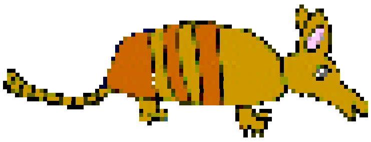
Hardening WiZCo Routers

1 Introduction – the crunchy Armadillo theory

The practices of Crunchy Armadillo theory have been familiar to me for many years. However, it was only in the last year or so that a mate of mine (Kevin Younger) has re-counted them to me with this charming twist.



The theory of the Crunchy Armadillo states that Security of a device should be crunchy on the outside and chewy in the middle.

This raises at least a couple of questions in my mind. The most urgent of these is, Is Kev’s cheery disposition down to his Armadillo munching . The second revolves around the exact internal nature of Armadillos, but I believe I’ll take his word for it that Armadillo are soft and chewy in the muddle.

The theory has a very serious point though – that a security regime is most economically applied at a perimeter. This is borne-out through history by Walled-Cities, forts and now firewalls. It is also applicable to computer hosts or advanced peripherals like routers. To prove the point how often have you heard hackers say “once the have an account on a machine, they **OWN** it”. Fortunately, there are precious few accounts on a Cisco device so our task is easy.

There are three stages to our Crunchy Armadillo theory :

1) Disable unnecessary network services and settings
2) Secure other system settings.
3) Enhance accounts and access-lists

This should result in an environment suitable for most secure conditions – the Crunchy Armadillo. For that extra secure device, we provide an extra stage -***the crushed Armadillo***

1.1 Learning by example

To demonstrate the changes, we will use this config taken from an IOS 11 router.

```
bert#show startup-config
hostname bert
enable password cisco
interface Serial0/0
ip address 81.2.94.82 255.255.255.252
interface FastEthernet1/0
ip address 81.2.94.88 255.255.255.252
ip route 0.0.0.0 0.0.0.0 81.2.94.83
snmp-server community public RO
snmp-server community private RW
line con 0
line aux 0
line vty 0 4
 password cisco
 login
!
```

2 The Quickening - or the hardening

2.1 Remove unnecessary network services and setting

2.1.1 Disabled small-services.

Small-services are basic services like *Discard, Chargen, and Echo* and are not required for success-full operations of a router. They can, however, be used in disruption of services attacks (try linking chargen to echo with Netcat or Arny to see the effect on device cpu).

```
no service udp-small-servers

no service tcp-small-servers
```

2.1.2 Disabled Cisco discover protocol.

Cisco discover protocol can disclose details of the operations of a router. To disable CDP on an interface basis use:

```
no cdp enable
```

Or on per router basis use:

```
no cdp run
```

2.1.3 Disable IP unreachables

If a router returns ICMP messages when a host is unreachable or blocked by accesses lists, it facilitates *firewalking* (I.e. the guessing of the access-list configuration) and the presence of machines.

```
no ip unreachables
```

2.1.4 Disable IP source routing.

The risk of source routing is over rated but allowing it through the perimeter router is tempting providence so treat it as dangerous.   Assume the stories are true and it could make impersonation attacks easier.

```
no ip source route
```

2.1.5 Disable IP directed-broadcast.

Disable this to reduce the risk of broadcast based flooding attacks (i.e. smurf) Prevent a subnet-specific broadcast with the directed-broadcast command. This prevents the flow of packets with the host portion of the destination address that are set to high values.

```
no IP directed-broadcast
```

2.1.6 Disabled IP redirects

The routers routing tables in theory can be subverted by ICMP redirect messages produced by a programme such as Nuke or Nuke2

```
no ip redirects
```

2.1.7 Disable SNMP:

SNMP is a powerful UDP based service that can change the configuration or shutdown the router. SNMP v2 or v3 are very much more secure than SNMP v1 which uses simple passwords (alright community strings). However many system management utilities only support SNMP v1.

To disable snmp.

```
no snmp-server
```

2.2 Secure other system settings

2.2.1 Use service password-encryption.

Prevents you displaying clear text passwords when you list the startup-config.

```
service password-encryption
```

2.2.2 Use enable secret in preference to enable *password.*

Enable secret uses a stronger algorithm than enable password.

```
enable secret
```

2.2.3 Disable the finger service

Finger discloses usage information to all and sundry.

```
no service finger
```

2.2.4 Harden SNMP v1

If you cant disable SNMP v1 ensure it is secured with access control list Use an

- Obscure read community string;
- Obscure write community string;
- access control list or access policy.

2.2.5 Disable http admin server

Ensure that web based admin is disabled by:

```
no ip http server
```

2.2.6 login Banner

It is good practice to have a login banner that discourages unauthorised access:

```
Banner login   £   Access is prohibited £
```

2.2.7 Disable other services

```
no ip mroute-cache

no ip proxy-arp
```

2.3 Enhance accounts and access-lists

2.3.1 Define an anti-spoof filter.

Spoof filters prevent a packet from an external network generating a packet that masquerades/appears as originating from an internal device

2.3.2 Private plus restricted address filter

This should include

```
access-list 102 deny ip 10.0.0.0     0. 255 . 255 .255 any log
access-list 102 deny ip 127.0.0.0     0. 255 . 255 .255 any  log
access-list 102 deny ip 224.0.0.0     0. 255 . 255 .255 any  log
access-list 102 deny ip 192.168.0.0     0. 0 . 255 .255 any  log
access-list 102 deny ip 172.16.0.0     0. 15. 255 .255 any  log
```

2.3.3 Define an egress filters.

Egress filters prevents any address leaving your network with an address other than those that are legitimate for your network. To do this, disallow any traffic with a source not on your internal network.

2.3.4 Define all other traffic filters.

Perimeter routers are the first line of defense. They should mirror the policy installed on the firewall otherwise it exposes this more complex device to all manner of attacks.

2.3.5 Define a logging host and level

```
logging trap errors
logging syslog-address
```

2.3.6 Apply passwords to the console and any VTY devices.

Access to the router must be controlled by passwords using the password command

2.3.7 Define timeout on VTY devices

```
exec-timeout 5 0
```

2.3.8 Define an access-list on VTY devices

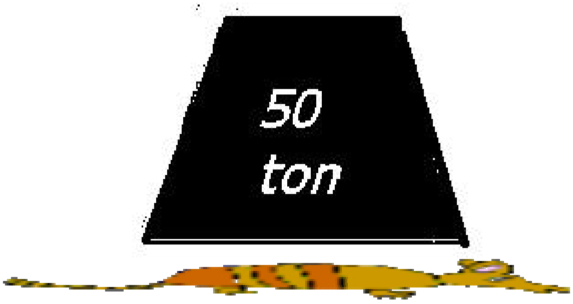
```
access-class 1 in
```

2.3.9 Example post- hardening

```
bert#show startup-config
hostname bert
!
no service finger

service password-encryption
!
no service udp-small-servers
no service tcp-small-servers
!
!
enable secret 5 $1$s1gN$TDLK8LhaSdgKlDUpR84OY1
enable password notused
!
no cdp run
no ip redirects
no ip unreachables
no ip http server

interface Serial0/0
 ip address 81.2.94.82 255.255.255.252
 ip access-group 102 in
 no ip directed-broadcast
 no ip source route
 no ip mroute-cache
 no ip proxy-arp
!
Banner login   £  Access is prohibited £
!
logging trap errors
logging 81.2.94.81

interface FastEthernet1/0
ip address 81.2.94.88 255.255.255.252
! ip access-group 103 in
! !
! We own addresses 82.2.94.0/24
! we also have a NOC at  193.193.97.65
! Management control
access-list 1 permit 193.193.97.65 0.0.0.252
access-list 1 permit 82.2.94.0 0.0.0.255
!
! Spoof filter
access-list 102 deny ip 81.2.94.0   0.0.0.255 any
! rfc 1918 filter
access-list 102 deny ip 10.0.0.0     0. 255 . 255 .255 any log
access-list 102 deny ip 127.0.0.0     0. 255 . 255 .255 any  log
access-list 102 deny ip 224.0.0.0     0. 255 . 255 .255 any  log
access-list 102 deny ip 192.168.0.0     0. 0 . 255 .255 any  log
access-list 102 deny ip 172.16.0.0     0. 15. 255 .255 any  log

!
! Traffic filter
access-list 102 permit tcp any host 81.2.94.89 eq www
access-list 102 permit tcp any host 81.2.94.88 eq smtp
access-list 102 permit tcp any host 81.2.94.90 eq ftp
!  explicit deny
access-list 103 deny ip any any
!
! Egress rules
access-list 103 permit ip 81.2.94.0   0.0.0.255 any
access-list 103 deny ip any any
snmp-server community x1xx  RO    1
snmp-server community x1xx  RW   1
line con 0
 password GMxQ4p98
 login
line aux 0
line vty 0 4
 access-class 1 in
 password Tm7gR3s
 login
```

2.4 Hardening still further – Crushed Armadillo

For those devices that need a little more control



2.4.1 Set up read-only accounts for general access & auditing

Set up an account that allows auditors to read configuration and stats.

```
privilege exec level 14  show startup-config
privilege exec level 14  show running-config

username auditor privilege 14  password 0 killemall
```

2.4.2 Only allow access by ssh

Set up ssh on the router.

Define a user

```
username user1 password 0 sad
```

Define an ssh key

```
Crypto key generate rsa
```

Set up any ssh parms

```
Ip ssh time-out
```

Make ssh the transport on vty, from example above change

```
line vty 0 4
 access-class 1 in
 password Tm7gR3s
 login
```

TO

```
 line vty 0 4
 access-class 1 in
 login local
transport  input ssh
```