Introduction

kaos.theory/security.research

- Because “shmoo group” was already taken
  - dr. kaos
  - fade
  - beth
  - digunix
  - arcon
  - atlas (no, not the leet one from CTF)
  - jonner

Today's Specials

- Two projects:
  - SAMAEL – a blackbox gateway that creates a secure, anonymizing transparent firewall, protecting its users from embarrassing public disclosure.
  - NARC - transforming the output of scan tools to produce quantifiable, meaningful, (and totally hot-looking) results.

SAMAEL:
Secure, Anonymizing, Megalomaniacal, Autonomous, Encrypting Linux

...and that's a mouthful

History

- 03/2005: At Interz0ne, we proposed the idea for an OS that provided transparent anonymity, and kaos.theory was born
- 01/2006: At ShmooCon, we introduced Anonym.OS (our first public release and the world's coolest OpenBSD LiveCD :)
- 04/2006: At LayerOne, we release build documentation for Anonym.OS (hey, it beat the hell out of a maintenance release)

But DEFCON-goer's demand more…

and we don't do 0days

Anonym.OS
WAS
t3h
COOL
(and soooooooooo 80’s)

SAMAEL
is
the
HOTNESS
(and Angelina Jolie uses it)

Motivations

- All your base are belong to the NSA[t&t]
- Proliferation of SOHO networks in *desperate* need of security, anonymity
- Security and anonymity *aren't* intuitive or easy to implement…
- but they ***ARE*** easy to fuck up, giving the illusion of security and anonymity

Design Goals

- As per Anonym.OS, our first incarnation:
  - Security of the system as well as the network it protects
  - Transparent anonymity for the private, paranoid, or just plain cautious
- Easy to use. Grandma should be able to plug it in and go, as easily as with a COTS router.

Architecture

- Gentoo Linux
- Netfilter
- Squid
- Privoxy
- Transocks
- Tor

Further

- Run a (fast) Tor server
- Vote
- Support Tor and the EFF
- Jump in and maintain these tools with us so we can tackle more cool projects for you

And now for something completely different…

Wicked Cool Demo

NARC

Motivations

- Large penetration tests (50,000+ hosts)
- Trending and vulnerability analysis
- Producing accurate, reliable reports quickly with a minimum of manual interaction

Security Reporting

- What doesn’t work:
  - Fear, Uncertainty, and Doubt
  - Data Overload
  - Over-simplification / Baffle with bullshit

Reporting to Multiple Levels

- Network Engineer:
  - Wants details, remediation steps at a technical level
  - No graphs, charts, or other distractions
- IT Manager / Director:
  - Departmental people/process issues
  - Summaries of technical findings
- VP:
  - Inter-organizational issues
  - High-level summaries
- Board of Directors:
  - Thumbs up / Thumbs down

Making Security Reporting Better

- Rely on objective, quantitative data
- Correlated data (average number of vulnerabilities by platform, service, etc)

What We've Got Here

- Import scripts for pulling data in from scanning tools
- Canned queries for objective data
- Pretty pictures and summarized issues

Live Demo

Further Development

- AJAXify
- Extensible import framework
- Fully-customizable reports

Q&A