University of Hertfordshire
School of Engineering and Computer Science
MSc (SW) Cyber Security

MODULE: 7COM1068

Coursework 2

PENETRATION TESTING PEOJECT REPORT

HAMDAN KAISER

STUDENT ID: 20030057

YEAR: 2021

Abstract

The main purpose of this project is to conduct a grey-box penetration testing to testing sustainability, analysis and findings of security holes that can be allow someone access to the system with an unauthorised access. This penetration is being done with the purpose of to check how the system could be effected, how risk the system is for the organisation, what and how much data could be stolen from the server and how much the system could be manipulated by the attacker. In order to take further actions against the system, this project consists of several number of penetration testing tasks that triggers few testing on the target machine which is the company's system according to our pre-prepared planning as we discussed on assignment 1. After the testing is being done, we will be preparing our penetration testing report.

After conducting vulnerability analysis, the result that we found scanning on the target shows that some of the open port allows attackers to let into their directories individually by which the information of user credentials can be found. Also, not only the credentials, but also we are able to access into the remote server and their root directories using these credentials as well. Three vulnerabilities were chosen to be exploited using the Kali Linux using VMware, metasploit, OpenVAS, Nessus and other methods as well.

Contents

Security testing of a Linux-based Computer System

1.0 Introduction

This penetration testing project is completed based on our penetration testing module, where we learnt security testing, vulnerability analysis, exploitation as well as post exploitation of a system. To take further actions against the security issues of a server, penetration testing against the network provides a layered and structured approach to defend risks that the client might face with an unauthorized access into the server (Shah, 2015). Likewise, this project includes the grey-box penetration testing on the given company's system. The companies system is monitored with a Linux based system where they are already concerned that their security is already been breached. The major purpose of this penetration test is that we are about to figure out the vulnerability of the system, which defines the security holes of the system as well as we will do some malicious attack to make sure how the system can be attacked by a third party attacker. After finding out such issues we are preparing this report to let the company know about their security system.

This penetration testing project was successfully done in response to the client requirements for estimating the system layers using the featured and up to date methods in vulnerability scanning, exploitation and post-exploitation. The first part of the project introduced how we are preparing ourselves to conduct the penetration, in the form of a Standard Operating Procedure (SOP) with the detail procedure of how we will be monitoring this and a Decision Tree. The second part, this report, involves conducting the vulnerability test and analysing the results with exploitation, for the purpose of reporting to the client, including the mitigation methods and the possible risks they need to overcome. This is very important for a company because the economic loss for cyber-attack is increasing over the years. And often, the financial loss arise from theft of information, stolen financial data, and carrying online transaction over the system etc. (nibusinessinfo, 2017) The reputational damage also involves in this massive effect as well. In July 2019, an attacker had gained unauthorised access to the personal data of over 100 million customers in a well-known organisation called Capital One. The suspected attacker, reportedly took benefits from an underdeveloped firewall. From the company later on had the incident to cost it between $100 million and $150 million in major for customer notifications, credit monitoring and legal support. (Swinhoe, 2020) A very famous riding organisation UBER had a loss of $148m (£113m) over a cyber-attack where the attacker stole user's information and exposed 57 million customers' data. (bbc.co.uk, 2017) As a result, The Company paid the hackers $100,000 to delete the data they grabbed from Uber's servers. (Maru, 2017)

This report illustrates the work that is being done on the following exploits and the risks they might need to recover. This is described in the Attack Narrative section, and then explains the three vulnerabilities from the risks and mitigation point of view. And so on, to explain the whole report.

2.0 Attack Narrative

This section of the report describes the following- more detail of target machine, the tools that were used conducting penetration test, the methods those were chosen, paths taken, exploitation and attacking patterns.

2.1: Remote System Discovery

For the purpose of this project, we have received an IP address considered as the organisation's systems address where the security has already been breached. To know this, first we did a basic scanning on the IP address where we found how many ports are open. This is important because most of open ports are used for service run into the system, the more open ports are, and the higher the risks are. (David, October 2016) Fig 2.1.1 we can see that the target IP was full of vulnerable.

2.2 Scanning and Enumeration

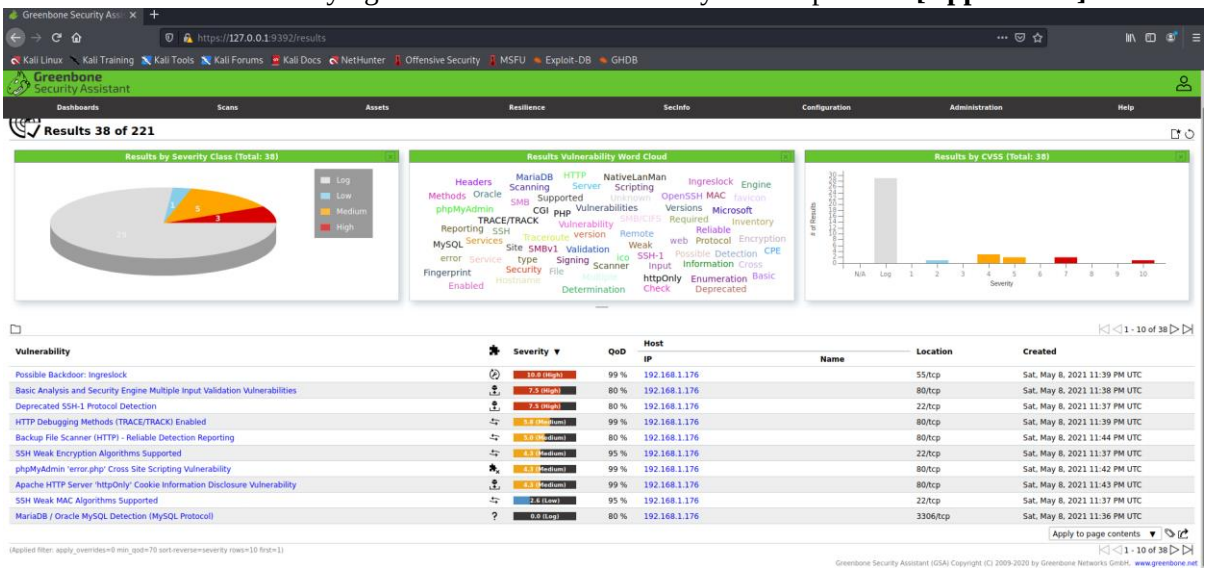
In this section, after receiving IP address, first we used nmap scanning that helps us to scan the particular IP address. By doing so, we found the lists of open ports which is shown in Fig 2.2.1. We found that

there are many open available ports. The open ports allows us to find the vulnerabilities. Among all the open ports, from SSH port we are able to access to the server remotely. In this figure, the lists of identified ports are found, also, we found that the SSH as well as telnet ports are also open. So from this scanning phase it is confirmed that we can have access to the ssh port and telnet port to find the remotely access directories and get into there.

2.3 Vulnerability Discovery

This section represents what methods and tools we have used to detect vulnerabilities. This vulnerability discovery allows us to detect and classifies the given system's weaknesses in networks and other side of the data equipment and anticipates the effectiveness of countermeasures. (Porter, 2019) Tools that we have used to scan for vulnerabilities are nmap, zenmap, nessuss, dirb, openVas. These scanning tools we aimed to achieve the threat levels as well as how much trusted the network is. Also it provides us path of the security holes. Some of the vulnerabilities are discussed below-

- OpenVAS Scanning Vulnerability: One major vulnerability we found from OpenVAS is the steal cookie-based authentication credentials, view and execute local files within the context of the webserver, compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database. Other attacks may also be possible **[Appendix C]**



- Nmap scanning vulnerability result: by scanning the target IP address with nmap, we found the lists of open ports that are available to breach. Some of the open ports are ssh, http, mysql e.t.c (shown in fig. 2.3.1). To see more information, please see **Appendix 2**

```
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 4.4 (protocol 1.99)
80/tcp   open  http        Apache httpd 1.3.37 ((Unix) PHP/4.4.4)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
3306/tcp open  mysql       MySQL (unauthorized)
5903/tcp open  vnc         VNC (protocol 3.7)
6000/tcp open  X11         (access denied)
6003/tcp open  X11         (access denied)
Device type: WAP|remote management|general purpose|broadband router|specia
Running (JUST GUESSING): Gemtek embedded (96%), Siemens embedded (96%), AV
nux 2.6.X|2.4.X (95%), Aastra embedded (95%), Comtrend embedded (95%), AVM
OS CPE: cpe:/h:gemtek:p360 cpe:/h:siemens:gigaset_se515dsl cpe:/o:avm:frit
o:linux:linux_kernel:2.6.24 cpe:/h:comtrend:ct536 cpe:/h:avm:fritz%21box_f
Aggressive OS guesses: Gemtek P360 WAP or Siemens Gigaset SE515dsl wireles
```

Fig 2.3.1: nmap vulnerability scanning results

- Metasploit vulnerability result: using metasploit scanning, in fig 2.3.2 in the left hand side, the lists of open ports we found from nmap scanning, and then we put the open ports to the right

hand side terminal, in the metasploit scanner and the following results appeared. It helps us to detect quick idea of what attacks might be worth conducting.

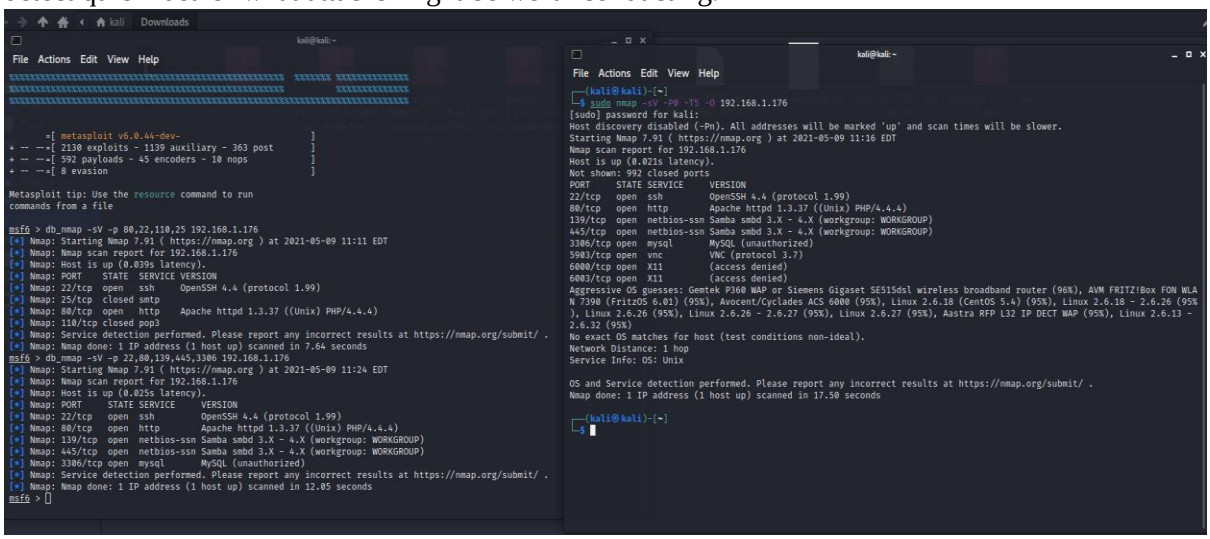
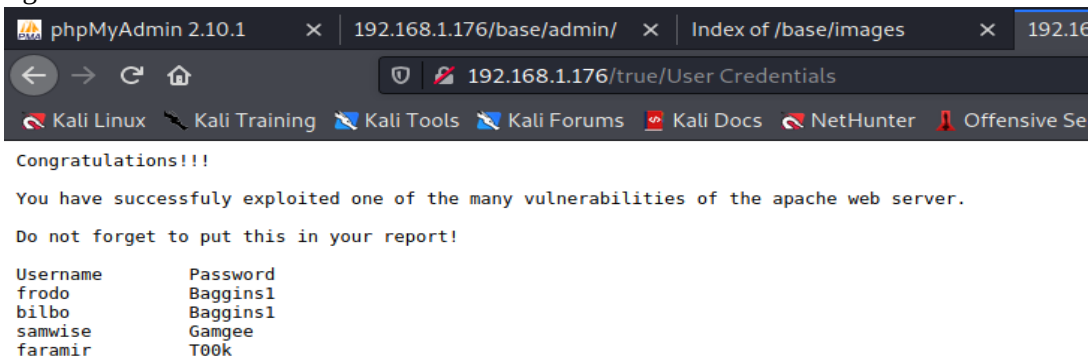


Fig 2.3.2: Vulnerability scanning using metasploit

- DIRB Vulnerability result: with the useful tool dirb, we found out all the hidden directories that can be remotely accessible. The main threat arise after scanning with DIRB because with this scanning we found all credentials to get access into the directories that can lead an attacker also to get into the root level.



Also, at the end of the report, a detailed contrast in between OpenVas as well as Nessus has been given. Please see **Appendix A** for detail.

- Zenmap Scanning: by scanning the target IP address with nmap, we found the lists of open ports that are available to breach. Some of the open ports are ssh, http, mysql e.t.c (shown in fig. 2.3.1). To see more information, please see **Appendix D**

2.3 Vulnerability Exploitation

In this section, we are going to mention about the security holes that we have found so far. Also, we have provided the detail of attack in this section that can help an attacker to get into the root level of the system. Once the attacker get into the root level of the system, he eventually can change the credential data and steal valuable information that is kept on the system. It is crucial that the security should be designed in such way that no attacker can breach into the security hole, otherwise, this could be a threat.

- Root Privilege Escalation: with this technique, we were able to get access the root of the system. It is vulnerable as well because once an attacker get into the systems root, the attacker might able to manipulate information inside of it. Likewise, we did a basic malicious attack. When we entered into the system, after getting root access like the fig 2.3.1

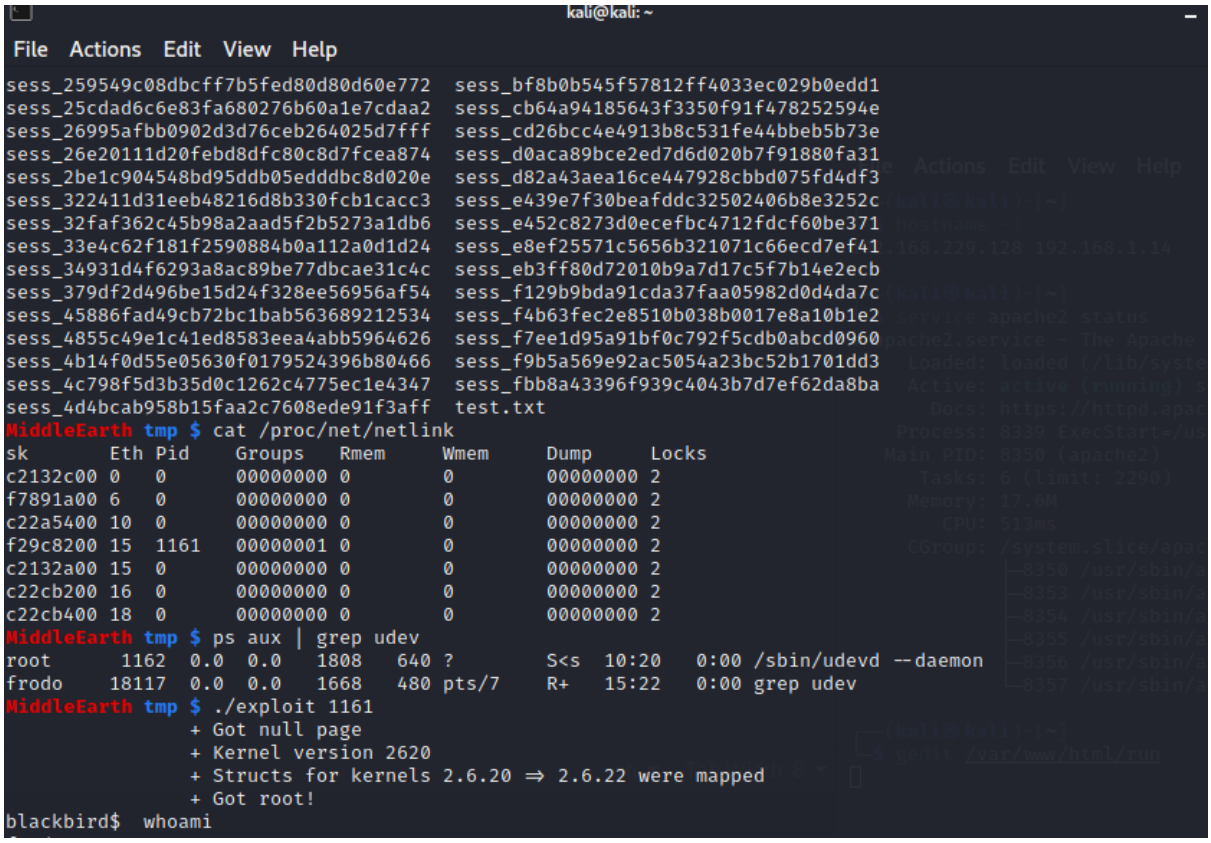


Fig 2.3.1: getting to the root of the target for malicious attack

We just exploit a privilege escalation file into the target system, before that, the target specifies only one particular file. After the escalation, we were able to exploit the file into the root system. Fig 2.3.2 shows the following output of exploitation

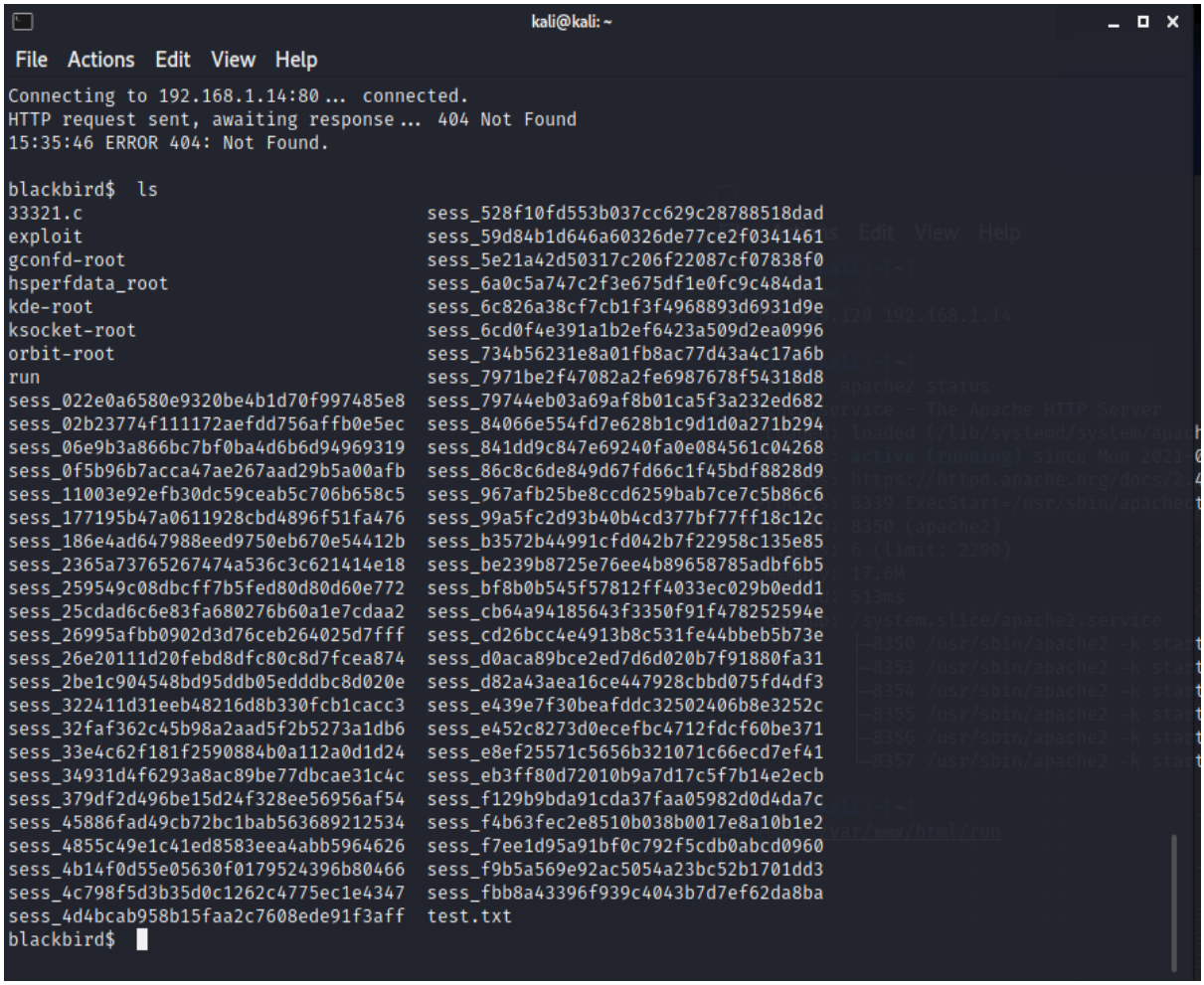


Fig 2.3.2: exploitation of file inside the target system

- Brute force attack on admin panel: with the brute force attack, the password from the admin user were uncovered. We were able to get all the credentials of the admin from the protected portion of the target IP address. We have done brute force attack using ncrack and hydra. Fig 2.3.3 and fig 2.3.4 shows the process and results pf brute force attack to get users credentials into the target system.

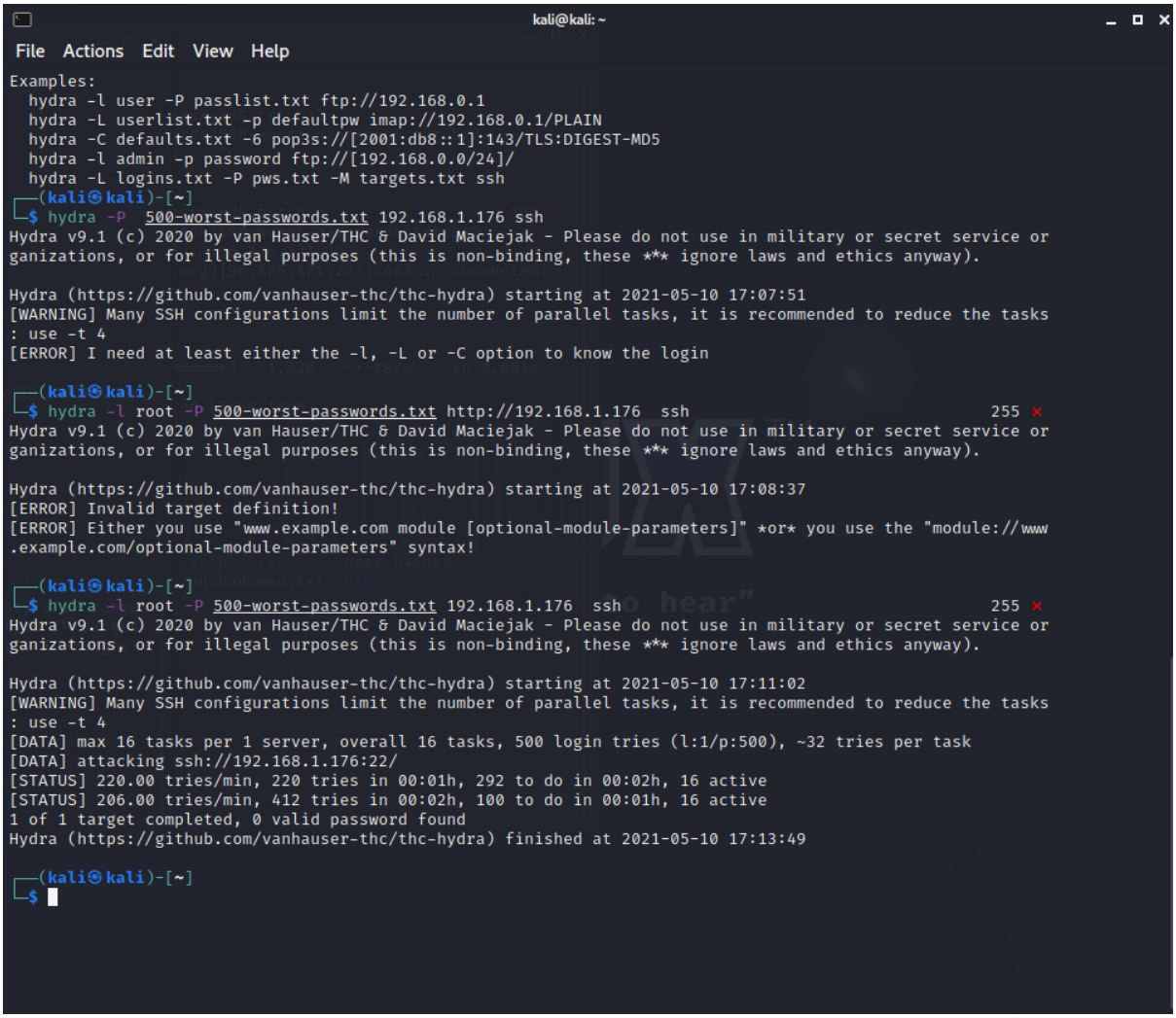


Fig 2.3.3 brute force attack with hydra

- User Access credential attack using ncrack: Although both hydra and ncrack has the same functionality which is brute force attack, two different tools had different approach. That's why we made a brute force attack using ncrack. Fig 2.3.4 shows the following results of ncrack.

Fig 2.3.4 Brute force attack using ncrack

3.0 Vulnerability Mitigation

Apart from the tools that we used for the vulnerability and exploitation. There are also more upgraded self-written tools that can be used for further attack. Vulnerabilities are massive factor that can wreak havoc in any business, of any size, at any time. However, if we look at the report in **Appendix B** of our OpenVAS report, we can see that the target has the highest level threat in tcp port 80, where Multiple Input Validation Vulnerabilities were found. Also, from the OpenVAS vulnerability detection result, we came to know that Successful exploitation could allow remote attackers to bypass security restrictions and to obtain a client's public host key during a connection attempt and use it to open and authenticate an SSH session to another server with the same access.

Apart from OpenVAS, from the report of Nessus scanner, we found that most of the vulnerable has a severity of multiple risks. The reason behind the vulnerability is that the versions that shows vulnerability, such versions may be affected by several issues, including buffer overflows, format string vulnerabilities, arbitrary code execution, 'safe mode' and clobbering of super-global. With such issues, an attacker could be able to overload the buffer that also exploit the attack to do some backdoor attacks, by which an attacker is able to steal some information that can be valuable. The detail has been provided in **Appendix C.**

Exploiting targets with privilege exploitation defines that the attacker can transfer files from any other machine or can be able to steal information from the victims machine as well. As we have done in our penetration test, when we done scanning with dirb scanning, we found the credentials and could easily get into the server, to avoid such problems, credentials should be encrypted in such manner even if the attacker get into the hidden directories the credentials could not be able to crack. This is how we can avoid the risk here.

Brute force attack using smart tools such as Hydra, ncrack, john can also be able to gather users credentials if the password pattern is likely to be common. Meanwhile in our testing, while we made brute force attack using these tools, some of vulnerabilities were found. It matches data with their string operation key search and hence made the server easy to exploit. This is a very common attack by the attacker. Very large companies are also affected by it. To avoid such issues, the most obvious way to prevent from brute-force attacks is to lock out accounts after a given number of wrong password attempts. (Esheridan, 2011)

There are some common risks associated with each of the given vulnerability and exploitation. The common factors are loss of financial situation, losses of user's personal data, losses of company's important documents and confidentiality, and damages of a company's reputation. There are many large companies where they had loss of million pounds and they were blamed at the same time by the users. This is how companies lose the trust of their people. To keep the basement strong, our team recommends you to put more strong security so that the system could be safe.

4.0 Conclusion

When conducting a large organisation, or any organisation that relies upon their online activities, it is highly recommended that the server and the system should be secured to avoid possible threats or risks that may come upon the company. Every year, millions of pounds have to pay to the attackers due to their successful post exploitation and they are selling users data to dark web or any other side. So this is very crucial to have more secured and layered security that cannot be breached.

5.0 Overall Conclusion and Reflections

The report has been made based on our learning outcomes from the module penetration testing. In this report, I have done scanning to the system in order to gather more information and let myself introduced with the target system. Secondly, by the process of determining vulnerabilities using few up to date tools I became more familiar with the possibilities of risks that are present into the target machine. And finally, after analysis possible risks and the security holes, I took some exploitation test and tried to breach into the system to cover the whole access in order to do malicious attack to make sure if I have the access to the root system to take control of it or not. Every of my tasks were successfully done except some technical issues that I faced during exploitation.

Finally, I have learned a lot of things during the entire experience. The most important things that I have learnt so far is, the process of analysing of different data, the ability of applying the best of my knowledge where I need to be. Also, this experience made me able to distinguish in between grey box and black box penetration testing. The most important thing that I need to mention is, I have covered different type of methodologies that need to be undertake before conducting a penetration test, also making of a good approach with a decision tree. I got introduced with many updated pen test tools that are very easy to use, and learnt some techniques to test a system which I believe will take me to the upper way during industrial experience.

6.0 References

bbc.co.uk, 2017. *Uber pays $148m over data breach cover-up.* [Online]
Available at: https://www.bbc.co.uk/news/technology-45666280

David, M. J., October 2016. *Extracting attack narratives from traffic datasets.* s.l., IEEE Xplore.

Esheridan, K., 2011. *Blocking Brute Force Attacks.* [Online]
Available at: https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks
[Accessed 8 05 2021].

Maru, P., 2017. *how Security vendors and experts have scrutinized this cyberattack.* [Online]
Available at: https://cio.economictimes.indiatimes.com/news/digital-security/uber-data-breach-heres-how-security-vendors-and-experts-have-scrutinized-this-cyberattack/61767950

nibusinessinfo, 2017. *Impact of cyber attack on your business.* [Online]
Available at: https://www.nibusinessinfo.co.uk/content/impact-cyber-attack-your-business
[Accessed MAR 2021].

Porter, O. R., 2019. *The Importance of Vulnerability Scans,* s.l.:
https://partneredsolutionsit.com/importance-of-vulnerability-scans/.

Swinhoe, D., 2020. *7 security incidents that cost CISOs their jobs.* [Online]
Available at: https://www.csoonline.com/article/3510640/7-security-incidents-that-cost-cisos-their-jobs.html
[Accessed 08 05 2021].

7.0 Appendices

Appendix A:

OpenVAS	Nessus
Open Source vulnerability tools	Not open source
Limited supportability	Has server side compatibility
Free for all	Paid version provides all the features
Calculates total vulnerabilities and results	Offers real time visibility
Common vulnerability coverage around 26000	Common vulnerability coverage around 47000

Appendix B:

OpenVAS Report

Scan Report

May 9, 2021

Summary

This document reports on the results of an automatic security scan. All dates are dis-played using the timezone Coordinated Universal Time, which is abbreviated UTC. The task was ws1. The scan started at Sat May 8 23:34:34 2021 UTC and ended at Sat May 8 23:44:33 2021 UTC. The report rst summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.1.176	3	5	1	0	0
Total: 1	3	5	1	0	0

Vendor security updates are not trusted.
Overrides are o. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level Log are not shown.
Issues with the threat level Debug are not shown.
Issues with the threat level False Positive are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 9 results selected by the ltering described above. Before ltering there were 221 results.

2 Results per Host

2.1 192.168.1.176

Host scan start Sat May 8 23:35:00 2021 UTC
Host scan end Sat May 8 23:44:28 2021 UTC

Service (Port)	Threat Level
80/tcp	High
22/tcp	High
55/tcp	High
80/tcp	Medium
22/tcp	Medium
22/tcp	Low

2.1.1 High 80/tcp

(CVSS: 7.5)
: Basic Analysis and Security Engine Multiple Input Validation Vulnerabilities
Summary
. . . continues on next page . . .

. . . continued from previous page . . .

Basic Analysis and Security Engine (BASE) is prone to multiple input-validation vulnerabilities because it fails to adequately sanitize user-supplied input. These vulnerabilities include an SQL-injection issue, a cross-site scripting issue, and a local □le-include issue.

Vulnerability Detection Result
Installed version: 1.2.6
Fixed version: 1.4.4

Impact
Exploiting these issues can allow an attacker to steal cookie-based authentication credentials, view and execute local □les within the context of the webserver, compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database. Other attacks may also be possible.

Solution:
Solution type: VendorFix
Updates are available. Please see the references for details.

A□ected Software/OS
These issues a□ect versions prior to BASE 1.4.4.

Vulnerability Detection Method
Details: Basic Analysis and Security Engine Multiple Input Validation Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.100323
Version used: 2020-10-20T15:03:35Z

References
cve: CVE-2009-4590
cve: CVE-2009-4591
cve: CVE-2009-4592
cve: CVE-2009-4837
cve: CVE-2009-4838
cve: CVE-2009-4839
bid: 36830
bid: 18298
url: http://www.securityfocus.com/bid/36830

[return to 192.168.1.176]

2.1.2 High 22/tcp

n (CVSS: 7.5)
: Deprecated SSH-1 Protocol Detection

Summary
. . . continues on next page . . .

. . . continued from previous page . . .

The host is running SSH and is providing / accepting one or more deprecated versions of the SSH protocol which have known cryptograhic □aws.

Vulnerability Detection Result

The service is providing / accepting the following deprecated versions of the SS ,!H protocol which have known cryptograhic flaws:
1.33
1.5

Impact

Successful exploitation could allows remote attackers to bypass security restrictions and to obtain a client's public host key during a connection attempt and use it to open and authenticate an SSH session to another server with the same access.

Solution:
Solution type: VendorFix
Recon□gure the SSH service to only provide / accept the SSH protocol version SSH-2.

A□ected Software/OS
Services providing / accepting the SSH protocol version SSH-1 (1.33 and 1.5).

Vulnerability Detection Method
Details: Deprecated SSH-1 Protocol Detection
OID:1.3.6.1.4.1.25623.1.0.801993
Version used: 2020-08-24T08:40:10Z

References
cve: CVE-2001-0361
cve: CVE-2001-0572
cve: CVE-2001-1473
bid: 2344
url: http://www.kb.cert.org/vuls/id/684820
url: http://xforce.iss.net/xforce/xfdb/6603

[return to 192.168.1.176]

2.1.3 High 55/tcp

n (CVSS: 10.0)
: Possible Backdoor: Ingreslock

Summary
A backdoor is installed on the remote host.

Vulnerability Detection Result

. . . continues on next page . . .

. . . continued from previous page . . .

The service is answering to an 'id;' command with the following response: uid=0(,!root) gid=0(root)

Impact
Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the a□ected isystem.

Solution:
Solution type: Workaround
A whole cleanup of the infected system is recommended.

Vulnerability Detection Method
Details: Possible Backdoor: Ingreslock
OID:1.3.6.1.4.1.25623.1.0.103549
Version used: 2020-08-24T08:40:10Z

[return to 192.168.1.176]

2.1.4 Medium 80/tcp

ium (CVSS: 5.8)
: HTTP Debugging Methods (TRACE/TRACK) Enabled

Summary
The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

Vulnerability Detection Result
The web server has the following HTTP methods enabled: TRACE

Impact
An attacker may use this □aw to trick your legitimate web users to give him their credentials.

Solution:
Solution type: Mitigation
Disable the TRACE and TRACK methods in your web server con□guration.
Please see the manual of your web server or the references for more information.

A□ected Software/OS
Web servers with enabled TRACE and/or TRACK methods.

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

It has been shown that web servers supporting this methods are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers.

Vulnerability Detection Method
Checks if HTTP methods such as TRACE and TRACK are enabled and can be used.
Details: HTTP Debugging Methods (TRACE/TRACK) Enabled
OID:1.3.6.1.4.1.25623.1.0.11213
Version used: 2021-02-15T07:14:40Z

References
cve: CVE-2003-1567
cve: CVE-2004-2320
cve: CVE-2004-2763
cve: CVE-2005-3398
cve: CVE-2006-4683
cve: CVE-2007-3008
cve: CVE-2008-7253
cve: CVE-2009-2823
cve: CVE-2010-0386
cve: CVE-2012-2223
cve: CVE-2014-7883
bid: 9506
bid: 9561
bid: 11604
bid: 15222
bid: 19915
bid: 24456
bid: 33374
bid: 36956
bid: 36990
bid: 37995
url: http://www.kb.cert.org/vuls/id/288308
url: http://www.kb.cert.org/vuls/id/867593
url: https://httpd.apache.org/docs/current/en/mod/core.html#traceenable
url: https://techcommunity.microsoft.com/t5/iis-support-blog/http-track-and-trac ,!e-verbs/ba-p/784482

url: https://owasp.org/www-community/attacks/Cross_Site_Tracing

ium (CVSS: 5.0)
: Backup File Scanner (HTTP) - Reliable Detection Reporting

Summary
The script reports backup les left on the web server.
Notes:
- 'Reliable Detection' means that a le was detected based on a strict (regex) and reliable pattern matching the response of the remote web server when a le was requested.

. . . continues on next page . . .

. . . continued from previous page . . .

- As the VT 'Backup File Scanner (HTTP)' (OID: 1.3.6.1.4.1.25623.1.0.140853) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.

Vulnerability Detection Result
The following backup files were identified (<URL>:<Matching pattern>):
http://192.168.1.176/phpmyadmin/config.inc.php~:^<\?(php|=)

Impact
Based on the information provided in this files an attacker might be able to gather sensitive information stored in these files.

Solution:
Solution type: Mitigation
Delete the backup files.

Vulnerability Detection Method
Reports previous enumerated backup files accessible on the remote web server.
Details: Backup File Scanner (HTTP) - Reliable Detection Reporting
OID:1.3.6.1.4.1.25623.1.0.108976
Version used: 2021-01-21T10:06:42Z

References
url: http://www.openwall.com/lists/oss-security/2017/10/31/1

ium (CVSS: 4.3)
: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability

Product detection result
cpe:/a:apache:http_server:1.3.37
Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1 ,!.0.117232)

Summary
Apache HTTP Server is prone to a cookie information disclosure vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to obtain sensitive information that may aid in further attacks.

Solution:
Solution type: VendorFix

. . . continues on next page . . .

. . . continued from previous page . . .

Update to Apache HTTP Server version 2.2.22 or later.

A□ected Software/OS
Apache HTTP Server versions 2.2.0 through 2.2.21.

Vulnerability Insight
The □aw is due to an error within the default error response for status code 400 when no custom ErrorDocument is con□gured, which can be exploited to expose 'httpOnly' cookies.

Vulnerability Detection Method
Details: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability
OID:1.3.6.1.4.1.25623.1.0.902830
Version used: 2021-02-25T13:36:35Z

Product Detection Result
Product: cpe:/a:apache:http_server:1.3.37
Method: Apache HTTP Server Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
cve: CVE-2012-0053
bid: 51706
url: http://secunia.com/advisories/47779
url: http://www.exploit-db.com/exploits/18442
url: http://rhn.redhat.com/errata/RHSA-2012-0128.html
url: http://httpd.apache.org/security/vulnerabilities_22.html
url: http://svn.apache.org/viewvc?view=revision&revision=1235454
url: http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.html

ium (CVSS: 4.3)
: phpMyAdmin 'error.php' Cross Site Scripting Vulnerability

Summary
The host is running phpMyAdmin and is prone to Cross-Site Scripting Vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successful exploitation will allow attackers to inject arbitrary HTML code within the error page and conduct phishing attacks.

Solution:
Solution type: WillNotFix

. . . continues on next page . . .

. . . continued from previous page . . .

No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

A□ected Software/OS
phpMyAdmin version 3.3.8.1 and prior.

Vulnerability Insight
The □aw is caused by input validation errors in the 'error.php' script when processing crafted BBcode tags containing '@' characters, which could allow attackers to inject arbitrary HTML code within the error page and conduct phishing attacks.

Vulnerability Detection Method
Details: phpMyAdmin 'error.php' Cross Site Scripting Vulnerability
OID:1.3.6.1.4.1.25623.1.0.801660
Version used: 2019-12-05T15:10:00Z

References
cve: CVE-2010-4480
url: http://www.exploit-db.com/exploits/15699/
url: http://www.vupen.com/english/advisories/2010/3133

[return to 192.168.1.176]

2.1.5 Medium 22/tcp

ium (CVSS: 4.3)
: SSH Weak Encryption Algorithms Supported

Summary
The remote SSH server is con□gured to allow weak encryption algorithms.

Vulnerability Detection Result
The following weak client-to-server encryption algorithms are supported by the r ,!emote service:

3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se

. . . continues on next page . . .

. . . continued from previous page . . .

The following weak server-to-client encryption algorithms are supported by the r ,!emote service:

3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se

Solution:
Solution type: Mitigation
Disable the weak encryption algorithms.

Vulnerability Insight
The `arcfour` cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.
The `none` algorithm speci□es that no encryption is to be done. Note that this method provides no con□dentiality protection, and it is NOT RECOMMENDED to use it.
A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

Vulnerability Detection Method
Check if remote ssh service supports Arcfour, none or CBC ciphers.
Details: SSH Weak Encryption Algorithms Supported
OID:1.3.6.1.4.1.25623.1.0.105611
Version used: 2020-08-24T08:40:10Z

References
url: https://tools.ietf.org/html/rfc4253#section-6.3
url: https://www.kb.cert.org/vuls/id/958563

[return to 192.168.1.176]

2.1.6 Low 22/tcp

(CVSS: 2.6)
: SSH Weak MAC Algorithms Supported

Summary
The remote SSH server is con□gured to allow weak MD5 and/or 96-bit MAC algorithms.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result
The following weak client-to-server MAC algorithms are supported by the remote s ,!ervice:

hmac-md5
hmac-md5-96
hmac-sha1-96
The following weak server-to-client MAC algorithms are supported by the remote s ,!ervice:

hmac-md5
hmac-md5-96
hmac-sha1-96

Solution:
Solution type: Mitigation
Disable the weak MAC algorithms.

Vulnerability Detection Method
Details: SSH Weak MAC Algorithms Supported
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: 2020-08-24T08:40:10Z

[return to 192.168.1.176]

Appendix C:

nmap and Zenmap Report

Starting Nmap 7.91 (https://nmap.org) at 2021-05-10 19:03 EDT

NSE: Loaded 153 scripts for scanning.

NSE: Script Pre-scanning.

Initiating NSE at 19:03

Completed NSE at 19:03, 0.00s elapsed

Initiating NSE at 19:03

Completed NSE at 19:03, 0.00s elapsed

Initiating NSE at 19:03

Completed NSE at 19:03, 0.00s elapsed

Initiating Ping Scan at 19:03

Scanning 192.168.1.176 [2 ports]

Completed Ping Scan at 19:03, 0.02s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 19:03

Completed Parallel DNS resolution of 1 host. at 19:03, 4.01s elapsed

Initiating Connect Scan at 19:03

Scanning 192.168.1.176 [1000 ports]

Discovered open port 445/tcp on 192.168.1.176

Discovered open port 80/tcp on 192.168.1.176

Discovered open port 139/tcp on 192.168.1.176

Discovered open port 22/tcp on 192.168.1.176

Discovered open port 3306/tcp on 192.168.1.176

Discovered open port 6000/tcp on 192.168.1.176

Discovered open port 6003/tcp on 192.168.1.176

Discovered open port 5903/tcp on 192.168.1.176

Completed Connect Scan at 19:03, 3.01s elapsed (1000 total ports)

Initiating Service scan at 19:03

Scanning 8 services on 192.168.1.176

Completed Service scan at 19:03, 11.12s elapsed (8 services on 1 host)

NSE: Script scanning 192.168.1.176.

Initiating NSE at 19:03

Completed NSE at 19:03, 1.53s elapsed

Initiating NSE at 19:03

Completed NSE at 19:03, 0.41s elapsed

Initiating NSE at 19:03

Completed NSE at 19:03, 0.00s elapsed

Nmap scan report for 192.168.1.176

Host is up (0.042s latency).

Not shown: 992 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 4.4 (protocol 1.99)

| ssh-hostkey:

| 2048 c9:73:b5:22:9b:a2:b7:25:86:71:cf:29:39:44:00:74 (RSA1)

| 1024 bb:f5:5a:7f:d9:d4:0c:60:51:2d:7c:f9:bf:be:45:8f (DSA)

|_ 2048 6e:05:71:b5:e0:2c:ed:32:ef:29:a6:fb:27:0b:b6:3e (RSA)

|_sshv1: Server supports SSHv1

80/tcp open http Apache httpd 1.3.37 ((Unix) PHP/4.4.4)

| http-methods:

|_ Supported Methods: GET HEAD POST OPTIONS

|_http-server-header: Apache/1.3.37 (Unix) PHP/4.4.4

|_http-title: Welcome... or not!

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open netbios-ssn Samba smbd 3.0.14a (workgroup: WORKGROUP)3306/tcp open mysql MySQL (unauthorized)

5903/tcp open vnc VNC (protocol 3.7)

| vnc-info:

| Protocol version: 3.7

| Security types:

| VNC Authentication (2)

| Tight (16)

| Tight auth subtypes:

|_ STDV VNCAUTH_ (2)

6000/tcp open X11 (access denied)

6003/tcp open X11 (access denied)

Service Info: OS: Unix

Host script results:

|_clock-skew: mean: -882d09h13m23s, deviation: 0s, median: -882d09h13m23s

| nbstat: NetBIOS name: MIDDLEEARTH, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

| Names:

| MIDDLEEARTH<00> Flags: <unique><active>

| MIDDLEEARTH<03> Flags: <unique><active>

| MIDDLEEARTH<20> Flags: <unique><active>

| WORKGROUP<00> Flags: <group><active>

|_ WORKGROUP<1e> Flags: <group><active>

| smb-os-discovery:

| OS: Unix (Samba 3.0.14a)

| Computer name: MiddleEarth

| NetBIOS computer name:

| Domain name: target.org

| FQDN: MiddleEarth.target.org

|_ System time: 2018-12-10T13:50:23+00:00

| smb-security-mode:

| account_used: guest

| authentication_level: user

| challenge_response: supported

|_ message_signing: supported

|_smb2-time: Protocol negotiation failed (SMB2)

NSE: Script Post-scanning.

Initiating NSE at 19:03

Completed NSE at 19:03, 0.00s elapsed

Initiating NSE at 19:03

Completed NSE at 19:03, 0.00s elapsed

Initiating NSE at 19:03

Completed NSE at 19:03, 0.00s elapsed

Read data files from: /usr/bin/../share/nmap

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 20.79 second

Appendix D:

Nessus Report

192.168.1.176

Vulnerabilities Total: 53

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	7.5	34460	Unsupported Web Server Detection
CRITICAL	10.0	58987	PHP Unsupported Version Detection
HIGH	7.5	42411	Microsoft Windows SMB Shares Unprivileged Access
HIGH	7.5	24906	PHP < 4.4.5 Multiple Vulnerabilities
HIGH	7.5	29833	PHP < 4.4.8 Multiple Vulnerabilities
HIGH	7.5	33849	PHP < 4.4.9 Multiple Vulnerabilities
HIGH	7.5	41014	PHP < 5.2.11 Multiple Vulnerabilities
HIGH	7.5	35067	PHP < 5.2.8 Multiple Vulnerabilities
HIGH	7.5	58988	PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution
HIGH	7.5	57537	PHP < 5.3.9 Multiple Vulnerabilities
HIGH	7.5	10882	SSH Protocol Version 1 Session Key Retrieval
HIGH	6.8	90509	Samba Badlock Vulnerability
HIGH	5.0	142591	PHP < 7.3.24 Multiple Vulnerabilities
MEDIUM	6.8	43351	PHP < 5.2.12 Multiple Vulnerabilities
MEDIUM	6.8	58966	PHP < 5.3.11 Multiple Vulnerabilities
MEDIUM	6.4	44921	PHP < 5.3.2 / 5.2.13 Multiple Vulnerabilities
MEDIUM	5.1	39480	PHP < 5.2.10 Multiple Vulnerabilities
MEDIUM	5.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	35750	PHP < 5.2.9 Multiple Vulnerabilities

MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	4.3	17696	Apache HTTP Server 403 Error Page UTF-7 Encoded XSS
MEDIUM	4.3	90317	SSH Weak Algorithms Supported
LOW	2.6	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6	71049	SSH Weak MAC Algorithms Enabled
LOW	2.6	10407	X Server Detection
INFO	N/A	48204	Apache HTTP Server Version
INFO	N/A	39520	Backported Security Patch Detection (SSH)
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	117886	Local Checks Not Enabled (info)
INFO	N/A	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	10719	MySQL Server Detection
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	11936	OS Identification
INFO	N/A	48243	PHP Version Detection
INFO	N/A	66334	Patch Report
INFO	N/A	70657	SSH Algorithms and Languages Supported
INFO	N/A	149334	SSH Password Authentication Accepted

INFO	N/A	10881	SSH Protocol Versions Supported
INFO	N/A	10267	SSH Server Type and Version Information
INFO	N/A	25240	Samba Server Detection
INFO	N/A	104887	Samba Version
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	11819	TFTP Daemon Detection
INFO	N/A	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	135860	WMI Not Available
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure