

Sick 1.2

Vulnerability Assessment And Penetration Testing Report

Business Confidential

Date: June 11th, 2021

Project: Sick 1.2

# Table of Contents

[Table of Contents 2](#_Toc9866461)

[Confidentiality Statement 3](#_Toc9866462)

[Disclaimer 3](#_Toc9866463)

[Contact Information 3](#_Toc9866464)

[Assessment Overview 4](#_Toc9866465)

[Assessment Components 4](#_Toc9866466)

[External Penetration Test 4](#_Toc9866467)

[Finding Severity Ratings 5](#_Toc9866468)

[Scope 6](#_Toc9866469)

[Scope Exclusions 6](#_Toc9866470)

[Client Allowances 6](#_Toc9866471)

Target.......................................................................................................................................................6

[Executive Summary 7](#_Toc9866472)

[Vulnerability Found 7](#_Toc9866473)

[Security Strengths 7](#_Toc9866474)

[SIEM alerts of vulnerability scans 8](#_Toc9866475)

[Vulnerabilities by Impact 8](#_Toc9866480)

**Tools**..........................................................................................................................................................27

# Confidentiality Statement

This document is the exclusive property of Sick 1.2 and Cyber Walkers Security . This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both Sick 1.2 and Cyber Walkers Security.

Cyber Walkers Security may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

# Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. Cyber Walkers Security prioritized the assessment to identify the weakest security controls an attacker would exploit. Cyber Walkers Security recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

# Contact Information

|  |  |
| --- | --- |
|  |  |

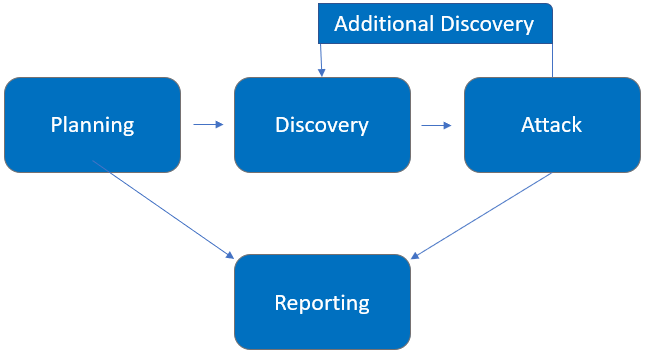
|  |  |  |
| --- | --- | --- |
| Name | Title | Contact Information |
| **Sick 1.2** | | |
| vulnhub | N/A | N/A |
| **Cyber Walkers Security Security** | | |
| Abhishek Joshi | Penetration Tester | Office:+918788295760  Email: [cyberwalker123@gmail.com](mailto:hadams@tcm-sec.com) |

# Assessment Overview

From June 11th, 2021 to June 11th, 2021, Sick 1.2 engaged Cyber Walkers Security to evaluate the security posture of its infrastructure compared to current industry best practices that included an external penetration test. All testing performed is based on the NIST *SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and customized testing frameworks*.

Phases of penetration testing activities include the following:

* Planning – Customer goals are gathered and rules of engagement obtained.
* Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
* Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
* Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



# Assessment Components

## External Penetration Test

An external penetration test emulates the role of an attacker attempting to gain access to an internal network without internal resources or inside knowledge. A Cyber Walkers Security engineer attempts to gather sensitive information through open-source intelligence (OSINT), including employee information, historical breached passwords, and more that can be leveraged against external systems to gain internal network access. The engineer also performs scanning and enumeration to identify potential vulnerabilities in hopes of exploitation.

# Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

| Severity | CVSS V3 Score Range | Definition |
| --- | --- | --- |
| Critical | 9.0-10.0 | Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately. |
| High | 7.0-8.9 | Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible. |
| Moderate | 4.0-6.9 | Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved. |
| Low | 0.1-3.9 | Vulnerabilities are non-exploitable but would reduce an organization’s attack surface. It is advised to form a plan of action and patch during the next maintenance window. |
| Informational | N/A | No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation. |

# Scope

|  |  |
| --- | --- |
| Assessment | Details |
| External Penetration Test | 192.168.0.0/24,  192.168.1.0/24 |

* Full scope information provided in “**Sick 1.2 Full Findings.xslx”**

## Scope Exclusions

Per client request, Cyber Walkers Security did not perform any Denial of Service attacks during testing.Sick 1.2 is a vulnerable machine i have to gather all the flags

## Client Allowances

Sick 1.2 did not provide any allowances to assist the testing.

## Target:

Sick 1.2 is a vulnerable machine i have to gather all the flags and find the Weakness and Security Loopholes. Sick 1.2 is a target we are performing a vulnerability assessment and penetration testing on their machine.

# Executive Summary

Cyber Walkers Security evaluated Sick 1.2 ’s external security posture through an external network penetration test from June 7th, 2021 to June 7th, 2019. By leveraging a series of attacks, Cyber Walkers Security found critical level vulnerabilities that allowed full internal network access to the Sick 1.2 headquarter office. It is highly recommended that Sick 1.2 address these vulnerabilities as soon as possible as the vulnerabilities are easily found through basic reconnaissance and exploitable without much effort.

## Vulnerabilities Found:

|  |  |
| --- | --- |
| Step | Vulnerabilities |
| 1 | Http Methods Allow |
| 2 | File upload |
| 3 | Privilege escalation |

# Security Strengths

## SIEM alerts of vulnerability scans

During the assessment, the Sick 1.2 security team alerted Cyber Walkers Security engineers of detected vulnerability scanning against their systems. The team was successfully able to identify the Cyber Walkers Security engineer’s attacker IP address within minutes of scanning and was capable of blacklisting Cyber Walkers Security from further scanning actions.

# Vulnerabilities by Impact

The following chart illustrates the vulnerabilities found by impact:

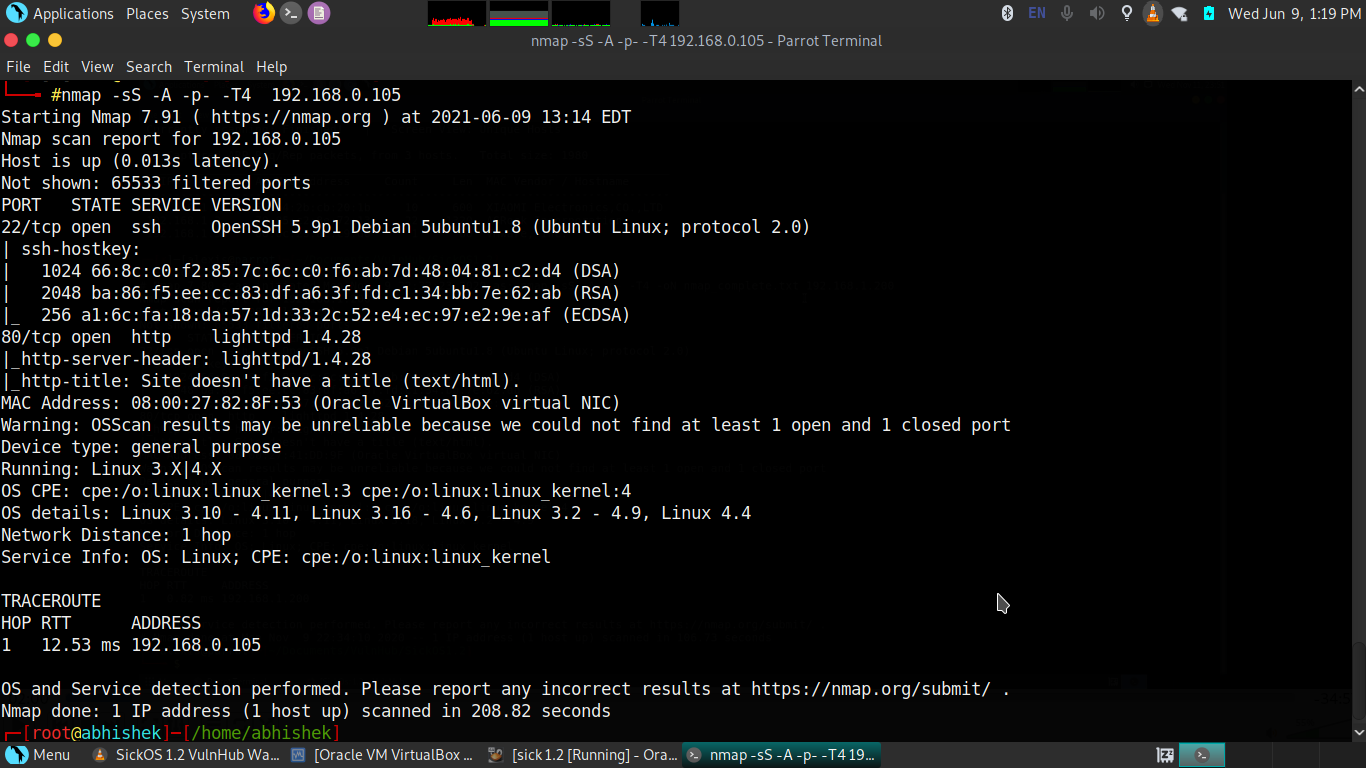
## Penetration Test Findings

Http Method Allow (Critical)

|  |  |
| --- | --- |
| Description: | These HTTP methods can be used for nefarious purposes if the web server is misconfigured. Additionally, Cross Site Tracing (XST), a form of cross site scripting using the server’s HTTP TRACE method, is examined. While GET and POST are by far the most common methods that are used to access information provided by a web server  PUT: This method allows a client to upload new files on the web server. An attacker can exploit it by uploading malicious files (e.g.: an asp file that executes commands by invoking cmd.exe), or by simply using the victim’s server as a file repository.  DELETE: This method allows a client to delete a file on the web server. An attacker can exploit it as a very simple and direct way to deface a web site or to mount a DoS attack.  CONNECT: This method could allow a client to use the web server as a proxy.  TRACE: This method simply echoes back to the client whatever string has been sent to the server, and is used mainly for debugging purposes. This method, originally assumed harmless, can be used to mount an attack known as Cross Site Tracing, which has been discovered by Jeremiah Grossman (see links at the bottom of the page). |
| Impact: | Critical |
| System: | 192.168.0.105 |
| References: | <https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/02-Configuration_and_Deployment_Management_Testing/06-Test_HTTP_Methods>  <https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/02-Configuration_and_Deployment_Management_Testing/06-Test_HTTP_Methods> |

**Exploitation Proof of Concept**

Cyber Walkers Security gather HTTP method allow on Sick 1.2 using these attacker can do malicious activity like uploading a payload,deleting a file.etc.. Below screenshot describe step by step POC(proof of concept) (**Note:** A full list of compromised accounts can be found in “**Sick 1.2 Full Findings.xslx”**.).



on this figure i scan the ports on “Sick 1.2 ” there are SSH and HTTP Ports was open

Using SSH port attacker gain the access with the help of password cracking algorithm FTP port also responsible for the gaining access on a system there are total “65535 PORTS” in a Network

Now i scan the directories of Sick 1.2 and find a “/test” parameter

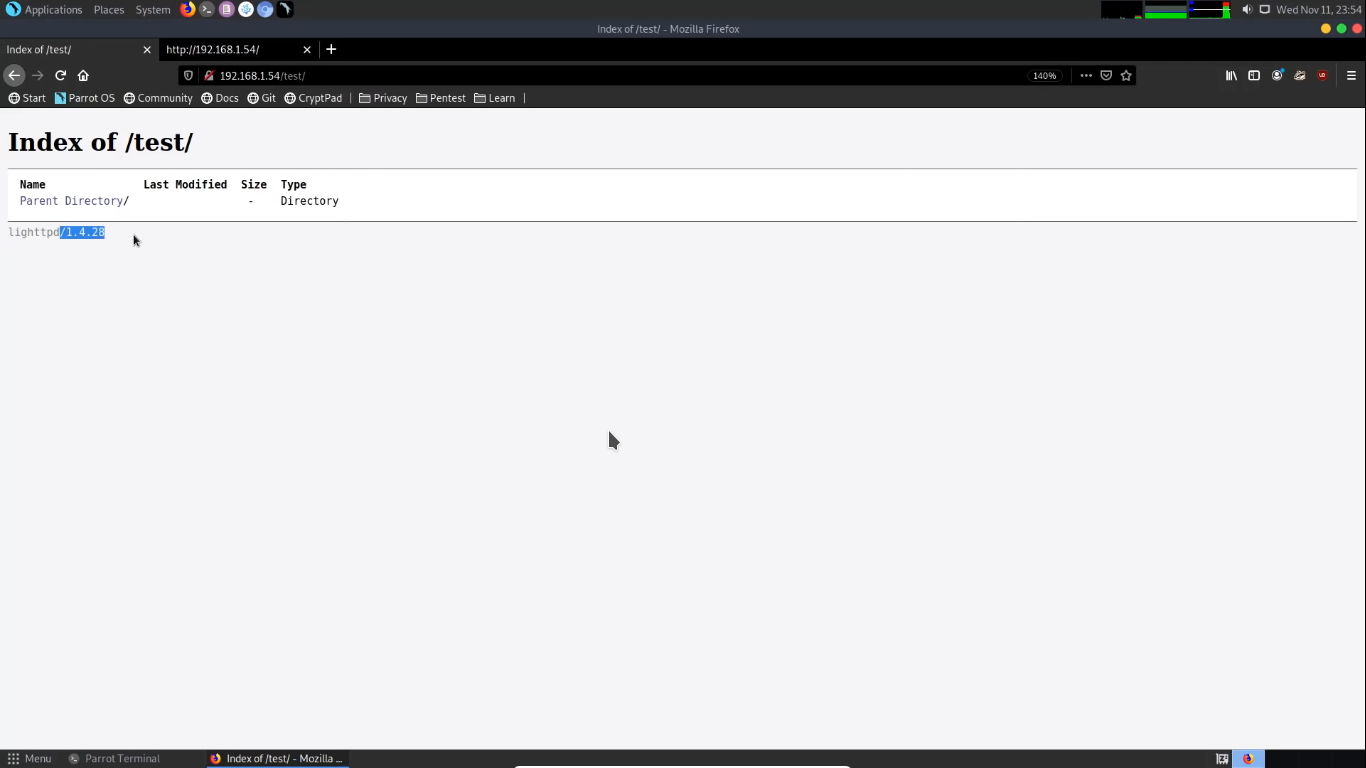
path:https://192.168.0.105/test



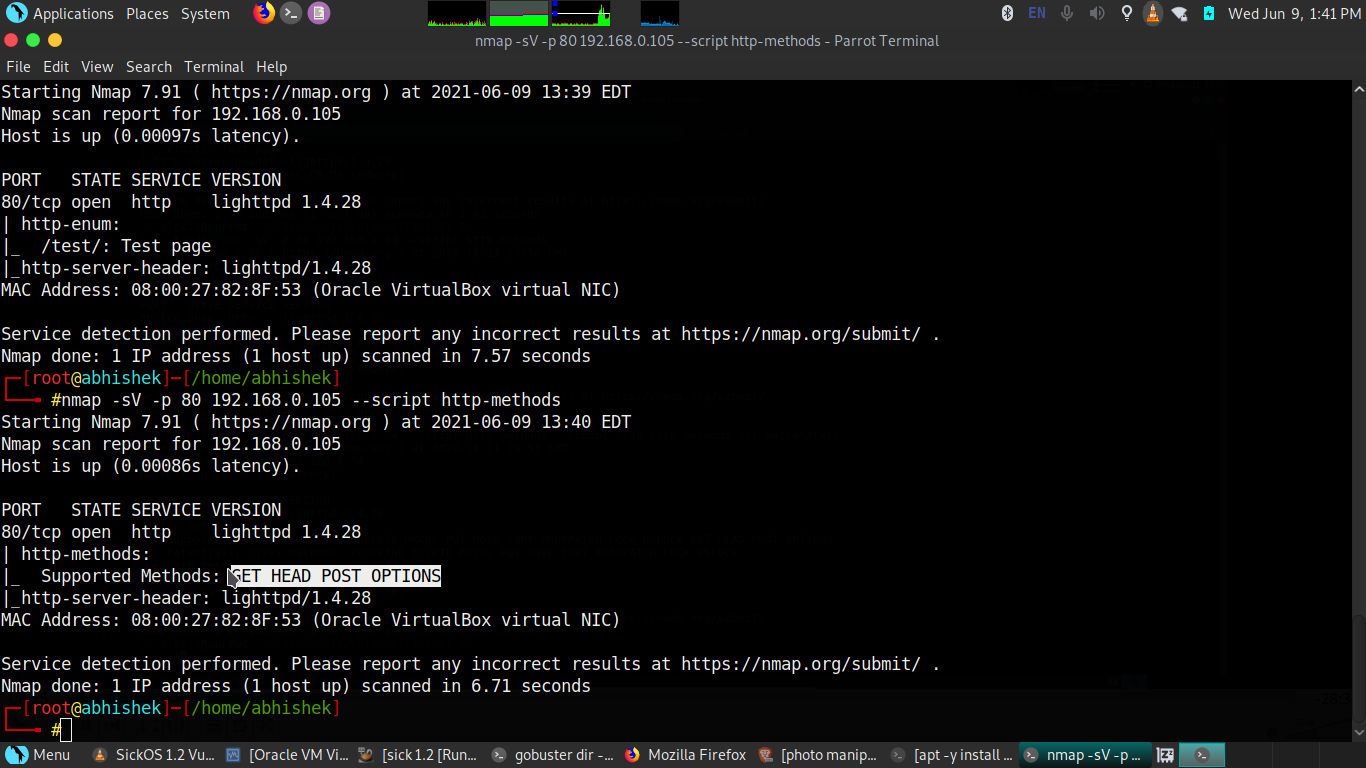
after finding the parameter check on browser for result

They have lowest version of httpd and “/test/ parameter allow sensitive HTTP method

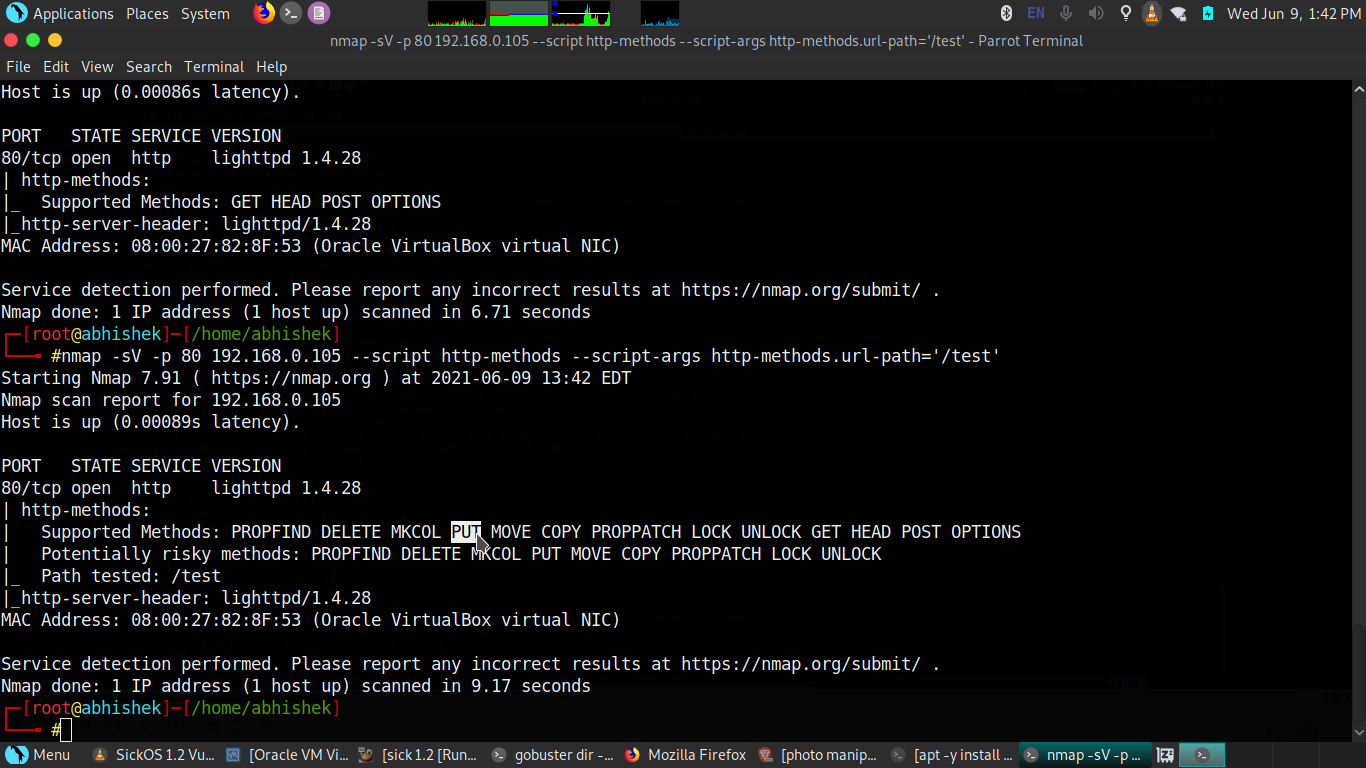
version :lighttpd v1.4.28



After finding the lower version cyber walker gather the http sensitive method allows



You can see “/test” parameter allow HTTP methods:



Now we have to UPLOAD a payload using PUT method which is also responsible for a

file uploadation vulnerability.

**Remediation**

|  |  |
| --- | --- |
| Who: | Sick 1.2 |
| Vector: | Remote |
| Action: | Disable the all sensitive http methods which allow attacker to do a malicious activities. |

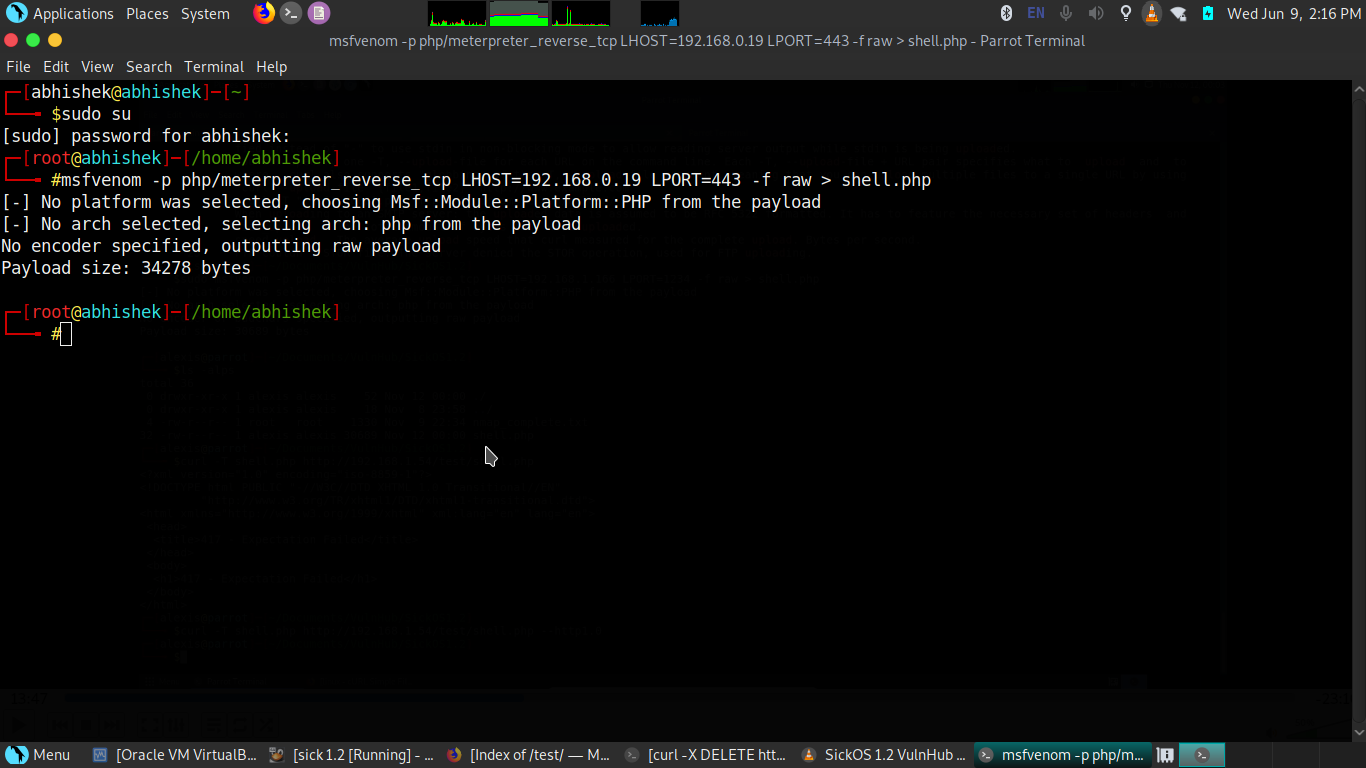
**File Upload Vulnerability** (**Critical**)

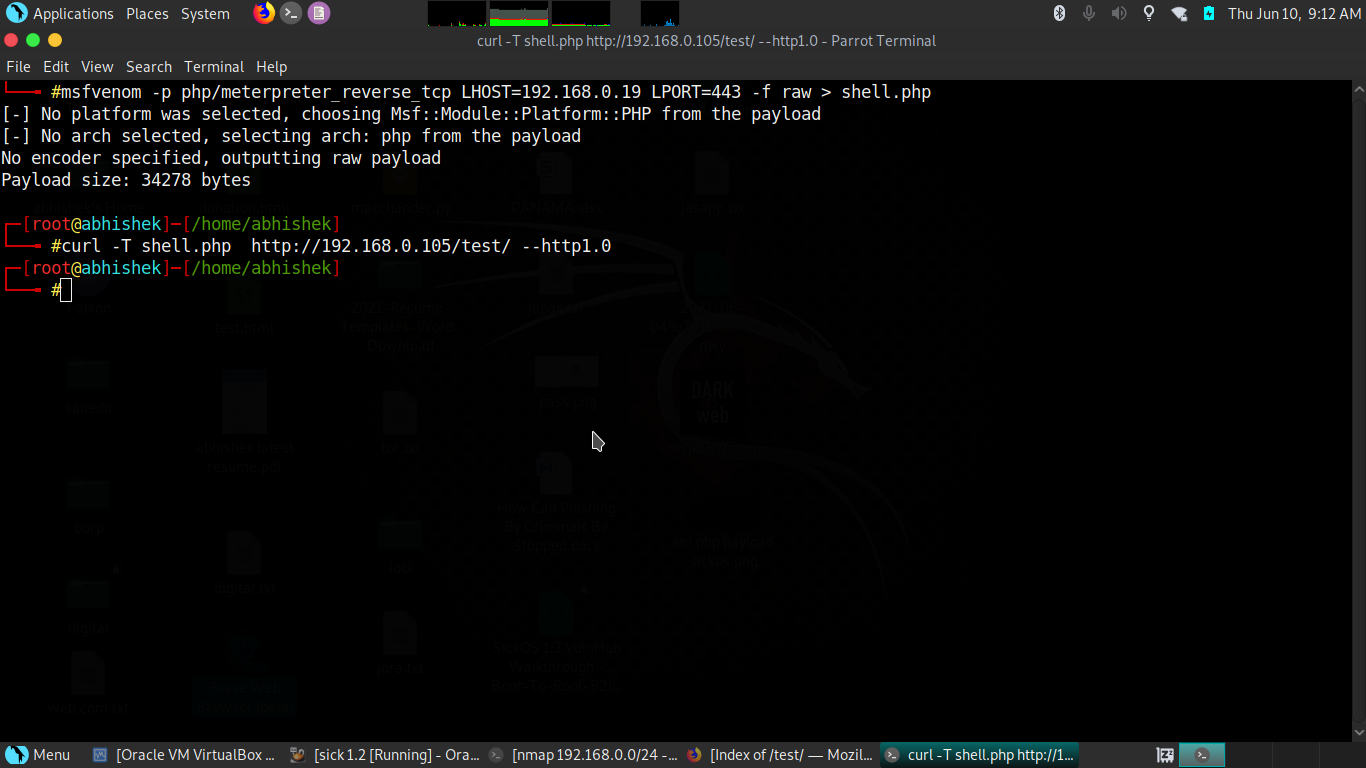
|  |  |
| --- | --- |
| Description: | exploiting the HTTP PUT method vulnerability through various techniques. First, we will determine if the HTTP PUT method is enabled on the target victim machine, a post which we will utilize several different methods to upload a Meterpreter reverse shell on the target and compromise the same. |
| Impact: | Critical |
| System: | 192.168.0.105 |
| References: | https://owasp.org/www-community/vulnerabilities/Unrestricted\_File\_Upload |

**Exploitation Proof of Concept**

Cyber Walkers Security upload the php payload on Sick 1.2 and gain the access of the system see the screenshot below for step by step POC(proof of concept) (**Note:** A full list of compromised accounts can be found in “**Sick 1.2 Full Findings.xslx”**.).

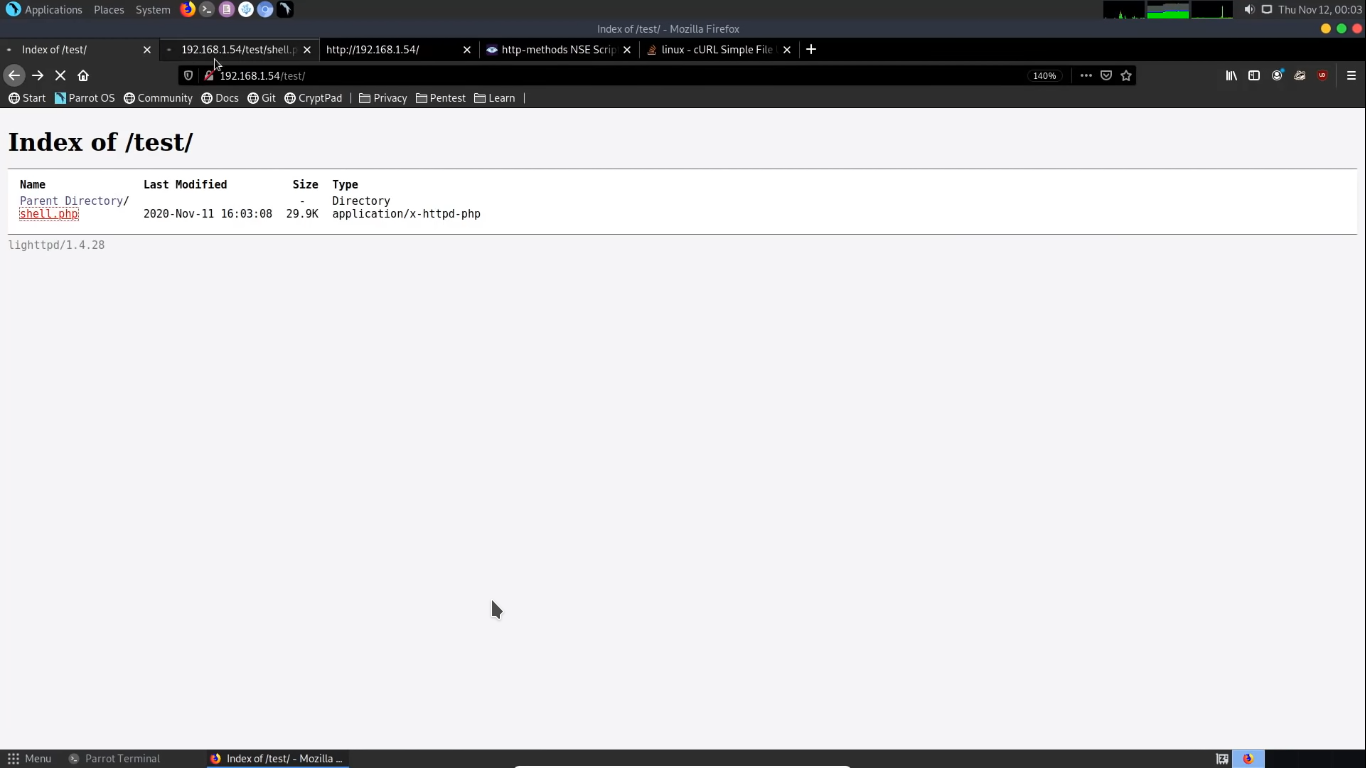
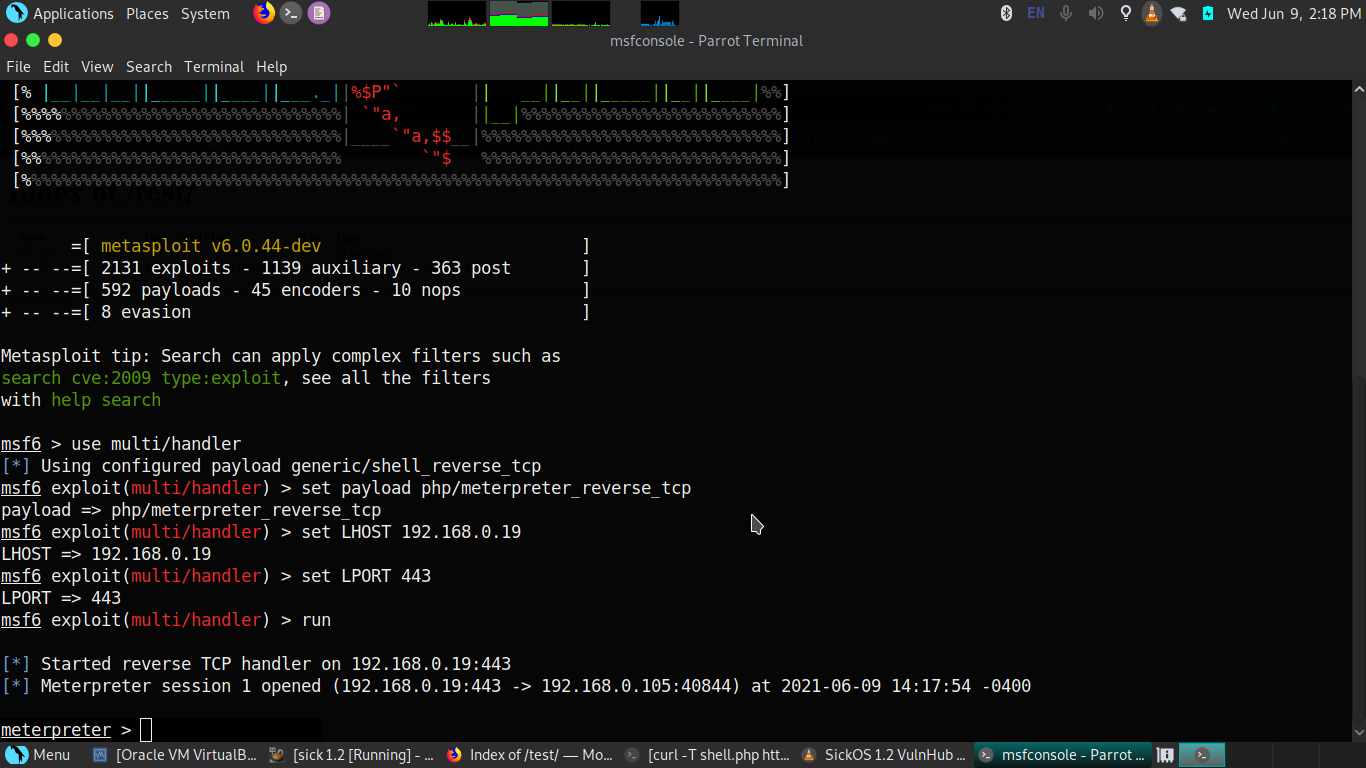
First creating a php payload through “msfvenom”:

After creating a payload start upload on Sick 1.2 “/T=test” parameter using “curl”

path:[](http://192.168.0.105/)http://192.168.0.105

After Uploading create a exploit environment on ”metasploit” for gaining the

access. You can see below image we got a meterpreter.



**Remediation**

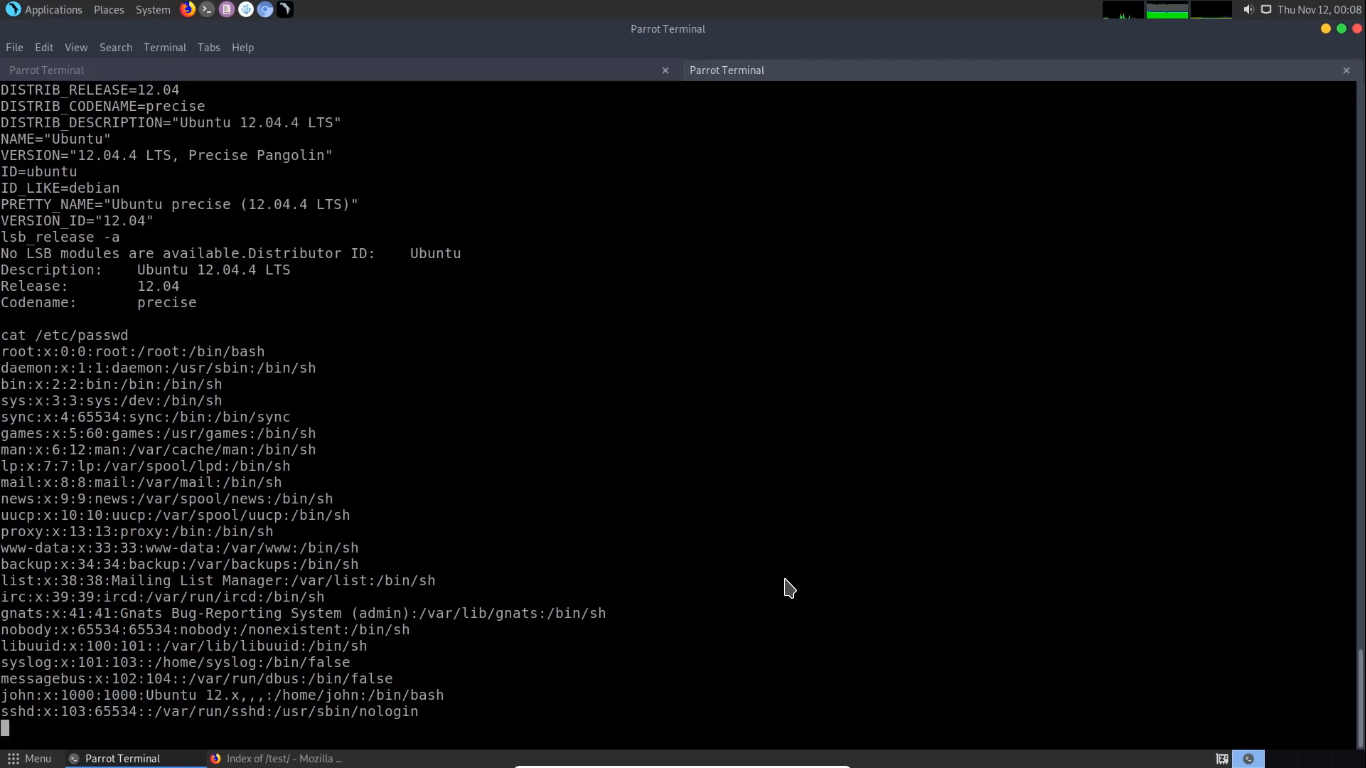
|  |  |
| --- | --- |
| Who: | Sick 1.2 |
| Vector: | Remote |
| Action: | Disable the PUT http method and dont allow any other extensions on your webpages |

Privilage Escalation (Critical)

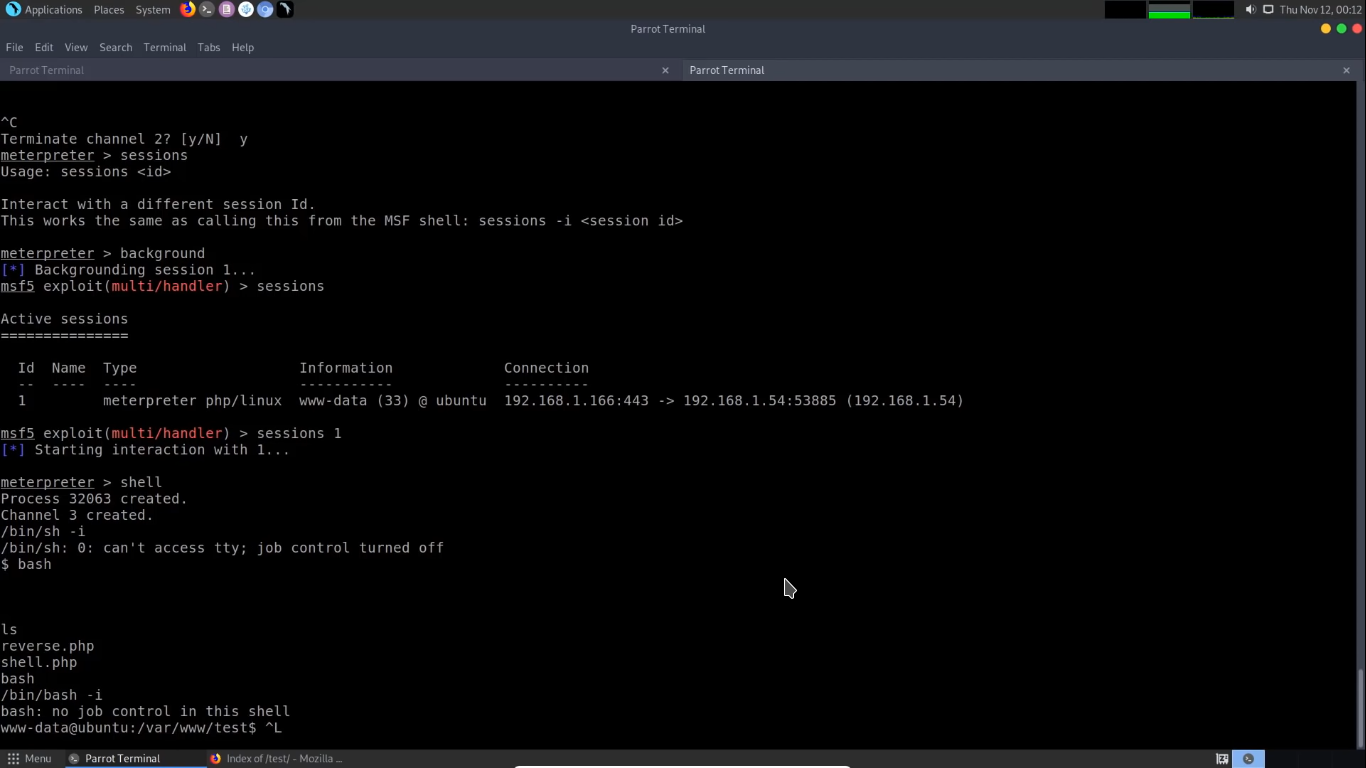
|  |  |
| --- | --- |
| Description: | Privilege escalation happens when a malicious user exploits a bug, design flaw, or configuration error in an application or operating system to gain elevated access to resources that should normally be unavailable to that user. The attacker can then use the newly gained privileges to steal confidential data, run administrative commands or deploy malware – and potentially do serious damage to your operating system, server applications, organization, and reputation. In this blog post, we will look at typical privilege escalation scenarios and learn how you can protect user accounts in your systems and applications to maintain a good security posture.Server-side source code is normally disclosed to clients as a result of typographical errors in scripts or because of misconfiguration, such as failing to grant executable permissions to a script or directory. Review the cause of the code disclosure and prevent it from happening. |
| Impact: | Critical |
| System: | 192.168.0.105 |
| References: | <https://www.netsparker.com/blog/web-security/privilege-escalation/>  <https://portswigger.net/web-security/access-control> |

Cyber Walkers Security gain the root access through finding a vulnerable application on Sick 1.2 the vulnerable application is “Chkroorkit” see below screenshot for step by step POC(proof of concept) (**Note:** A full list of compromised accounts can be found in “**Sick 1.2 Full Findings.xslx”**.).

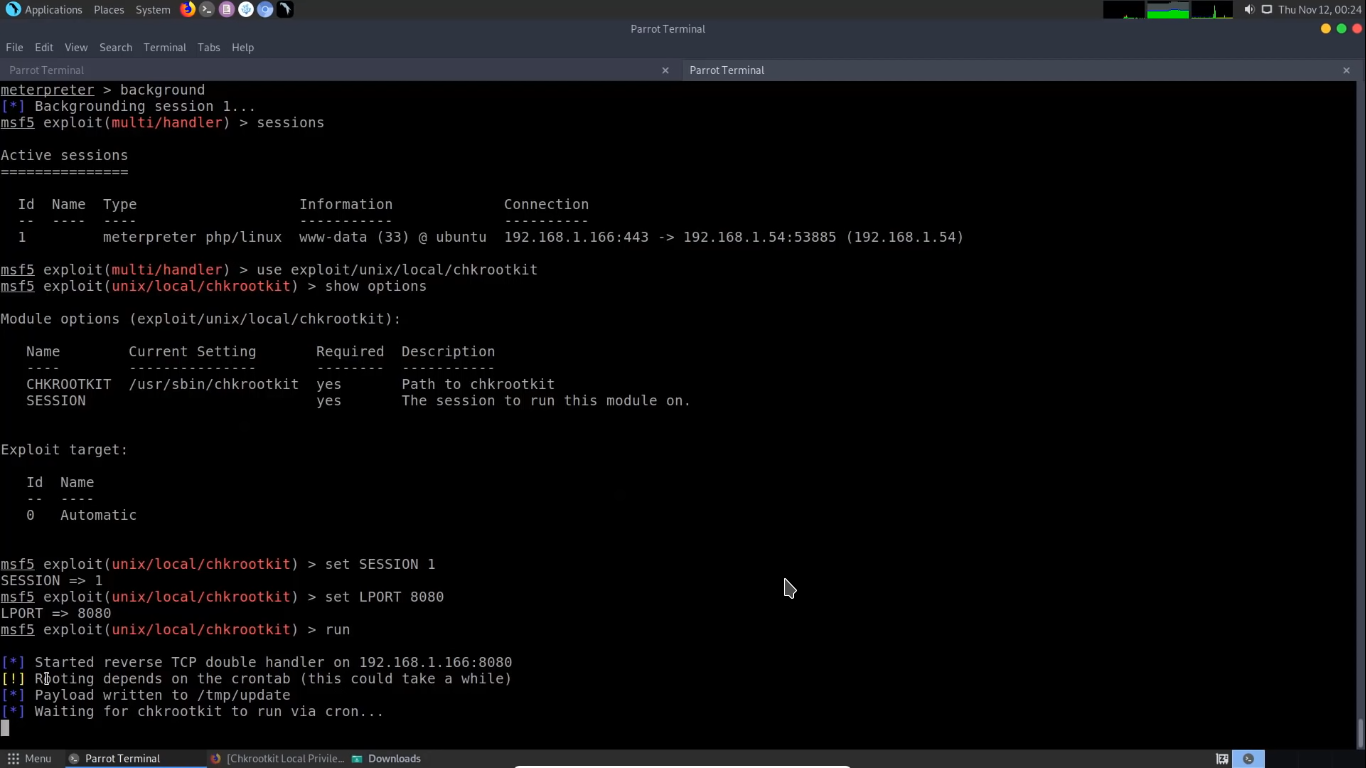
Found john user ons Sick 1.2

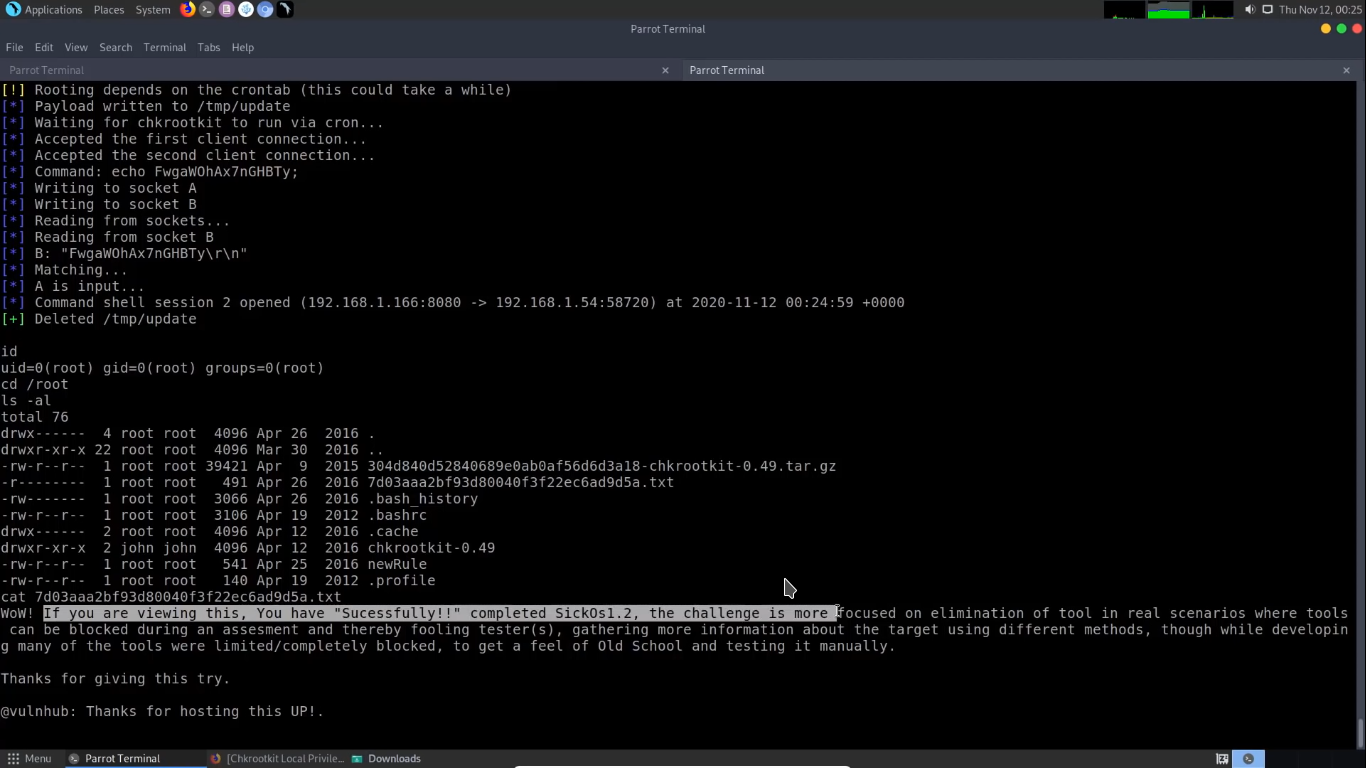


After this gain a terminal access through “/bin/bash -i” script:



Find “Chkrootkit” vulnerable version:





**Remediation**

|  |  |
| --- | --- |
| Who: | Sick 1.2 |
| Vector: | Remote |
| Action: | Up-to date your server,system,web application each and everything.Privilege escalation is one of the most a common[types of cyber crime](https://securitytrails.com/blog/types-of-cyber-crime), and a usual step in the attacker’s trajectory toward successful data theft or other goal. As privilege escalation works to exploit both human psychology (with social engineering tactics) and security vulnerabilities commonly found in operating systems and applications, following strategic tactics to maintain a good security posture can go far in preventing an organization’s ordeal with privilege escalation. |

Tools:

1. Nmap
2. Go buster
3. hydra
4. Metasploit
5. rapid 7

