ATTACK DEFENSE

by PentesterAcademy

Name	Finger Recon: Basics
URL	https://www.attackdefense.com/challengedetails?cid=535
Type	Network Recon : Finger Servers

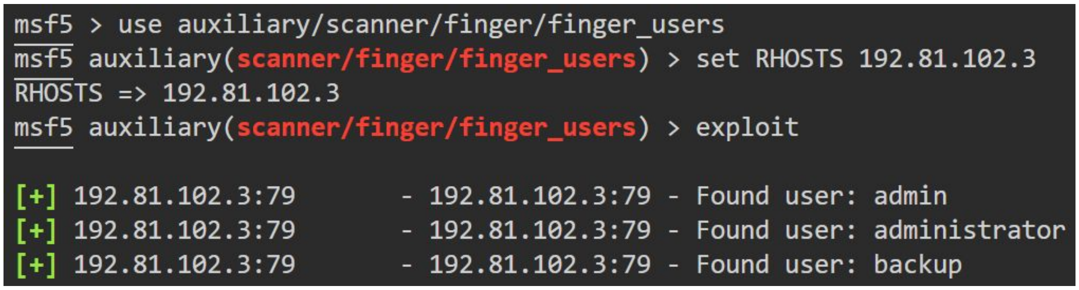
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Q1. How many of users present in user list /usr/share/metasploit-framework/data/wordlist/unix_users.txt, are also present on the server?

Answer: 27

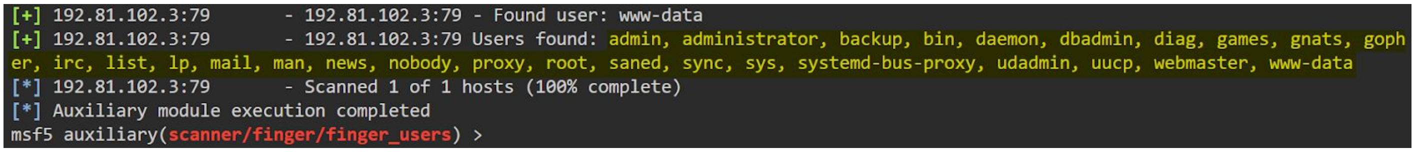
Commands:

msfconsole
use auxiliary/scanner/finger/finger_users
set RHOSTS 192.81.102.3
exploit



```
msf5 > use auxiliary/scanner/finger/finger_users
msf5 auxiliary(scanner/finger/finger_users) > set RHOSTS 192.81.102.3
RHOSTS => 192.81.102.3
msf5 auxiliary(scanner/finger/finger_users) > exploit

[+] 192.81.102.3:79       - 192.81.102.3:79 - Found user: admin
[+] 192.81.102.3:79       - 192.81.102.3:79 - Found user: administrator
[+] 192.81.102.3:79       - 192.81.102.3:79 - Found user: backup
```

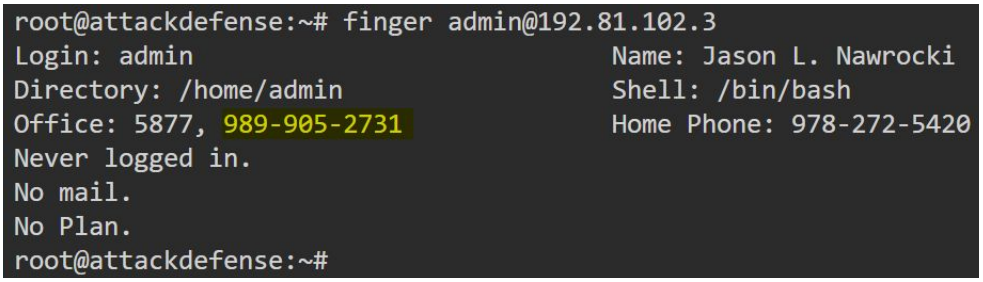


```
[+] 192.81.102.3:79       - 192.81.102.3:79 - Found user: www-data
[+] 192.81.102.3:79       - 192.81.102.3:79 Users found: admin, administrator, backup, bin, daemon, dbadmin, diag, games, gnats, goph
er, irc, list, lp, mail, man, news, nobody, proxy, root, saned, sync, sys, systemd-bus-proxy, udadmin, uucp, webmaster, www-data
[*] 192.81.102.3:79       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/finger/finger_users) >
```

Q2. What is the office phone number of user admin?

Answer: 989-905-2731

Command: finger admin@192.81.102.3



```
root@attackdefense:~# finger admin@192.81.102.3
Login: admin                            Name: Jason L. Nawrocki
Directory: /home/admin                  Shell: /bin/bash
Office: 5877, 989-905-2731              Home Phone: 978-272-5420
Never logged in.
No mail.
No Plan.
root@attackdefense:~#
```

Q3. Three flags are deliberately hidden in the information served by finger service. Find all three flags.

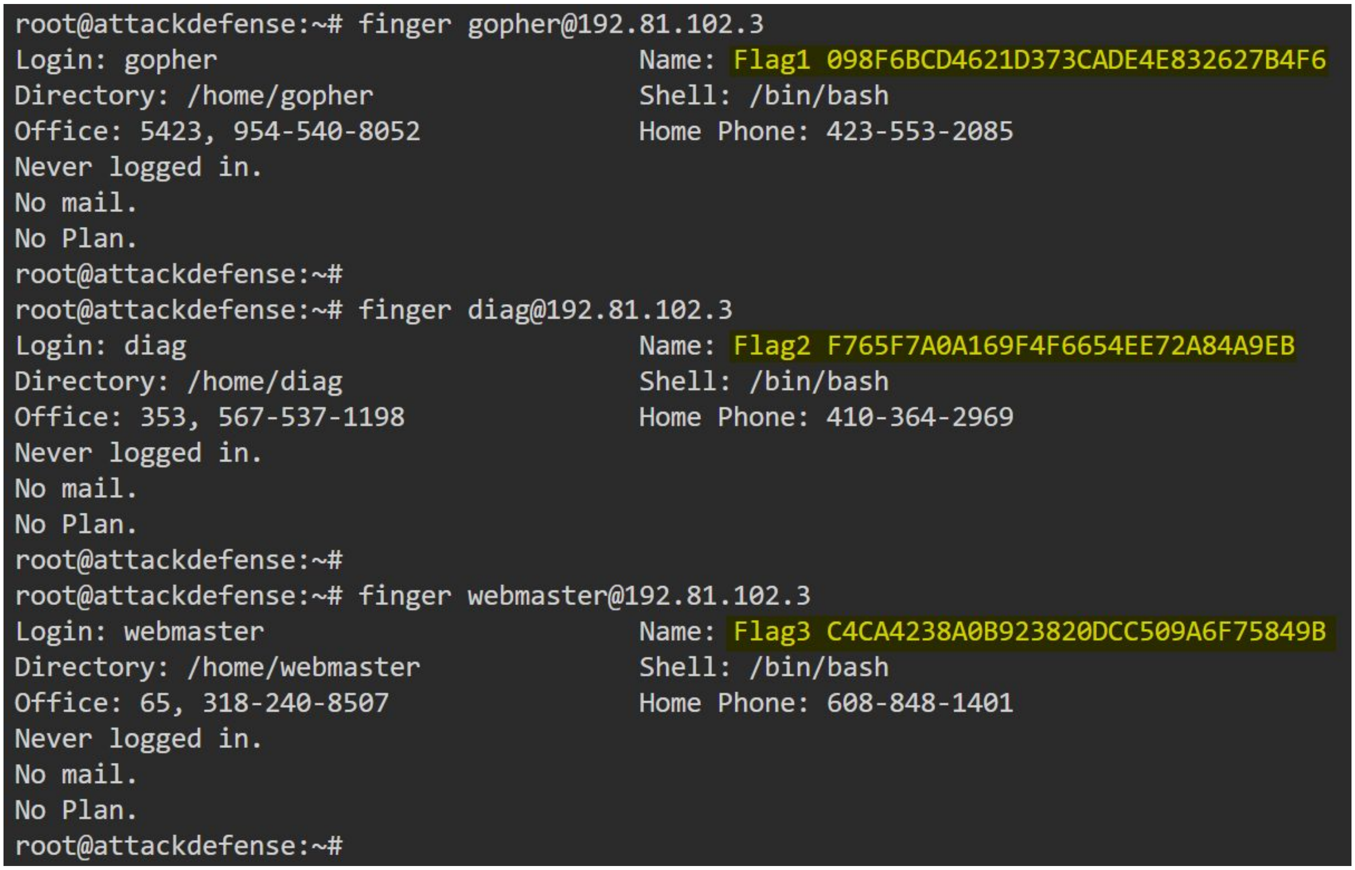
Answer:
Flag1: 098F6BCD4621D373CADE4E832627B4F6
Flag2: F765F7A0A169F4F6654EE72A84A9EB
Flag3: C4CA4238A0B923820DCC509A6F75849B

Solution:

Retrieve information of all user using finger service. Users gopher, diag and webmaster have flag in their name.

Commands:

```
finger gopher@192.81.102.3
finger diag@192.81.102.3
finger webmaster@192.81.102.3
```

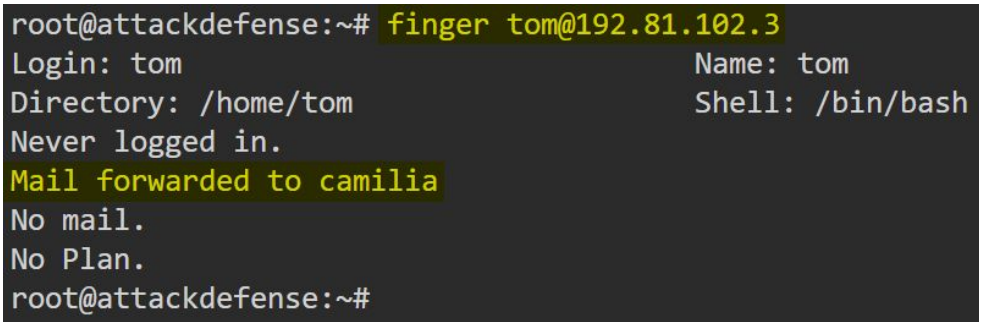


```
root@attackdefense:~# finger gopher@192.81.102.3
Login: gopher                           Name: Flag1 098F6BCD4621D373CADE4E832627B4F6
Directory: /home/gopher                 Shell: /bin/bash
Office: 5423, 954-540-8052              Home Phone: 423-553-2085
Never logged in.
No mail.
No Plan.
root@attackdefense:~#
root@attackdefense:~# finger diag@192.81.102.3
Login: diag                             Name: Flag2 F765F7A0A169F4F6654EE72A84A9EB
Directory: /home/diag                   Shell: /bin/bash
Office: 353, 567-537-1198               Home Phone: 410-364-2969
Never logged in.
No mail.
No Plan.
root@attackdefense:~#
root@attackdefense:~# finger webmaster@192.81.102.3
Login: webmaster                        Name: Flag3 C4CA4238A0B923820DCC509A6F75849B
Directory: /home/webmaster              Shell: /bin/bash
Office: 65, 318-240-8507                Home Phone: 608-848-1401
Never logged in.
No mail.
No Plan.
root@attackdefense:~#
```

Q4. The email of user "tom" are forwarded to which user?

Answer: camilia

Command: finger tom@192.81.102.3

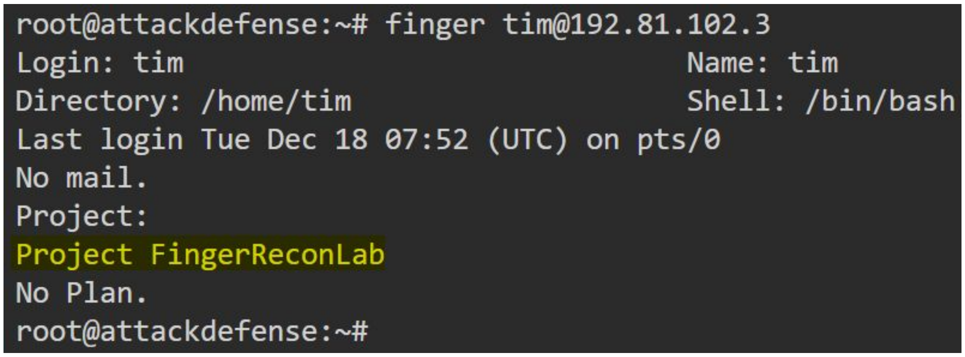


```
root@attackdefense:~# finger tom@192.81.102.3
Login: tom                              Name: tom
Directory: /home/tom                    Shell: /bin/bash
Never logged in.
Mail forwarded to camilia
No mail.
No Plan.
root@attackdefense:~#
```

Q5. Find the details of project on which user “tim” is working.

Answer: Project FingerReconLab

Command: finger tim@192.81.102.3

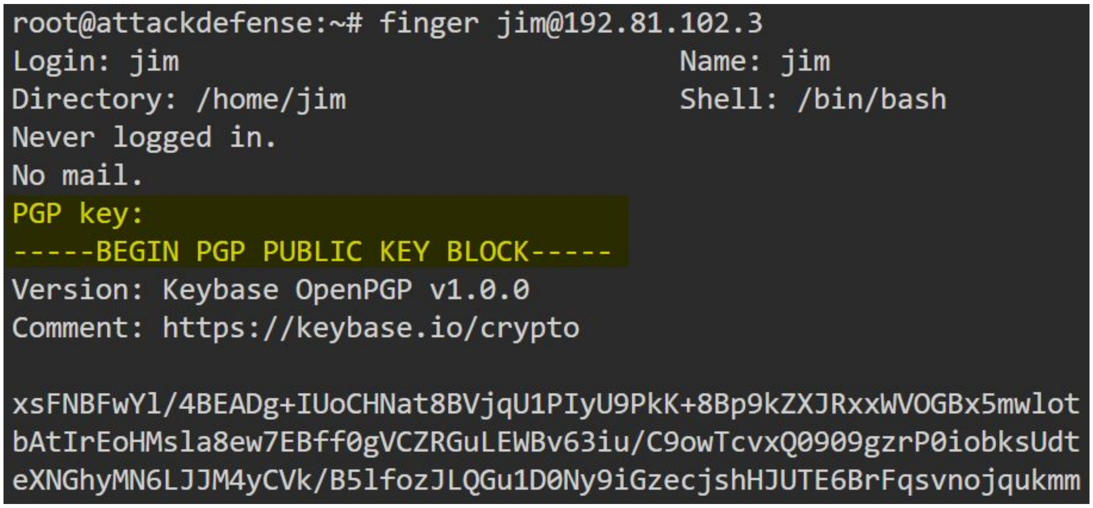


```
root@attackdefense:~# finger tim@192.81.102.3
Login: tim                              Name: tim
Directory: /home/tim                    Shell: /bin/bash
Last login Tue Dec 18 07:52 (UTC) on pts/0
No mail.
Project:
Project FingerReconLab
No Plan.
root@attackdefense:~#
```

Q6. Which users among “tim”,”jim”,”jil”,”tom” and “john” have a pgpkey?

Answer: jim

Commands: finger jim@192.81.102.3



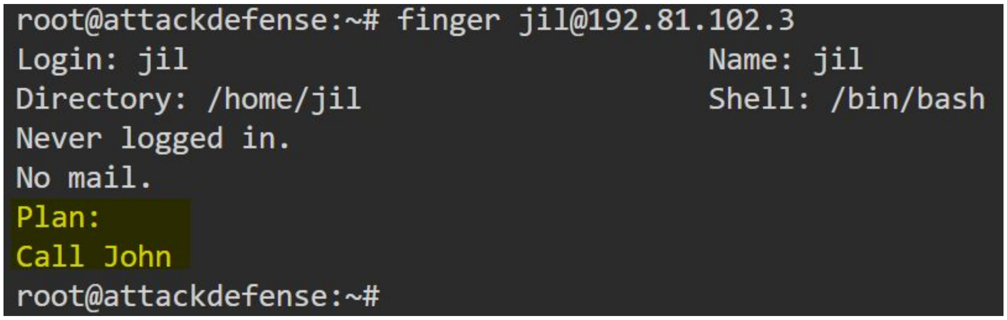
```
root@attackdefense:~# finger jim@192.81.102.3
Login: jim                              Name: jim
Directory: /home/jim                    Shell: /bin/bash
Never logged in.
No mail.
PGP key:
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: Keybase OpenPGP v1.0.0
Comment: https://keybase.io/crypto

xsFNBFwYl/4BEADg+IUoCHNat8BVjqU1PIyU9PkK+8Bp9kZXJRxxWVOGBx5mwlot
bAtIrEoHMsla8ew7EBff0gVCZRGuLEWBv63iu/C9owTcvxQ0909gzrP0iobksUdt
eXNGhyMN6LJJM4yCVk/B5lfozJLQGu1D0Ny9iGzecjshHJUTE6BrFqsvnojqukmm
```

Q7. What is the plan of user “jil”?

Answer: Call John

Commands: finger jil@192.81.102.3

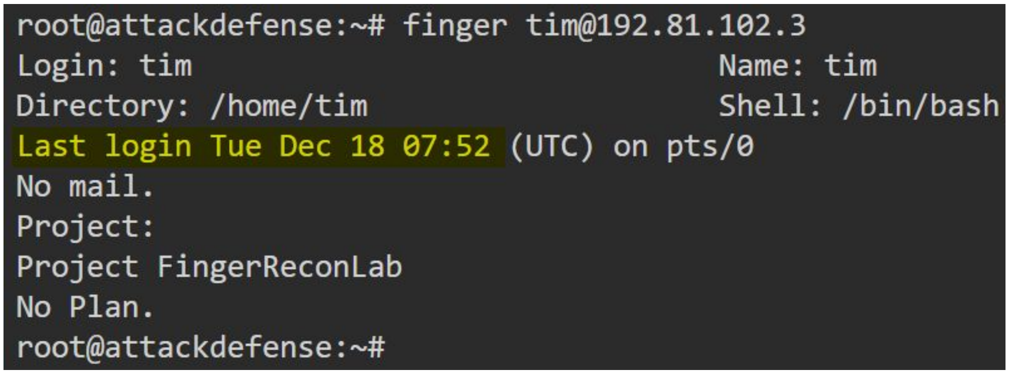


```
root@attackdefense:~# finger jil@192.81.102.3
Login: jil                                      Name: jil
Directory: /home/jil                            Shell: /bin/bash
Never logged in.
No mail.
Plan:
Call John
root@attackdefense:~#
```

Q8. Find the date and time at which user “tim” logged in to the system.

Answer: Dec 18 07:52

Commands: finger tim@192.81.102.3



```
root@attackdefense:~# finger tim@192.81.102.3
Login: tim                                      Name: tim
Directory: /home/tim                            Shell: /bin/bash
Last login Tue Dec 18 07:52 (UTC) on pts/0
No mail.
Project:
Project FingerReconLab
No Plan.
root@attackdefense:~#
```

References:

1. fingerd (https://linux.die.net/man/8/fingerd)
2. finger (https://linux.die.net/man/1/finger)
3. Metasploit Module: Finger Service User Enumerator (https://www.rapid7.com/db/modules/auxiliary/scanner/finger/finger_users)