ISP and NSP Security Workshop

APRICOT 2013

Day 5

In conclusion

- You've spent five days listening to us talk
- And you've configured and played in the lab some of what we've talked about

- You should be feeling comfortable about going back to your job and using what you've learned

Some Simple Best Practices

- Always null route unused address space within your network
  - If you have prefixes you know are unused, route them towards null0 on your routers.
  - Prevents ARP cache exhaustion, broadcasts, and prevents address theft
- Enable port security and limit the number of MACs on customer ports
- Always filter ingress traffic from customers with uRPF or ACLs (source address validation)
- Authenticate all of your network protocols
- Filter BGP sessions ingress and egress
  - Make sure you don't accept prefixes you don't want or shouldn't carry
- Set maximum-prefix/prefix-limit on BGP sessions (including customers, transits, and peers)
- Never use OSPF as a CE-PE protocol

Some Simple Best Practices

- Give high priority to network control traffic
- Ideally, have an out-of-band management path to all POPs.
- Restrict DHCP and Router Advertisements on customer ports
- Separate customers into separate VLANs if you can
- Use local-proxy-arp and private VLANs to restrict device-to-device communications
- Use an anomaly detection system – even if it's just netflow and a suspicious eye!
- Use RANCID or similar to monitor configuration changes on network elements.
- Ensure you are logging to central locations via syslog / SNMP traps.
- Monitor critical network element resources, e.g. memory, bandwidth utilisation, interface utilisation, RIB/FIB utilisation, CAM utilisation…

Some Simple Best Practices

- **ALWAYS ENCRYPT YOUR MANAGEMENT TRAFFIC!**
  - Avoid the use of clear text as much as possible.
  - Limit clear text traffic to the shortest and most trusted path possible.
- Make use of jump or bastion hosts and ACLs to restrict management traffic to these hosts.
- **Have a security plan** that includes incident management processes
  - Identify who, what, and how
  - Practice and test the plan
  - Make sure you know how to reach your peers and transit providers, and how their security plans work!
- Join security working groups such as NSP-SEC.
- Keep an eye on mailing lists like NANOG, PacNOG, APOPS, Bugtraq, Full-Disclosure.

Some Simple Best Practices

- Use least-privileged mode where possible
  - If you're logging in to check interface stats, you probably don't need superuser mode.
  - Define profiles for staff that restrict them to the appropriate privilege level.
- Keep on top of OS releases for your network elements, particularly if security patches are released.
  - ACLs and Control Plane Policing can mitigate this, to an extent.
- When implementing IPv6, be careful and ensure that your ACLs, filters, CoPP, etc incorporate the fact that all protocols will start listening on the IPv6 addresses.
- Don't block all ICMP – there are some really important parts of it.
  - Question: What can break when ICMP is blanket-blocked?

Some security references

- ITU X.805
- ISO 15408 Common Criteria
- ISO/IEC 27001
- Team Cymru – http://cymru.org

- An interesting look at leaky ISPs at IXPs – Monkeying Around on the APE
  - http://www.apricot.net/apricot2010/__data/assets/pdf_file/0006/18915/IXPs_02_Monkeying-around-on-the-APE_Mike-Jager.pdf

- Feel free to ask the instructors or contact us!

Some tools we used this week…

- tcpdump – http://www.tcpdump.org
- Wireshark – http://www.wireshark.org
- Cacti – http://www.cacti.net
- Scrutinizer (Netflow tool) - http://www.plixer.com
- Perl Net::RawIP tools for generating attack traffic
- Ettercap – http://ettercap.sourceforge.net
- Yersenia – http://yersinia.net
- nmap – http://nmap.org
- Good old **ping** - on a unix host near you
- Nessus – http://nessus.org

Final exam Pg 1/73

1. Write a one page essay detailing the techniques you have learned during the workshop
2. What is a prefix hijack?
3. What is BCP38?
4. What is OOB?
5. What can you use SNMP for?
6. Where should you use prefix-lists?

Final exam Pg 2/73

7. When would you use telnet to manage devices?
8. What's the first thing to do with usernames and passwords on new equipment?
9. Why is it important to have NTP configured?
10. Is SYSLOG clear text or encrypted?
11. Why is [10] important?
12. Why should you use maximum-prefix/prefix-limit on BGP sessions?
13. What does Daniel's t-shirt today mean?

Final exam Pg 3/73

14. What filters should you use on EBGP sessions? (3 answers)
15. What interfaces should your IGP never run on?
16. What's a bogon?
17. Can we have your SSH private keys?
18. What's the advantages of RTBH over ACLs or filters?
19. What's the difference between strict and loose RPF?

Final exam Pg 4/73

20. Who is the best dressed instructor this week?
21. Does MPLS secure customer traffic?
22. Name three network telemetry tools
23. What's a flow?
24. What should an Infrastructure ACL protect?
25. What type of hats do attackers wear?
26. What does ARP do? Bonus point: what replaces ARP in IPv6?

Final exam

27. What does CIA stand for?
28. Would RTBH work in a L3VPN?
29. Is spanning-tree a good idea?
30. Is your lab pod secure?
31. What's DynaMIPS?

32. Who's had a good time this week?