:20	1 2 Initiating NSE at 17:45

Completed NSE at 18:20, 2.38s elapsed	Completed NSE at 17:45, 2.38s elapsed
Initiating NSE at 18:20	Initiating NSE at 17:45
Completed NSE at 18:20, 0.02s elapsed	Completed NSE at 17:45, 0.02s elapsed
Nmap scan report for 10.11.17.133	Nmap scan report for 10.11.17.135
Host is up (0.00042s latency).	Host is up (0.00024s latency).
Not shown: 1952 closed ports, 44 open filtered ports	Not shown: 1953 closed ports, 44 open filtered ports
PORT STATE SERVICE VERSION	PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.7 (Ubuntu Linux; protocol 2.0)	22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.7 (Ubuntu Linux; protocol 2.0)
_banner: SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.7	_banner: SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.7
ssh-hostkey:	ssh-hostkey:
1024 9b:b1:af:cc:79:66:12:38:6b:68:30:83:fa:94:39:73 (DSA)	1024 9b:b1:af:cc:79:66:12:38:6b:68:30:83:fa:94:39:73 (DSA)
2048 ca:b1:d4:d8:0f:3f:39:30:f1:27:21:d9:b:be:2b:4c:26 (RSA)	2048 ca:b1:d4:d8:0f:3f:39:30:f1:27:21:d4b:be:2b:4c:26 (RSA)
_ 256 db:f9:1a:38:38:b8:b1:42:35:bc:a1:a0:f:b6:3e:0d:e1 (ECDSA)	_ 256 db:f9:1a:38:38:b8:b1:42:35:bc:a1:a5f:b6:3e:0d:e1 (ECDSA)

1   ssh2-enum-algos: 1 1	1   ssh2-enum-algos: 1 6
1   kex_algorithms: (8) 1 2	1   kex_algorithms: (8) 1 7
1   <a href="mailto:curve25519-sha256@libssh.org">curve25519-sha256@libssh.org</a> 1 3	1   <a href="mailto:curve25519-sha256@libssh.org">curve25519-sha256@libssh.org</a> 1 8
1   ecdh-sha2-nistp256 1 4	1   ecdh-sha2-nistp256 1 9
1   ecdh-sha2-nistp384 1 5	1   ecdh-sha2-nistp384 1 0
1   ecdh-sha2-nistp521 1 6	1   ecdh-sha2-nistp521 1 1
1   diffie-hellman-group- 1exchange-sha256 7	1   diffie-hellman-group- 2exchange-sha256 2
1   diffie-hellman-group- 1exchange-sha1 8	1   diffie-hellman-group- 2exchange-sha1 3
1   diffie-hellman-group14- 1sha1 9	1   diffie-hellman-group14- 2sha1 4
1   diffie-hellman-group1-sha1 2 0	1   diffie-hellman-group1-sha1 2 5
1   server_host_key_algorithms: 2 (4) 1	1   server_host_key_algorithms: 2 (4) 6
1   ssh-rsa 2 2	1   ssh-rsa 2 7
1   ssh-dss 2 3	1   ssh-dss 2 8

1 2 4	ecdsa-sha2-nistp256	1 2 5	ecdsa-sha2-nistp256
1 2 5	ssh-ed25519	1 3 0	ssh-ed25519
1 2 6	encryption_algorithms: (16)	1 3 1	encryption_algorithms: (16)
1 2 7	aes128-ctr	1 3 2	aes128-ctr
1 2 8	aes192-ctr	1 3 3	aes192-ctr
1 2 9	aes256-ctr	1 3 4	aes256-ctr
1 3 0	arcfour256	1 3 5	arcfour256
1 3 1	arcfour128	1 3 6	arcfour128
1 3 2	<a href="#">aes128-gcm@openssh.com</a>	1 3 7	<a href="#">aes128-gcm@openssh.com</a>
1 3 3	<a href="#">aes256-gcm@openssh.com</a>	1 3 8	<a href="#">aes256-gcm@openssh.com</a>
1 3 4	<a href="#">chacha20-poly1305@openssh.com</a>	1 3 9	<a href="#">chacha20-poly1305@openssh.com</a>
1 3 5	aes128-cbc	1 4 0	aes128-cbc
1 3 6	3des-cbc	1 4 1	3des-cbc

1 3 7	blowfish-cbc	1 4 2	blowfish-cbc
1 3 8	cast128-cbc	1 4 3	cast128-cbc
1 3 9	aes192-cbc	1 4 4	aes192-cbc
1 4 0	aes256-cbc	1 4 5	aes256-cbc
1 4 1	arcfour	1 4 6	arcfour
1 4 2	<a href="mailto:rijndael-cbc@lysator.liu.se">rijndael-cbc@lysator.liu.se</a>	1 4 7	<a href="mailto:rijndael-cbc@lysator.liu.se">rijndael-cbc@lysator.liu.se</a>
1 4 3	mac_algorithms: (19)	1 4 8	mac_algorithms: (19)
1 4 4	<a href="mailto:hmac-md5-etm@openssh.com">hmac-md5-etm@openssh.com</a>	1 4 9	<a href="mailto:hmac-md5-etm@openssh.com">hmac-md5-etm@openssh.com</a>
1 4 5	<a href="mailto:hmac-sha1-etm@openssh.com">hmac-sha1-etm@openssh.com</a>	1 5 0	<a href="mailto:hmac-sha1-etm@openssh.com">hmac-sha1-etm@openssh.com</a>
1 4 6	<a href="mailto:umac-64-etm@openssh.com">umac-64-etm@openssh.com</a>	1 5 1	<a href="mailto:umac-64-etm@openssh.com">umac-64-etm@openssh.com</a>
1 4 7	<a href="mailto:umac-128-etm@openssh.com">umac-128-etm@openssh.com</a>	1 5 2	<a href="mailto:umac-128-etm@openssh.com">umac-128-etm@openssh.com</a>
1 4 8	<a href="mailto:hmac-sha2-256-etm@openssh.com">hmac-sha2-256-etm@openssh.com</a>	1 5 3	<a href="mailto:hmac-sha2-256-etm@openssh.com">hmac-sha2-256-etm@openssh.com</a>
1 4 9	<a href="mailto:hmac-sha2-512-etm@openssh.com">hmac-sha2-512-etm@openssh.com</a>	1 5 4	<a href="mailto:hmac-sha2-512-etm@openssh.com">hmac-sha2-512-etm@openssh.com</a>

1 E C	<a href="#">hmac-ripemd160-etm@openssh.com</a>	1 E E	<a href="#">hmac-ripemd160-etm@openssh.com</a>
1 E 1	<a href="#">hmac-sha1-96-etm@openssh.com</a>	1 E E	<a href="#">hmac-sha1-96-etm@openssh.com</a>
1 E 2	<a href="#">hmac-md5-96-etm@openssh.com</a>	1 E 7	<a href="#">hmac-md5-96-etm@openssh.com</a>
1 E 3	hmac-md5	1 E 8	hmac-md5
1 E 4	hmac-sha1	1 E 9	hmac-sha1
1 E E	<a href="#">umac-64@openssh.com</a>	1 E C	<a href="#">umac-64@openssh.com</a>
1 E E	<a href="#">umac-128@openssh.com</a>	1 E 1	<a href="#">umac-128@openssh.com</a>
1 E 7	hmac-sha2-256	1 E 2	hmac-sha2-256
1 E 8	hmac-sha2-512	1 E 3	hmac-sha2-512
1 E 9	hmac-ripemd160	1 E 4	hmac-ripemd160
1 E C	<a href="#">hmac-ripemd160@openssh.com</a>	1 E E	<a href="#">hmac-ripemd160@openssh.com</a>
1 E 1	hmac-sha1-96	1 E E	hmac-sha1-96
1 E 2	hmac-md5-96	1 E 7	hmac-md5-96

1   compression_algorithms: (2)	1   compression_algorithms: (2)
6	6
3	8
1   none	1   none
6	6
4	9
1   _ <a href="mailto:zlib@openssh.com">zlib@openssh.com</a>	1   _ <a href="mailto:zlib@openssh.com">zlib@openssh.com</a>
6	7
5	0
1   1099/tcp open java-rmi Java RMI Registry	
6	
6	
1   rmi-dumpregistry:	
6	
7	
1   karaf-root	
6	
8	
1   javax.management.remote.rmi.RMIServerImpl_Stub	
6	
9	
1   @10.11.17.133:44444	
6	
7	
0	
1   extends	
6	
7	
1	
1   java.rmi.server.RemoteStub	
6	
7	
2	
1   extends	
6	
7	
3	
1   _ java.rmi.server.RemoteObject	
6	
7   ject	
4	
1   18080/tcp open http Jetty	1   18080/tcp open http Jetty
6   8.1.15.v20140411	6   8.1.15.v20140411
7	7
5	1

	1   http-auth-finder: 7 2
	1   Spidering limited to: 7 maxdepth=3; maxpagecount=20; 3 withinhost=10.11.17.135
	1   url met 7 hod 4
	1   _ http://10.11.17.135:8080/ FORM 7 5
1   _http-comments- 7  _displayer: Couldn't find any 6  _comments.	1   http-comments-displayer: 7 6
	1   Spidering limited to: 7 maxdepth=3; maxpagecount=20; 7 withinhost=10.11.17.135
	1   7 8
	1   Path: http://10.11.17.135:8080/ 7 9
	1   Line number: 31 8 0
	1   Comment: 8 1
	1   <!-- <script 1   type="text/javascript" data- 8   main="src/main.js" 2   src="vendor/requirejs/require.js"& gt;</script>-->
	1   8 3



	1   Path: 8 <a href="http://10.11.17.135:8080/vendor/requirejs/require.js">http://10.11.17.135:8080/vendor/requirejs/require.js</a> 4
	1   Line number: 1 8 5
	1   Comment: 8 6
	1   /** vim: 8 et:ts=4:sw=4:sts=4 7
	1   * @license RequireJS 2.1.14 Copyright (c) 2010-2014, 8 The Dojo Foundation All Rights 8 Reserved.
	1   * Available via the MIT 8 or new BSD license. 9
	1   * see: 9 <a href="http://github.com/jrburke/requirejs">http://github.com/jrburke/requirejs</a> for 0 details
	1   */ 9 1
	1   9 2
	1   Path: <a href="http://10.11.17.135:8080/">http://10.11.17.135:8080/</a> 9 3
	1   Line number: 10 9 4
	1   Comment: 9 5

	1         <!-- HTML5 shim and 9 Respond.js IE8 support of HTML5 6 elements and media queries -->
	1   9   7
	1         Path: 9 <a href="http://10.11.17.135:8080/assets/opendaylight-&lt;br/&gt;8 dlux-0.1.0.css">http://10.11.17.135:8080/assets/opendaylight- 8 dlux-0.1.0.css</a>
	1         Line number: 7508 9   9
	2         Comment: 0   0
	2         /* 0   1
	2         * Copyright (c) 2014 0 Cisco Systems, Inc. and 2 others. All rights reserved.
	2         * 0   3
	2         * This program and the 0 accompanying materials are made 4 available under the
	2         * terms of the Eclipse 0 Public License v1.0 which 5 accompanies this distribution,
	2         * and is available at 0 <a href="http://www.eclipse.org/legal/epl-v10.html">http://www.eclipse.org/legal/epl-v10.html</a> 6
	2         */ 0   7
	2   0   8

	2   Path: <a href="http://10.11.17.135:8080/">http://10.11.17.135:8080/</a> 0 9
	2   Line number: 17 1 0
	2   Comment: 1 1
	2   <!-- compiled CSS -- 1 > 2
	2   1 3
	2   Path: <a href="http://10.11.17.135:8080/">http://10.11.17.135:8080/</a> 1 4
	2   Line number: 32 1 5
	2   Comment: 1 6
	2   <!--<script 1 type="text/javascript" 7 src="src/feature_verification.js"& gt;</script>-->
	2   1 8
	2   Path: <a href="http://10.11.17.135:8080/">http://10.11.17.135:8080/</a> 1 9
	2   Line number: 33 2 0

	2   Comment:
	2
	1
	2   <!-- the font-awesome
	2   is different from the 'official'
	2   one -->
	2
	2
	3
	2   Path: <a href="http://10.11.17.135:8080/">http://10.11.17.135:8080/</a>
	2
	4
	2   Line number: 148
	2
	5
	2   Comment:
	2
	6
	2   <!-- Change this to a
	2   button or input when using this as
	7   a form -->
	2
	2
	8
	2   Path:
	2   <a href="http://10.11.17.135:8080/assets/opendaylight-dlux-0.1.0.css">http://10.11.17.135:8080/assets/opendaylight-</a>
	9   <a href="http://10.11.17.135:8080/assets/opendaylight-dlux-0.1.0.css">dlux-0.1.0.css</a>
	2   Line number: 6698
	3
	0
	2   Comment:
	3
	1
	2   /*
	3
	2
	2   * Copyright (c) 2014
	3   Cisco Systems, Inc. and
	3   others. All rights reserved.

	2   *
	3
	4
	2   * This program and the
	3 accompanying materials are made
	5 available under the
	2   * terms of the Eclipse
	3 Public License v1.0 which
	6 accompanies this distribution,
	2   * and is available at
	3 <a href="http://www.eclipse.org/legal/epl-v10.html">http://www.eclipse.org/legal/epl-v10.html</a>
	7
	2   */
	3
	8
	2
	3
	9
	2   Path: <a href="http://10.11.17.135:8080/">http://10.11.17.135:8080/</a>
	4
	0
	2   Line number: 12
	4
	1
	2   Comment:
	4
	2
	2   &lt;!--[if lt IE 9]&gt;
	4
	3
	2   &lt;script
	4 src="assets/js/html5shiv.js"&gt;&l
	4 t;/script&gt;
	2   &lt;script
	4 src="assets/js/respond.min.js"&gt;
	5 &lt;/script&gt;
	2   _ &lt;![endif]--&gt;
	4
	6

	2   _http-date: Thu, 02 Jun 2016 4 20:21:11 GMT; -59d01h24m15s from 7 local time.
	2   http-grep: 4 8
	2   (1) <a href="http://10.11.17.135:8080/">http://10.11.17.135:8080/</a> : 4 9
	2   (1) ip: 5 0
	2   _ + 10.11.17.135 5 1
1   http-headers: 7 7	2   http-headers: 5 2
1   Content-Type: 7 text/html; charset=ISO-8859-1 8	2   Date: Thu, 02 Jun 2016 5 20:21:11 GMT 3
1   Cache-Control: must- 7 revalidate, no-cache, no-store 9	2   Server: 5 Jetty(8.1.15.v20140411) 4
	2   Last-Modified: Thu, 02 Jun 5 2016 14:30:38 GMT 5
	2   ETag: "1f60-5344c732c5f80" 5 6
	2   Accept-Ranges: bytes 5 7
1   Content-Length: 1365 8 0	2   Content-Length: 8032 5 8
	2   Vary: Accept-Encoding 5 9

1   Connection: close 8 1	2   Connection: close 6 0
1   Server: 8 Jetty(8.1.15.v20140411) 2	2   Content-Type: text/html 6 1
1   8 3	2   6 2
1   _ (Request type: GET) 8 4	2   _ (Request type: HEAD) 6 3
1   http-methods: 8 5	2   http-methods: 6 4
1   Supported Methods: GET HEAD 8 TRACE OPTIONS 6	2   Supported Methods: GET 6 HEAD POST OPTIONS 5
1   _ Potentially risky methods: 8 TRACE 7	
1   _http-mobileversion-checker: No 8 mobile version detected. 8	2   _http-mobileversion-checker: No 6 mobile version detected. 6
	2   _http-open-proxy: Proxy might be 6 redirecting requests 7
1   _http-referer-checker: Couldn't 8 find any cross-domain scripts. 9	2   http-referer-checker: 6 8
	2   Spidering limited to: 6 maxpagecount=30 9
	2   <a href="http://code.jquery.com/jquery-1.10.2.js">http://code.jquery.com/jquery-1.10.2.js</a> 7 0

	<a href="http://ajax.googleapis.com/ajax/libs/angularjs/1.4.8/angular.min.js">http://ajax.googleapis.com/ajax/libs/angularjs/1.4.8/angular.min.js</a>
	<a href="http://code.jquery.com/ui/1.11.4/jquery-ui.js">http://code.jquery.com/ui/1.11.4/jquery-ui.js</a>
1  _http-server-header: 9 Jetty(8.1.15.v20140411) 0	2  _http-server-header: 7 Jetty(8.1.15.v20140411) 3
1  _http-title: Error 403 Forbidden 9 1	2  _http-title: OpenDaylight Dlux 7 4
1   http-traceroute: 9 2	2   http-traceroute: 7 5
1  _ Possible reverse proxy 9 detected. 3	2  _ Possible reverse proxy 7 detected. 6
1   http-useragent-tester: 9 4	2   http-useragent-tester: 7 7
1   9 5	2   7 8
1   Allowed User Agents: 9 6	2   Allowed User Agents: 7 9
1   Mozilla/5.0 (compatible; 9 Nmap Scripting Engine; 7 <a href="https://nmap.org/book/nse.html">https://nmap.org/book/nse.html</a> )	2   Mozilla/5.0 (compatible; 8 Nmap Scripting Engine; 0 <a href="https://nmap.org/book/nse.html">https://nmap.org/book/nse.html</a> )
1   libwww 9 8	2   libwww 8 1
1   lwp-trivial 9 9	2   lwp-trivial 8 2
2   libcurl-agent/1.0 0 0	2   libcurl-agent/1.0 8 3



2 0 1	PHP/	2 8 4	PHP/
2 0 2	Python-urllib/2.5	2 8 5	Python-urllib/2.5
2 0 3	GT::WWW	2 8 6	GT::WWW
2 0 4	Snoopy	2 8 7	Snoopy
2 0 5	MFC_Tear_Sample	2 8 8	MFC_Tear_Sample
2 0 6	HTTP::Lite	2 8 9	HTTP::Lite
2 0 7	PHPCrawl	2 9 0	PHPCrawl
2 0 8	URI::Fetch	2 9 1	URI::Fetch
2 0 9	Zend_Http_Client	2 9 2	Zend_Http_Client
2 1 0	http client	2 9 3	http client
2 1 1	PECL::HTTP	2 9 4	PECL::HTTP
2 1 2	Wget/1.13.4 (linux-gnu)	2 9 5	Wget/1.13.4 (linux-gnu)
2 1 3	WWW-Mechanize/1.34	2 9 6	WWW-Mechanize/1.34

2   _ 1 4	2   _ 9 7
2   _http-xssed: No previously 1 reported XSS vuln. 5	2   _http-xssed: No previously 9 reported XSS vuln. 8
2 8181/tcp open http Jetty 1 8.1.15.v20140411 6	2 8181/tcp open http Jetty 9 8.1.15.v20140411 9
2   _http-comments-displayer: 1 Couldn't find any comments. 7	3   _http-comments-displayer: 0 Couldn't find any comments. 0
	3   _http-date: Thu, 02 Jun 2016 0 20:21:11 GMT; -59d01h24m12s from 1 local time.
2   http-headers: 1 8	3   http-headers: 0 2
2   Content-Type: 1 text/html; charset=ISO-8859-1 9	3   Date: Thu, 02 Jun 2016 0 20:21:12 GMT 3
2   Cache-Control: must- 2 revalidate, no-cache, no-store 0	3   Server: 0 Jetty(8.1.15.v20140411) 4
2   Content-Length: 1365 2 1	3   Content-Length: 202 0 5
2   Connection: close 2 2	3   Connection: close 0 6
2   Server: 2 Jetty(8.1.15.v20140411) 3	3   Content-Type: text/html; 0 charset=iso-8859-1 7
2   2 4	3   0 8

2   _ (Request type: GET) 2   5	3   _ (Request type: GET) 3   5
2   http-methods: 2   6	3   3
2   Supported Methods: GET HEAD 2   TRACE OPTIONS 7	3   3
2   Potentially risky methods: 2   TRACE 8	3   3
2   _http-mobileversion-checker: No 2   mobile version detected. 9	3   _http-mobileversion-checker: No 1   mobile version detected. 10
2   _http-referer-checker: Couldn't 3   find any cross-domain scripts. 10	3   _http-referer-checker: Couldn't 1   find any cross-domain scripts. 11
2   _http-server-header: 3   Jetty(8.1.15.v20140411) 11	3   _http-server-header: 1   Jetty(8.1.15.v20140411) 12
2   _http-title: Error 403 Forbidden 3   12	3   _http-title: 403 Forbidden 3   13
2   http-traceroute: 3   13	3   http-traceroute: 3   14
2   _ Possible reverse proxy 3   detected. 14	3   _ Possible reverse proxy 1   detected. 15
2   http-useragent-tester: 3   15	3   http-useragent-tester: 3   16
2   3   16	3   3   17

2   Allowed User Agents:	3   Allowed User Agents:
3	1
7	8
2   Mozilla/5.0 (compatible;	3   Mozilla/5.0 (compatible;
3   Nmap Scripting Engine;	1   Nmap Scripting Engine;
8   <a href="https://nmap.org/book/nse.html">https://nmap.org/book/nse.html</a> )	9   <a href="https://nmap.org/book/nse.html">https://nmap.org/book/nse.html</a> )
2   libwww	3   libwww
3	2
9	0
2   lwp-trivial	3   lwp-trivial
4	2
0	1
2   libcurl-agent/1.0	3   libcurl-agent/1.0
4	2
1	2
2   PHP/	3   PHP/
4	2
2	3
2   Python-urllib/2.5	3   Python-urllib/2.5
4	2
3	4
2   GT::WWW	3   GT::WWW
4	2
4	5
2   Snoopy	3   Snoopy
4	2
5	6
2   MFC_Tear_Sample	3   MFC_Tear_Sample
4	2
6	7
2   HTTP::Lite	3   HTTP::Lite
4	2
7	8
2   PHPCrawl	3   PHPCrawl
4	2
8	9
2   URI::Fetch	3   URI::Fetch
4	3
9	0

2   Zend_Http_Client 5 0	3   Zend_Http_Client 3 1
2   http client 5 1	3   http client 3 2
2   PECL::HTTP 5 2	3   PECL::HTTP 3 3
2   Wget/1.13.4 (linux-gnu) 5 3	3   Wget/1.13.4 (linux-gnu) 3 4
2   WWW-Mechanize/1.34 5 4	3   WWW-Mechanize/1.34 3 5
2   _ 5 5	3   _ 3 6
2   _http-xssed: No previously 5 reported XSS vuln. 6	3   _http-xssed: No previously 3 reported XSS vuln. 7
2   MAC Address: 5 00:50:56:A6:16:B1 (VMware) 7	3   MAC Address: 3 00:50:56:A6:16:C8 (VMware) 8
2   Device type: general purpose 5 8	3   Device type: general purpose 3 9
2   Running: Linux 3.X 4.X 5 9	3   Running: Linux 3.X 4.X 4 0
2   OS CPE: 6 cpe:/o:linux:linux_kernel:3 0 cpe:/o:linux:linux_kernel:4	3   OS CPE: 4 cpe:/o:linux:linux_kernel:3 1 cpe:/o:linux:linux_kernel:4
2   OS details: Linux 3.2 - 4.4 6 1	3   OS details: Linux 3.2 - 4.4 4 2
2   Uptime guess: 8.183 days 5 (since Sat Jul 23 13:55:48 2016) 7	3   Uptime guess: 6.228 days 3 (since Mon Jul 25 12:16:53 2016) 4 3

2 Network Distance: 1 hop 6 3	3 Network Distance: 1 hop 4 4
2 TCP Sequence Prediction: 6 Difficulty=263 (Good luck!) 4	3 TCP Sequence Prediction: 4 Difficulty=256 (Good luck!) 5
2 IP ID Sequence Generation: All 6 zeros 5	3 IP ID Sequence Generation: All 4 zeros 6
2 Service Info: OS: Linux; CPE: 6 cpe:/o:linux:linux_kernel 6	3 Service Info: OS: Linux; CPE: 4 cpe:/o:linux:linux_kernel 7
2 6 7	3 4 8
2 Host script results: 6 8	3 Host script results: 4 9
2  _fcrdns: FAIL (No PTR record) 6 9	3  _fcrdns: FAIL (No PTR record) 5 0
2   firewalk: 7 0	3   firewalk: 5 1
2   7 HOP HOST PROTOCOL BLOCKE 1 D PORTS	3   5 HOP HOST PROTOCOL BLOCKE 2 D PORTS
2  _0 10.11.17.39 udp 3,12 7 0,137,389,500,502,829,996,1051,106 4 5	3  _0 10.11.17.39 udp 23,1 5 35,177,639,1028,1039,1645,1804,366 4 4,4672
2  _ipidseq: All zeros 7 3	3  _ipidseq: All zeros 5 4
2  _path-mtu: PMTU == 1500 7 4	3  _path-mtu: PMTU == 1500 5 5

2   qscan:	3   qscan:
7	5
5	6
2   PORT FAMILY MEAN	3   PORT FAMILY MEAN
7 (us) STDDEV LOSS (%)	5 (us) STDDEV LOSS (%)
6	7
2	3
7 1 0 235.40 37.32 0	5
7 .0%	6
2   22 0 230.80 78.96	3   1 0 160.80 35.02
7 0.0%	5 0.0%
8	8
2	3
7 1099 0 237.60 54.46 0	5 22 0 183.70 57.58 0
9 .0%	9 .0%
2	3
8 8080 0 219.60 42.14 0	6 8080 0 166.70 77.00 0
0 .0%	0 .0%
2   _8181 0 219.30 43.06	3   _8181 0 156.10 30.23
8 0.0%	6 0.0%
1	1
2   traceroute-geolocation:	3   traceroute-geolocation:
8	6
2	2
2   HOP RTT ADDRESS GEOLO	3   HOP RTT ADDRESS GEOLO
8 CATION	6 CATION
3	3
2   _ 1 0.43 10.11.17.133 - , -	3   _ 1 0.24 10.11.17.135 - , -
8	6
4	4
2	3
8	6
5	5
2 TRACEROUTE	3 TRACEROUTE
8	6
6	6

2 HOP RTT ADDRESS	3 HOP RTT ADDRESS
6	6
7	7
2 1 0.43 ms 10.11.17.133	3 1 0.24 ms 10.11.17.135
8	6
8	8
2	3
8	6
9	9
2 NSE: Script Post-scanning.	3 NSE: Script Post-scanning.
9	7
0	0
2 Initiating NSE at 18:20	3 Initiating NSE at 17:45
9	7
1	1
2 Completed NSE at 18:20, 0.00s	3 Completed NSE at 17:45, 0.00s
9 elapsed	7 elapsed
2	2
2 Initiating NSE at 18:20	3 Initiating NSE at 17:45
9	7
3	3
2 Completed NSE at 18:20, 0.00s	3 Completed NSE at 17:45, 0.00s
9 elapsed	7 elapsed
4	4
2 Initiating NSE at 18:20	3 Initiating NSE at 17:45
9	7
5	5
2 Completed NSE at 18:20, 0.00s	3 Completed NSE at 17:45, 0.00s
9 elapsed	7 elapsed
6	6
2 Read data files from:	3 Read data files from:
9 /usr/bin/../../share/nmap	7 /usr/bin/../../share/nmap
7	7
2 OS and Service detection	3 OS and Service detection
9 performed. Please report any	7 performed. Please report any
8 incorrect results at	8 incorrect results at
<a href="https://nmap.org/submit/">https://nmap.org/submit/</a> .	<a href="https://nmap.org/submit/">https://nmap.org/submit/</a> .



<pre> 2 Nmap done: 1 IP address (1 host g up) scanned in 1129.98 seconds t </pre>	<pre> 3 Nmap done: 1 IP address (1 host 7 up) scanned in 1129.93 seconds t </pre>
<pre> 3 Raw packets sent: 2716 C (99.128KB)   Rcvd: 2046 (98.422KB) C </pre>	<pre> 3 Raw packets sent: 2706 8 (97.384KB)   Rcvd: 2046 (98.627KB) C </pre>
<pre> &lt;/output&gt;&lt;host comment=""&gt;&lt;status state="up"&gt;&lt;/status&gt;&lt;address addrtype="ipv4" vendor="" addr="10.11.17.133"&gt;&lt;/address&gt;&lt;add ress addrtype="mac" vendor="VMware" addr="00:50:56:A6:16:B1"&gt;&lt;/address &gt;&lt;hostnames&gt;&lt;/hostnames&gt;&lt;ports&gt;&lt;ex traports count="1952" state="closed"&gt;&lt;/extraports&gt;&lt;extra ports count="44" state="open filtered"&gt;&lt;/extraports &gt;&lt;port protocol="tcp" portid="22"&gt;&lt;state reason="syn- ack" state="open" reason_ttl="64"&gt;&lt;/state&gt;&lt;service product="OpenSSH" name="ssh" extrainfo="Ubuntu Linux; protocol 2.0" version="6.6.1p1 Ubuntu 3 2ubuntu2.7" conf="10" C method="probed"&gt;&lt;/service&gt;&lt;/port&gt;&lt; 1 port protocol="tcp" portid="1099"&gt;&lt;state reason="syn- ack" state="open" reason_ttl="64"&gt;&lt;/state&gt;&lt;service p roduct="Java RMI Registry" method="probed" conf="10" name="java- rmi"&gt;&lt;/service&gt;&lt;/port&gt;&lt;port protocol="tcp" portid="8080"&gt;&lt;state reason="syn- ack" state="open" reason_ttl="64"&gt;&lt;/state&gt;&lt;service p roduct="Jetty" version="8.1.15.v20140411" method="probed" conf="10" name="http"&gt;&lt;/service&gt;&lt;/port&gt;&lt;port protocol="tcp" portid="8181"&gt;&lt;state reason="syn- ack" state="open" reason_ttl="64"&gt;&lt;/state&gt;&lt;service product="Jetty" </pre>	<pre> &lt;/output&gt;&lt;host comment=""&gt;&lt;status state="up"&gt;&lt;/status&gt;&lt;address addrtype="ipv4" vendor="" addr="10.11.17.135"&gt;&lt;/address&gt;&lt;add ress addrtype="mac" vendor="VMware" addr="00:50:56:A6:16:C8"&gt;&lt;/address &gt;&lt;hostnames&gt;&lt;/hostnames&gt;&lt;ports&gt;&lt;ex traports count="1953" state="closed"&gt;&lt;/extraports&gt;&lt;extra ports count="44" state="open filtered"&gt;&lt;/extraports &gt;&lt;port protocol="tcp" portid="22"&gt;&lt;state reason="syn- ack" state="open" reason_ttl="64"&gt;&lt;/state&gt;&lt;service product="OpenSSH" name="ssh" extrainfo="Ubuntu Linux; protocol 2.0" version="6.6.1p1 Ubuntu 3 2ubuntu2.7" conf="10" 8 method="probed"&gt;&lt;/service&gt;&lt;/port&gt;&lt; 1 port protocol="tcp" portid="8080"&gt;&lt;state reason="syn- ack" state="open" reason_ttl="64"&gt;&lt;/state&gt;&lt;service product="Jetty" version="8.1.15.v20140411" method="probed" conf="10" name="http"&gt;&lt;/service&gt;&lt;/port&gt;&lt;port protocol="tcp" portid="8181"&gt;&lt;state reason="syn- ack" state="open" reason_ttl="64"&gt;&lt;/state&gt;&lt;service product="Jetty" version="8.1.15.v20140411" method="probed" conf="10" name="http"&gt;&lt;/service&gt;&lt;/port&gt;&lt;por ts&gt;&lt;os&gt;&lt;portused state="open" portid="22" proto="tcp"&gt;&lt;/portused&gt;&lt;portused state="closed" portid="1" proto="tcp"&gt;&lt;/portused&gt;&lt;portused </pre>

```

version="8.1.15.v20140411"
method="probed" conf="10"
name="http"></service></port></ports><os><portused state="open"
portid="22"
proto="tcp"></portused><portused
state="closed" portid="1"
proto="tcp"></portused><portused
state="closed" portid="2"
proto="udp"></portused><osmatch
line="59764" name="Linux 3.2 -
4.4" accuracy="100"><osclass
type="general purpose"
osfamily="Linux" vendor="Linux"
osgen="4.X"
accuracy="100"></osclass></osmatch
></os><uptime lastboot="Sat Jul
23 13:55:48 2016"
seconds="707054"></uptime><tcpsequ
ence index="263"
values="C3A165E5,B4E902DB,DA14ED26
,C4595CAD,EB699E7E,6A43EE13"
difficulty="Good
luck!"></tcpsequence><ipidsequence
values="0,0,0,0,0,0" class="All
zeros"></ipidsequence><tcptssequen
ce
values="A891D8F,A891DA8,A891DC1,A8
91DDA,A891DF3,A891E0C"
class="other"></tcptssequence><tra
ce port="" proto=""><hop
rtt="0.43" host=""
ipaddr="10.11.17.133"
ttl="1"></hop></trace></host><runs
tats><finished timestr="Sun Jul 31
18:20:02 2016"
time="1470003602"></finished><host
s down="0" total="1"
up="1"></hosts></runstats></nmapru
n>

```

```

state="closed" portid="2"
proto="udp"></portused><osmatch
line="59764" name="Linux 3.2 -
4.4" accuracy="100"><osclass
type="general purpose"
osfamily="Linux" vendor="Linux"
osgen="4.X"
accuracy="100"></osclass></osmatch
></os><uptime lastboot="Mon Jul
25 12:16:53 2016"
seconds="538132"></uptime><tcpsequ
ence index="256"
values="4B015D9B,FD34DB46,A9CEBC9B
,D60FDF05,7B9211A2,9DEC9D36"
difficulty="Good
luck!"></tcpsequence><ipidsequence
values="0,0,0,0,0,0" class="All
zeros"></ipidsequence><tcptssequen
ce
values="804B9DF,804B9F8,804BA11,80
4BA2A,804BA43,804BA5C"
class="other"></tcptssequence><tra
ce port="" proto=""><hop
rtt="0.24" host=""
ipaddr="10.11.17.135"
ttl="1"></hop></trace></host><runs
tats><finished timestr="Sun Jul 31
17:45:45 2016"
time="1470001545"></finished><host
s down="0" total="1"
up="1"></hosts></runstats></nmapru
n>

```

## Nikto

n	1	root@kali:~# nikto -h "10.11.17.133:8080" -vhost 10.11.17.133	n	1	root@kali:~# nikto -h "10.11.17.135:8080" -vhost 10.11.17.135
	2	- Nikto v2.1.6		2	- Nikto v2.1.6
	3	-----		3	-----
n	4	+ Target IP: 10.11.17.133	n	4	+ Target IP: 10.11.17.135
	5	+ Target Hostname: 10.11.17.133		5	+ Target Hostname: 10.11.17.135
	6	+ Target Port: 8080		6	+ Target Port: 8080
n	7	+ Start Time: 2016-08-20 09:56:06 (GMT-4)	n	7	+ Start Time: 2016-08-20 09:46:27 (GMT-4)
	8	-----		8	-----
	9	+ Server: Jetty(8.1.15.v20140411)		9	+ Server: Jetty(8.1.15.v20140411)
t	10	+ The anti-clickjacking X-Frame-Options header is not present.	t	10	+ Server leaks inodes via ETags, header found with file /, fields: 0xda50x5357905500b00
	11	+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS			
	12	+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type			
	13	+ No CGI Directories found (use '-C all' to force check all possible dirs)			
	14	+ Jetty(8.1.15.v20140411) appears to be outdated (current is at least Jetty(9.2.10-v20150310)). Jetty 8.1.16.v20140903 and 7.6.16.v20140903 are also current.		11	+ Jetty(8.1.15.v20140411) appears to be outdated (current is at least Jetty(9.0.6))
	15	+ Allowed HTTP Methods: GET, HEAD, TRACE, OPTIONS		12	+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
	16	+ Default account found for 'opendaylight' at /auth/ (ID 'admin', PW 'admin'). Generic account discovered..		13	+ OSVDB-3233: /icons/README: Apache default file found.
	17	+ OSVDB-3092: /auth/: This might be interesting...			
	18	+ 7579 requests: 0 error(s) and 7 item(s) reported on remote host		14	+ 8348 requests: 0 error(s) and 4 item(s) reported on remote host
	19	+ End Time: 2016-08-20 09:56:19 (GMT-4) (13 seconds)		15	+ End Time: 2016-08-20 09:46:41 (GMT-4) (14 seconds)
	20	-----		16	-----
	21	+ 1 host(s) tested		17	+ 1 host(s) tested
	22			18	

## Uniscan

<a href="#">n</a> 1	root@kali:~# uniscan -u 10.11.17.133:8080 -qd	<a href="#">n</a> 1	root@kali:~# uniscan -u 10.11.17.135:8080 -qd
2	##### ####	2	##### ###
3	# Uniscan project #	3	# Uniscan project #
4	# http://uniscan.sourceforge.net/ #	4	# http://uniscan.sourceforge.net/ #
5	##### ####	5	##### ###
6	V. 6.3	6	V. 6.3
7		7	
<a href="#">n</a> 8		<a href="#">n</a>	
9	Scan date: 20-8-2016 10:51:6	8	Scan date: 20-8-2016 10:37:48
10	===== ===== ===== ===	9	===== ===== ===== =====
<a href="#">n</a> 11	Domain: http://10.11.17.133:8080/	<a href="#">n</a> 10	Domain: http://10.11.17.135:8080/
12	Server: Jetty(8.1.15.v20140411)	11	Server: Jetty(8.1.15.v20140411)
<a href="#">n</a> 13	IP: 10.11.17.133	<a href="#">n</a> 12	IP: 10.11.17.135
14	===== ===== ===== ===	13	===== ===== ===== =====
15		14	
16	Directory check:	15	Directory check:
17	===== ===== ===== ===	16	===== ===== ===== =====
18		17	
19	Crawler Started:	18	Crawler Started:
20	Plugin name: phpinfo() Disclosure v.1 Loaded.	19	Plugin name: phpinfo() Disclosure v.1 Loaded.
21	Plugin name: Upload Form Detect v.1.1 Loaded.	20	Plugin name: Upload Form Detect v.1.1 Loaded.
22	Plugin name: FCKeditor upload test v.1 Loaded.	21	Plugin name: FCKeditor upload test v.1 Loaded.
23	Plugin name: Web Backdoor Disclosure v.1.1 Loaded.	22	Plugin name: Web Backdoor Disclosure v.1.1 Loaded.
24	Plugin name: Code Disclosure v.1.1 Loaded.	23	Plugin name: Code Disclosure v.1.1 Loaded.

25	Plugin name: Timthumb <= 1.32 vulnerability v.1 Loaded.	24	Plugin name: Timthumb <= 1.32 vulnerability v.1 Loaded.
26	Plugin name: E-mail Detection v.1.1 Loaded.	25	Plugin name: E-mail Detection v.1.1 Loaded.
27	Plugin name: External Host Detect v.1.2 Loaded.	26	Plugin name: External Host Detect v.1.2 Loaded.
<a href="#">n</a> 28	[+] Crawling finished, 1 URL's found!	<a href="#">n</a> 27	[+] Crawling finished, 15 URL's found!
29		28	
30	PHPinfo() Disclosure:	29	PHPinfo() Disclosure:
31		30	
32	File Upload Forms:	31	File Upload Forms:
33		32	
34	FCKeditor File Upload:	33	FCKeditor File Upload:
35		34	
36	Web Backdoors:	35	Web Backdoors:
37		36	
38	Source Code Disclosure:	37	Source Code Disclosure:
39		38	
40	Timthumb:	39	Timthumb:
41		40	
42	E-mails:	41	E-mails:
43		42	
44	External hosts:	43	External hosts:
<a href="#">n</a>		<a href="#">n</a> 44	[+] External Host Found: http://code.jquery.com
		45	[+] External Host Found: http://ajax.googleapis.com
45		46	
46	Ignored Files:	47	Ignored Files:
47	=====	48	=====
	=====		=====
	=====		=====
	===		
48	Dynamic tests:	49	Dynamic tests:
49	Plugin name: Learning New Directories v.1.2 Loaded.	50	Plugin name: Learning New Directories v.1.2 Loaded.
50	Plugin name: FCKeditor tests v.1.1 Loaded.	51	Plugin name: FCKeditor tests v.1.1 Loaded.
51	Plugin name: Timthumb <= 1.32 vulnerability v.1 Loaded.	52	Plugin name: Timthumb <= 1.32 vulnerability v.1 Loaded.
52	Plugin name: Find Backup Files v.1.2 Loaded.	53	Plugin name: Find Backup Files v.1.2 Loaded.
53	Plugin name: Blind SQL-injection tests v.1.3 Loaded.	54	Plugin name: Blind SQL-injection tests v.1.3 Loaded.

54	Plugin name: Local File Include tests v.1.1 Loaded.	55	Plugin name: Local File Include tests v.1.1 Loaded.
55	Plugin name: PHP CGI Argument Injection v.1.1 Loaded.	56	Plugin name: PHP CGI Argument Injection v.1.1 Loaded.
56	Plugin name: Remote Command Execution tests v.1.1 Loaded.	57	Plugin name: Remote Command Execution tests v.1.1 Loaded.
57	Plugin name: Remote File Include tests v.1.2 Loaded.	58	Plugin name: Remote File Include tests v.1.2 Loaded.
58	Plugin name: SQL-injection tests v.1.2 Loaded.	59	Plugin name: SQL-injection tests v.1.2 Loaded.
59	Plugin name: Cross-Site Scripting tests v.1.2 Loaded.	60	Plugin name: Cross-Site Scripting tests v.1.2 Loaded.
60	Plugin name: Web Shell Finder v.1.3 Loaded.	61	Plugin name: Web Shell Finder v.1.3 Loaded.
61	[+] 0 New directories added	62	[+] 3 New directories added
62		63	
63		64	
64	FCKeditor tests:	65	FCKeditor tests:
65		66	
66		67	
67	Timthumb < 1.33 vulnerability:	68	Timthumb < 1.33 vulnerability:
68		69	
69		70	
70	Backup Files:	71	Backup Files:
71		72	
72		73	
73	Blind SQL Injection:	74	Blind SQL Injection:
74		75	
75		76	
76	Local File Include:	77	Local File Include:
77		78	
78		79	
79	PHP CGI Argument Injection:	80	PHP CGI Argument Injection:

80		81	
81		82	
82	Remote Command Execution:	83	Remote Command Execution:
83		84	
84		85	
85	Remote File Include:	86	Remote File Include:
86		87	
87		88	
88	SQL Injection:	89	SQL Injection:
89		90	
90		91	
91	Cross-Site Scripting (XSS):	92	Cross-Site Scripting (XSS):
92		93	
93		94	
94	Web Shell Finder:	95	Web Shell Finder:
95	=====	96	=====
	=====		=====
	=====		=====
	===		
96	Scan end date: 20-8-2016 10:51:34	97	Scan end date: 20-8-2016 10:38:16
<a href="#">t</a>		<a href="#">t</a>	
97		98	

## Masscan

<a href="#">n</a>	1	root@kali:~# masscan -p0-65535 10.11.17.133	<a href="#">n</a>	1	root@kali:~# masscan -p0-65535 10.11.17.135
	2			2	
<a href="#">n</a>	3	Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2016-08-20 14:49:16 GMT	<a href="#">n</a>	3	Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2016-08-20 14:16:48 GMT
	4	-- forced options: -sS -Pn -n -- randomize-hosts -v --send-eth		4	-- forced options: -sS -Pn -n -- randomize-hosts -v --send-eth
	5	Initiating SYN Stealth Scan		5	Initiating SYN Stealth Scan
	6	Scanning 1 hosts [65536 ports/host]		6	Scanning 1 hosts [65536 ports/host]

<a href="#">t</a>	7	Discovered open port 1790/tcp on 10.11.17.133	<a href="#">t</a>		
	8	Discovered open port 22/tcp on 10.11.17.133			
	9	Discovered open port 54743/tcp on 10.11.17.133			
	10	Discovered open port 44444/tcp on 10.11.17.133			
	11	Discovered open port 8181/tcp on 10.11.17.133		7	Discovered open port 8181/tcp on 10.11.17.135
	12	Discovered open port 8101/tcp on 10.11.17.133		8	Discovered open port 22/tcp on 10.11.17.135
	13	Discovered open port 1099/tcp on 10.11.17.133		9	Discovered open port 1099/tcp on 10.11.17.135
	14	Discovered open port 40004/tcp on 10.11.17.133			
	15	Discovered open port 8185/tcp on 10.11.17.133			
	16	Discovered open port 6633/tcp on 10.11.17.133			
	17	Discovered open port 34343/tcp on 10.11.17.133			
	18	Discovered open port 6653/tcp on 10.11.17.133			
	19	Discovered open port 8080/tcp on 10.11.17.133		10	Discovered open port 8080/tcp on 10.11.17.135
	20				

## DnsTracer

<a href="#">n</a>	1	root@kali:~# dnstracer -r 3 -v 10.11.17.133:8080	<a href="#">n</a>	1	root@kali:~# dnstracer -r 3 -v 10.11.17.135:8080
	2	Tracing to 10.11.17.133:8080[a] via 10.12.1.11, maximum of 3 retries		2	Tracing to 10.11.17.135:8080[a] via 10.12.1.11, maximum of 3 retries
	3	10.12.1.11 (10.12.1.11) IP HEADER		3	10.12.1.11 (10.12.1.11) IP HEADER
	4	- Destination address: 10.12.1.11		4	- Destination address: 10.12.1.11
	5	DNS HEADER (send)		5	DNS HEADER (send)
<a href="#">n</a>	6	- Identifier: 0x3459	<a href="#">n</a>	6	- Identifier: 0x774B
	7	- Flags: 0x00 (Q )		7	- Flags: 0x00 (Q )
	8	- Opcode: 0 (Standard query)		8	- Opcode: 0 (Standard query)
	9	- Return code: 0 (No error)		9	- Return code: 0 (No error)
	10	- Number questions: 1		10	- Number questions: 1



	11	- Number answer RR: 0		1 1	- Number answer RR: 0
	12	- Number authority RR: 0		1 2	- Number authority RR: 0
	13	- Number additional RR: 0		1 3	- Number additional RR: 0
	14	QUESTIONS (send)		1 4	QUESTIONS (send)
<a href="#">n</a>	15	- Queryname: (2)10(2)11(2)17(8)133:8080	<a href="#">n</a>	1 5	- Queryname: (2)10(2)11(2)17(8)135:8080
	16	- Type: 1 (A)		1 6	- Type: 1 (A)
	17	- Class: 1 (Internet)		1 7	- Class: 1 (Internet)
	18	DNS HEADER (recv)		1 8	DNS HEADER (recv)
<a href="#">n</a>	19	- Identifier: 0x3459	<a href="#">n</a>	1 9	- Identifier: 0x774B
	20	- Flags: 0x8080 (R RA )		2 0	- Flags: 0x8083 (R RA )
	21	- Opcode: 0 (Standard query)		2 1	- Opcode: 0 (Standard query)
<a href="#">n</a>	22	- Return code: 0 (No error)	<a href="#">n</a>	2 2	- Return code: 3 (Name error)
	23	- Number questions: 1		2 3	- Number questions: 1
	24	- Number answer RR: 0		2 4	- Number answer RR: 0
<a href="#">n</a>	25	- Number authority RR: 13	<a href="#">n</a>	2 5	- Number authority RR: 1
	26	- Number additional RR: 12		2 6	- Number additional RR: 0
	27	QUESTIONS (recv)		2 7	QUESTIONS (recv)
<a href="#">n</a>	28	- Queryname: (2)10(2)11(2)17(8)133:8080	<a href="#">n</a>	2 8	- Queryname: (2)10(2)11(2)17(8)135:8080
	29	- Type: 1 (A)		2 9	- Type: 1 (A)
	30	- Class: 1 (Internet)		3 0	- Class: 1 (Internet)
	31	AUTHORITY RR		3 1	AUTHORITY RR
	32	- Domainname: (1).		3 2	- Domainname: (1).

<a href="#">n</a>	33	- Type: 2 (NS)	<a href="#">n</a>	3	- Type: 6 (SOA)
	34	- Class: 1 (Internet)		3	- Class: 1 (Internet)
				4	
<a href="#">t</a>	35	- TTL: 69872 (19h24m32s)	<a href="#">t</a>	3	- TTL: 3699 (1h1m39s)
				5	
	36	- Resource length: 4		3	- Resource length: 64
				6	
	37	- Resource data: (1)b(12)root-servers(3)net			
	38	AUTHORITY RR			
	39	- Domainname: (1).			
	40	- Type: 2 (NS)			
	41	- Class: 1 (Internet)			
	42	- TTL: 69872 (19h24m32s)			
	43	- Resource length: 4			
	44	- Resource data: (1)a(12)root-servers(3)net		3	- Resource data: serial:
				7	2016062300 mname: (1)a(12)root-servers(3)net rname:
					(5)nstld(12)verisign-grs(3)com
	45	AUTHORITY RR		3	
				8	
	46	- Domainname: (1).			
	47	- Type: 2 (NS)			
	48	- Class: 1 (Internet)			
	49	- TTL: 69872 (19h24m32s)			
	50	- Resource length: 4			
	51	- Resource data: (1)l(12)root-servers(3)net			
	52	AUTHORITY RR			
	53	- Domainname: (1).			
	54	- Type: 2 (NS)			
	55	- Class: 1 (Internet)			
	56	- TTL: 69872 (19h24m32s)			
	57	- Resource length: 4			
	58	- Resource data: (1)e(12)root-servers(3)net			
	59	AUTHORITY RR			
	60	- Domainname: (1).			
	61	- Type: 2 (NS)			
	62	- Class: 1 (Internet)			
	63	- TTL: 69872 (19h24m32s)			
	64	- Resource length: 4			
	65	- Resource data: (1)g(12)root-servers(3)net			
	66	AUTHORITY RR			

67	- Domainname: (1).			
68	- Type: 2 (NS)			
69	- Class: 1 (Internet)			
70	- TTL: 69872 (19h24m32s)			
71	- Resource length: 4			
72	- Resource data: (1)m(12)root-servers(3)net			
73	AUTHORITY RR			
74	- Domainname: (1).			
75	- Type: 2 (NS)			
76	- Class: 1 (Internet)			
77	- TTL: 69872 (19h24m32s)			
78	- Resource length: 4			
79	- Resource data: (1)f(12)root-servers(3)net			
80	AUTHORITY RR			
81	- Domainname: (1).			
82	- Type: 2 (NS)			
83	- Class: 1 (Internet)			
84	- TTL: 69872 (19h24m32s)			
85	- Resource length: 4			
86	- Resource data: (1)c(12)root-servers(3)net			
87	AUTHORITY RR			
88	- Domainname: (1).			
89	- Type: 2 (NS)			
90	- Class: 1 (Internet)			
91	- TTL: 69872 (19h24m32s)			
92	- Resource length: 4			
93	- Resource data: (1)h(12)root-servers(3)net			
94	AUTHORITY RR			
95	- Domainname: (1).			
96	- Type: 2 (NS)			
97	- Class: 1 (Internet)			
98	- TTL: 69872 (19h24m32s)			
99	- Resource length: 4			
100	- Resource data: (1)j(12)root-servers(3)net			
101	AUTHORITY RR			
102	- Domainname: (1).			
103	- Type: 2 (NS)			

104	- Class: 1 (Internet)			
105	- TTL: 69872 (19h24m32s)			
106	- Resource length: 4			
107	- Resource data: (1)d(12)root-servers(3)net			
108	AUTHORITY RR			
109	- Domainname: (1).			
110	- Type: 2 (NS)			
111	- Class: 1 (Internet)			
112	- TTL: 69872 (19h24m32s)			
113	- Resource length: 4			
114	- Resource data: (1)i(12)root-servers(3)net			
115	AUTHORITY RR			
116	- Domainname: (1).			
117	- Type: 2 (NS)			
118	- Class: 1 (Internet)			
119	- TTL: 69872 (19h24m32s)			
120	- Resource length: 20			
121	- Resource data: (1)k(12)root-servers(3)net			
122	ADDITIONAL RR			
123	- Domainname: (1)g(12)root-servers(3)net			
124	- Type: 1 (A)			
125	- Class: 1 (Internet)			
126	- TTL: 69515 (19h18m35s)			

12 7	- Resource length: 4			
12 8	- Resource data: 192.112.36.4			
12 9	ADDITIONAL RR			
13 0	- Domainname: (1)f(12)root-servers(3)net			
13 1	- Type: 28 (unknown)			
13 2	- Class: 1 (Internet)			
13 3	- TTL: 69515 (19h18m35s)			
13 4	- Resource length: 16			
13 5	- Resource data: 2001:0500:002f:0000:0000:0000:0000:000f			
13 6	ADDITIONAL RR			
13 7	- Domainname: (1)f(12)root-servers(3)net			
13 8	- Type: 1 (A)			
13 9	- Class: 1 (Internet)			
14 0	- TTL: 69515 (19h18m35s)			
14 1	- Resource length: 4			
14 2	- Resource data: 192.5.5.241			
14 3	ADDITIONAL RR			
14 4	- Domainname: (1)e(12)root-servers(3)net			
14 5	- Type: 1 (A)			
14 6	- Class: 1 (Internet)			
14 7	- TTL: 371098 (4d7h4m58s)			
14 8	- Resource length: 4			
14 9	- Resource data: 192.203.230.10			

15 0	ADDITIONAL RR			
15 1	- Domainname: (1)d(12)root-servers(3)net			
15 2	- Type: 28 (unknown)			
15 3	- Class: 1 (Internet)			
15 4	- TTL: 70569 (19h36m9s)			
15 5	- Resource length: 16			
15 6	- Resource data: 2001:0500:002d:0000:0000:0000:0000:000d			
15 7	ADDITIONAL RR			
15 8	- Domainname: (1)d(12)root-servers(3)net			
15 9	- Type: 1 (A)			
16 0	- Class: 1 (Internet)			
16 1	- TTL: 70079 (19h27m59s)			
16 2	- Resource length: 4			
16 3	- Resource data: 199.7.91.13			
16 4	ADDITIONAL RR			
16 5	- Domainname: (1)c(12)root-servers(3)net			
16 6	- Type: 28 (unknown)			
16 7	- Class: 1 (Internet)			
16 8	- TTL: 69515 (19h18m35s)			
16 9	- Resource length: 16			
17 0	- Resource data: 2001:0500:0002:0000:0000:0000:0000:000c			
17 1	ADDITIONAL RR			

17 2	- Domainname: (1)c(12)root-servers(3)net			
17 3	- Type: 1 (A)			
17 4	- Class: 1 (Internet)			
17 5	- TTL: 69515 (19h18m35s)			
17 6	- Resource length: 4			
17 7	- Resource data: 192.33.4.12			
17 8	ADDITIONAL RR			
17 9	- Domainname: (1)b(12)root-servers(3)net			
18 0	- Type: 28 (unknown)			
18 1	- Class: 1 (Internet)			
18 2	- TTL: 69515 (19h18m35s)			
18 3	- Resource length: 16			
18 4	- Resource data: 2001:0500:0084:0000:0000:0000:0000:000b			
18 5	ADDITIONAL RR			
18 6	- Domainname: (1)b(12)root-servers(3)net			
18 7	- Type: 1 (A)			
18 8	- Class: 1 (Internet)			
18 9	- TTL: 69515 (19h18m35s)			
19 0	- Resource length: 4			
19 1	- Resource data: 192.228.79.201			
19 2	ADDITIONAL RR			
19 3	- Domainname: (1)a(12)root-servers(3)net			
19 4	- Type: 28 (unknown)			

19 5	- Class: 1 (Internet)			
19 6	- TTL: 501515 (5d19h18m35s)			
19 7	- Resource length: 16			
19 8	- Resource data: 2001:0503:ba3e:0000:0000:0000:0002:0030			
19 9	ADDITIONAL RR			
20 0	- Domainname: (1)a(12)root-servers(3)net			
20 1	- Type: 1 (A)			
20 2	- Class: 1 (Internet)			
20 3	- TTL: 501515 (5d19h18m35s)			
20 4	- Resource length: 4			
20 5	- Resource data: 198.41.0.4			
20 6	Refers backwards			
20 7			3 9	

### DotDotPwn

<a href="#"><u>n</u></a>	1	root@kali:~# dotdotpwn.pl -m http -h 10.11.17.133:8080 -M GET	<a href="#"><u>n</u></a>	1	root@kali:~# dotdotpwn.pl -m http -h 10.11.17.135:8080 -M GET
	2	[+] Report name: Reports/10.11.17.133:8080_08-21-2016_12-19.txt		2	[+] Report name: Reports/10.11.17.135:8080_08-21-2016_12-16.txt
	3	[===== TARGET INFORMATION =====]		3	[===== TARGET INFORMATION =====]
<a href="#"><u>n</u></a>	4	[+] Hostname: 10.11.17.133:8080	<a href="#"><u>n</u></a>	4	[+] Hostname: 10.11.17.135:8080
	5	[+] Protocol: http		5	[+] Protocol: http
	6	[+] Port: 80		6	[+] Port: 80
	7	[===== TRAVERSAL ENGINE =====]		7	[===== TRAVERSAL ENGINE =====]
	8	[+] Creating Traversal patterns (mix of dots and slashes)		8	[+] Creating Traversal patterns (mix of dots and slashes)



9	[+] Multiplying 6 times the traversal patterns (-d switch)	9	[+] Multiplying 6 times the traversal patterns (-d switch)
10	[+] Creating the Special Traversal patterns	10	[+] Creating the Special Traversal patterns
11	[+] Translating (back)slashes in the filenames	11	[+] Translating (back)slashes in the filenames
12	[+] Adapting the filenames according to the OS type detected (generic)	12	[+] Adapting the filenames according to the OS type detected (generic)
13	[+] Including Special suffixes	13	[+] Including Special suffixes
14	[+] Traversal Engine DONE ! - Total traversal tests created: 19680	14	[+] Traversal Engine DONE ! - Total traversal tests created: 19680
15	[===== TESTING RESULTS =====]	15	[===== TESTING RESULTS =====]
16	[+] Ready to launch 3.33 traversals per second	16	[+] Ready to launch 3.33 traversals per second
17	[+] Press Enter to start the testing (You can stop it pressing Ctrl + C)	17	[+] Press Enter to start the testing (You can stop it pressing Ctrl + C)
<a href="#">n</a> 18	[*] HTTP Status: 400   Testing Path: http://10.11.17.133:8080:80/../../etc/passwd	<a href="#">n</a> 18	[*] HTTP Status: 400   Testing Path: http://10.11.17.135:8080:80/../../etc/passwd
19	[*] HTTP Status: 400   Testing Path: http://10.11.17.133:8080:80/../../etc/issue	19	[*] HTTP Status: 400   Testing Path: http://10.11.17.135:8080:80/../../etc/issue
20	[*] HTTP Status: 400   Testing Path: http://10.11.17.133:8080:80/../../boot.ini	20	[*] HTTP Status: 400   Testing Path: http://10.11.17.135:8080:80/../../boot.ini
21	[*] HTTP Status: 400   Testing Path: http://10.11.17.133:8080:80/../../windows/system32/drivers/etc/hosts	21	[*] HTTP Status: 400   Testing Path: http://10.11.17.135:8080:80/../../windows/system32/drivers/etc/hosts
22	[*] HTTP Status: 400   Testing Path: http://10.11.17.133:8080:80/../../etc/passwd	22	[*] HTTP Status: 400   Testing Path: http://10.11.17.135:8080:80/../../etc/passwd
23	[*] HTTP Status: 400   Testing Path: http://10.11.17.133:8080:80/../../etc/issue	23	[*] HTTP Status: 400   Testing Path: http://10.11.17.135:8080:80/../../etc/issue
24	[*] HTTP Status: 400   Testing Path: http://10.11.17.133:8080:80/../../boot.ini	24	[*] HTTP Status: 400   Testing Path: http://10.11.17.135:8080:80/../../boot.ini
25	[*] HTTP Status: 400   Testing Path: http://10.11.17.133:8080:80/../../windows/system32/drivers/etc/hosts	25	[*] HTTP Status: 400   Testing Path: http://10.11.17.135:8080:80/../../windows/system32/drivers/etc/hosts
26	[*] HTTP Status: 400   Testing Path: http://10.11.17.133:8080:80/../../etc/passwd	26	[*] HTTP Status: 400   Testing Path: http://10.11.17.135:8080:80/../../etc/passwd
27	[*] HTTP Status: 400   Testing Path: http://10.11.17.133:8080:80/../../etc/issue	27	[*] HTTP Status: 400   Testing Path: http://10.11.17.135:8080:80/../../etc/issue

2	[*] HTTP Status: 400   Testing Path: 8 http://10.11.17.133:8080:80/../../../../boot.i ni	2	[*] HTTP Status: 400   Testing Path: 8 http://10.11.17.135:8080:80/../../../../boot.i ni
2	[*] HTTP Status: 400   Testing Path: 9 http://10.11.17.133:8080:80/../../../../windo ws/system32/drivers/etc/hosts	2	[*] HTTP Status: 400   Testing Path: 9 http://10.11.17.135:8080:80/../../../../windo ws/system32/drivers/etc/hosts
3	[*] HTTP Status: 400   Testing Path: 0 http://10.11.17.133:8080:80/../../../../etc/ passwd	3	[*] HTTP Status: 400   Testing Path: 0 http://10.11.17.135:8080:80/../../../../etc/ passwd
3	[*] HTTP Status: 400   Testing Path: 1 http://10.11.17.133:8080:80/../../../../etc/ issue	3	[*] HTTP Status: 400   Testing Path: 1 http://10.11.17.135:8080:80/../../../../etc/ issue
3	[*] HTTP Status: 400   Testing Path: 2 http://10.11.17.133:8080:80/../../../../boo t.ini	3	[*] HTTP Status: 400   Testing Path: 2 http://10.11.17.135:8080:80/../../../../boo t.ini
3	[*] HTTP Status: 400   Testing Path: 3 http://10.11.17.133:8080:80/../../../../win dows/system32/drivers/etc/hosts	3	[*] HTTP Status: 400   Testing Path: 3 http://10.11.17.135:8080:80/../../../../win dows/system32/drivers/etc/hosts
3	[*] HTTP Status: 400   Testing Path: 4 http://10.11.17.133:8080:80/../../../../et c/passwd	3	[*] HTTP Status: 400   Testing Path: 4 http://10.11.17.135:8080:80/../../../../et c/passwd
3	[*] HTTP Status: 400   Testing Path: 5 http://10.11.17.133:8080:80/../../../../et c/issue	3	[*] HTTP Status: 400   Testing Path: 5 http://10.11.17.135:8080:80/../../../../et c/issue
3	[*] HTTP Status: 400   Testing Path: 6 http://10.11.17.133:8080:80/../../../../b oot.ini	3	[*] HTTP Status: 400   Testing Path: 6 http://10.11.17.135:8080:80/../../../../b oot.ini
3	[*] HTTP Status: 400   Testing Path: 7 http://10.11.17.133:8080:80/../../../../wi ndows/system32/drivers/etc/hosts	3	[*] HTTP Status: 400   Testing Path: 7 http://10.11.17.135:8080:80/../../../../wi ndows/system32/drivers/etc/hosts
3	[*] HTTP Status: 400   Testing Path: 8 http://10.11.17.133:8080:80/../../../../.. etc/passwd	3	[*] HTTP Status: 400   Testing Path: 8 http://10.11.17.135:8080:80/../../../../.. etc/passwd
3	[*] HTTP Status: 400   Testing Path: 9 http://10.11.17.133:8080:80/../../../../.. etc/issue	3	[*] HTTP Status: 400   Testing Path: 9 http://10.11.17.135:8080:80/../../../../.. etc/issue
4	[*] HTTP Status: 400   Testing Path: 0 http://10.11.17.133:8080:80/../../../../.. boot.ini	4	[*] HTTP Status: 400   Testing Path: 0 http://10.11.17.135:8080:80/../../../../.. boot.ini
4	[*] HTTP Status: 400   Testing Path: 1 http://10.11.17.133:8080:80/../../../../.. windows/system32/drivers/etc/hosts	4	[*] HTTP Status: 400   Testing Path: 1 http://10.11.17.135:8080:80/../../../../.. windows/system32/drivers/etc/hosts
4		4	
4	[+] Total Traversals found: 0	4	[+] Total Traversals found: 1994
<a href="#">n</a> 3		<a href="#">n</a> 3	

4	[-] Fuzz testing aborted	4	[-] Fuzz testing aborted
4		4	
<a href="#">t</a> 4	[+] Report saved:	<a href="#">t</a> 4	[+] Report saved:
5	Reports/10.11.17.133:8080_08-21-2016_12-19.txt	5	Reports/10.11.17.135:8080_08-21-2016_12-16.txt
4		4	
6		6	

### Enum4linux

<a href="#">n</a> 1	root@kali:~# enum4linux -U -o 10.11.17.133	<a href="#">n</a> 1	root@kali:~# enum4linux -U -o 10.11.17.135
2	Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Aug 21 15:35:43 2016	2	Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Aug 21 15:13:38 2016
3		3	
4	=====	4	=====
5	Target Information	5	Target Information
6	=====	6	=====
<a href="#">n</a> 7	Target ..... 10.11.17.133	<a href="#">n</a> 7	Target ..... 10.11.17.135
8	RID Range ..... 500-550,1000-1050	8	RID Range ..... 500-550,1000-1050
9	Username ..... "	9	Username ..... "
10	Password ..... "	10	Password ..... "
11	Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none	11	Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
12		12	
13		13	
14	=====	14	=====
<a href="#">n</a> 15	Enumerating Workgroup/Domain on 10.11.17.133	<a href="#">n</a> 15	Enumerating Workgroup/Domain on 10.11.17.135
16	=====	16	=====
<a href="#">n</a> 17	[E] Can't find workgroup/domain	<a href="#">n</a> 17	[+] Got domain/workgroup name: WORKGROUP
18			
19		18	

	2	=====		1	=====
	0	===		9	===
<a href="#">n</a>	2	Session Check on 10.11.17.133	<a href="#">n</a>	2	Session Check on 10.11.17.135
	1			0	
	2	=====		2	=====
	2	===		1	===
<a href="#">t</a>	2	Use of uninitialized value	<a href="#">t</a>		
	3	\$global_workgroup in concatenation (.) or			
		string at ./enum4linux.pl line 437.			
	2	[E] Server doesn't allow session using		2	[+]
	4	username ", password ". Aborting		2	Server 10.11.17.135 allows sessions using
		remainder of tests.			username ", password "
				2	
				3	
				2	=====
				4	=====
				2	Getting domain SID for
				5	10.11.17.135
				2	=====
				6	=====
				2	Domain Name: EVERYONE
				7	
				2	Domain Sid: (NULL SID)
				8	
				2	[+] Can't determine if host is part of
				9	domain or part of a workgroup
				3	
				0	
				3	=====
				1	=====
				3	OS information on 10.11.17.135
				2	
				3	=====
				3	=====
				3	[+] Got OS info for 10.11.17.135 from
				4	smbclient: Domain=[EVERYONE]
					OS=[Windows 6.1] Server=[Samba 4.3.9-
					Ubuntu]
				3	[+] Got OS info for 10.11.17.135 from
				5	srvinfo:
				3	OPENDAYLIGHT-LIWk Sv PrQ Unx NT
				6	SNT OpenDayLight-Lithium server (Samba,
					Ubuntu)
				3	platform_id : 500
				7	
				3	os version : 6.1
				8	

			3	server type : 0x809a03
			9	
			4	
			0	
			4	=====
			1	
			4	Users on 10.11.17.135
			2	
			4	=====
			3	
			4	index: 0x1 RID: 0x3e8 acb: 0x00000010
			4	Account: openflow Name: openflow Desc:
			4	index: 0x2 RID: 0x3e9 acb: 0x00000010
			5	Account: root Name: root Desc:
			4	
			6	
			4	user:[openflow] rid:[0x3e8]
			7	
			4	user:[root] rid:[0x3e9]
			8	
			4	enum4linux complete on Sun Aug 21
			9	15:13:39 2016
			5	
			0	
2			5	
5			1	

## Amap

<a href="#"><u>n</u></a>	1	root@kali:~# amap -bqv 10.11.17.133 8080	<a href="#"><u>n</u></a>	1	root@kali:~# amap -bqv 10.11.17.135 8080
	2	Using trigger file /etc/amap/appdefs.trig ... loaded 30 triggers		2	Using trigger file /etc/amap/appdefs.trig ... loaded 30 triggers
	3	Using response file /etc/amap/appdefs.resp ... loaded 346 responses		3	Using response file /etc/amap/appdefs.resp ... loaded 346 responses
	4	Using trigger file /etc/amap/appdefs.rpc ... loaded 450 triggers		4	Using trigger file /etc/amap/appdefs.rpc ... loaded 450 triggers
	5			5	
<a href="#"><u>n</u></a>	6	amap v5.4 (www.thc.org/thc-amap) started at 2016-08-21 16:32:51 - APPLICATION MAPPING mode	<a href="#"><u>n</u></a>	6	amap v5.4 (www.thc.org/thc-amap) started at 2016-08-21

				16:32:35 - APPLICATION MAPPING mode
	7		7	
	8	Total amount of tasks to perform in plain connect mode: 23	8	Total amount of tasks to perform in plain connect mode: 23
	9	Waiting for timeout on 23 connections ...	9	Waiting for timeout on 23 connections ...
<a href="#">n</a>	10	Protocol on 10.11.17.133:8080/tcp matches http - banner: HTTP/1.1 403 Forbidden\r\nContent-Type text/html; charset=ISO-8859-1\r\nCache-Control must-revalidate,no-cache,no-store\r\nContent-Length 1365\r\nServer Jetty(8.1.15.v20140411)\r\n\r\n<html>\n<head>\n<meta http-equiv="Content-Type" content="text/html; cha	<a href="#">n</a>	10 Protocol on 10.11.17.135:8080/tcp matches http - banner: HTTP/1.1 200 OK\r\nDate Thu, 23 Jun 2016 190803 GMT\r\nServer Jetty(8.1.15.v20140411)\r\nX-Frame-Options SAMEORIGIN\r\nLast-Modified Fri, 17 Jun 2016 130620 GMT\r\nETag "da5-5357905500b00"\r\nAccept-Ranges bytes\r\nContent-Length 3493\r\nVary Accept-Enco
			11	Protocol on 10.11.17.135:8080/tcp matches http-apache-2 - banner: HTTP/1.1 400 Bad Request\r\nDate Thu, 23 Jun 2016 190803 GMT\r\nServer Jetty(8.1.15.v20140411)\r\nContent-Length 307\r\nConnection close\r\nContent-Type text/html; charset=iso-8859-1\r\n\r\n<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n<html><head>
	11		12	
<a href="#">t</a>	12	amap v5.4 finished at 2016-08-21 16:32:57	<a href="#">t</a>	13 amap v5.4 finished at 2016-08-21 16:32:41
	13		14	

## Troubleshooting

### Common Errors:

#### ModSecurity:

*Mod\_security is not installing*

##### **What it means:**

Depending on the type of error displayed, there could be any number of reasons for this issue ranging from not having the correct permissions to using the wrong version of mod\_security.

##### **What to do:**

Ensure the following are correct/ present:

- Using root permissions
- Install command is: `apt-get install libapache2-modsecurity` and not `apt-get install libapache2-modsecurity`
- The apache version you are using is at least 2.4.7 (where your configuration file is named apache2 within /etc/apache2)

If these instructions still do not work, try using the following tutorials:

- [ModSecurity: Open Source Web Application Firewall](#)
- [HowtoForge: Linux Tutorials](#)
- [Digital Ocean: How to Set Up mod\\_security with Apache on Debian/ Ubuntu](#)

*I am unable to verify mod\_security (receiving an error like: apachectl: command not found)*

##### **What it means:**

This error usually indicates that the verify command was entered incorrectly, or that the server needs to be restarted in order for the enabling to take effect.

##### **What to do:**

To remedy this, make sure your syntax is

```
sudo apachectl -M | grep --color security2
```

Then, reload apache:

```
sudo service apache2 reload
```

---

ModRewrite:

*While installing Mod\_rewrite, I receive a the following sudo error: 'a2enmod: command not found'*

**What it means:**

Most likely, the apache server needs to have it's enabled mod file restarted. This happens occasionally but the fix is quite simple

**What to do:**

Simply restart apache with the following command:

```
sudo /etc/init.d/apache2 restart
```

After the server restarts, create a new php file anywhere within your allowed directories with a simple info print:

<pre>&lt;?php phpinfo(); ?&gt;</pre>	<table> <tr> <th data-bbox="440 716 607 779">Loaded Modules</th><td data-bbox="607 716 1437 854"> core mod_so mod_watchdog http_core mod_log_config mod_logio mod_version  mod_unixd mod_access_compat mod_alias mod_auth_basic mod_auth_core  mod_authn_file mod_authz_core mod_authz_host mod_authz_user mod_cgi mod_c  mod_dir mod_env mod_filter mod_headers mod_mime prefork mod_negotiation mo  mod_rewrite mod_security2 mod_setenvif mod_status mod_unique_id mod_userdir </td></tr> </table>	Loaded Modules	core mod_so mod_watchdog http_core mod_log_config mod_logio mod_version mod_unixd mod_access_compat mod_alias mod_auth_basic mod_auth_core mod_authn_file mod_authz_core mod_authz_host mod_authz_user mod_cgi mod_c mod_dir mod_env mod_filter mod_headers mod_mime prefork mod_negotiation mo mod_rewrite mod_security2 mod_setenvif mod_status mod_unique_id mod_userdir
Loaded Modules	core mod_so mod_watchdog http_core mod_log_config mod_logio mod_version mod_unixd mod_access_compat mod_alias mod_auth_basic mod_auth_core mod_authn_file mod_authz_core mod_authz_host mod_authz_user mod_cgi mod_c mod_dir mod_env mod_filter mod_headers mod_mime prefork mod_negotiation mo mod_rewrite mod_security2 mod_setenvif mod_status mod_unique_id mod_userdir		

You should be able to scroll to the section labeled "loaded modules" and see mod\_rewrite enabled

Syslog/ Syslog-ng:

*Syslog-ng "Error binding socket; addr='AF\_INET(\$CLIENT)', error ='Cannot assign requested address (99)' Error initializing message pipeline"<sup>16</sup>*

**What it means:**

This error states that it is unable to use the socket provided. Until it can bind, you will be unable to send or receive information from your client-host. This message typically appears once you attempt to restart the syslog-ng service.

**What to do:**

So far, the best way to fix this error is to ensure that the correct IP address has been listed within the host-server's source section. Meaning, your source configuration should look similar to this:

```
source s_network { syslog(ip(xxx.xxx.xxx.xxx) transport("tcp")); };
```

Where IP is the host's ip address and **not** the client's address. So if your host address is 10.11.17.11 that is the address that belongs in the IP field. When you have corrected the IP address, restart syslog-ng once more.

<sup>16</sup> (Joseph and Pelletier, Syslog-ng "Error binding socket; addr='AF\_INET(\$CLIENT)', error ='Cannot assign requested address (99)' Error initializing message pipeline; 2016)

Common Errors: ModRewrite:



*Error resolving reference; content='source', name='s\_network', location='/etc/syslog-ng/syslog-ng.conf:135:21' or Error resolving reference content='string', name='string', location ='/etc/syslog-ng.conf:line#:column#' (where string is anything within the single quotes)*

**What it means:**

This error states that there is a syntax error regarding the server's source parameter. This typically happens when using syslog-ng's older syntax or if you are inconsistent with your naming conventions.

**What to do:**

Review the sources section within the configuration file to make sure everything matches up.

```
log { source(s_src); source(s_network); destination(d_local); };
```

can be understood as

```
log {source(source_type); source(network_source_will_be_using_)
destination(type_of_destination); };
```

Therefore, you must make sure that in your sources section, your configuration reads

```
source s_network { syslog(ip(10.11.17.231) transport("tcp")); };
```

and not

```
source s_net { syslog(ip(10.11.17.231) transport("tcp")); };
```

or anything that would not match with the second source argument in the log configuration. The same principle applies to the source type and destination type.

*WARNING: Your configuration file uses an obsoleted keyword, please update your configuration;  
keyword='log\_prefix',  
change='program\_override'*

**What it means:**

This error may occur if syslog-ng undergoes another major update and deprecates the syntax you originally used.

**What to do:**

Visit the official documentation for syslog-ng concerning client-server and server-host configuration to find the latest updates, or simply perform a search for update notes in relation to syslog-ng

Link to Documentation: [Balabit.com](https://balabit.com)

*My packets aren't sending*

**What it means:**

If your packets are not being received by the host, there could be an issue with how they are being sent/received. At some point, there was an error within the packet structure that disallowed the packet to be sent.

**What to do:**

The best way to debug this issue is to track the details of each UDP packet being sent and received. To do this, make sure you have tcpdump installed on the server you are having issues with.<sup>17</sup>

```
sudo apt-get install tcpdump
```

After the package is installed, run a quick test to see how your packets are being handled. Below is an example of the command used alongside the results it produced (note the `-v` is necessary to see detailed information):

```
openflow@TrustedPC:/etc/syslog-ng$ sudo tcpdump host 10.11.17.135 -v
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535
bytes
12:08:50.266954 IP (tos 0x0, ttl 64, id 48888, offset 0, flags [DF], proto
TCP (6), length 56)
    10.11.17.135.41427 > TrustedPC.601: Flags [P.], cksum 0x4926 (correct),
seq 2046638940:2046638944, ack 4071257404, win 229, options [nop,nop,TS val
88550894 ecr 18323991], length 4
12:08:50.266996 IP (tos 0x0, ttl 64, id 62388, offset 0, flags [DF], proto
TCP (6), length 52)
    TrustedPC.601 > 10.11.17.135.41427: Flags [.], cksum 0x37aa (incorrect ->
0x1a5b), ack 4, win 252, options [nop,nop,TS val 18361892 ecr 88550894],
length 0
12:08:50.267168 IP (tos 0x0, ttl 64, id 48889, offset 0, flags [DF], proto
TCP (6), length 265)
    10.11.17.135.41427 > TrustedPC.601: Flags [P.], cksum 0x2678 (correct),
seq 4:217, ack 1, win 229, options [nop,nop,TS val 88550894 ecr 18361892],
length 213
12:08:50.267177 IP (tos 0x0, ttl 64, id 62389, offset 0, flags [DF], proto
TCP (6), length 52)
    TrustedPC.601 > 10.11.17.135.41427: Flags [.], cksum 0x37aa (incorrect ->
0x197e), ack 217, win 260, options [nop,nop,TS val 18361892 ecr 88550894],
length 0
12:08:55.273134 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has
10.11.17.135 tell TrustedPC, length 28
12:08:55.273343 ARP, Ethernet (len 6), IPv4 (len 4), Reply 10.11.17.135 is-at
00:50:56:a6:3c:4a (oui Unknown), length 46
12:09:02.209561 IP (tos 0x0, ttl 64, id 48890, offset 0, flags [DF], proto
TCP (6), length 56)
```

<sup>17</sup> (Joseph and Pelletier, Syslog-ng "Error binding socket; addr='AF\_INET(\$CLIENT)', error ='Cannot assign requested address (99)' Error initializing message pipeline; 2016)

```

10.11.17.135.41427 > TrustedPC.601: Flags [P.], cksum 0xaa91 (correct),
seq 217:221, ack 1, win 229, options [nop,nop,TS val 88553880 ecr 18361892],
length 4
12:09:02.209601 IP (tos 0x0, ttl 64, id 62390, offset 0, flags [DF], proto
TCP (6), length 52)
    TrustedPC.601 > 10.11.17.135.41427: Flags [.], cksum 0x37aa (incorrect ->
0x0226), ack 221, win 260, options [nop,nop,TS val 18364878 ecr 88553880],
length 0
12:09:02.209781 IP (tos 0x0, ttl 64, id 48891, offset 0, flags [DF], proto
TCP (6), length 204)
    10.11.17.135.41427 > TrustedPC.601: Flags [P.], cksum 0xbc7b (correct),
seq 221:373, ack 1, win 229, options [nop,nop,TS val 88553880 ecr 18364878],
length 152
12:09:02.209790 IP (tos 0x0, ttl 64, id 62391, offset 0, flags [DF], proto
TCP (6), length 52)
    TrustedPC.601 > 10.11.17.135.41427: Flags [.], cksum 0x37aa (incorrect ->
0x0185), ack 373, win 269, options [nop,nop,TS val 18364878 ecr 88553880],
length 0
12:09:02.210178 IP (tos 0x0, ttl 64, id 48892, offset 0, flags [DF], proto
TCP (6), length 56)
    10.11.17.135.41427 > TrustedPC.601: Flags [P.], cksum 0x9f49 (correct),
seq 373:377, ack 1, win 229, options [nop,nop,TS val 88553880 ecr 18364878],
length 4
12:09:02.210187 IP (tos 0x0, ttl 64, id 62392, offset 0, flags [DF], proto
TCP (6), length 52)
    TrustedPC.601 > 10.11.17.135.41427: Flags [.], cksum 0x37aa (incorrect ->
0x0181), ack 377, win 269, options [nop,nop,TS val 18364878 ecr 88553880],
length 0
12:09:02.210336 IP (tos 0x0, ttl 64, id 48893, offset 0, flags [DF], proto
TCP (6), length 322)
    10.11.17.135.41427 > TrustedPC.601: Flags [P.], cksum 0x0c28 (correct),
seq 377:647, ack 1, win 229, options [nop,nop,TS val 88553880 ecr 18364878],
length 270
12:09:02.210343 IP (tos 0x0, ttl 64, id 62393, offset 0, flags [DF], proto
TCP (6), length 52)
    TrustedPC.601 > 10.11.17.135.41427: Flags [.], cksum 0x37aa (incorrect ->
0x006b), ack 647, win 277, options [nop,nop,TS val 18364878 ecr 88553880],
length 0
12:09:02.278670 IP (tos 0x0, ttl 64, id 48894, offset 0, flags [DF], proto
TCP (6), length 56)
    10.11.17.135.41427 > TrustedPC.601: Flags [P.], cksum 0x9e29 (correct),
seq 647:651, ack 1, win 229, options [nop,nop,TS val 88553897 ecr 18364878],
length 4
12:09:02.278683 IP (tos 0x0, ttl 64, id 62394, offset 0, flags [DF], proto
TCP (6), length 52)
    TrustedPC.601 > 10.11.17.135.41427: Flags [.], cksum 0x37aa (incorrect ->
0x0045), ack 651, win 277, options [nop,nop,TS val 18364895 ecr 88553897],
length 0
12:09:02.278855 IP (tos 0x0, ttl 64, id 48895, offset 0, flags [DF], proto
TCP (6), length 193)
    
```

```
10.11.17.135.41427 > TrustedPC.601: Flags [P.], cksum 0x424c (correct),
seq 651:792, ack 1, win 229, options [nop,nop,TS val 88553897 ecr 18364895],
length 141
12:09:02.278864 IP (tos 0x0, ttl 64, id 62395, offset 0, flags [DF], proto
TCP (6), length 52)
    TrustedPC.601 > 10.11.17.135.41427: Flags [.], cksum 0x37aa (incorrect ->
0xffaf), ack 792, win 285, options [nop,nop,TS val 18364895 ecr 88553897],
length 0
^C
18 packets captured
18 packets received by filter
0 packets dropped by kernel
```

## Helpful Links and Resources:

Learn Regex:

<http://regexr.com/>

<http://regexone.com/>

Mod Rewrite:

[https://httpd.apache.org/docs/current/mod/mod\\_rewrite.html](https://httpd.apache.org/docs/current/mod/mod_rewrite.html)

[http://code.tutsplus.com/tutorials/an-in-depth-guide-to-mod\\_rewrite-for-apache--net-6708](http://code.tutsplus.com/tutorials/an-in-depth-guide-to-mod_rewrite-for-apache--net-6708)

Mod Security:

<https://www.modsecurity.org/>

<https://www.digitalocean.com/community/tutorials/how-to-set-up-modsecurity-with-apache-on-ubuntu-14-04-and-debian-8>

<http://www.inmotionhosting.com/support/website/modsecurity/what-is-modsecurity-and-why-is-it-important>

[https://www.howtoforge.com/changing-apache-server-name-to-whatever-you-want-with-mod\\_security-on-debian-6](https://www.howtoforge.com/changing-apache-server-name-to-whatever-you-want-with-mod_security-on-debian-6)

Apache:

<http://www.apache.org/>

<https://httpd.apache.org/>

Ajax and Angular Help:

<http://www.w3schools.com/>

Syslog-ng:

<https://www.balabit.com/network-security/syslog-ng>

## Works Cited

- A, Jesin. 2015. *How To Set Up ModSecurity with Apache on Ubuntu 14.04 and Debian 8*. June 05. Accessed jUNE 15, 2016. <https://www.digitalocean.com/community/tutorials/how-to-set-up-modsecurity-with-apache-on-ubuntu-14-04-and-debian-8>.
- Even, Loras R. 2000. *IDFAQ: What is a HoneyPot?* July 12. Accessed June 24, 2016. <https://www.sans.org/security-resources/idfaq/what-is-a-honeypot/1/9>.
- Farmad, Alireza Razavi. unknown. *HowtoForge*. unknown unknown. Accessed June 16, 2016. [https://www.howtoforge.com/changing-apache-server-name-to-whatever-you-want-with-mod\\_security-on-debian-6](https://www.howtoforge.com/changing-apache-server-name-to-whatever-you-want-with-mod_security-on-debian-6).
- Garret, Jesse James. n.d. "The traditional model for web applications (left) compared to the Ajax model (right)." Adaptive Path. *Adaptive Path*.
- Grigorik, Ilya. 2016. *HTTP caching*. May 18. <https://developers.google.com/web/fundamentals/performance/optimizing-content-efficiency/http-caching?hl=en>.
- Guzel, Burak. 2009. *HTTP Headers for Dummies*. December 2009. <http://code.tutsplus.com/tutorials/http-headers-for-dummies--net-8039>.
- Joseph, Vallie. n.d. "Syslog-Explanation." IBM-Joint Study. *Syslog-Explanation*. Poughkeepsie.
- Joseph, Vallie, and Julie Pelletier. 2016. *Syslog-ng "Error binding socket; addr='AF\_INET(\$CLIENT)', error = 'Cannot assign requested address (99)' Error initializing message pipeline;*. Poughkeepsie, NY, June 7.
- Mewbies. 2010. *AUDITING USERS WITH SYSLOG-NG*. August 06. [http://mewbies.com/how\\_to\\_log\\_users\\_using\\_syslog-ng\\_tutorial.htm](http://mewbies.com/how_to_log_users_using_syslog-ng_tutorial.htm).
- Sverdolv, Etel. 2012. *How To Set Up Mod\_Rewrite*. July 10. Accessed June 15, 2016. [https://www.digitalocean.com/community/tutorials/how-to-set-up-mod\\_rewrite](https://www.digitalocean.com/community/tutorials/how-to-set-up-mod_rewrite).
- Syslog-ng. 2015. *4.2 Configuring syslog-ng on server hosts*. April 15. <https://www.balabit.com/sites/default/files/documents/syslog-ng-ose-latest-guides/en/syslog-ng-ose-guide-admin/html/configure-servers.html>.
- . 2015. "Chapter 1. Introduction to syslog-ng." *Balabit*. April 15. <https://www.balabit.com/sites/default/files/documents/syslog-ng-ose-latest-guides/en/syslog-ng-ose-guide-admin/html/ch01s01.html>.
- . 2015. *Chapter 4. The syslog-ng OSE quick-start guide*. April 15. <https://www.balabit.com/sites/default/files/documents/syslog-ng-ose-latest-guides/en/syslog-ng-ose-guide-admin/html/chapter-quickstart.html>.
- . 2015. "The syslog-ng Open Source Edition 3.7 Administrator Guide." *Balabit*. April 15. <https://www.balabit.com/sites/default/files/documents/syslog-ng-ose-latest-guides/en/syslog-ng-ose-guide-admin/html/preface.html>.

- W3Schools. 2016. *AngularJS Scope*. June 15. Accessed June 15, 2016.  
[http://www.w3schools.com/angular/angular\\_scopes.asp](http://www.w3schools.com/angular/angular_scopes.asp).
- Weber, Johannes. 2014. *Basic syslog-ng Installation*. August 24. Accessed June 15, 2016.  
<http://blog.webernetz.net/2014/07/24/basic-syslog-ng-installation/>.
- Weeda, Eric. 2015. *About Longtail*.