الملاحق

==========

S1

==========

```
S1>enable

S1#

S1#config t

S1(config)#vlan 10

S1(config-vlan)#name IT-LIBYA

S1(config-vlan)#exit

S1(config)#

S1(config)#vlan 20

S1(config-vlan)#name IT

S1(config-vlan)#exit

S1(config)#

S1(config)#interface range e1 -9

S1(config-if-range)#

S1(config-if-range)#switchport access vlan 10

S1(config-if-range)#exit

S1(config)#

S1(config)#interface range e10 -18

S1(config-if-range)#

S1(config-if-range)#switchport access vlan 20

S1(config-if-range)#exit
```

```
S1(config)#
S1(config)#int e0
S1(config-if)#swithport mode trunk
S1(config-if)#
S1(config-if)#exit
S1(config)#S1(config)#do wr
Building configuration... [OK
```

==========

R1

==========

```
R1#
R1#config t
R1(config)#int f1/0
R1(config-if)#ip address 12.0.0.6 255.255.255.248
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
R1(config)#int f3/0
R1(config-if)#ip address 192.168.1.2 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
R1(config)#
R1(config)#router rip
```

```
R1(config-router)#version 2
R1(config-router)#network 192.168.1.0
R1(config-router)#network 12.0.0.0
R1(config-router)#exit
R1(config)#
R1(config)#do sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set
     12.0.0.0/29 is subnetted, 1 subnets
C       12.0.0.0 is directly connected, FastEthernet1/0
R    192.168.50.0/24 [120/1] via 192.168.1.1, 00:00:27, FastEthernet3/0
     192.168.1.0/30 is subnetted, 1 subnets
C       192.168.1.0 is directly connected, FastEthernet3/0
R    192.168.2.0/24 [120/2] via 192.168.1.1, 00:00:27, FastEthernet3/0
R1(config)#do wr
Building configuration...
[OK]
```

Router on a Statick

```
R1(config)#

R1(config)#int f0/0

R1(config-if)#no shutdown

R1(config-if)#exit

R1(config)#

R1(config)#interface f0/0.10

R1(config-subif)#encapsulation dot1Q 10

R1(config-subif)#ip address 10.0.0.254 255.255.255.0

R1(config-subif)#exit

R1(config)#

R1(config)#int f0/0.20

R1(config-subif)#encapsulation dot1Q 20

R1(config-subif)#ip address 11.0.0.254 255.255.255.0

R1(config-subif)#exit

R1(config)#

R1(config)#

R1(config)#router rip

R1(config-router)#version 2

R1(config-router)#network 10.0.0.0

R1(config-router)#network 11.0.0.0

R1(config-router)#network 12.0.0.0

R1(config-router)#network 192.168.1.0

R1(config-router)#exit
```

```
R1(config)#
R1(config)#do sh ip int br
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            unassigned      YES NVRAM  up                    up
FastEthernet0/0.10         10.0.0.254      YES manual up                    up
FastEthernet0/0.20         11.0.0.254      YES manual up                    up
FastEthernet1/0            192.168.1.2     YES NVRAM  up                    up
Serial2/0                  unassigned      YES NVRAM  administratively down down
Serial2/1                  unassigned      YES NVRAM  administratively down down
Serial2/2                  unassigned      YES NVRAM  administratively down down
Serial2/3                  unassigned      YES NVRAM  administratively down down
FastEthernet3/0            12.0.0.6        YES NVRAM  up                    up
R1(config)#
R1(config)#
R1(config)#do sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
    10.0.0.0/24 is subnetted, 1 subnets
```

```
C       10.0.0.0 is directly connected, FastEthernet0/0.10
     11.0.0.0/24 is subnetted, 1 subnets
C       11.0.0.0 is directly connected, FastEthernet0/0.20
     12.0.0.0/29 is subnetted, 1 subnets
C       12.0.0.0 is directly connected, FastEthernet3/0
R    192.168.50.0/24 [120/1] via 192.168.1.1, 00:00:02, FastEthernet1/0
     192.168.1.0/30 is subnetted, 1 subnets
C       192.168.1.0 is directly connected, FastEthernet1/0
R    192.168.2.0/24 [120/2] via 192.168.1.1, 00:00:04, FastEthernet1/0
R1(config)#
R1(config)#
R1(config)#do wr
Building configuration...
[OK]
R1(config)#
```

==========

R2

==========

```
R2#
R2#config t
R2(config)#
R2(config)#int f0/0
R2(config-if)#ip address 192.168.50.1 255.255.255.252
R2(config-if)#no shutdown
```

```
R2(config-if)#exit
R2(config)#
R2(config)#int f1/0
R2(config-if)#ip address 192.168.2.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
R2(config)#int s2/0
R2(config-if)#ip address 200.50.30.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
```

Static Nat , Default Route and RIP

```
R2(config)#ip nat inside source static 192.168.2.2 200.50.30.10
R2(config)#ip nat inside source static 192.168.2.3 200.50.30.11
R2(config)#ip nat inside source static 192.168.2.4 200.50.30.12
R2(config)#ip nat inside source static 192.168.2.5 200.50.30.13
R2(config)#ip nat inside source static 192.168.2.98 200.50.30.14
R2(config)#ip nat inside source static 192.168.2.99 200.50.30.15
R2(config)#
R2(config)#int f1/0
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#
```

```
R2(config)#int s2/0
R2(config-if)#ip nat outside
R2(config-if)#exit
R2(config)#
R2(config)#do sh ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 200.50.30.10       192.168.2.2        ---                ---
--- 200.50.30.11       192.168.2.3        ---                ---
--- 200.50.30.12       192.168.2.4        ---                ---
--- 200.50.30.13       192.168.2.5        ---                ---
--- 200.50.30.14       192.168.2.98       ---                ---
--- 200.50.30.15       192.168.2.99       ---                ---
R2(config)#
R2(config)#ip route 0.0.0.0 0.0.0.0 200.50.30.2
R2(config)#
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 192.168.50.0
R2(config-router)#network 192.168.2.0
R2(config-router)#exit
R2(config)#
R2(config)#do sh ip rou
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
```

N1 – OSPF NSSA external type 1, N2 – OSPF NSSA external type 2

E1 – OSPF external type 1, E2 – OSPF external type 2

i – IS-IS, su – IS-IS summary, L1 – IS-IS level-1, L2 – IS-IS level-2

ia – IS-IS inter area, * – candidate default, U – per-user static route

o – ODR, P – periodic downloaded static route

Gateway of last resort is 200.50.30.2 to network 0.0.0.0

C 200.50.30.0/24 is directly connected, Serial2/0

R 12.0.0.0/8 [120/2] via 192.168.50.2, 00:00:13, FastEthernet0/0

192.168.50.0/30 is subnetted, 1 subnets

C 192.168.50.0 is directly connected, FastEthernet0/0

R 192.168.1.0/24 [120/1] via 192.168.50.2, 00:00:13, FastEthernet0/0

C 192.168.2.0/24 is directly connected, FastEthernet1/0

S* 0.0.0.0/0 [1/0] via 200.50.30.2

بعد كسر Vlan في R1

R2(config)#sh ip route

Codes: C – connected, S – static, R – RIP, M – mobile, B – BGP

D – EIGRP, EX – EIGRP external, O – OSPF, IA – OSPF inter area

N1 – OSPF NSSA external type 1, N2 – OSPF NSSA external type 2

E1 – OSPF external type 1, E2 – OSPF external type 2

i – IS-IS, su – IS-IS summary, L1 – IS-IS level-1, L2 – IS-IS level-2

ia – IS-IS inter area, * – candidate default, U – per-user static route

o – ODR, P – periodic downloaded static route

Gateway of last resort is not set

R 10.0.0.0/8 [120/2] via 192.168.50.2, 00:00:03, FastEthernet0/0

R 11.0.0.0/8 [120/2] via 192.168.50.2, 00:00:03, FastEthernet0/0

R 12.0.0.0/8 [120/2] via 192.168.50.2, 00:00:03, FastEthernet0/0

192.168.50.0/30 is subnetted, 1 subnets

C 192.168.50.0 is directly connected, FastEthernet0/0

R 192.168.1.0/24 [120/1] via 192.168.50.2, 00:00:03, FastEthernet0/0

C 192.168.2.0/24 is directly connected, FastEthernet1/0

R2(config)#

R2(config)#do wr

Building configuration...

[OK]

R2(config)#

==========

ACL

==========

R2#config t

R2(config)#ip access-list standard IT-LIBYA

R2(config-std-nacl)#permit 192.168.2.0 0.0.0.255

R2(config-std-nacl)#deny any

R2(config-std-nacl)#exit

R2(config)#

R2(config)#int f0/0

R2(config-if)#

```
R2(config-if)#ip access-group IT-LIBYA out
R2(config-if)#exit
R2(config)#
R2(config)#do sh access-lists
Standard IP access list IT-LIBYA
    10 permit 192.168.2.0, wildcard bits 0.0.0.255 (5 matches)
    20 deny   any (30 matches)
R2(config)#
```

==========

Cisco-ASA Firewall

==========

```
Cisco-ASA> ena
Password:
Cisco-ASA# config t
Cisco-ASA(config)# int g0
Cisco-ASA(config-if)# ip address 192.168.50.2 255.255.255.252
Cisco-ASA(config-if)# no shutdown
Cisco-ASA(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
Cisco-ASA(config-if)# security-level 0
Cisco-ASA(config-if)# exit
Cisco-ASA(config)#
Cisco-ASA(config)# int g1
Cisco-ASA(config-if)# ip address 192.168.1.1 255.255.255.252
```

```
Cisco-ASA(config-if)# no shutdown
Cisco-ASA(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
Cisco-ASA(config-if)# security-level 100
Cisco-ASA(config-if)# exit
Cisco-ASA(config)# sh nameif
Interface              Name                Security
GigabitEthernet0       outside             0
GigabitEthernet1       inside              100
Cisco-ASA(config)#
Cisco-ASA(config)#
Cisco-ASA(config)# router rip
Cisco-ASA(config-router)# version 2
Cisco-ASA(config-router)# network 192.168.1.0
Cisco-ASA(config-router)# network 192.168.50.0
Cisco-ASA(config-router)# exit
Cisco-ASA(config)#
Cisco-ASA(config)# sh route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
```

P – periodic downloaded static route

Gateway of last resort is not set

R 12.0.0.0 255.0.0.0 [120/1] via 192.168.1.2, 0:00:14, inside

C 192.168.50.0 255.255.255.252 is directly connected, outside

C 192.168.1.0 255.255.255.252 is directly connected, inside

R 192.168.2.0 255.255.255.0 [120/1] via 192.168.50.1, 0:00:12, outside

Cisco-ASA(config)#

Cisco-ASA(config)# copy run start

Source filename [running-config]?

Cryptochecksum: 318174f1 a187f625 c67fd86a ad11d22f

2139 bytes copied in 1.330 secs (2139 bytes/sec)

Cisco-ASA(config)#

Router on a Staick بعد

Cisco-ASA(config)# sh route

Codes: C – connected, S – static, I – IGRP, R – RIP, M – mobile, B – BGP

D – EIGRP, EX – EIGRP external, O – OSPF, IA – OSPF inter area

N1 – OSPF NSSA external type 1, N2 – OSPF NSSA external type 2

E1 – OSPF external type 1, E2 – OSPF external type 2, E – EGP

i – IS-IS, L1 – IS-IS level-1, L2 – IS-IS level-2, ia – IS-IS inter area

* – candidate default, U – per-user static route, o – ODR

P – periodic downloaded static route

Gateway of last resort is not set

R 10.0.0.0 255.0.0.0 [120/1] via 192.168.1.2, 0:00:19, inside

R 11.0.0.0 255.0.0.0 [120/1] via 192.168.1.2, 0:00:19, inside

```
R    12.0.0.0 255.0.0.0 [120/1] via 192.168.1.2, 0:00:19, inside

C    192.168.50.0 255.255.255.252 is directly connected, outside

C    192.168.1.0 255.255.255.252 is directly connected, inside

R    192.168.2.0 255.255.255.0 [120/1] via 192.168.50.1, 0:00:25, outside

Cisco-ASA(config)#
```

==========

INTERNET

==========

```
INTERNET#

INTERNET#config t

INTERNET(config)#

INTERNET(config-if)#int s2/0

INTERNET(config-if)#ip address 200.50.30.2 255.255.255.0

INTERNET(config-if)#no shutdown

INTERNET(config-if)#exit

INTERNET(config)#

INTERNET(config)#int s2/1

INTERNET(config-if)#ip address 140.90.60.1 255.255.255.0

INTERNET(config-if)#no shutdown

INTERNET(config-if)#exit

INTERNET(config)#

INTERNET(config)#do sh ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
```

```
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
  140.90.0.0/24 is subnetted, 1 subnets
C       140.90.60.0 is directly connected, Serial2/1
C    200.50.30.0/24 is directly connected, Serial2/0
INTERNET(config)#
INTERNET(config)#do copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
INTERNET(config)#
```

==========

R3

==========

```
R3#config t
R3(config)#
R3(config)#int f0/0
R3(config-if)#ip address 192.168.100.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#
R3(config)#int s2/0
R3(config-if)#ip address 140.90.60.2 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#
```

PAT NAT and Default Route

```
R3(config)#
R3(config)#access-list 1 permit 192.168.100.0 0.0.0.255
R3(config)#
R3(config)#ip nat pool IT-LIBYA 140.90.60.2 140.90.60.2 prefix-length 24
R3(config)#
R3(config)#ip nat inside source list 1 pool IT-LIBYA overload
```

```
R3(config)#
R3(config)#int f0/0
R3(config-if)#ip nat inside
R3(config-if)#exit
R3(config)#
R3(config)#int s2/0
R3(config-if)#ip nat outside
R3(config-if)#exit
R3(config)#
R3(config)#do sh ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Outside interfaces:
  Serial2/0
Inside interfaces:
  FastEthernet0/0
Hits: 0  Misses: 0
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool IT-LIBYA refcount 0
 pool IT-LIBYA: netmask 255.255.255.0
        start 140.90.60.2 end 140.90.60.2
        type generic, total addresses 1, allocated 0 (0%), misses 0
```

```
Appl doors: 0

Normal doors: 0

Queued Packets: 0

R3(config)#ip route 0.0.0.0 0.0.0.0 140.90.60.1

R3(config)#

R3(config)#do sh ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

       E1 - OSPF external type 1, E2 - OSPF external type 2

       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

       ia - IS-IS inter area, * - candidate default, U - per-user static route

       o - ODR, P - periodic downloaded static route

Gateway of last resort is 140.90.60.1 to network 0.0.0.0

140.90.0.0/24 is subnetted, 1 subnets

C       140.90.60.0 is directly connected, Serial2/0

C    192.168.100.0/24 is directly connected, FastEthernet0/0

S*   0.0.0.0/0 [1/0] via 140.90.60.1

R3(config)#

R3(config)#do wr

Building configuration...

[OK]
```

==========

SSH-Honeypot Configuration Files

==========

SSH-Honeypot ملف اعدادات

/opt/cowrie/etc/cowrie.cfg

DO NOT EDIT THIS FILE!

Changes to default files will be lost on update and are difficult to

Manage and support

Please make any changes to system defaults by overriding them in cowrie.cfg

To override a specific setting, copy the name of the stanza and

Setting to the file where you wish to override it

==========

General Cowrie Options

==========

[honeypot]

Sensor name is used to identify this Cowrie instance. Used by the database

If not specified, the logging modules will instead use the IP address of the

server as the sensor name

(default: not specified)

sensor_name=myhostname

Hostname for the honeypot. Displayed by the shell prompt of the virtual

environment

(default: svr04)

hostname = server

Directory where to save log files in

(default: log)

log_path = var/log/cowrie

==========

SSH Specific Options

==========

[ssh]

Enable SSH support

(default: true)

enabled = true

Public and private SSH key files. If these don't exist, they are created

automatically

rsa_public_key = ${honeypot:state_path}/ssh_host_rsa_key.pub

rsa_private_key = ${honeypot:state_path}/ssh_host_rsa_key

dsa_public_key = ${honeypot:state_path}/ssh_host_dsa_key.pub

dsa_private_key = ${honeypot:state_path}/ssh_host_dsa_key

SSH version string as present to the client

Version string MUST start with SSH-2.0- or SSH-1.99

Use these to disguise your honeypot from a simple SSH version scan

Examples:

SSH-2.0-OpenSSH_5.1p1 Debian-5

SSH-1.99-OpenSSH_4.7

SSH-1.99-Sun_SSH_1.1

SSH-2.0-OpenSSH_4.2p1 Debian-7ubuntu3.1

SSH-2.0-OpenSSH_4.3

SSH-2.0-OpenSSH_4.6

SSH-2.0-OpenSSH_5.1p1 Debian-5

SSH-2.0-OpenSSH_5.1p1 FreeBSD-20080901

SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu6

SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7

version = SSH-2.0-OpenSSH_6.7p1 Ubuntu-5ubuntu1.3

compression = zlib@openssh.com,zlib,none

Endpoint to listen on for incoming SSH connections.

See https://twistedmatrix.com/documents/current/core/howto/endpoints.htmlservers

(default: listen_endpoints = tcp:22:interface=0.0.0.0)

(use systemd: endpoint for systemd activation)

listen_endpoints = systemd:domain=INET:index=0

For both IPv4 and IPv6: listen_endpoints = tcp6:2222:interface=\:\:

Listening on multiple endpoints is supported with a single space seperator

e.g listen_endpoints = "tcp:2222:interface=0.0.0.0 tcp:1022:interface=0.0.0.0" will result listening both on ports 2222 and 1022

use authbind for port numbers under 1024

listen_endpoints = tcp:22:interface=0.0.0.0

Enable the SFTP subsystem

(default: true)

sftp_enabled = true

==========

ملف تعديل Username and Password عبر المسار التالي:

==========

/opt/cowrie/etc/userdb.example

Example userdb.txt

.This file may be copied to etc/userdb.txt

.If etc/userdb.txt is not present, built-in defaults will be used

':' separated fields, file is processed line for line

processing will stop on first match

Field #1 contains the username

Field #2 is currently unused

Field #3 contains the password

'*' for password allows any password

'!' at the start of a password will not grant this password access

'/' can be used to write a regular expression

root:x:root

ملف Logs الخاص بي SSH-Honeypot

opt/cowrie/var/log/cowrie/cowrie.log/

'HoneyPotSSHTransport,1,192.168.2.13] 'root' trying auth 'password

T21:49:36.982519Z [SSHService 'ssh-userauth' on 01-03-2020

HoneyPotSSHTransport,1,192.168.2.13] Could not read etc/userdb.txt, default database activated

T21:49:36.982806Z [SSHService 'ssh-userauth' on 01-03-2020 HoneyPotSSHTransport,1,192.168.2.13] login attempt [root/] succeeded

T21:49:36.984264Z [SSHService 'ssh-userauth' on 01-03-2020 HoneyPotSSHTransport,1,192.168.2.13] Initialized emulated server as architecture: linux-x64-lsb

T21:49:36.984742Z [SSHService 'ssh-userauth' on 01-03-2020 'HoneyPotSSHTransport,1,192.168.2.13] 'root' authenticated with 'password

T21:49:36.985057Z [SSHService 'ssh-userauth' on 01-03-2020 'HoneyPotSSHTransport,1,192.168.2.13] starting service 'ssh-connection

T21:49:36.986266Z [SSHService 'ssh-connection' on 01-03-2020 HoneyPotSSHTransport,1,192.168.2.13] got channel 'session' request