Intro to OpSec

Ethan House (ehouse@csh.rit.edu)

Aug 29, 2016

Computer Science House

What is Computer OpSec?

What is Computer OpSec?

Barriers

- Security is about creating barriers
- Put up enough to keep the bad people out

What is Computer OpSec?

A State of Mind

- For security to work it must always be your first thought
- This is rarely the case so it's up to standards to keep us there

What is Computer OpSec?

What we're going to discuss

- Theory of Security
- Apply this to Linux
- Gearing this towards users new to Linux

What is Computer OpSec?

My Credentials

- Spent 8 months securing servers on a classified network
- 5 Years dealing with CSH'ers

Proper Head Space

Proper Head Space

Be in Control

- If it's your machine, know what's happening on it
  - Be SURE there are no keys, hidden accounts, unused services still running
- Don't assume internet code is safe
- curl -s https://files.ehouse.io/ehouse/install.sh | sh
  - Don't... Ever... Do... This

Proper Head Space

Trust but Verify

- Ensure that what you're doing makes sense
- Verify that the person is who they say they are

Proper Head Space

Minimize Access

- Don't hand out access unless there is a need
- Remove that access once the need is gone

Proper Head Space

Physical Access

- All security fails when the hacker has physical access
- Takes seconds to pop the hard drives out of a server or place a MitM network device

Proper Head Space

Separate Dissimilar Traffic/Access

- Keep dissimilar information separate
- Don't share machines, databases, or network segments
    - Drink Machines shouldn't see Database Traffic
- Proper network segments and VLAN's solve this

Proper Head Space

Secured at Rest, Encrypted in Motion

- Nothing of importance should be left around in cleartext
  - Never leave passwords laying around on disk
- Everything in travel should be password/key protected
  - That email you just sent? Protected with SSL

Theories Applied

Theories Applied

Strong Passwords

- None of this matters if your password is `tits123`
- Strong Passwords
  - `npO7nT^Ixz&j*XxaYb`
    - 94 Bits
  - `worldexactthreadsomehow`
    - 91 Bits
- Terrible Passwords
  - `hunter2`
    - 24 Bits

Theories Applied

Password Generatores!

- Both of these sites generate STRONG passwords
  - XKCD Password Generator
  - CSH Written Password Generator

Theories Applied

Storing Passwords

- Password stores discourage password reuse
- Common options to store passwords and accounts
  - Lastpass
  - Keepass
  - Pass

Theories Applied

No Passwords

- Use SSH keys as much as possible
- Disable accounts like root

Theories Applied

Two Factor Auth

- Linux/PAM supports it

Theories Applied

Adaptive Filter

- You have log's, use them
- Tools like Denyhost and fail2ban create filters from failed login attempt

Theories Applied

PATCH YOUR SHIT

- Software security updates should be applied weekly
- daily as Zero Days are announced
- Everything we've learned is useless without this

Finally

Finally

In Summary

- Proper Headspace
- Strong and unique passwords are a must
- Always stay on top of updates
- On $>$ Off $>$ In the hands of the Chinese

Finally

My Other Work

- This Presentations
- Other Work

Sources

- Entropy Calculator
- XKCD Password Generator
- CSH Written Password Generator