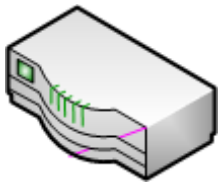
Remote rootshell on a SOHO class router

Confidence 2009
Krakow 15.05.2009r.

Michal Sajdak



Summary

- Network appliances
- Common flaws in SOHO http servers / web management software
- Live presentation – Asmax & Linksys
- GoAhead http server issues – live presentation
- What's next?

Network appliances

- Standard software
  - Linux/*BSD
  - Bunch of Open Source Software
- Web based administration – it's so sexy!
  (is it?)
- Hardware
  - x86, ARM, MIPS, …

Network appliances

- How to build a custom network appliance?
  - Download linux/*BSD
  - Get some hardware
  - Install functionally stripped OS on the hardware
  - Multiplicate, market & sell
  - ;-)

Network appliances

- Why? A LOT of functionality is already:
  - Developed
  - Tested
  - Supported
  - Free
  - (in)Secure
- Web based administration – it's so sexy!
  (is it?)

Network appliances

- ASA 8.0 (Adaptive Security Appliance - Cisco)
  - Pix OS 8.0 uses Linux…and a lot of Open Source
  - Full list of OS licenses: http://www.cisco.com/en/US/docs/security/asa/asa80/license/opensrce.html
  - x86 architecture
  - Web based administration ;-)

Network appliances – today.

Open Source Software Licenses for ASA and PIX Security Appliances, 8.0

- Apache License
- Artistic License
- ASN1C, v.0.9.18 License
- BSD 1.0 License
- BSD Gettext License
- Curl License
- CYRUS SASL 2.1.21 License
- expat License
- FreeBSD 6.0-Release
- Genhash (ipcad, v. 3.6.6) License
- GNU Free Documentation License
- The GNU General Public License (GPL)
- GNU LESSER GENERAL PUBLIC LICENSE
- HSQLDB License
- iconv 2.0 License
- ICU Licens
- J2RE Standard Edition License
- libjs Mozilla License
- libtecla License
- libxml2 License
- Linux 2.6 License
- Linux-PAM License
- LZMA SDK License
- LUA License
- …

Network appliances – what's new?

- It can all be attacked – using known methods
- Example
  - Analyzing Complex Systems The BlackBerry Case
  - Attacking Blackberry Enterprise Server (via old, buggy Open Source libraries).
  - http://www.blackhat.com/presentations/bh-europe-06/bh-eu-06-fx.pdf

Moving to SOHO routers

- pdp showed some nice techniques
  - http://www.gnucitizen.org/blog/router-hacking-challenge/
- I focused on web management software

Common flaws in SOHO http servers / web management software

- HTTP server
  - Using old, buggy http servers
  - These servers seem to be just buggy…
  - Bugs are publicly available (eg. in changelogs)

Common flaws in SOHO http servers / web management software

- Web software
  - Using old cgi-style programming
    - Not to reveal source code ?
    - Not to install resource intensive scripting language (like php / python) ?
  - Maintenance scripts/mechanisms
  - Vulnerable to classic attack techniques based on passing malicious input

Common flaws in SOHO http servers / web management software

- Configuration flaws
  - Authentication / Authorization checks
  - No http server hardening
  - http server runs at root (of course)
  - No chrooting / other OS hardening

Common flaws in SOHO http servers / web management software

- „Business” issues
  - Security = unnecessary cost
  - Baseline versions of http server / web software are buggy
  - Vendors add custom bugs
  - Network people seem to misunderstand application issues (and software people seem to misunderstand network issues…)

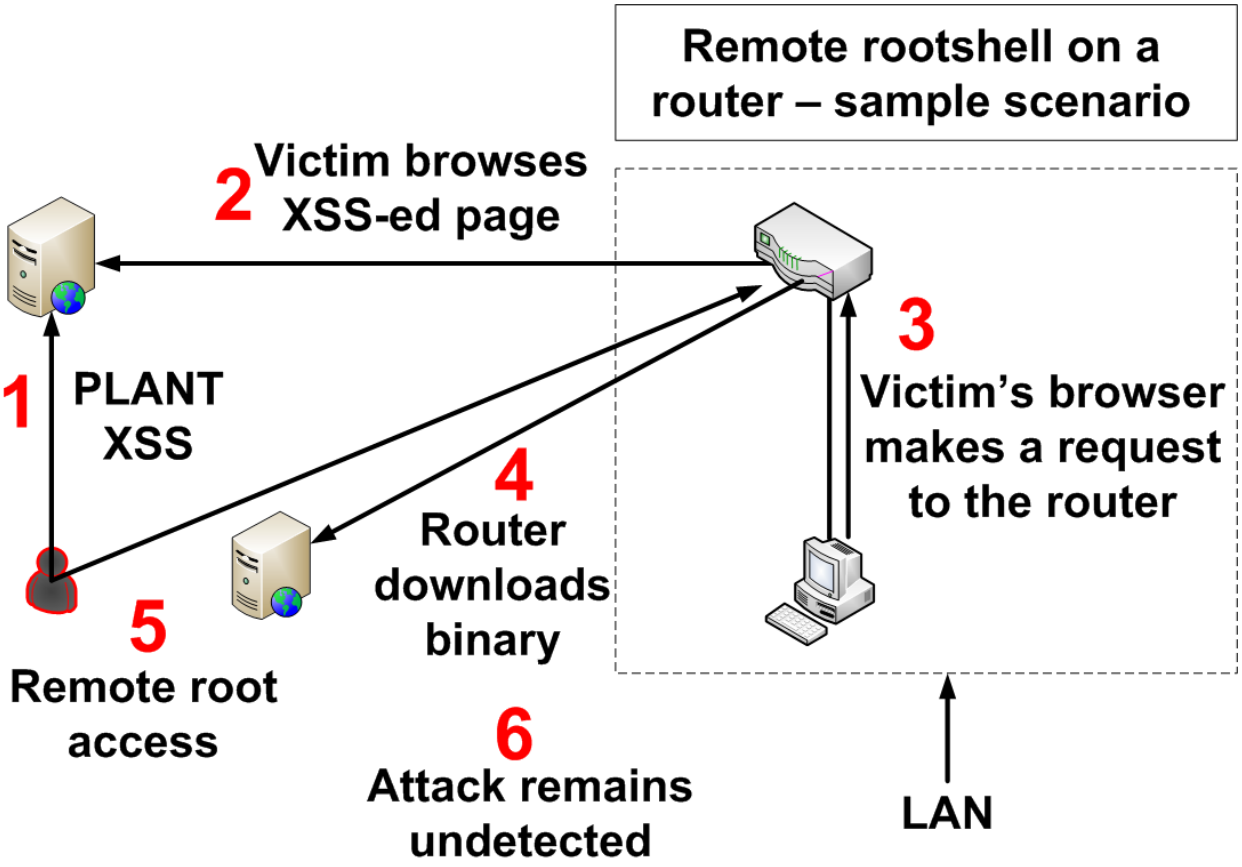
Lets look at ASMAX

- Model: AR 804 gu (ADSL + WiFi)
- Firmware Version: 66.34.1 (newest available)
- Hardware: MIPS

Lets look at ASMAX

- Live presentation (please wait until I switch on the router ;-)

Sample attack scenario



Sample attack scenario - Get the Facts ;-)

- Bypass firewall rules (at least for incoming traffic)
- Works no matter what strong admin passwd is set
- Doesn’t need JavaScript to go off
- The attack seems to originate from the victim’s workstation
- Attack is somehow initiated from the interior network (i.e. not heavily firewalled/protected)
- Hard to notice for a „relay” victim

Lets look at ASMAX

- MIPS architecture (little endian)
  - Need a cross compiler
  - GCC
  - http://www.ifp.illinois.edu/~nakazato/tips/xgcc.html
  - http://cross-lfs.org/view/1.0.0/mips/index.html

Lets look at ASMAX

- http://www.routertech.org/index.php
  - Build / install your own firmware
  - „Flashing custom firmwares onto a router is not for novices, as the process may well "brick" the router.”
  - „Please take this warning very seriously. If you are not adept at recovering bricked routers, and if you are not familiar with the PC-Tool, then do not install this firmware!”

Lets look at ASMAX

- Attack – recap
  - Locate auth bypass in web management software (can try default credentials…)
  - Locate code execution issue in web management software
  - Use CSRF to attack from inside the LAN
  - Install remote root shell

Lets look at ASMAX

- Other attacks scenarios?
- Yeah, but I focused on this one ☺

Lets look at ASMAX

- Vendor's reaction
  - My research – late '08
  - Info send on 30.12.08
  - Main contact email – not valid ;-)
  - Contacted Polish distributor – initial resonse
  - No other information till now (although I send some reminders…)

Lets look at Linksys

- Model: WAG54G2 (ADSL + WiFi)
- Firmware Version:V1.00.10
- Hardware: ARM

Lets look at Linksys

- Live presentation (please wait until I switch on the router ;-)

Lets look at Linksys

- Vendor's reaction
  - Info send on 18.03.09
  - Quick response (within one day)
  - Quick confirmation of the issue (within few days)
  - No fix till now (dev team is working on the issue…)

Lets look at GoAhead http server

- Windows platform
  - Command execution
  - Source dosclosure
  - DoS

Lets look at GoAhead http server

- Command execution
  - Once they had dir traversal
  - They fixed the issue, but forgot about cgi module…
  - … which leads to command execution

Lets look at GoAhead http server

- Command execution
  - cgi.c
  - 65: if ((cgiName = gstrchr(&cgiBuf[1], '/')) == NULL) {
  - websError(wp, 200, T("Missing CGI name"));
  - return 1;
  - }
  - cgiName++;
  - 70: if ((cp = gstrchr(cgiName, '/')) != NULL) {
  - *cp = '\0';
  - }

Lets look at GoAhead http server

- Source disclosure
  - No strict extension validation
  - Request to test.asp…%20. %20.. %20.
  - WebServer detects request as „no-extension” which defaults to text
  - Request is passed to the OS fopen(test.asp…%20. %20.. %20.)
  - OS strips appended …s and %20s
  - OS opens test.asp
  - The http server server it as txt

Lets look at GoAhead http server

- DoS
  - http://msdn.microsoft.com/en-us/library/aa365247.aspx
  - MS says: "Do not use the following reserved device names for the name of a file: CON, PRN, AUX, NUL, COM1, COM2, COM3, COM4, COM5, COM6, COM7, COM8, COM9, LPT1, LPT2, LPT3, LPT4, LPT5, LPT6, LPT7, LPT8, and LPT9. Also avoid these names followed immediately by an extension; for example, NUL.txt is not recommended.„
  - If MS says so, lets try to use it ;-)

So what?

- Botnets
  - http://en.wikipedia.org/wiki/Psyb0t
  - Detected in January ‘09
  - Botnet with test-run in march ‘09 (DDoS-ing DroneBL)
  - > 80.000 routers in the botnet
  - Shutdowned quickly after detection
  - Thx to Borys Bohater for pointing me out this

So what?

- Psyb0t – wiki entry
  - The primary attack vector is SSH or telnet access. Using brute-forcing, it tries to gain access from over 6000 usernames and 13000 passwords.
  - However, 90% of infections are caused by insecure configuration, mostly no or default administration password and allowed remote administration.
  - Recommended countermeasures are to change default access credentials to more secure ones and to update router/modem firmware. In case of infection suspicion, it is advised to perform hard reset of the router.

So what?

- Sample CSRF+auth_bypass+command_exec attack scenario works against any admin passwd
- It doesn't need remote ssh/telnet access
- It needs a victim browsing a malicious (?) web site

Protection

- Upgrade firmwares (who does that?)
- Force vendors to publish security updates (and to deliver secure web management…)
- Disable web management?
- Use links? ;-)

Protection

- Quick fixes
  - Proxy config in web browser
  - For a private address match - point to nonexistent proxy
  - http://en.wikipedia.org/wiki/Proxy_auto-config
  - Auto config works nice in corporate networks (assuming that you use auto config…)
  - Thx to *Lieven Desmet* for pointing me the idea ☺
  - Use FoxyProxy or other 'advanced' browser proxy client
  - Change the IP
  - Watch out – you can completely disable web based access to your internal network (eg to intranet)

What's next ?

- The research was / is non-commercial
- Interested in research, not hacking the net :-P
- Experimental web-site – check if we can own your router
  - Thx to Lukasz Pilorz pointing me to the idea

What's next ?

- Phase 1 – preliminary testing – ASMAX, Linksys, Pentagram, EDIMAX, D-Link.
- Phase 2 – checking other SOHO routers (LiveBox?)

What's next ?

- Phase 3 – checking some enterprise class machines (with different access levels)
  - First try - ASA (Cisco) – we will have remote/local access to the appliance (thanks to ProIdea)
  - F5 BIG-IP? (it would be nice to find web vulns in the WAF's management console ;-)

Contact info?

- Wanna help? (have fun? ;-)
  - /msg /me
  - michal.sajdak@gmail.com
  - http://securitum.pl/dh/

Possibly hazardous material

- Educational use only
- No cracking please

QA?