Operating Systems

- Windows 10 (2016)
- Windows Server 2012r2
- Windows 7
- Ubuntu 16.04
- CentOS 7.4
- Kali Rolling
- Android 7.0

Address Types

Internal Blue Team addresses
Each device in every Blue Team network has its primary network interface connected to the exercise network and assigned with an address from the range 10.0.0.0/16. Internal adresses are unique only within the corresponding Blue Team network and need to be translated for communication beyond the Global Gateway.

Global addresses
Global addresses are unique within the scope of the exercise. They are assigned differently for Global and Blue Team devices. The devices in the Global network have their primary network interface connected to the exercise network and assigned with the global address from the range 4.122.55.0/24. Blue Team devices do not have their global address assigned to a physical interface. Instead, for communication with the Global network and the Internet, the internal addresses are translated to **global addresses** and vice versa on the Global Gateway. Blue Team global addresses have the format 10.X.0.0/16, where X denotes the number {1 - 6} of the Blue Team.

Exercise public addresses
Blue Team devices in the DMZ segments can be reached from the Global segment by addresses that are considered public within the scope of the exercise. These addresses are used to access services in the DMZ (e.g. mailserver, webserver) by users in the Global segment. The exercise public addresses have the format 9.66.XX.0/25, where X denotes the number {1 - 6} of the Blue Team.

Management addresses
Every device (excluding the tablets) participating in the exercise has a secondary network interface connected to a star-shaped management network with the Global Gateway at its center. The management network is independent from the exercise network. It is used only for scoring and when maintenance access to the device is needed during the exercise. Management addresses are from the range 10.7.0.0/16

Internet

GLOBAL
4.122.55.0/24

red-team{1-6}
4.122.55.111-116
4.122.55.211-216
10.7.100.111-116

red-team7
4.122.55.117
4.122.55.217
10.7.100.117

global-web
4.122.55.2
10.7.100.2

global-mail
4.122.55.4
10.7.100.4

desktop2
4.122.55.6
10.7.100.6

test{1-6}
4.122.55.21-26
10.7.100.21-26

global-dns
4.122.55.3
10.7.100.3

desktop1
4.122.55.5
10.7.100.5

global-app
4.122.55.7
10.7.100.7

nagios-global
4.122.55.250
10.7.100.250

MGMT

4.122.55.254
Flow Capture
Interface

10.X.0.0/16
Static
NAT
10.0.0.0/16
Blue Team X

MGMT
10.7.0.0/16

central-config
10.7.96.97

central-scoring
10.7.96.96

scoring-blue{1-6}
10.7.10{1-6}.250

10.7.100.254

Global Gateway

9.66.1.1
9.66.6.1

9.66.X.0/30
Where X is the number
of the Blue Team

VPN-BT1
10.0.5.0/24

tablet-bt1
10.1.5.2
10.0.5.2

Blue
Team 1

MGMT
10.7.101.1

10.0.5.1
9.66.1.2

10.0.1.2
10.0.4.2
10.0.2.2
10.0.3.2

Static NAT
9.66.11.0/25

CISCO ASA

MGMT

DMZ-BT1
10.0.1.0/24

mail.firechmel.ex
9.66.11.12
10.1.1.12
10.0.1.12
10.7.101.12

dns.firechmel.ex
9.66.11.13
10.1.1.13
10.0.1.13
10.7.101.13

www.firechmel.ex
9.66.11.14
10.1.1.14
10.0.1.14
10.7.101.14

MGMT

SRV-BT1
10.0.2.0/24

dc
10.1.2.22
10.0.2.22
10.7.101.22

files
10.1.2.23
10.0.2.23
10.7.101.23

backup
10.1.2.24
10.0.2.24
10.7.101.24

menu
10.1.2.25
10.0.2.25
10.7.101.25

db.chmel.ex
10.1.2.26
10.0.2.26
10.7.101.26

ocs.chmel.ex
10.1.2.27
10.0.2.27
10.7.101.27

ups.chmel.ex
10.1.2.28
10.0.2.28
10.7.101.28

monitoring
10.1.2.29
10.0.2.29
10.7.101.29

MGMT

OPS-BT1
10.0.3.0/24

ops-desktop1
10.1.3.32
10.0.3.32
10.7.101.32

ops-desktop2
10.1.3.33
10.0.3.33
10.7.101.33

insider
10.1.3.34
10.0.3.34
10.7.101.34

MGMT

USR-BT1
10.0.4.0/24

desktop1
10.1.4.42
10.0.4.42
10.7.101.42

desktop2
10.1.4.43
10.0.4.43
10.7.101.43

desktop3
10.1.4.44
10.0.4.44
10.7.101.44

desktop4
10.1.4.45
10.0.4.45
10.7.101.45

admin1
10.1.4.46
10.0.4.46
10.7.101.46

admin2
10.1.4.47
10.0.4.47
10.7.101.47

admin3
10.1.4.48
10.0.4.48
10.7.101.48

admin4
10.1.4.49
10.0.4.49
10.7.101.49

VPN-BT6
10.0.5.0/24

tablet-bt6
10.6.5.2
10.0.5.2

Blue
Team 6

MGMT
10.7.106.1

9.66.6.2
10.0.5.1

10.0.1.2
10.0.4.2
10.0.2.2
10.0.3.2

Static NAT
9.66.66.0/25

CISCO ASA

MGMT

DMZ-BT6
10.0.1.0/24

mail.firechmel.ex
9.66.66.12
10.6.1.12
10.0.1.12
10.7.106.12

dns.firechmel.ex
9.66.66.13
10.6.1.13
10.0.1.13
10.7.106.13

www.firechmel.ex
9.66.66.14
10.6.1.14
10.0.1.14
10.7.106.14

MGMT

SRV-BT6
10.0.2.0/24

dc
10.6.2.22
10.0.2.22
10.7.106.22

files
10.6.2.23
10.0.2.23
10.7.106.23

backup
10.6.2.24
10.0.2.24
10.7.106.24

menu
10.6.2.25
10.0.2.25
10.7.106.25

db.chmel.ex
10.6.2.26
10.0.2.26
10.7.106.26

ocs.chmel.ex
10.6.2.27
10.0.2.27
10.7.106.27

ups.chmel.ex
10.6.2.28
10.0.2.28
10.7.106.28

monitoring
10.6.2.29
10.0.2.29
10.7.106.29

MGMT

OPS-BT6
10.0.3.0/24

ops-desktop1
10.6.3.32
10.0.3.32
10.7.106.32

ops-desktop2
10.1.3.33
10.0.3.33
10.7.101.33

insider
10.6.3.34
10.0.3.34
10.7.106.34

MGMT

USR-BT6
10.0.4.0/24

desktop1
10.6.4.42
10.0.4.42
10.7.106.42

desktop2
10.6.4.43
10.0.4.43
10.7.106.43

desktop3
10.6.4.44
10.0.4.44
10.7.106.44

desktop4
10.6.4.45
10.0.4.45
10.7.106.45

admin1
10.6.4.46
10.0.4.46
10.7.106.46

admin2
10.6.4.47
10.0.4.47
10.7.106.47

admin3
10.6.4.48
10.0.4.48
10.7.106.48

admin4
10.6.4.49
10.0.4.49
10.7.106.49