SprayPAL:
How Capturing and Replaying Attack Traffic Can Save Your IDS/IPS

Dr. Patrick Engebretson
Mr. Kyle Cronin
Dr. Josh Pauli

Rundown

1. Introductions
2. Why we all need a PAL
3. Building our PAL
4. Spray it - don’t say it
5. Community PAL
6. Bros spraying bros
7. Good night, Black Hat!

Introductions

- Dr. Patrick Engebretson
  - Asst. Prof. of Info. Assurance at Dakota State Univ.
  - Network security
- Mr. Kyle Cronin
  - Doctoral student at Dakota State Univ.
  - SysAdmin ftw
- Dr. Josh Pauli
  - Assoc. Prof. of Info. Assurance at Dakota State Univ.
  - Software Security

Why we all need a PAL

- IDS/IPS need to be tested, but shizzle can't break

Why we all need a PAL

- Not to learn ONLY offensive techniques, kids!

Why we all need a PAL

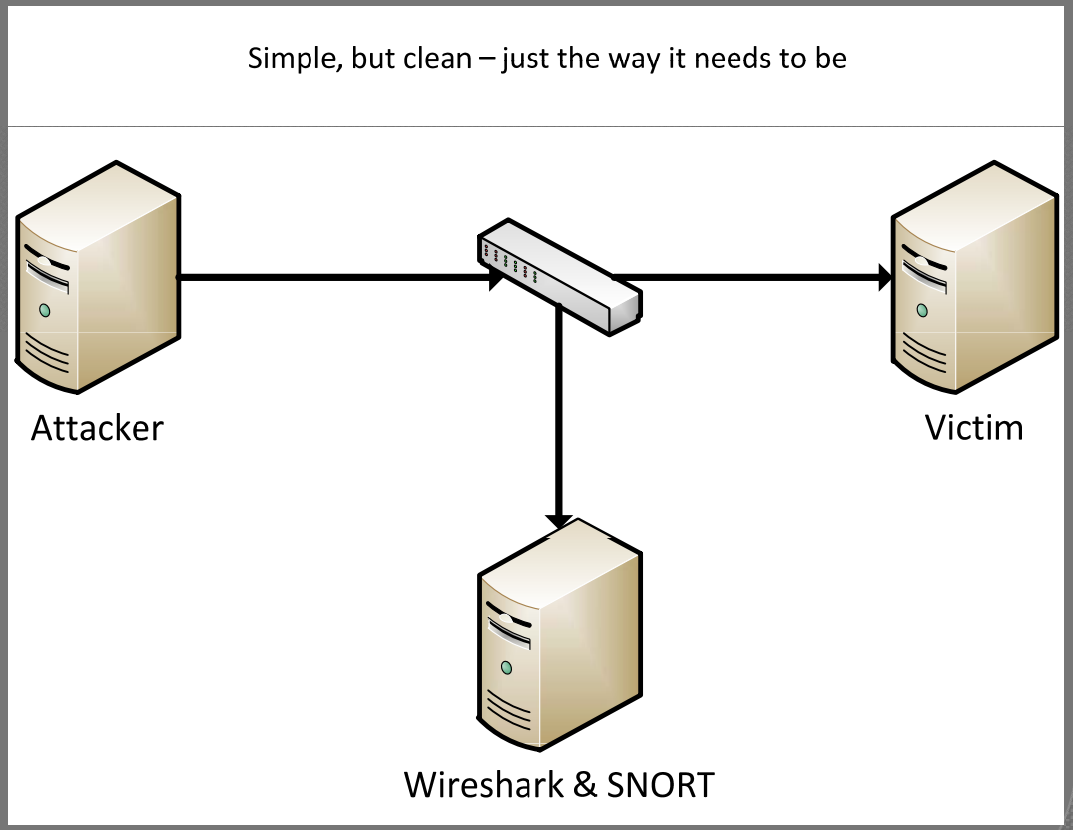
- Dr. E is a CAPEC fanboi from his research
- No need to reinvent attack descriptions
- Just use them for more than "we just read about attacks and….."

Building our PAL

- So fresh & so clean

- VMs are good, too

- SNORT
- Wireshark
- BT4
- Victim (various)



Building our PAL

1. Identify CAPEC Attack that you want to model
2. Craft Attack Traffic to Mimick CAPEC Attack on 'Attacker'
3. Ensure SNORT is running with up-to-date ruleset that matches chosen ID from step #1
4. Ensure Wireshark is running with no other traffic captured (clean slate)
5. Execute attack on 'Victim'

Spray it - don’t say it

- Easy manipulation - who doesn’t want that?

- Level 2 and 3 of the packets

Spray it - don't say it

- One victim?
- Several victims?

- One attack?
- Piggy-backed attacks?

- You have choices, folks…

Community PAL

1. Ensure SNORT rule(s) fired; comment with specific CAPEC ID number
2. Stop and "cleanse" .pcap in Wireshark as needed
3. Save .pcap with the same ID number as chosen CAPEC attack
4. Save .pcap in the correct directory to be available to SprayPAL
5. Test .pcap in SprayPAL with specific layer 2 & 3 attributes

Community PAL

Get it while it's hot, get it while it's buttered….

- Pound it here: http://ia.dsu.edu/spraypal
- Pound him here: Pat.Engebretson@dsu.edu

Bros spraying bros

Epic, Fabulous, Incredible, Hilarious, Ridiculous, Remarkable, Excellent, Phenomenal Demo

Good night, Black Hat!

?