Pen-Testing the Backbone

Raven, NMRC
raven@nmrc.org
White box, black box?

- Black box testing is good for external recon and data gathering.
- However, it's far more difficult and likely to be destructive in implementation.
- Many or most backbone vulnerabilities are denial-of-service oriented.
- Since people get unhappy when you break their ISP, white-box testing is preferred.
Initial Reconnaissance

- Choose your target – search the registars for their address blocks, allocated autonomous systems, and other data. (Contacts if not role account, etc.)

- Look on route servers and Internet maps to try to determine their peering.

- Throw everything you get into Google, recurse when necessary to build a profile of the network.

- Check mailing list archives for likely config details and public peering points.
Vendor-specific details

- Each vendor has their own advisory and vulnerability disclosure practices. Become familiar with these for each vendor on your target network.
- Acquire CCO, Juniper, etc. site logins when necessary to supplement vulnerability information.
- Don't forget the switches – this should go for all your network gear.
Code train vulnerabilities

- Check the vulnerabilities specific to each code train implemented in your network.
- Also check vulnerabilities in stacks/implementations that your current code train is derived from. BSD stack vulnerabilities are worth checking for Cisco IOS and JunOS boxes, for example.
- Some scanners incorporate these checks, but many may need to be done by hand. Beware of unintentional DoS while scanning.
Failure paths and trust relationships

- Architectural review – check for redundancy, network robustness, and security.
- Do your authentication means have redundancy? Fallback? What is the weakest form of authentication one can force?
- Once authenticated, is trust transitive? Can one log in directly from one backbone router to another? Are source IP addresses restricted?
- Is there a single point of transit or authentication failure? What happens when it fails?
Failure and Trust II

- If there is centralized authentication, how many servers are there? Are they hardened?
- Are authentication credentials sent cleartext?
- Where can you access the authentication server from? Often it's whitelisted in ACLs, so once owned, it's a free ticket into the infrastructure.
- Can one set up a MitM attack against the authentication server to harvest credentials?
ObSlide – Physical Security

- Make sure all data centers and peering points have good physical security.
- Test this. Repeatedly. Often.
- Many of these attacks are only possible with local injection or access. Make sure that doesn't happen.
- Good physical security is half the game.
Data Leaks

- Check for data leaks at the network border – connect to the switch and fire up a sniffer. This is particularly valuable at an exchange point with a port in promiscuous mode.
  - Cisco Discovery Protocol
  - Routing protocol information
  - Leaked switching data
Protocol injection – speak my route?

- If you can see the data, you can spoof the data.
- Fake a routing announcement and inject it. See if it gets picked up.
- For cheapass DoS, tear down links with spoofed packets. (Almost no clients want this level of testing.)
- Many routing protocols are unauthenticated. This is insecure.
Rogue router

- Connecting a new router to many data centers is easier than you'd think.
- Plug in to the exchanging switch.
- Depending on what data is being advertised, try to speak their routing protocols with a similar configuration.
- Depending on your contract with the client, you may even be able to replace their router with one of your own.
Pwn3d router

- If you have been able to get authentication credentials, or force a login (cisco/cisco, admin/company name, etc.), router hijack is possible.
- Traffic redirection into a tunnel of your choice is possible.
- You may be able to advertise additional netblocks in a preferred fashion without authorization, affecting routing for the whole network.
Netblock hijack

- It is also possible to announce and route other peoples' netblocks without authorization, if you can convince your upstream to take the route.

- This has happened – spammers stole a legitimately owned large netblock, announced it through their ISP, spammed for about a week, and disconnected. This left the original owners nullrouted for a week, blacklisted everywhere, and with a huge mob of angry people at their door.
Configuration Review

- Check the configurations of your client against:
  - Secure BGP Template
    http://www.cymru.com/Documents/secure-bgp-template.html
  - Secure IOS Template
    http://www.cymru.com/Documents/secure-ios-template.html
  - Secure JunOS Template
  - Secure JunOS BGP Template
Peering Security

- Check the peering configuration of your target network.
- Data may be advertised from route servers.
- Ensure that authentication is in place for peering changes.
- Ensure that machines which are used for network policy are well secured.
Thank you

- Feel free to contact me regarding this talk, or with feedback or additional ideas, at raven@nmrc.org