Device & Infrastructure Security

Network Security Workshop

Issue Date: 30 May 2015
Revision: 2.0-draft

APNIC

Overview

- Server Hardening
- Logging and Monitoring
- Backup and Recovery
- L2 Device (Switch) Security
- L3 Device (Router) Security
- Bogons

Server Hardening

- Use netstat to check which ports you are currently listening on your Linux machine.
  - Close unnecessary ports
- Remove unused applications. Minimal software means less possible vulnerabilities
- Perform regular software patches and update.
- Disable unwanted services and remove from startup items
- Use TCP wrappers and properly configure hosts.allow and hosts.deny files.
- **Rule of thumb:** *deny all, allow as necessary*

Server Hardening - Accounts

- Disable default accounts and groups that are not needed
- Use strong authentication
- Good password policy
  - Minimum number of characters
  - Combination of alphabets, numbers, special characters, upper and lower case
  - Implement password aging
  - Force users to change password on first login
  - Prevent use of previous passwords
- Lock account after a number of failed logins

Backup and Recovery

- A backup system is a fundamental element of any disaster recovery plan
- Provides for disaster recovery of key network services and any file
- Physical vs Logical backup
  - Physical backup – create copy of the files into some other location, such as disks or tapes
  - Logical backup – remote, cloud services

Backup and Recovery

- Type of Backup
  - Full backup – entire dataset regardless whether it has been altered or not; take longer
  - Incremental backups – only backs up data that has been changed since last backup
  - Differential backups – backups data that has changed since the last full backup
  - Copy backups – full backups without a reset of archive bits
- Backup intervals
  - Daily incremental
- Backup media
  - Offline backups: Magnetic Tapes, Optical drives, Hard disk
  - Offsite backups: Network, NAS, Data center

Backup and Recovery

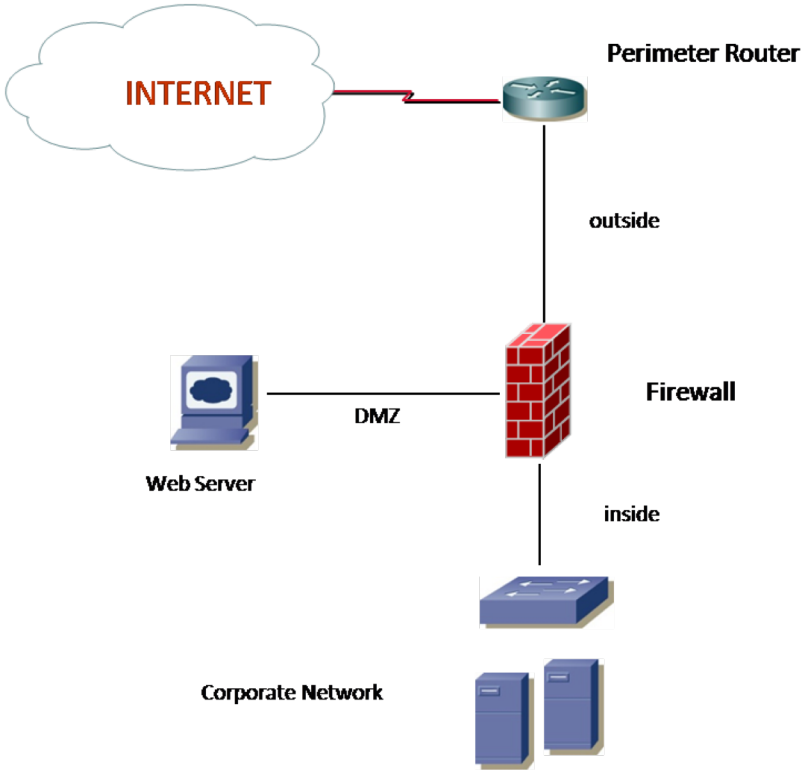
- Always test that your backups are restorable
- Restoration should be within a reasonable period of time
  - time to recover
  - Priority of some files over others

Logging

- All security-related events must be logged
- Audits must be performed on a regular basis
- In a Linux system:
  - monitor log messages using `logwatch`
  - Perform system accounting using `auditd`

Network Devices

- Attack areas:
  - Default passwords
  - Broadcasting packets replicated on all ports
  - rogue devices participate in STP and mislead it
  - packet flooding using spoofed MAC addresses
  - Gaining management access



Network Devices

- Change the default settings
- Allow management sessions only from approved sources
- Use AAA server to authenticate administrators, authorize their actions and perform accounting of all actions
- Encrypt sessions
- Limit device access
  - Console sessions should also be authenticated
- Admin actions should be authorized through a AAA server
- Disable password recovery

Increasing Port Security

- CAM entry aging
- Static or permanent CAM entries
- Limit MAC addresses per port
- Disable unused port
- Port authentication with IEEE 802.1X

Mitigation of ARP Spoofing

- Static ARP entries
- Secure ARP inspection
  - Secure ARP Discovery (SAD)
- Separate VLANs with unique IP subnets
- Private VLAN
- IEEE 802.1X port authentication

Port Authentication using 802.1X

- 802.1X is an IEEE standard defining layer 2 protocol used for authentication purposes
- 3 authentication protocols
  - EAP-MD5 (challenge response auth protocol)
  - EAP-OTP (proprietary one-time password)
  - EAP-TLS (using digital certificates)

Spanning Tree Protocol

- Used to prevent loops in a switched LAN by disabling redundant links (IEEE 802.1D)
- STP takes 30-50 seconds to converge
- Misplacement of the root bridge can cause suboptimal paths
- Loss of the root bridge has the most effect on performance
- STP does not include any security by default

Trunking

- Allows multiple VLANs to be carried over one physical link. This may expose the whole network to a single port if not configured properly.
- An intruder can also interfere with VTP messages and cause VLANs to disappear
- Must disable trunking on a port

VLAN Trunking Protocol (VTP)

- used to make VLAN management easier in large switched LAN environments
- VTP should use authentication to prevent unauthorised devices from participating in VTP
- VTP can use MD5 to authenticate VTP messages
- The same password has to be used on all devices in a VTP domain
- Replay attacks are not possible

VLAN/Trunking Best Practices

- Always use a dedicated VLAN ID for all trunk ports
- Disable unused ports and put them in an unused vlan
- Do not use VLAN 1 for anything
- Disable auto-trunking on user facing ports (DTP off)
- Explicitly configure trunking on infrastructure ports
- Use all tagged mode for the native VLAN on trunks
- Use PC Voice VLAN access on phones that support it
- Use 802.1q tag on all the trunk ports

VLAN 1

- A special VLAN used as a default vlan assigned to L2 device ports.
- Generic rule: “network administrators should pruse any VLAN, and in particular VLAN 1, from all theports where that VLAN is not strictly needed”

Network Devices: Routers

- Use strong authentication
- Disable unused services
- Modify insecure default settings
- Authenticate IGP messages
- Check software versions for security-related bugs

Network Hardening (Layer 3)

- Interior gateway protocol (IGP) - exchange routing information between routers inside the network
  - OSPF, EIGRP, RIPv2, IS-IS
- Exterior Gateway Protocol (EGP) - exchange routes with Internet Service Providers (ISPs)
  - BGP

Threats to Routing Protocols

- Deliberate exposure – attacker takes control of a router and intentionally releases routing information to other entities
- Sniffing – attackers monitor and/or record the routing exchanges between authorized routers to sniff for routing information
- Traffic analysis – attackers gain routing information by analyzing the characteristics of the data traffic on a subverted link
- Spoofing – illegitimate device assumes the identity of a legitimate one.
- Falsification – attacker sends false routing information
- Interference – attacker inhibits the exchanges by legitimate routers
- Overload – attackers place excess burden on legitimate routers

RFC 4593

Securing Routing Protocols

- an authentication mechanism should be used to prevent accidental or deliberate adjacencies from being established
  - password system should be secret and changed regularly
- authenticate routing updates
- security only verifies the source of the information
  - no encryption of the routing update contents
  - any packet interception will allow read-access

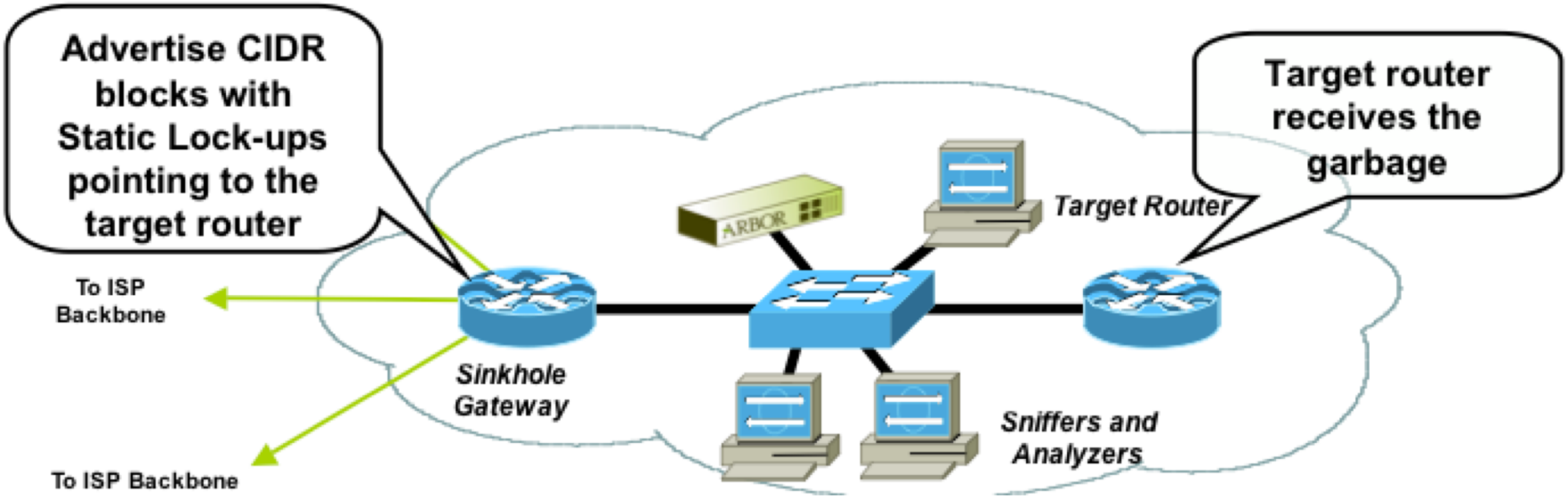
BGP Security (BGPsec)

- Extension to BGP that provides improved security for BGP routing
- Currently an IETF Internet draft
- Implemented via a new optional non-transitive BGP path attribute that contains a digital signature
- BGP Prefix Origin Validation (using RPKI)
- BGP Path Validation

BGP Security

- **Real-time Blackhole Routing (RTBH)**
  - Packets are forwarded to a router's bit bucket – either a null interface or a discard interface)
  - desired packets are dropped with minimal or no performance impact
  - Employing uRPF in conjunction with RTBH can provide source-based solution vs destination-based
- **BGP Diversion**
  - Uses BGP to divert traffic to sinkholes or any packet "scrubbing" centers for further analysis
  - Divert via resetting BGP next hop to ip address of analysis system(s) or matching community tags that result in different BGP next hops being assigned for a given prefix
- **BGP Route Tagging**
  - Tag routes using BGP communities to apply filtering, rate limiting, QoS, firewall, or any other policy on packets

Sinkholes


Advertise CIDR blocks with Static Lock-ups pointing to the target router
Target router receives the garbage
ARBOR
Target Router
To ISP Backbone
Sinkhole Gateway
Sniffers and Analyzers
To ISP Backbone

Cisco IOS Features

- **Control Plane Policing**
  - allows users to configure a QoS filter that manages the traffic flow of control plane packets to protect the control plane of Cisco IOS routers and switches against reconnaissance and denial-of-service (DoS) attacks
  - Control plane can help maintain packet forwarding despite an attack or heavy traffic load
- **Unicast RPF**
  - limits malicious traffic by enabling a router to verify the reachability of the source address in packets being forwarded.

Bogons

- Bogons – Martians and netblocks that have not been allocated to an RIR by IANA.
- Fullbogons – a larger set which also includes IP space that has been allocated to an RIR, but not assigned by that RIR to an actual ISP or other end-users.

Reference: http://www.team-cymru.org/Services/Bogons/bgp.html

Bogons (BGP)

```
Cisco Router Traditional bogons
router bgp <your asn>
  neighbor x.x.x.x remote-as 65333
  neighbor x.x.x.x ebgp-multihop 255
  neighbor x.x.x.x description <your description>
  neighbor x.x.x.x prefix-list cymru-out out
  neighbor x.x.x.x route-map CYMRUBOGONS in
  neighbor x.x.x.x password <your password>
  neighbor x.x.x.x maximum-prefix 100 threshold
90
```

Reference: http://www.team-cymru.org/Services/Bogons/bgp.html

Bogons (BGP)

```
! Remember to configure your Cisco router to handle the new style
! community syntax.
ip bgp-community new-format
!
! Set a bogon next-hop on all routers that receive the bogons.
ip route 192.0.2.1 255.255.255.255 null0
!
! Configure a community list to accept the bogon prefixes into the
! route-map.
ip community-list 10 permit 65333:888
!
! Configure the route-map.  Remember to apply it to the proper
! peering sessions.
route-map CYMRUBOGONS permit 10
  description Filter bogons learned from cymru.com bogon route-servers
  match community 10
  set ip next-hop 192.0.2.1
!
ip prefix-list cymru-out seq 5 deny 0.0.0.0/0 le 32
```

Bogons (BGP Peer-Group)

```
router bgp <your asn>
  neighbor cymru-bogon peer-group
  neighbor cymru-bogon ebgp-multihop 255
  neighbor cymru-bogon description <general description>
  neighbor cymru-bogon prefix-list cymru-out out
  neighbor cymru-bogon route-map CYMRUBOGONS in
  neighbor cymru-bogon maximum-prefix 100 threshold 90
! You'll need to increase the maximum to at least 50000 with
an
! appropriate thresholds if you're receiving one or both
fullbogons
! feeds.
!
  neighbor x.x.x.x remote-as 65333
  neighbor x.x.x.x peer-group cymru-bogon
  neighbor x.x.x.x description <specific description>
  neighbor x.x.x.x password <your password>
```

RFC2827 (BCP38) – Ingress Filtering

- If an ISP is aggregating routing announcements for multiple downstream networks, strict traffic filtering should be used to prohibit traffic which claims to have originated from outside of these aggregated announcements.
- The ONLY valid source IP address for packets originating from a customer network is the one assigned by the ISP (whether statically or dynamically assigned).
- An edge router could check every packet on ingress to ensure the user is not spoofing the source address on the packets which he is originating.

Guideline for BCP38

- Networks connecting to the Internet
  - Must use inbound and outbound packet filters to protect network
- Configuration example
  - Outbound—only allow my network source addresses out
  - Inbound—only allow specific ports to specific destinations in
- Use the following techniques
  - Static ACLs on the edge of the network
  - Unicast RPF strict mode
  - IP source guard

BCP 140 – RFC5358

- Prevents use of recursive nameservers in Reflector Attacks
- http://tools.ietf.org/html/bcp140
- Recommendations
  - Disable recursive service when not necessary
  - Implementing client authorization
- Accept queries from customers only – client authorization

```
aclmy-net  {       192.0.2.0/24;  2001:db8::/32; };
options    {       recursion      yes;
           allow-query    {       my-net; };      };
```

Questions

THANK YOU

www.facebook.com/APNIC

www.twitter.com/apnic

www.youtube.com/apnicmultimedia

www.flickr.com/apnic

www.weibo.com/APNICrir

APNIC