Agenda

• History of the SIG
• Overview of projects
• Community response
• Why the Fedora Project should care
• How you can help
History

• Born at Def Con 24
• Originally penetration testing-focused on build infrastructure
• “If we’re going to get into cyber, we’d better harden the **** up”
• Organizational contrarians a-la Zenko’s Red Team: How to Succeed by Thinking Like the Enemy
• Really took off at Def Con 25
Current projects

• Enterprise Linux Exploit Mapper (ELEM)
  • [https://github.com/fedoraredteam/elem](https://github.com/fedoraredteam/elem) *

• Cyber Test Lab
  • [https://github.com/fedoraredteam/cyber-test-lab](https://github.com/fedoraredteam/cyber-test-lab) *

• Red Container
  • [https://github.com/fedoraredteam/red-container](https://github.com/fedoraredteam/red-container) *

• cyber-range-target
  • [https://github.com/fedoraredteam/cyber-range-target](https://github.com/fedoraredteam/cyber-range-target)

• Compliance / [fedoraredteam.compliant](https://github.com/fedoraredteam/compliance) *
  • [https://github.com/fedoraredteam/compliance](https://github.com/fedoraredteam/compliance)

* Has community contributions
ELEM

- Maps local vulnerabilities to known exploits
- Crowdsourced exploit curation, STRIDE
- Shows value of supported open source
- https://youtu.be/NX931nfyAmg
Cyber Test Lab

• Inspired by Cyber ITL ([http://cyber-itl.org/](http://cyber-itl.org/))
• Quantitative analysis of risk on a per-ELF binary basis
• “How hard would it be for a security researcher to find a new 0-day in THIS binary?”
What CTL does

• Static analysis (alpha today)
• Dynamic analysis (fuzzing in the future)
• On per-binary basis
  • Position independent execution (ASLR)
  • Fortified functions
  • Stack protection (NX bit)
  • Read-only relocations (RELRO)
  • Immediate binding
  • Cyclomatic complexity, cycle cost
  • Function size, branch frequency (future)
  • Function riskiness (future)
CTL Example Output

```json
"results": {
  "complexity": { "r2 aa": { "afCc": 4, "afC": 112 } },
  "usr/bin/agr": {
    "report-functions": [ "__memcpy_chk", "strtol", "tcsetattr", "strrchr", "__libc_start_main", ... 
    "hardening-check": {
      "Read-only relocations": "yes",
      "Position Independent Executable": "no, normal executable!",
      "Stack protected": "yes",
      "Fortify Source functions": "yes (some protected functions found)",
      "Immediate binding": "no, not found!" 
    },
    "filename": "usr/bin/agr"
  }
}

"metadata": { "spec_data": {
  "Group": " Applications/Text",
  "Name": " AGReader",
  "License": " GPL+",
  "URL": " http://main.aminet.net/misc/unix/", ...
```
CTL Pending Update
Red Container

• The world doesn’t need another Kali Linux
• Kali, Black Arch, Parrot, lots of offensive distros
• Primarily a packaging effort, make the tools easy to consume
• Open Container Initiative changes this game
• Containerize offensive tools, make them easy to install anywhere
• Want to run MSF with PostgreSQL backend? Great! Do it on RHEL, Debian, Windows...
cyber-range-target

• “Cyber Range” is a thing
• Training, certification, R&D
• Need to be able to deliberately make a system vulnerable to specific CVEs
• Ansible role, elegant AF

---

- hosts: webservers
  remote_user: admin
  become: true
  roles:
    - fedoraredteam.cyber-range-target
  vars:
    cves_to_test:
      - CVE-2014-6271
Compliance

• Security compliance sucks, but for many it’s a legal requirement, i.e., FISMA
• But does it work?
• Red team approach to compliance using FRT tooling
• Constructive feedback
• Ansible role to implement controls, cross platform
  • fedoraredteam.compliant
Community Response

Fedora launches their own CTL: 
fedoraproject.org/wiki/SIGs/Red_

Awesome!

Inspired by Sarah’s Defcon 25 C1TL talk:
youtu.be/BufzX-zeZvQ

Planet Mudge

Hey cool, Sarah’s talk was awesome! Glad to see it’s posted!

Thanks for the good work. It’s exactly what we were hoping for!
Community Response

Psyched that the @fedora Red Team SIG is building their own ITL and assurance program for *their* products.

As head of security at @Stripe it’s things like this that I look for to quantify risks within my environment and to strategically choose safer products and solutions!
Articles


Other articles

34c3 shout out

https://youtu.be/gaWlv3XxYko?t=50m
Why you should care

• Big opportunity here for the Fedora Project
• Make Fedora Linux more secure
• Make all Linuxes more secure
• Thought leadership
• It’s the right thing to do
How you can help

1. Amplification
2. Pull requests
Thank you