

Security

Cisco Router Challenge 31

Outline

This challenge involves the configuration of a priority group.

Objectives

The objectives of this challenge are to:

- Define an access-list.
- Define an priority-group.
- Define a route-cache.

Example

```
> en
# config t
(config)# access-list ?
  <1-99>                IP standard access list
  <100-199>              IP extended access list
  <1000-1099>            IPX SAP access list
  <1100-1199>            Extended 48-bit MAC address access list
  <1200-1299>            IPX summary address access list
  <1300-1999>            IP standard access list (expanded range)
  <200-299>              Protocol type-code access list
  <2000-2699>            IP extended access list (expanded range)
  <700-799>              48-bit MAC address access list
  <800-899>              IPX standard access list
  <900-999>              IPX extended access list
  dynamic-extended      Extend the dynamic ACL absolute timer
  rate-limit             Simple rate-limit specific access list

(config)# access-list 105 ?
  deny                  Specify packets to reject
  dynamic               Specify a DYNAMIC list of PERMITs or DENYs
  permit                Specify packets to forward
  remark                Access list entry comment
(config)# access-list 105 permit tcp host 144.93.24.10 host 131.33.204.2 eq dns
(config)# access-list 105 deny tcp host 154.31.216.9 host 26.100.164.1 eq dns
(config)# access-list 105 permit tcp 243.76.220.0 255.255.0.0 89.36.160.0
255.255.0.0 eq dns
(config)# access-list 105 deny tcp 102.65.178.0 255.255.0.0 5.101.146.0 255.255.0.0
eq dns
(config)# access-list 105 permit ip ?
  A.B.C.D               Source address
```

```

any      Any source host
host     A single source host
(config)# access-list 105 permit ip any
A.B.C.D  Destination address
any      Any destination host
eq       Match only packets on a given port number
gt       Match only packets with a greater port number
host     A single destination host
lt       Match only packets with a lower port number
neq      Match only packets not on a given port number
range    Match only packets in the range of port numbers
(config)# access-list 105 permit ip any any
(config)# int e0
(config-if)# ip access-group 105 in
(config)# exit
(config)# priority-list 1 protocol ?
arp      IP ARP
bridge   Bridging
cdp      Cisco Discovery Protocol
compressedtcp  Compressed TCP
ip       IP
ipx      Novell IPX
llc2     llc2
pad      PAD links
snapshot Snapshot routing support
(config)# priority-list 1 protocol ip ?
high
medium
normal
low
(config)# priority-list 1 protocol ip high ?
fragments  Prioritize fragmented IP packets
gt         Prioritize packets greater than a specified size
list       To specify an access list
lt         Prioritize packets less than a specified size
tcp        Prioritize TCP packets 'to' or 'from' the specified port
udp        Prioritize UDP packets 'to' or 'from' the specified port
<cr>
(config)# priority-list 1 protocol ip high list ?
<1-199>    IP access list
<1300-2699> IP expanded access list
(config)# priority-list 1 protocol ip high list 105
(config)# int e0
(config-if)#priority-group ?
<1-16>    Priority group
(config-if)#priority-group 1
(config-if)# ip route-cache ?
cef       Enable Cisco Express Forwarding
flow      Enable Flow fast-switching cache
policy    Enable fast-switching policy cache for outgoing packets
same-interface  Enable fast-switching on the same interface
<cr>
(config-if)# ip route-cache
(config-if)# int e1
(config-if)# ip route-cache

```

Cisco Router Challenge 33

Outline

This challenge involves the configuration of services on the router.

Objectives

The objectives of this challenge are to:

- Define encrypted passwords.
- Define timestamps.
- Disable TCP small services.
- Disable UDP small services.

Example

```
> en
# config t
(config)# service ?
  compress-config      Compress the configuration file
  config               TFTP load config files
  dhcp                Enable DHCP server and relay agent
  disable-ip-fast-frag Disable IP particle-based fast fragmentation
  exec-callback        Enable exec callback
  exec-wait            Delay EXEC startup on noisy lines
  finger               Allow responses to finger requests
  hide-telnet-addresses Hide destination addresses in telnet command
  linenumber           enable line number banner for each exec
  nagle                Enable Nagle's congestion control algorithm
  old-slip-prompts     Allow old scripts to operate with slip/ppp
  pad                  Enable PAD commands
  password-encryption Encrypt system passwords
  prompt               Enable mode specific prompt
  pt-vty-logging       Log significant VTY-Async events
  sequence-numbers    Stamp logger messages with a sequence number
  slave-log            Enable log capability of slave IPs
  tcp-keepalives-in    Generate keepalives on idle incoming network
                       connections
  tcp-keepalives-out   Generate keepalives on idle outgoing network
                       connections
  tcp-small-servers   Enable small TCP servers (e.g., ECHO)
  telnet-zeroidle      Set TCP window 0 when connection is idle
  timestamps         Timestamp debug/log messages
  udp-small-servers  Enable small UDP servers (e.g., ECHO)
(config)# service timestamps ?
  debug   Timestamp debug messages
  log     Timestamp log messages
  <cr>
(config)# service timestamps log ?
  datetime  Timestamp with date and time
  uptime    Timestamp with system uptime
  <cr>
(config)# service timestamps log datetime
(config)# sequence-numbers
```

```

compress-config      Compress the configuration file
config              TFTP load config files
dhcp                Enable DHCP server and relay agent
disable-ip-fast-frag Disable IP particle-based fast fragmentation
exec-callback        Enable exec callback
exec-wait            Delay EXEC startup on noisy lines
finger              Allow responses to finger requests
hide-telnet-addresses Hide destination addresses in telnet command
linenumber           enable line number banner for each exec
nagle                Enable Nagle's congestion control algorithm
old-slip-prompts     Allow old scripts to operate with slip/ppp
pad                  Enable PAD commands
password-encryption Encrypt system passwords
prompt              Enable mode specific prompt
pt-vty-logging       Log significant VTY-Async events
sequence-numbers     Stamp logger messages with a sequence number
slave-log            Enable log capability of slave IPs
tcp-keepalives-in    Generate keepalives on idle incoming network
                    connections
tcp-keepalives-out   Generate keepalives on idle outgoing network
                    connections
tcp-small-servers    Enable small TCP servers (e.g., ECHO)
telnet-zeroidle      Set TCP window 0 when connection is idle
timestamps           Timestamp debug/log messages
udp-small-servers    Enable small UDP servers (e.g., ECHO)
(config)# service sequence-numbers
(config)# service dhcp
(config)# service finger

(config)# no service tcp-small-servers
(config)# no service udp-small-servers
(config)# service password-encryption

```

Cisco Router Challenge 38

Outline

This challenge involves the configuration of AAA.

Objectives

The objectives of this challenge are to:

- Define AAA details.

Example

```

> en
# config t
(config)# aaa new-model

```

```
(config)# aaa authen logging def radius
(config)# aaa authen ppp def radius
(config)# aaa authen banner new york
(config)# aaa authen fail personal device
(config)# aaa author network default radius
(config)# aaa author exec default radius
```

Cisco Router Challenge 39

Outline

This challenge involves the configuration of Tacacs+.

Objectives

The objectives of this challenge are to:

- Setup of Tacacs+.

Example

```
> en
# config t
(config)# aaa new-model
(config)# aaa authen logging def tacacs+
(config)# aaa authen ppp def tacacs+
(config)# aaa authen banner new york
(config)# aaa authen fail personal device
(config)# aaa author network default tacacs+
(config)# aaa author exec default tacacs+
```

Cisco Router Challenge 40

Outline

This challenge involves the configuration of restrictions on the local HTTP server.

Objectives

The objectives of this challenge are to:

- Setup an ACL to permit a single host.
- Apply ACL to restrict access to the HTTP server to only one host.

Example

```
> en
# config t
(config)# access-list 7 permit host 23.17.220.3
(config)# access-list 7 deny any
(config)# ip http server
(config)# ip http ?
  access-class    Restrict access by access-class
  authentication  Set http authentication method
  path            Set base path for HTML
  port            HTTP port
  server          Enable HTTP server
(config)# ip http access-class ?
<1-99> Access list number
(config)# ip http access-class 7
```

Cisco Router Challenge 41

Outline

This challenge involves the configuration of the HTTP server which denies a single host.

Objectives

The objectives of this challenge are to:

- Setup an ACL which denies a single host.
- Apply the ACL to deny the host access to the HTTP server.

Example

```
> en
# config t
(config)# access-list 7 deny host 23.17.220.3
(config)# access-list 7 permit any
(config)# ip http server
(config)# ip http access-class 7
```

Cisco Router Challenge 42

Outline

This challenge involves the configuration of permitting a single host access to the Telnet server.

Objectives

The objectives of this challenge are to:

- Setup an ACL to allow a single host access.
- Apply the ACL to the Telnet server so that only a single host can get access.

Example

```
> en
# config t
(config)# access-list 1 permit host 202.179.77.6
(config)# access-list 1 deny any
(config)# line vty 0 15
(config-line)# login
(config-line)# access-class ?
  <1-199>      IP access list
  <1300-2699>  IP expanded access list
  WORD        Access-list name
(config-line)# access-class 1 ?
  in  Filter incoming connections
  out Filter outgoing connections
(config-line)# access-class 1 in
```

Cisco Router Challenge 43

Outline

This challenge involves the configuration to deny a single host access to the Telnet server.

Objectives

The objectives of this challenge are to:

- Setup an ACL to deny a single host access.
- Apply the ACL to the Telnet server so that only a single host cannot get access.

Example

```
> en
# config t
(config)# access-list 1 deny host 202.179.77.6
(config)# access-list 1 permit any
(config)# line vty 0 15
(config-line)# login
(config-line)# access-class ?
(config-line)# access-class 1 in
```

Cisco Router Challenge 44

Outline

This challenge involves the configuration of IP Inspect.

Objectives

The objectives of this challenge are to:

- Setup limits for the number of connections over one-minute.
- Setup limits for the number of open connections.
- Define SYN waits.

Example

```
> en
# config t
(config)# ip inspect ?
  alert-off          Disable alert
  audit-trail        Enable the logging of session information (addresses and
                    bytes)
  dns-timeout        Specify timeout for DNS
  max-incomplete     Specify maximum number of incomplete connections before
                    clamping
  name               Specify an inspection rule
  one-minute         Specify one-minute-sample watermarks for clamping
  tcp                Config timeout values for tcp connections
  udp                Config timeout values for udp flows
  <cr>
(config)# ip inspect one-minute ?
  high Specify high-watermark for clamping
  low  Specify low-watermark for clamping
```

```

(config)# ip inspect one-minute low 360
(config)# ip inspect one-minute high 410
(config)# ip inspect max-incomplete low 720
(config)# ip inspect max-incomplete high 770
(config)# ip inspect dns-timeout 1
(config)# ip inspect tcp ?
  finwait-time    Specify timeout for TCP connections after a FIN
  idle-time       Specify idle timeout for tcp connections
  max-incomplete  Specify max half-open connection per host
  synwait-time    Specify timeout for TCP connections after a SYN and no
                  further data
(config)# ip inspect tcp synwait-time ?
  <1-2147483>    Timeout in seconds
(config)# ip inspect tcp synwait-time 35
(config)# ip inspect tcp finwait-time 5

(config)# ip inspect tcp max-incomplete ?
  host           Specify max half-open connection per host
(config)# ip inspect tcp max-incomplete host 800
(config)# ip inspect tcp ?
  finwait-time    Specify timeout for TCP connections after a FIN
  idle-time       Specify idle timeout for tcp connections
  max-incomplete  Specify max half-open connection per host
  synwait-time    Specify timeout for TCP connections after a SYN and no
                  further data
(config)# ip inspect tcp idle-time 70
(config)# ip inspect udp idle-time 57

```

Cisco Router Challenge 45

Outline

This challenge involves the configuration of a context based access-list (CBAC).

Objectives

The objectives of this challenge are to:

- Setup a CBAC.
- Define the protocols which the CBAC applies to.

Example

```

> en
# config t
(config)# access-list 105 permit ip any any
(config)# int fa0/0
(config-if)# ip access-group 105 in
(config-if)# exit
(config)# ip inspect name cisco ?

```

```

cuseeme      CUSeeMe Protocol
fragment     IP fragment inspection
ftp          File Transfer Protocol
h323         H.323 Protocol (e.g, MS NetMeeting, Intel Video Phone)
http         HTTP Protocol
netshow      Microsoft NetShow Protocol
rcmd         R commands (r-exec, r-login, r-sh)
realaudio    Real Audio Protocol
rpc          Remote Procedure Call Protocol
rtsp         Real Time Streaming Protocol
smtp         Simple Mail Transfer Protocol
sqlnet       SQL Net Protocol
streamworks  StreamWorks Protocol
tcp          Transmission Control Protocol
tftp         TFTP Protocol
udp          User Datagram Protocol
vdolive      VDOLive Protocol
(config)# ip inspect name cisco tcp
(config)# ip inspect name cisco udp
(config)# ip inspect name cisco ftp
(config)# ip inspect name cisco sqlnet
(config)# int e0
(config-if)# ip inspect ?
      WORD Name of inspection defined
(config-if)# ip inspect cisco
(config-if)# ip inspect cisco in
(config-if)# exit
(config)# access-list 106 deny ip any any
(config)# int s0
(config-if)# ip access-group 106 in

```

Cisco Router Challenge 46

Outline

This challenge involves the configuration of a port map.

Objectives

The objectives of this challenge are to:

- Define the port-mapping for various protocols.

Example

```

> en
# config t
(config)# ip port-map http port 1126
(config)# ip port-map ftp port 1188
(config)# ip port-map smtp port 1897

```

```

(config)# ip port-map telnet port 1189
(config)# exit
# show ip port-map
Default mapping: vdolive          port 7000          system defined
Default mapping: sunrpc           port 111           system defined
Default mapping: netshow         port 1755          system defined
Default mapping: cuseeme         port 7648          system defined
Default mapping: tftp            port 69            system defined
Default mapping: rtsp            port 8554          system defined
Default mapping: realmedia       port 7070          system defined
Default mapping: streamworks     port 1558          system defined
Default mapping: ftp             port 21            system defined
Default mapping: telnet          port 23            system defined
Default mapping: rtsp            port 554           system defined
Default mapping: h323            port 1720          system defined
Default mapping: sip             port 5060          system defined
Default mapping: smtp            port 25            system defined
Default mapping: http            port 80            system defined
Default mapping: msrpc           port 135           system defined
Default mapping: exec            port 512           system defined
Default mapping: login           port 513           system defined
Default mapping: sql-net         port 1521          system defined
Default mapping: shell           port 514           system defined
Default mapping: mgcp            port 2427          system defined
Default mapping: http            port 1126          user defined
Default mapping: ftp             port 1188          user defined
Default mapping: smtp            port 1897          user defined
Default mapping: telnet          port 1189          user defined

```

Cisco Router Challenge 47

Outline

This challenge involves the configuration of an audit trail.

Objectives

The objectives of this challenge are to:

- Setup logging.
- Define an audit-trail.

Example

```

> en
# config t
(config)# logging on
(config)# logging 150.74.40.1
(config)# logging ?
  Hostname or A.B.C.D  IP address of the logging host

```

```

buffered          Set buffered logging parameters
cns-events       Set CNS Event logging level
console         Set console logging level
count           Count every log message and timestamp last occurrence
exception       Limit size of exception flush output
facility        Facility parameter for syslog messages
history        Configure syslog history table
host           Set syslog server host name or IP address
monitor        Set terminal line (monitor) logging level
on             Enable logging to all supported destinations
rate-limit     Set messages per second limit
source-interface Specify interface for source address in logging
transactions
trap           Set syslog server logging level
(config)# logging host 18.46.203.4
(config)# logging trap ?
<0-7>          Logging severity level
alerts        Immediate action needed          (severity=1)
critical      Critical conditions              (severity=2)
debugging    Debugging messages              (severity=7)
emergencies  System is unusable              (severity=0)
errors       Error conditions                (severity=3)
informational Informational messages            (severity=6)
notifications Normal but significant conditions (severity=5)
warnings     Warning conditions            (severity=4)
<cr>
(config)# logging trap warning

(config)# logging monitor warning

(config)# logging console warning

(config)# logging buffer ?
<0-7>          Logging severity level
<4096-2147483647> Logging buffer size
alerts        Immediate action needed          (severity=1)
critical      Critical conditions              (severity=2)
debugging    Debugging messages              (severity=7)
emergencies  System is unusable              (severity=0)
errors       Error conditions                (severity=3)
informational Informational messages            (severity=6)
notifications Normal but significant conditions (severity=5)
warnings     Warning conditions            (severity=4)
<cr>
(config)# logging buffer warnings
(config)# logging buffer 981997
(config)# ip inspect audit-trail
(config)# no ip inspect alert-off

```

Cisco Router Challenge 48

Outline

This challenge involves the configuration to deny an incoming SYN packet.

Objectives

The objectives of this challenge are to:

- Apply an extended ACL which detects the SYN packet.

Example

```
> en
#config t
(config)# access-list 107 deny tcp any any ?
  ack          Match on the ACK bit
  dscp         Match packets with given dscp value
  eq          Match only packets on a given port number
  established Match established connections
  fin         Match on the FIN bit
  fragments   Check non-initial fragments
  gt          Match only packets with a greater port number
  log         Log matches against this entry
  log-input   Log matches against this entry, including input interface
  lt          Match only packets with a lower port number
  neq         Match only packets not on a given port number
  precedence  Match packets with given precedence value
  psh         Match on the PSH bit
  range       Match only packets in the range of port numbers
  rst         Match on the RST bit
  syn         Match on the SYN bit
  time-range  Specify a time-range
  tos         Match packets with given TOS value
  urg         Match on the URG bit
  <cr>
(config)# access-list 107 deny tcp any any established
(config)# access-list 107 permit tcp any any
(config)# int s0
(config-if)# ip access-group ?
  <1-199>      IP access list (standard or extended)
  <1300-2699> IP expanded access list (standard or extended)
  WORD        Access-list name
(config-if)# ip access-group 107 ?
  in          inbound packets
  out         outbound packets
(config-if)# ip access-group 107 in
```

Cisco Router Challenge 54

Outline

This challenge involves the configuration of an authentication proxy.

Objectives

The objectives of this challenge are to:

- Define AAA.
- Setup an authentication proxy.

Example

```
> en
# config t
(config)# aaa new-model

(config)# ip http ?
  access-class      Restrict access by access-class
  authentication    Set http authentication method
  path              Set base path for HTML
  port              HTTP port
  server            Enable HTTP server
(config)# ip http authentication ?
  aaa              Use AAA access control methods
  enable          Use enable passwords
  local           Use local username and passwords
  tacacs          Use tacacs to authorize user
(config)# ip http authentication aaa

(config)# ip auth-proxy ?
  auth-cache-time  Authorization Cache Timeout in min
  auth-proxy-audit Authentication Proxy Auditing
  auth-proxy-banner Authentication Proxy Banner
  name             Specify an Authentication Proxy Rule
  <cr>
(config)# ip auth-proxy auth-cache-time ?
  <1-35791>        Timeout in minutes
(config)# ip auth-proxy auth-cache-time 45

(config)# ip auth-proxy name yellow http

(config)# int fa0

(config-if)# ip auth-proxy ?
  WORD            Name of authenticaion proxy rule
(config-if)# ip auth-proxy yellow
(config-if)# exit
# show ip auth-proxy configuration
# sh ip auth-proxy config
Authentication global cache time is 40 minutes
Authentication Proxy Rule Configuration
Auth-proxy name testing
  http list not specified auth-cache-time 40 minutes
Authentication Proxy Rule Configuration
Auth-proxy name testing
```

Cisco Router Challenge 55

Outline

This challenge involves the configuration of IDS rules.

Objectives

The objectives of this challenge are to:

- Setup IDS rules.
- Define a SPAM filter.

Example

```
> en
# config t
(config)# ip audit ?
  attack    Specify default action for attack signatures
  info      Specify default action for informational signatures
  name      Specify an IDS audit rule
  notify    Specify the notification mechanisms (nr-director or log) for the
            alarms
  po        Specify nr-director's PostOffice information (for sending events
            to the nr-directors)
  signature Add a policy to a signature
  smtp      Specify SMTP Mail spam threshold
(config)# ip audit notify ?
  log       Send events as syslog messages
  nr-director Send events to the nr-director
(config)# ip audit notify log
(config)# logging 132.191.125.3

(config)# ip audit ?
  attack    Specify default action for attack signatures
  info      Specify default action for informational signatures
  name      Specify an IDS audit rule
  notify    Specify the notification mechanisms (nr-director or log) for the
            alarms
  po        Specify nr-director's PostOffice information (for sending events
            to the nr-directors)
  signature Add a policy to a signature
  smtp      Specify SMTP Mail spam threshold
(config)# ip audit info ?
  action    Specify the actions
(config)# ip audit info action ?
  alarm     Generate events for matching signatures
  drop      Drop packets matching signatures
  reset     Reset the connection (if applicable)
(config)# ip audit info action drop
(config)# ip audit attack action reset
(config)# ip audit signature ?
  <1-65535> Signature to be configured
(config)# ip audit signature 1005 disable
(config)# ip audit smtp ?
  spam      Specify the threshold for spam signature
```

```
<cr>
(config)# ip audit smtp spam ?
<1-65535> Threshold of correspondents to trigger alarm
(config)# ip audit smtp spam 4
```

Cisco Router Challenge 56

Outline

This challenge involves setting up IKE for a VPN connection.

Objectives

The objectives of this challenge are to:

- Define the IKE policy.
- Define encryption.
- Define hash function.
- Define authentication type.
- Define identity type.
- Define authentication key and address (for pre-share authentication).
- Define the transform set.

Example

```
> en
# config t
(config)# crypto isakmp enable
(config)# crypto isakmp policy 111
(config-isakmp)# encryption des
(config-isakmp)# hash sha
(config-isakmp)# authentication pre-share
(config-isakmp)# group 1
(config-isakmp)# exit
(config)# crypto isakmp identity hostname
(config)# crypto isakmp key test address 192.168.1.1
(config)# crypto ipsec transform-set test esp-des
```

Cisco Router Challenge 57

Outline

This challenge involves setting up a crypto map and applying it to an interface.

Objectives

The objectives of this challenge are to:

- Define a Crypto access-list, to identify the traffic to encrypt.
- Define IKE.
- Define a crypto map.
- Bind the ACL with the crypto map.
- Apply crypto map to E0.

Example

```
> en
# config t
(config)# hostname newhampshire
(config)# access-list 109 permit ip 50.93.142.0 0.0.255.255
      136.163.130.0 0.0.255.255
(config)# crypto isakmp enable
(config)# crypto isakmp policy 111
(config-isakmp)# encryption des
(config-isakmp)# hash sha
(config-isakmp)# authentication pre-share
(config-isakmp)# group 1
(config-isakmp)# exit
(config)# crypto isakmp identity hostname
(config)# crypto isakmp key test address 192.168.1.1
(config)# crypto ipsec transform-set finland esp-des
(config)# crypto map manchester 10 ipsec-isakmp
(config-crypto-map)# match address 109
(config-crypto-map)# set peer 144.55.62.1
(config-crypto-map)# set transform-set finland
(config-crypto-map)# exit
(config)# int e0
(config-if)# ip address 192.168.1.1 255.255.255.0
(config-if)# no shut
(config-if)# crypto map manchester
```

Cisco Router Challenge 58

Outline

This challenge involves setting an access-list to allow IPSec.

Objectives

The objectives of this challenge are to:

- Create an access-list which allows AHP, ESP and ISAKMP.
- Applies the access-list.

Example

```
> en
# config t
(config)# hostname london

london (config)# access-list 101 permit ahp host 117.84.81.2 host
61.222.47.2

london (config)# access-list 101 permit esp host 117.84.81.2 host
61.222.47.2

london (config)# access-list 101 permit udp host 117.84.81.2 host
61.222.47.2 eq isakmp

london (config)# int e0
london (config-if)# ip address 136.22.25.1 255.252.0.0
london (config-if)# no shut
london (config-if)# ip access-group 101 in
```

Cisco Router Challenge 60

Outline

This challenge involves setting blocking SNMP.

Objectives

The objectives of this challenge are to:

- Define an access-list to block SNMP.
- Applies the access-list.
- Disable SNMP-server commands.

Example

```
> en
# config t
(config)# access-list 110 deny udp any any eq snmp
(config)# int e0
(config-if)# ip access-group 110 in
(config-if)# exit
(config)# service timestamps log datetime
(config)# service sequence-numbers
(config)# service dhcp
(config)# service finger
(config)# no service tcp-small-servers
(config)# no service udp-small-servers
(config)# service password-encryption
(config)# no snmp-server community annt RO
(config)# no snmp-server contact steven
(config)# no snmp-server location uk
(config)# no snmp-server host 78.113.70.11
(config)# no snmp-server enable traps
(config)# no snmp-server chassis-ID paris
```

Cisco Router Challenge 61

Outline

This challenge involves manually configuring RSA keys for peers.

Objectives

The objectives of this challenge are to:

- Define the public key for a given host.
- Specify the key.

Example

```
> en
# config t
(config)# crypto key pubkey-chain rsa
(config-pubkey-chain)# addressed-key 142.217.4.10
(config-pubkey-key)# key-string 01234567 01234567 01234567 01234567
(config-pubkey-key)# key-string 01234567 01234567 01234567 01234567
(config-pubkey-key)# key-string 01234567 01234567 01234567 01234567
(config-pubkey-key)# key-string 01234567 01234567 01234567 01234567
(config-pubkey-key)# key-string 01234567 01234567 01234567 01234567
(config-pubkey-key)# key-string 01234567 01234567 01234567 01234567
(config-pubkey-key)# key-string 01234567 01234567 01234567 0123
(config-pubkey-key)# exit
(config-pubkey-chain)# exit
(config)# exit
# show crypto key pubkey rsa
```

Cisco Router Challenge 62

Outline

This challenge involves the setup of authenticated routing protocols.

Objectives

The objectives of this challenge are to:

- Define EIGRP.
- Apply MD5 authentication on an interface.
- Define the authentication key chain.

Example

```
# config t
(config)# router eigrp 142
(config-router)# network 205.104.0.0
(config-router)# int s0
(config-if)# ip address 205.118.116.6 255.255.255.224
(config-if)# ip authentication mode eigrp 142 md5
(config-if)# ip authentication key-chain eigrp 142 ann
(config-if)# exit
(config)# key chain ann
(config-keychain)# key 1
(config-keychain-key)# key-string hotel
(config-keychain-key)# exit
```

Router Challenge 124: SSH Explained

Outline: This challenge involves an analysis of SSH.

Objectives: The objectives of this challenge are to explain SSH.

Explanation

The TELNET protocol is insecure as the text is passed as plain text. An improved method is to use SSH, which encrypts data. It requires that the domain-name and an RSA key pair:

```
ap# config t
Enter configuration commands, one per line. End with CNTL/Z.
ap(config)# ip domain-name test.com
ap(config)# crypto key generate rsa
How many bits in the modulus [512]:
% Generating 512 bit RSA keys ...[OK]
```

To view the public key:

```
ap#show crypto key mypubkey rsa
% Key pair was generated at: 00:42:19 UTC Mar 1 2002
Key name: ap.test.com
Usage: General Purpose Key
Key is not exportable.
Key Data:
 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00DDD8C6 4B744520
 F1499B01 49C485A2 20C9FB37 8CD11053 039D344B 3C5BD55E E84E17C8 FD62DA08
 32020F80 910AFBCC 6D402F90 96E8A59B 40467A3E 8FEED18B B1020301 0001
% Key pair was generated at: 00:42:21 UTC Mar 1 2002
```

```
Key name: ap.test.com.server
Usage: Encryption Key
Key is not exportable.
Key Data:
 307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00B435A4 C007251B
 312319CA 0E919F76 72D2D5A9 36B4710C CC4DE0C4 080D2B47 55970CA5 39F21170
 D07C0000 832F6A1C 81411423 BE52CBF4 ECBE417E 1C3C09D1 2BBC90DF 8DA398DB
 AE8EFA46 282AEC54 F0909F82 466A19DD EBEFAEDE 7B4B992F 5F020301 0001
```

An SSH client such as putty can then be used to connect to the access point:

... graphic missed out on version see help file.

after which the client shows the message:

... graphic missed out on version see help file.

and the SSH connection is made, such as:

... graphic missed out on version see help file.

To get rid of keys:

```
ap(config)# crypto key zero
```

and to set the timeout and authentication retries:

```
ap(config)# ip ssh time-out 60
ap(config)# ip ssh authentication-retries 2
```

which sets the timeout to 60 seconds, and a maximum of two retries. Finally, to prevent Telnet sessions:

```
ap(config)#line vty 0 4
ap(config-line)# transport input ssh
```

Cisco Router Challenge 128

Outline

This challenge involves configuring intercept.

Objectives

The objectives of this challenge are to:

- Define a host to intercept.
- Enable intercept

Example

```
> enable
# config t
(config)# access-list 150 tcp permit tcp any host 172.10.1.1
(config)# ip tcp intercept list 150
(config)# ip tcp intercept mode intercept
```

Cisco Router Challenge 125

Outline

This challenge involves defining protocols that should be inspected.

Objectives

The objectives of this challenge are to:

- Define the name of the inspection.
- Applied it on a port

Example

```
> enable
# config t
(config)# ip inspect ?
  L2-transparent  Transparent Mode commands
  alert-off       Disable alert
  audit-trail     Enable the logging of session information (addresses and
                 bytes)
  dns-timeout    Specify timeout for DNS
  hashtable-size Specify size of hashtable
  max-incomplete Specify maximum number of incomplete connections before
                 clamping
  name           Specify an inspection rule
  one-minute     Specify one-minute-sample watermarks for clamping
  tcp           Config timeout values for tcp connections
  udp           Config timeout values for udp flows
  <cr>
(config)# ip inspect name ?
  WORD Name of inspection defined
(config)# ip inspect name test ?
  cuseeme      CUSeeMe Protocol
  esmtp       Extended SMTP
```

```

fragment      IP fragment inspection
ftp           File Transfer Protocol
h323          H.323 Protocol (e.g, MS NetMeeting, Intel Video Phone)
http          HTTP Protocol
icmp          ICMP Protocol
netshow       Microsoft NetShow Protocol
rcmd          R commands (r-exec, r-login, r-sh)
realaudio     Real Audio Protocol
rpc           Remote Procedure Call Protocol
rtsp          Real Time Streaming Protocol
sip           SIP Protocol
skinny        Skinny Client Control Protocol
smtp          Simple Mail Transfer Protocol
sqlnet        SQL Net Protocol
streamworks   StreamWorks Protocol
tcp           Transmission Control Protocol
tftp          TFTP Protocol
udp           User Datagram Protocol
vdolive       VDOLive Protocol
(config)# ip inspect name test ftp
(config)# ip inspect name test h323
(config)# ip inspect name test http
(config)# int e0
(config-if)# ip inspect ?
WORD Name of inspection defined
(config-if)# ip inspect test in
(config-if)# int e1
(config-if)# ip inspect ?
WORD Name of inspection defined
(config-if)# ip inspect test out

```

Explanation

Inspection rules are used to define the traffic types and applications that are to be inspected. First the applications to be monitored are defined, such as:

```

(config)#ip inspect name BILLS ?
cuseeme       CUSeeMe Protocol
fragment      IP fragment inspection
ftp           File Transfer Protocol
h323          H.323 Protocol (e.g, MS NetMeeting, Intel Video Phone)
http          HTTP Protocol
netshow       Microsoft NetShow Protocol
rcmd          R commands (r-exec, r-login, r-sh)
realaudio     Real Audio Protocol
rpc           Remote Procedure Call Protocol
rtsp          Real Time Streaming Protocol
smtp          Simple Mail Transfer Protocol
sqlnet        SQL Net Protocol
streamworks   StreamWorks Protocol
tcp           Transmission Control Protocol
tftp          TFTP Protocol
udp           User Datagram Protocol
vdolive       VDOLive Protocol

```

such as for HTTP, FTP and TCP:

```

(config)# ip inspect name BILLS http

```

```

(config)# ip inspect name BILLS ftp
(config)# ip inspect name BILLS tcp
(config)# exit
#show ip inspect all
Session audit trail is disabled
Session alert is enabled
one-minute (sampling period) thresholds are [400:500] connections
max-incomplete sessions thresholds are [400:500]
max-incomplete tcp connections per host is 50. Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
Inspection Rule Configuration
Inspection name BILLS
  http alert is on audit-trail is off timeout 3600
  ftp alert is on audit-trail is off timeout 3600
  tcp alert is on audit-trail is off timeout 3600

```

Note that the name of the rule is case sensitive, such as:

```

#show ip inspect name bills
%Inspect name bills is not defined

# show ip inspect name BILLS
Inspection name BILLS
  http alert is on audit-trail is off timeout 3600
  ftp alert is on audit-trail is off timeout 3600
  tcp alert is on audit-trail is off timeout 3600
(config)# ip inspect audit-trail
Inspection name BILLS
  http alert is on audit-trail is on timeout 3600
  ftp alert is on audit-trail is on timeout 3600
  tcp alert is on audit-trail is on timeout 3600

```

1.1.1 Applying an Inspection Rule to an interface

CBACs are used along with ACLs, as the CBAC modifies the ACL in order that it operates correctly. An inspection rule is applied in a similar way to an ACL, such as:

```

(config)# access-list 101 permit ip 10.0.0.1 0.0.0.255 any
(config)# access-list 101 deny ip any any

(config)#int fa0
(config-if)#ip inspect ?
  WORD  Name of inspection defined

(config-if)#ip inspect BILLS ?
  in    Inbound inspection
  out   Outbound inspection

(config-if)#ip inspect BILLS in
(config-if)#ip access-group 101 in

```

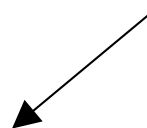
Notice no traffic is allowed on the incoming port. The CBAC fixes this.

and:

```

(config)# access-list 102 permit tcp any host 10.0.0.1 eq www
(config)# access-list 102 deny ip any any

```



```
(config)#int s0
(config-if)#ip access-group 102 in
```

which applies the BILLS inspection rule onto the FA0 interface for the incoming direction. Thus when a host on the network which connects to the FA0 interface initiates a connection with a remote Web server, the inspection rule kicks in and modifies ACL number 102, to allow the conversation between the hosts. If there was no inspection rule the reply would be blocked. If a host from outside the network (connected to S0) tries to connect to a node inside the network with it being first being initiated, its traffic would be blocked, as the CBAC will have no record of a connection.

To test a CBAC:

```
#sh ip inspect config
Session audit trail is enabled
Session alert is enabled
one-minute (sampling period) thresholds are [400:500] connections
max-incomplete sessions thresholds are [400:500]
max-incomplete tcp connections per host is 50. Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
Inspection Rule Configuration
Inspection name BILLS
  http alert is on audit-trail is on timeout 3600
  ftp alert is on audit-trail is on timeout 3600
  tcp alert is on audit-trail is on timeout 3600
```

and on the interface:

```
#sh ip inspect interface
Interface Configuration
Interface FastEthernet0
  Inbound inspection rule is BILLS
    http alert is on audit-trail is on timeout 3600
    ftp alert is on audit-trail is on timeout 3600
    tcp alert is on audit-trail is on timeout 3600
  Outgoing inspection rule is not set
  Inbound access list is 101
  Outgoing access list is not set
```

Cisco Router Challenge 126

Outline

This challenge involves defining protocols that should be inspected.

Objectives

The objectives of this challenge are to:

- Define minimum password lengths
- Define services.

Example

```

> en
# config t
(config)# security ?
    authentication  Authentication security CLIs
    passwords       Password security CLIs

(config)# security passwords ?
    min-length      Minimum length of passwords

(config)# security passwords min ?
    <0-16>          Minimum length of all user/enable passwords
(config)# service ?
    compress-config  Compress the configuration file
    config           TFTP load config files
    dhcp             Enable DHCP server and relay agent
    disable-ip-fast-frag  Disable IP particle-based fast fragmentation
    exec-callback    Enable exec callback
    exec-wait        Delay EXEC startup on noisy lines
    finger           Allow responses to finger requests
    hide-telnet-addresses  Hide destination addresses in telnet command
    linenumbers      enable line number banner for each exec
    nagle            Enable Nagle's congestion control algorithm
    old-slip-prompts Allow old scripts to operate with slip/ppp
    pad              Enable PAD commands
    password-encryption Encrypt system passwords
    prompt           Enable mode specific prompt
    pt-vty-logging   Log significant VTY-Async events
    sequence-numbers Stamp logger messages with a sequence number
    slave-log        Enable log capability of slave IPs
    tcp-keepalives-in  Generate keepalives on idle incoming network
                    connections
    tcp-keepalives-out  Generate keepalives on idle outgoing network
                    connections
    tcp-small-servers Enable small TCP servers (e.g., ECHO)
    telnet-zeroidle  Set TCP window 0 when connection is idle
    timestamps       Timestamp debug/log messages
    udp-small-servers Enable small UDP servers (e.g., ECHO)
(config)# service timestamps ?
    debug           Timestamp debug messages
    log             Timestamp log messages
    <cr>
(config)# service timestamps log ?
    datetime        Timestamp with date and time
    uptime          Timestamp with system uptime
    <cr>
(config)# service timestamps log datetime
(config)# sequence-numbers ?
    compress-config  Compress the configuration file
    config           TFTP load config files
    dhcp             Enable DHCP server and relay agent
    disable-ip-fast-frag  Disable IP particle-based fast fragmentation
    exec-callback    Enable exec callback
    exec-wait        Delay EXEC startup on noisy lines
    finger           Allow responses to finger requests
    hide-telnet-addresses  Hide destination addresses in telnet command
    linenumbers      enable line number banner for each exec

```

```

nagle                Enable Nagle's congestion control algorithm
old-slip-prompts     Allow old scripts to operate with slip/ppp
pad                  Enable PAD commands
password-encryption Encrypt system passwords
prompt              Enable mode specific prompt
pt-vty-logging       Log significant VTY-Async events
sequence-numbers     Stamp logger messages with a sequence number
slave-log            Enable log capability of slave IPs
tcp-keepalives-in    Generate keepalives on idle incoming network
                    connections
tcp-keepalives-out   Generate keepalives on idle outgoing network
                    connections
tcp-small-servers    Enable small TCP servers (e.g., ECHO)
telnet-zeroidle      Set TCP window 0 when connection is idle
timestamps           Timestamp debug/log messages
udp-small-servers    Enable small UDP servers (e.g., ECHO)
(config)# service sequence-numbers
(config)# service dhcp
(config)# service finger

(config)# no service tcp-small-servers
(config)# no service udp-small-servers
(config)# service password-encryption

```

Cisco Switch Challenge 48

Outline

This challenge involves enabling 802.1x authentication.

Objectives

The objectives of this challenge are to:

- Enable 802.1x.
- Define re-authentication.

Example

```

> en
# config t
(config)# int fa0/1
(config-if)# dot1x ?
  default                Configure Dot1x with default values for this port
  host-mode              Set the Host mode for 802.1x on this interface
  max-req                Max No.of Retries
  port-control            set the port-control value
  reauthentication       Enable or Disable Reauthentication for this port
  timeout                Various Timeouts

(config-if)# dot1x port-control ?
  auto                   PortState will be set to AUTO
  force-authorized       PortState set to Authorized

```

```

    force-unauthorized PortState will be set to Unauthorized
(config-if)# dot1x port-control auto
(config-if)# dot1x reauthentication ?
    <cr>
(config-if)# dot1x re-authentication

(config-if)# dot1x t ?
    quiet-period      QuietPeriod in Seconds
    reauth-period     Time after which an automatic re-authentication should be
                    initiated
    server-timeout    Timeout for Radius Retries
    supp-timeout      Timeout for Supplicant retries
    tx-period         Timeout for Supplicant Re-transmissions

(config-if)# dot1x t r ?
    <1-65535> Enter a value between 1 and 65535

(config-if)# dot1x timeout reauth-period 180

```

Cisco Switch Challenge 49

Outline

This challenge involves enabling port security and the BPDU guard (to defined against spanning-tree attacks).

Objectives

The objectives of this challenge are to:

- Enable BPDU guard.
- Enable port-security.
- Define a maximum number of MAC addresses on a port.
- Define a MAC address on a port.

Example

```

> en
# config t
Switch(config)# spanning-tree ?
    backbonefast  Enable BackboneFast Feature
    etherchannel  Spanning tree etherchannel specific configuration
    extend        Spanning Tree 802.1t extensions
    loopguard     Spanning tree loopguard options
    mode          Spanning tree operating mode
    mst           Multiple spanning tree configuration
    pathcost      Spanning tree pathcost options
    portfast      Spanning tree portfast options
    uplinkfast    Enable UplinkFast Feature

```

```

vlan                VLAN Switch Spanning Tree

Switch(config)# spanning-tree portfast ?
  bpdudfilter      Enable portfast bdpu filter on this switch
  bpduguard        Enable portfast bdpu guard on this switch
  default          Enable portfast by default on all access ports

Switch(config)# spanning-tree portfast bpduguard ?
  default          Enable bdpu guard by default on all portfast ports

Switch(config)# spanning-tree portfast bpduguard def ?
  <cr>

Switch(config)# spanning-tree portfast bpduguard def
Switch(config)# int fa0/1
Switch(config-if)# sw po ?
  aging            Port-security aging commands
  mac-address      Secure mac address
  maximum          Max secure addr
  violation        Security Violation Mode
  <cr>
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security max ?
  <1-5120>         Maximum addresses

Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# switchport port-security mac-address ?
  H.H.H           48 bit mac address
  sticky          Configure dynamic secure addresses as sticky
Switch(config-if)# switchport port-security mac-address 0000.1111.2222

```

Cisco Switch Challenge 50

Outline

This challenge involves defending against an attacker depleting the DHCP pool using DHCP snooping.

Objectives

The objectives of this challenge are to:

- Enable DHCP snooping.
- Apply DHCP snooping on an interface.

Example

```

> en
# config t
Switch(config)# ip dhcp ?
  conflict          DHCP address conflict parameters
  database          Configure DHCP database agents
  excluded-address  Prevent DHCP from assigning certain addresses
  limited-broadcast-address Use all 1's broadcast address
  ping             Specify ping parameters used by DHCP
  pool             Configure DHCP address pools
  relay            DHCP relay agent parameters
  smart-relay      Enable Smart Relay feature
  snooping         DHCP Snooping
Switch(config)# ip dhcp snooping ?
  information      DHCP Snooping information
  vlan            DHCP Snooping vlan
  <cr>
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan ?
  <1-4094>         DHCP Snooping vlan first number
Switch(config)# ip dhcp snooping vlan 4
Switch(config)# int fa0/1
Switch(config-if)# ip dhcp ?
  snooping        DHCP Snooping
Switch(config-if)# ip dhcp snooping ?
  limit           DHCP Snooping limit
  trust          DHCP Snooping trust config
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)# ip dhcp snooping limit ?
  rate           DHCP Snooping limit

Switch(config-if)# ip dhcp snooping limte rate ?
  <1-4294967294> DHCP snooping rate limit
Switch(config-if)# ip dhcp snooping limte rate 30

```