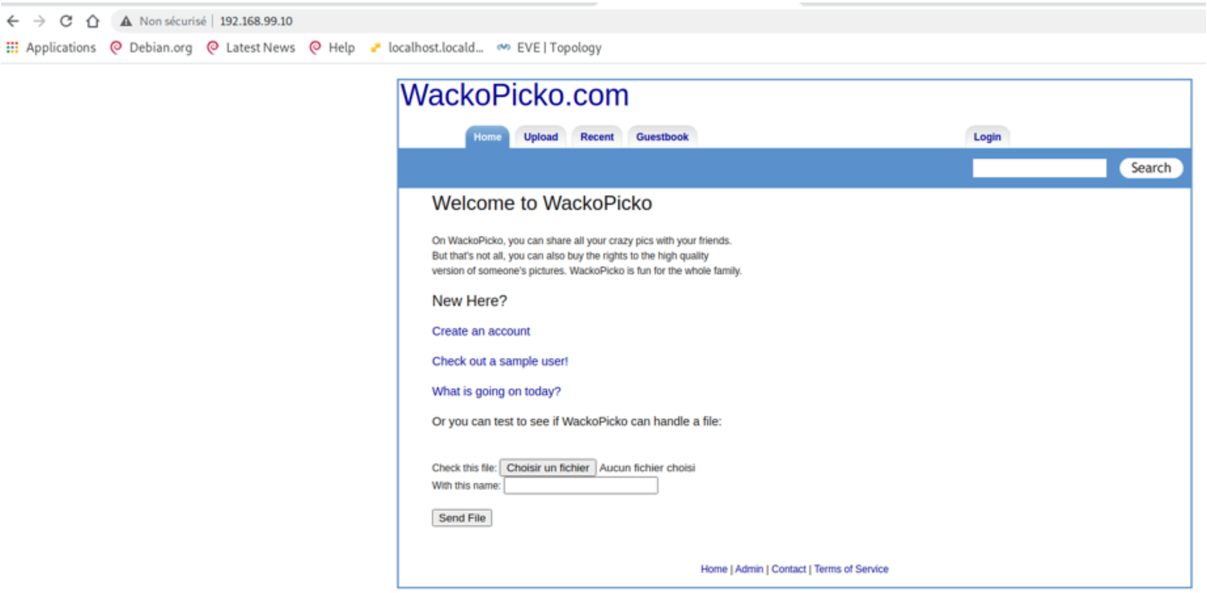
jalon 2

- Faire un tableau avec l'ensemble des services et des versions des différentes applications:

Service	Version
SSH	OpenSSH 6.0p1 Debian 4+deb7u2 (protocol 2.0)
SSH	OpenSSH 7.9p1 Debian 10+deb10u4 (protocol 2.0)
SSH	OpenSSH 9.9p1 Debian 3 (protocol 2.0)
domain	ISC BIND 9.8.4-rpz2+rl005.12-P1
domain	dnsmasq 2.80
NetBIOS-SSN	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
http	Samba SWAT administration server
http	Apache Tomcat/Coyote JSP engine 1.1
http	Apache httpd 2.2.22 ((Debian))
http	Custom HTTP server (ESP8266 – “hello from esp8266 and binome 14 + mac:…”)
ssl/http	Apache httpd 2.2.22 ((Debian))
ssl/imap	Dovecot imapd
SMTP	Postfix smtpd
IMAP	Dovecot imapd
java-object	Java Object Serialization
commplex-link?	(empreinte non reconnue)
telnet	BusyBox telnetd 1.14.0 or later (DD-WRT v3.0 std 09/19/19 r41074)

Copie d’écran des pages d’accueil des différents serveurs web en fonction des différents port et ip relevé avec le nmap

192.168.99.10



WackoPicko.com

Welcome to WackoPicko

On WackoPicko, you can share all your crazy pics with your friends. But that's not all, you can also buy the rights to the high quality version of someone's pictures. WackoPicko is fun for the whole family.

New Here?

Create an account

Check out a sample user!

What is going on today?

Or you can test to see if WackoPicko can handle a file:

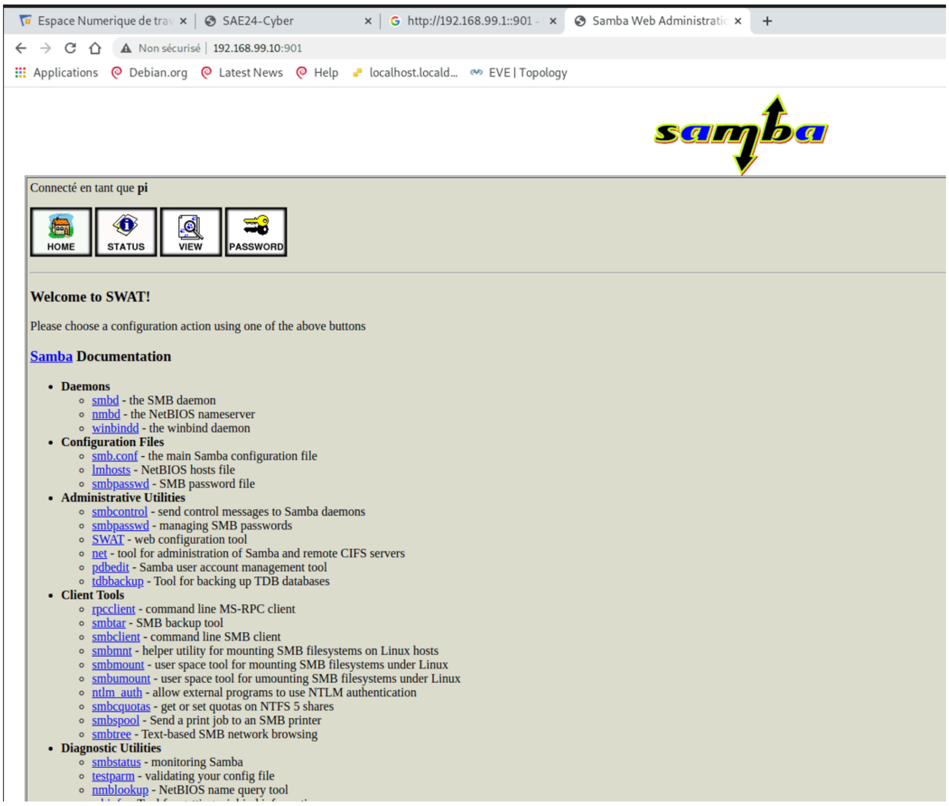
Check this file: Choisir un fichier Aucun fichier choisi

With this name:

Send File

Home | Admin | Contact | Terms of Service

192.168.99.10:901



Connecté en tant que **pi**

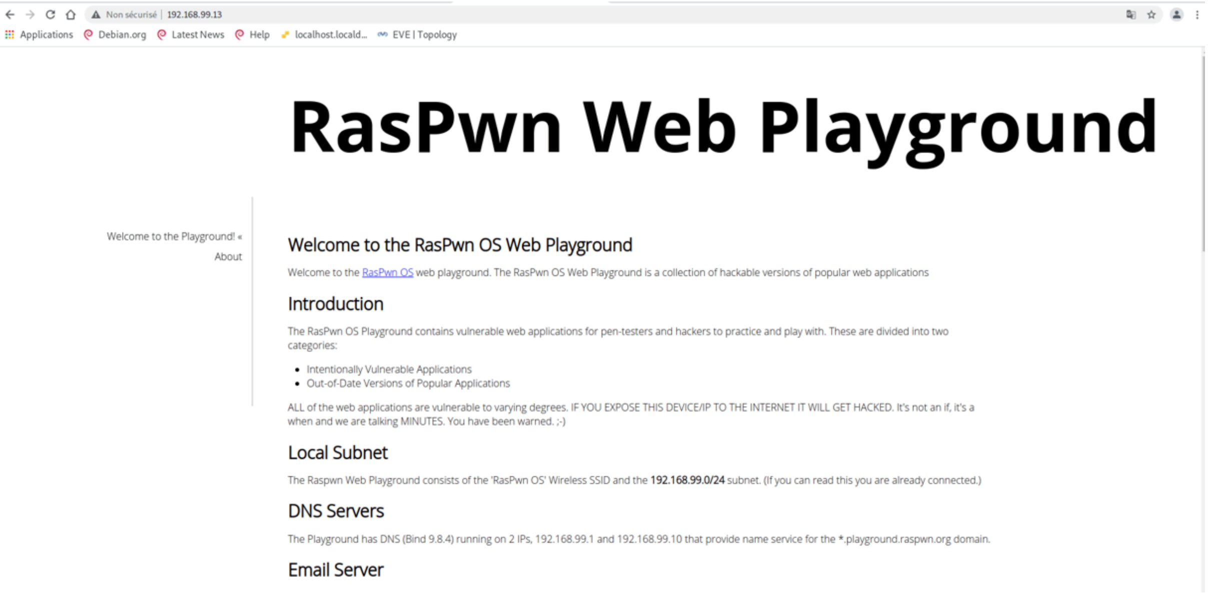
Welcome to SWAT!

Please choose a configuration action using one of the above buttons

Samba Documentation

- **Daemons**
  - smbd - the SMB daemon
  - nmbd - the NetBIOS nameserver
  - winbindd - the winbind daemon
- **Configuration Files**
  - smb.conf - the main Samba configuration file
  - lmhosts - NetBIOS hosts file
  - smbpasswd - SMB password file
- **Administrative Utilities**
  - smbcontrol - send control messages to Samba daemons
  - smbpasswd - managing SMB passwords
  - SWAT - web configuration tool
  - net - tool for administration of Samba and remote CIFS servers
  - pdbedit - Samba user account management tool
  - tdbbackup - Tool for backing up TDB databases
- **Client Tools**
  - rpcclient - command line MS-RPC client
  - smbtar - SMB backup tool
  - smbclient - command line SMB client
  - smbmnt - helper utility for mounting SMB filesystems on Linux hosts
  - smbmount - user space tool for mounting SMB filesystems under Linux
  - smbumount - user space tool for umounting SMB filesystems under Linux
  - ntlm_auth - allow external programs to use NTLM authentication
  - smbcquotas - get or set quotas on NTFS 5 shares
  - smbspool - Send a print job to an SMB printer
  - smbtree - Text-based SMB network browsing
- **Diagnostic Utilities**
  - smbstatus - monitoring Samba
  - testparm - validating your config file
  - nmblookup - NetBIOS name query tool

192.168.99.13



RasPwn Web Playground

Welcome to the RasPwn OS Web Playground

Welcome to the RasPwn OS web playground. The RasPwn OS Web Playground is a collection of hackable versions of popular web applications

Introduction

The RasPwn OS Playground contains vulnerable web applications for pen-testers and hackers to practice and play with. These are divided into two categories:

- Intentionally Vulnerable Applications
- Out-of-Date Versions of Popular Applications

ALL of the web applications are vulnerable to varying degrees. IF YOU EXPOSE THIS DEVICE/IP TO THE INTERNET IT WILL GET HACKED. It's not an if, it's a when and we are talking MINUTES. You have been warned. ;-)

Local Subnet

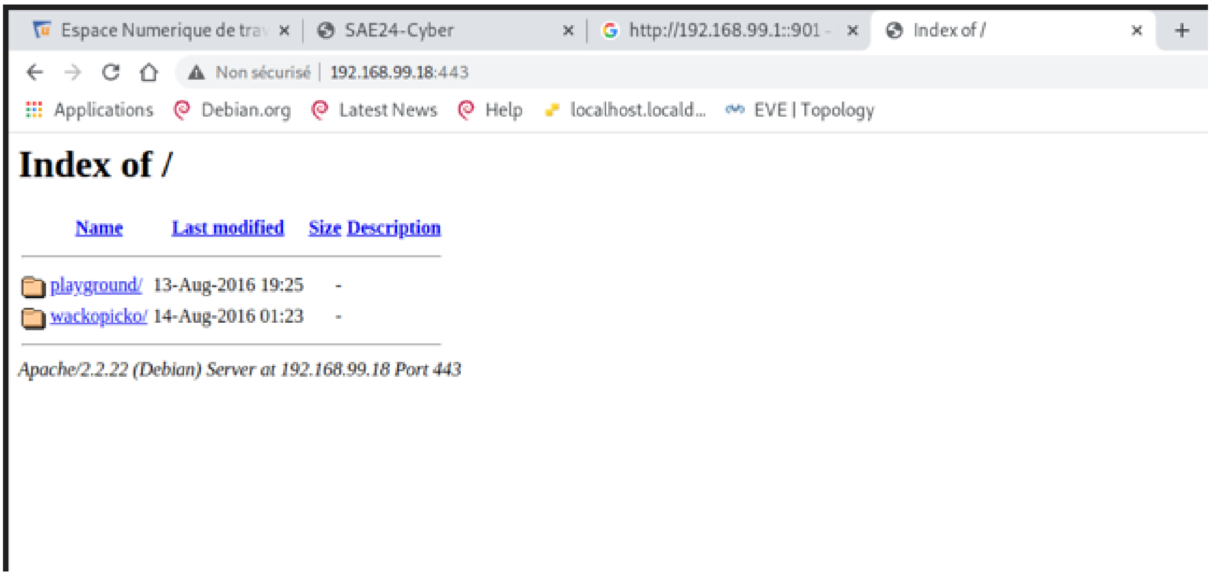
The Raspwn Web Playground consists of the 'RasPwn OS' Wireless SSID and the **192.168.99.0/24** subnet. (If you can read this you are already connected.)

DNS Servers

The Playground has DNS (Bind 9.8.4) running on 2 IPs, 192.168.99.1 and 192.168.99.10 that provide name service for the *.playground.raspwn.org domain.

Email Server

192.168.99.18:443

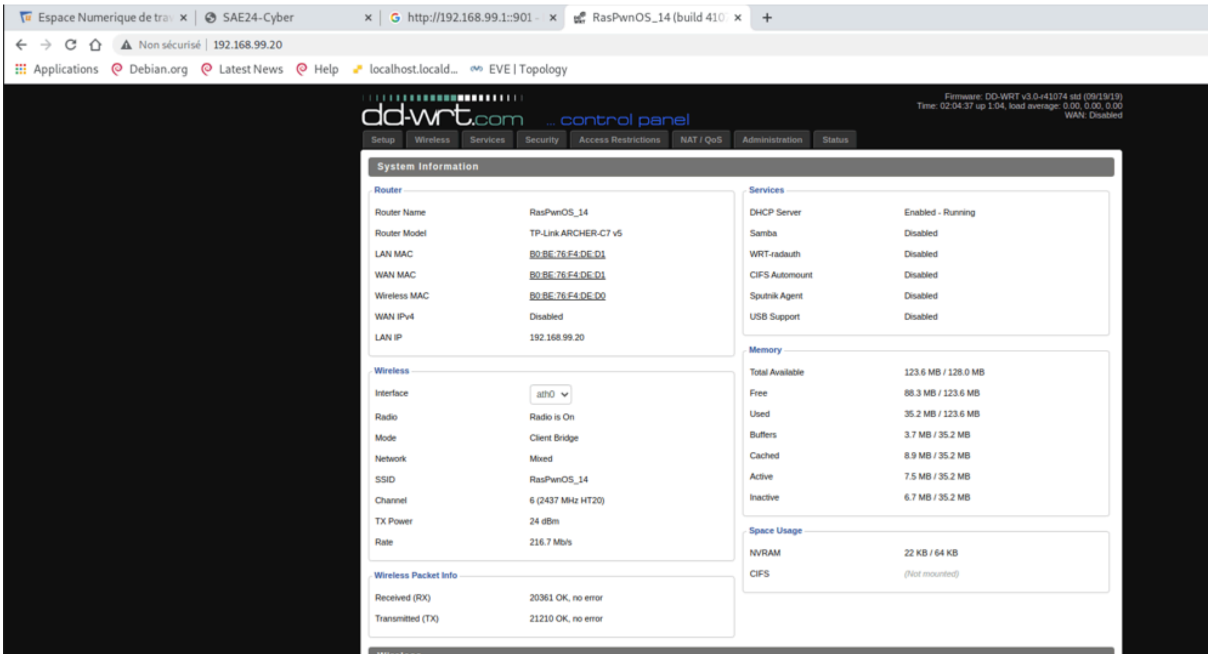


Index of /

Name	Last modified	Size	Description
playground/	13-Aug-2016 19:25	-	
wackopicko/	14-Aug-2016 01:23	-	

Apache/2.2.22 (Debian) Server at 192.168.99.18 Port 443

192.168.99.20



Firmware: DD-WRT v3.0-r41074 std (09/19/19)
Time: 02:04:37 up 1:04, load average: 0.00, 0.00, 0.00
WAN: Disabled

System Information

Router

Router Name	RasPwnOS_14
Router Model	TP-Link ARCHER-C7 v5
LAN MAC	B0:BE:76:F4:DE:D1
WAN MAC	B0:BE:76:F4:DE:D1
Wireless MAC	B0:BE:76:F4:DE:D0
WAN IPv4	Disabled
LAN IP	192.168.99.20

Wireless

Interface	ath0
Radio	Radio is On
Mode	Client Bridge
Network	Mixed
SSID	RasPwnOS_14
Channel	6 (2437 MHz HT20)
TX Power	24 dBm
Rate	216.7 Mb/s

Wireless Packet Info

Received (RX)	20361 OK, no error
Transmitted (TX)	21210 OK, no error

Services

DHCP Server	Enabled - Running
Samba	Disabled
WRT-radauth	Disabled
CIFS Automount	Disabled
Sputnik Agent	Disabled
USB Support	Disabled

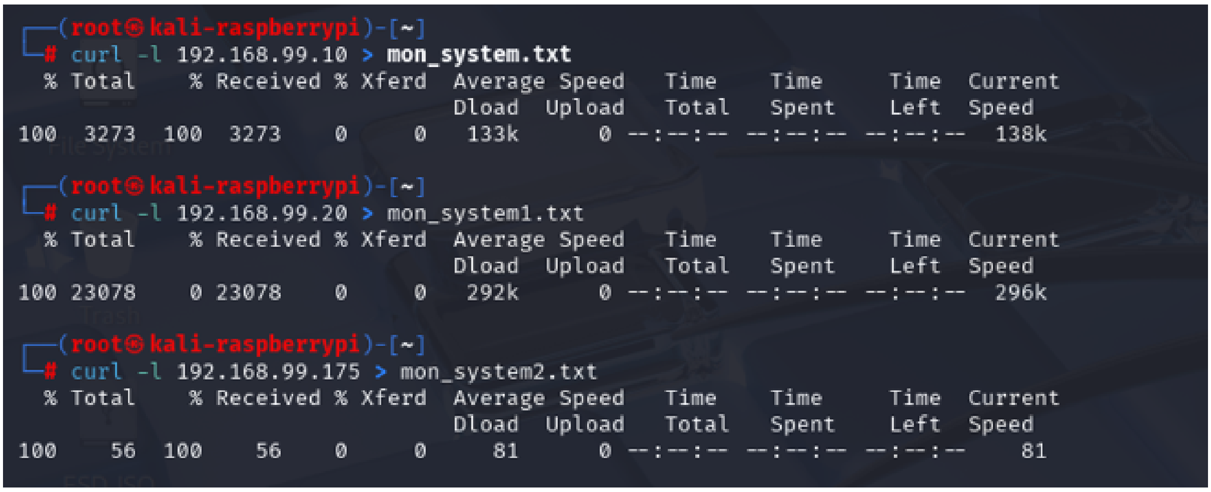
Memory

Total Available	123.6 MB / 128.0 MB
Free	88.3 MB / 123.6 MB
Used	35.2 MB / 123.6 MB
Buffers	3.7 MB / 35.2 MB
Cached	8.9 MB / 35.2 MB
Active	7.5 MB / 35.2 MB
Inactive	6.7 MB / 35.2 MB

Space Usage

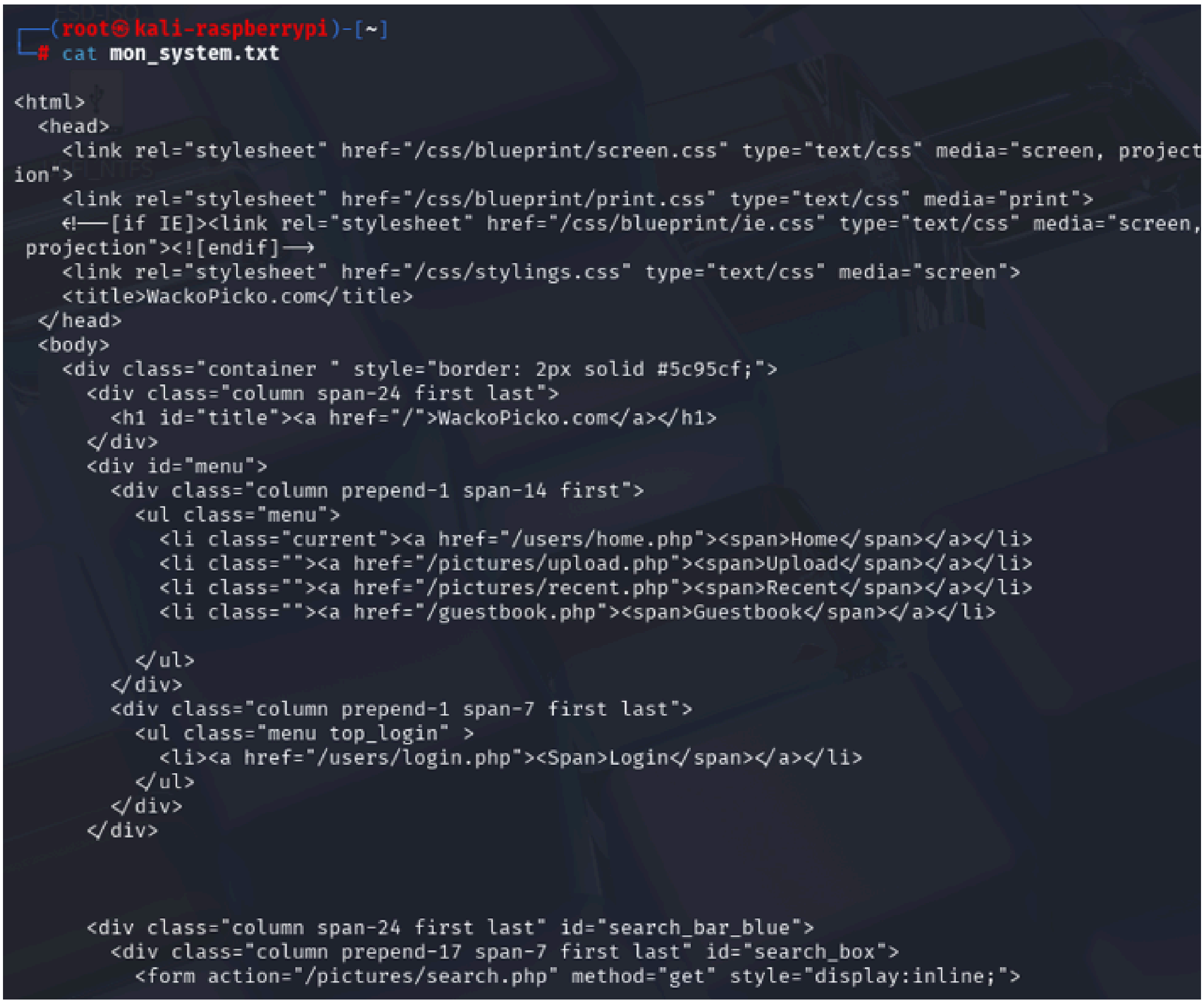
NVRAM	22 KB / 64 KB
CIFS	*(Not mounted)*

Vérification fonctionnelle du fichier mon_systeme.txt (curl -l @IP> ….):

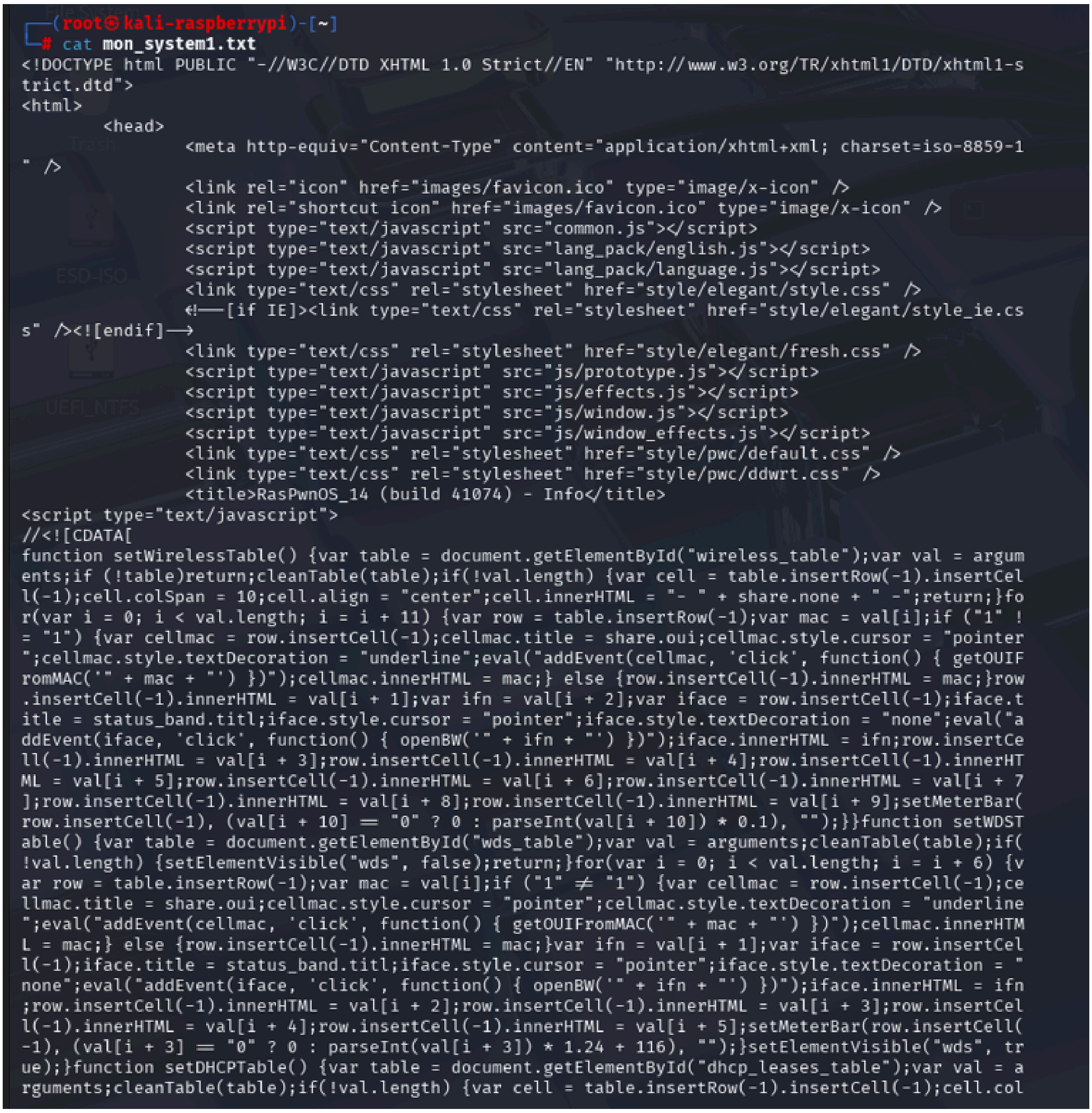


```
┌──(root㉿kali-raspberrypi)-[~]
└─# curl -l 192.168.99.10 > mon_system.txt
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  3273  100  3273    0     0   133k      0 --:--:-- --:--:-- --:--:--  138k

┌──(root㉿kali-raspberrypi)-[~]
└─# curl -l 192.168.99.20 > mon_system1.txt
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 23078    0 23078    0     0   292k      0 --:--:-- --:--:-- --:--:--  296k

┌──(root㉿kali-raspberrypi)-[~]
└─# curl -l 192.168.99.175 > mon_system2.txt
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    56  100    56    0     0     81      0 --:--:-- --:--:-- --:--:--    81
```

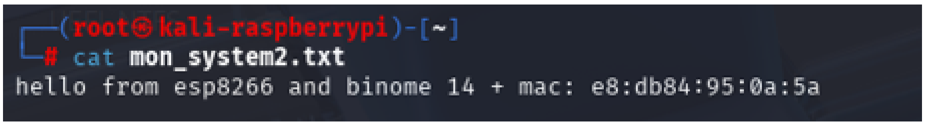
contenue des fichiers



```
┌──(root㉿kali-raspberrypi)-[~]
└─# cat mon_system.txt

<html>
  <head>
    <link rel="stylesheet" href="/css/blueprint/screen.css" type="text/css" media="screen, project
ion">
    <link rel="stylesheet" href="/css/blueprint/print.css" type="text/css" media="print">
    <!--[if IE]><link rel="stylesheet" href="/css/blueprint/ie.css" type="text/css" media="screen,
 projection"><![endif]-->
    <link rel="stylesheet" href="/css/stylings.css" type="text/css" media="screen">
    <title>WackoPicko.com</title>
  </head>
  <body>
    <div class="container " style="border: 2px solid #5c95cf;">
      <div class="column span-24 first last">
        <h1 id="title"><a href="/">WackoPicko.com</a></h1>
      </div>
      <div id="menu">
        <div class="column prepend-1 span-14 first">
          <ul class="menu">
            <li class="current"><a href="/users/home.php"><span>Home</span></a></li>
            <li class=""><a href="/pictures/upload.php"><span>Upload</span></a></li>
            <li class=""><a href="/pictures/recent.php"><span>Recent</span></a></li>
            <li class=""><a href="/guestbook.php"><span>Guestbook</span></a></li>

          </ul>
        </div>
        <div class="column prepend-1 span-7 first last">
          <ul class="menu top_login" >
            <li><a href="/users/login.php"><Span>Login</span></a></li>
          </ul>
        </div>
      </div>



      <div class="column span-24 first last" id="search_bar_blue">
        <div class="column prepend-17 span-7 first last" id="search_box">
          <form action="/pictures/search.php" method="get" style="display:inline;">
```

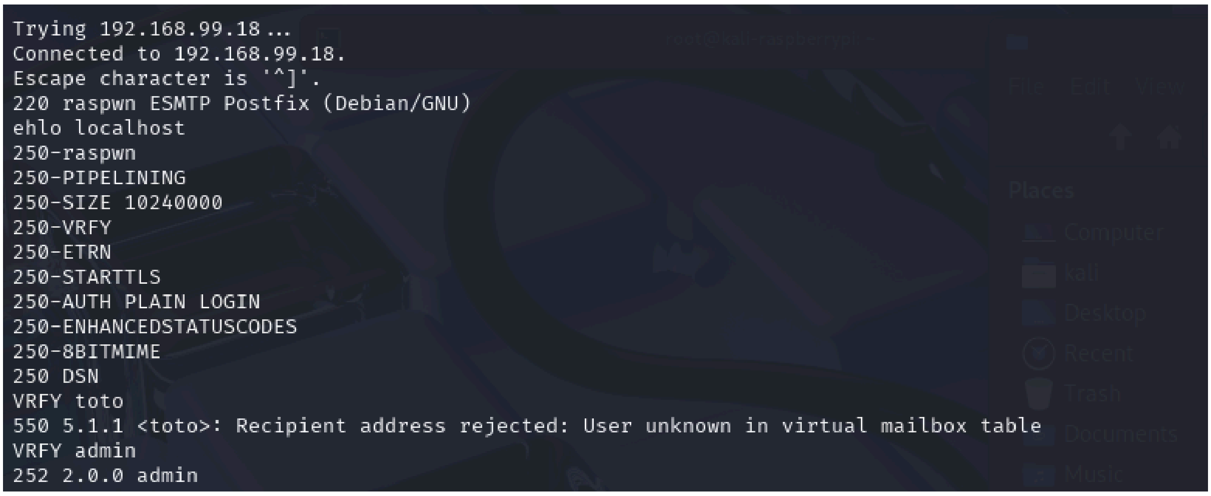


```
┌──(root㉿kali-raspberrypi)-[~]
└─# cat mon_system1.txt
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-s
trict.dtd">
<html>
        <head>
                <meta http-equiv="Content-Type" content="application/xhtml+xml; charset=iso-8859-1
" />
                <link rel="icon" href="images/favicon.ico" type="image/x-icon" />
                <link rel="shortcut icon" href="images/favicon.ico" type="image/x-icon" />
                <script type="text/javascript" src="common.js"></script>
                <script type="text/javascript" src="lang_pack/english.js"></script>
                <script type="text/javascript" src="lang_pack/language.js"></script>
                <link type="text/css" rel="stylesheet" href="style/elegant/style.css" />
                <!--[if IE]><link type="text/css" rel="stylesheet" href="style/elegant/style_ie.cs
s" /><![endif]-->
                <link type="text/css" rel="stylesheet" href="style/elegant/fresh.css" />
                <script type="text/javascript" src="js/prototype.js"></script>
                <script type="text/javascript" src="js/effects.js"></script>
                <script type="text/javascript" src="js/window.js"></script>
                <script type="text/javascript" src="js/window_effects.js"></script>
                <link type="text/css" rel="stylesheet" href="style/pwc/default.css" />
                <link type="text/css" rel="stylesheet" href="style/pwc/ddwrt.css" />
                <title>RasPwnOS_14 (build 41074) - Info</title>
<script type="text/javascript">
//<![CDATA[
function setWirelessTable() {var table = document.getElementById("wireless_table");var val = argum
ents;if (!table)return;cleanTable(table);if(!val.length) {var cell = table.insertRow(-1).insertCel
l(-1);cell.colSpan = 10;cell.align = "center";cell.innerHTML = "- " + share.none + " -";return;}fo
r(var i = 0; i < val.length; i = i + 11) {var row = table.insertRow(-1);var mac = val[i];if ("1" !
= "1") {var cellmac = row.insertCell(-1);cellmac.title = share.oui;cellmac.style.cursor = "pointer
";cellmac.style.textDecoration = "underline";eval("addEvent(cellmac, 'click', function() { getOUIF
romMAC('" + mac + "') })");cellmac.innerHTML = mac;} else {row.insertCell(-1).innerHTML = mac;}row
.insertCell(-1).innerHTML = val[i + 1];var ifn = val[i + 2];var iface = row.insertCell(-1);iface.t
itle = status_band.titl;iface.style.cursor = "pointer";iface.style.textDecoration = "none";eval("a
ddEvent(iface, 'click', function() { openBW('" + ifn + "') })");iface.innerHTML = ifn;row.insertCe
ll(-1).innerHTML = val[i + 3];row.insertCell(-1).innerHTML = val[i + 4];row.insertCell(-1).innerHT
ML = val[i + 5];row.insertCell(-1).innerHTML = val[i + 6];row.insertCell(-1).innerHTML = val[i + 7
];row.insertCell(-1).innerHTML = val[i + 8];row.insertCell(-1).innerHTML = val[i + 9];setMeterBar(
row.insertCell(-1), (val[i + 10] == "0" ? 0 : parseInt(val[i + 10]) * 0.1), "");}}function setWDST
able() {var table = document.getElementById("wds_table");var val = arguments;cleanTable(table);if(
!val.length) {setElementVisible("wds", false);return;}for(var i = 0; i < val.length; i = i + 6) {v
ar row = table.insertRow(-1);var mac = val[i];if ("1" != "1") {var cellmac = row.insertCell(-1);ce
llmac.title = share.oui;cellmac.style.cursor = "pointer";cellmac.style.textDecoration = "underline
";eval("addEvent(cellmac, 'click', function() { getOUIFromMAC('" + mac + "') })");cellmac.innerHTM
L = mac;} else {row.insertCell(-1).innerHTML = mac;}var ifn = val[i + 1];var iface = row.insertCel
l(-1);iface.title = status_band.titl;iface.style.cursor = "pointer";iface.style.textDecoration = "
none";eval("addEvent(iface, 'click', function() { openBW('" + ifn + "') })");iface.innerHTML = ifn
;row.insertCell(-1).innerHTML = val[i + 2];row.insertCell(-1).innerHTML = val[i + 3];row.insertCel
l(-1).innerHTML = val[i + 4];row.insertCell(-1).innerHTML = val[i + 5];setMeterBar(row.insertCell(
-1), (val[i + 3] == "0" ? 0 : parseInt(val[i + 3]) * 1.24 + 116), "");}setElementVisible("wds", tr
ue);}function setDHCPTable() {var table = document.getElementById("dhcp_leases_table");var val = a
rguments;cleanTable(table);if(!val.length) {var cell = table.insertRow(-1).insertCell(-1);cell.col
```



```
┌──(root㉿kali-raspberrypi)-[~]
└─# cat mon_system2.txt
hello from esp8266 and binome 14 + mac: e8:db84:95:0a:5a
```

commande VRFY



```
Trying 192.168.99.18...
Connected to 192.168.99.18.
Escape character is '^]'.
220 raspwn ESMTP Postfix (Debian/GNU)
ehlo localhost
250-raspwn
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-AUTH PLAIN LOGIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
VRFY toto
550 5.1.1 <toto>: Recipient address rejected: User unknown in virtual mailbox table
VRFY admin
252 2.0.0 admin
```

Le test VRFY permet de vérifier l’existence d’une @ email sur le serveur SMTP sans envoyer de message. Ici, la tentative VRFY toto a été rejetée (« User unknown »), indiquant que l’utilisateur n’existe pas dans la table virtuelle. En revanche, VRFY admin a répondu positivement (« 252 2.0.0 »), confirmant que la @ email « admin » est valide et accessible.