Project Ludus:
Advanced security tool for your router

Kalin Ivanov & Ondřej Lukáš

Internet a Technologie 19

www.stratosphereips.org/ludus
Plan

- Why Ludus?
- Defense as a game
- Collaborative defense
- External Security Metric
- Ludus tool

MAKE HONEYPOTS GREAT AGAIN
Motivation and Goals of Ludus

- Collaboration with cz.nic and TAČR
- Model attackers’ behaviour and use it to create better defense
- Protect users against attacks from the Internet
- Use honeypots in smart way
- Design External Metrics to capture the Security level of devices
Troubles with Honeypots

- Where to put them!?
- Static and predictable
- How to use the data?
- Bringing your device in the spotlight!?
Influence of honeypots on the real services visibility

- **Router1 (no HP)**
- **Router2 (3HP)**

![Graph showing the influence of honeypots on the real services visibility between 2017-08-13 and 2017-08-27. The graph compares Router1 (no HP) and Router2 (3HP).](image-url)
Troubles with Honeypots

● Where to put them?!
● Static and predictable
● How to use the data?
● Bringing your device in the spotlight?!
Do you want to play a game?
Game-Theoretical Approach

- Model attacks as a game
- Find the optimal strategy
- Minimize attacker’s utility
- Save resources
Game-Theoretical Approach

- Model attacks as a game
- Find the optimal strategy
- Minimize attacker’s utility
- Save resources
Game-Theoretical Approach

- Model attacks as a game
- Find the optimal strategy
- Minimize attacker’s utility
- Save resources
Joining Forces with Others

- Information Sets $\Rightarrow$ less information for attackers $\Rightarrow$ lower utility
- Constraints in number of honeypots
Joining Forces with Others

- Information Sets ⇒ less information for attackers ⇒ lower utility
- Constraints in number of honeypots

$$P_{D1} = \{22\}$$

$$P_{D2} = \{80\}$$

Attacker's perspective

$$\{22, 80\}$$

$$\{80, 22\}$$
You can’t manage what you can’t measure.
Data

2 Sources:
1. Packet metadata
2. Suricata alert data

Suricata signatures
1| Not Suspicious Traffic
2| Unknown Traffic
3| Potentially Bad Traffic
4| Attempted Information Leak
5| Information Leak
6| Large Scale Information Leak
7| Attempted Denial of Service
8| Denial of Service
Dashboards

Local dashboard for each user

Publicly AAA Data
(Anonymized, Aggregated, Available)

Check out the public Kibana visualizations:
Metrics

- Overall Security
- Honeypots/Production Ports
- Entropy of attack
Example
Example
Example

209.239.90.114
Emerging Markets Communications de Argentina S.R.L
Added on 2019-10-23 22:12:54 GMT
United States
System administrator is connecting from 112.175.124.2
Reject the connection request !!!

95.210.229.87
Skyllogic S.p.a.
Added on 2019-10-24 21:52:40 GMT
United Kingdom, Fulham
System administrator is connecting from 112.175.124.2,
Reject the connection request !!!

https://www.shodan.io/
Ludus tool

- fully automated
- adapts and updates strategies
- anonymizes and visualizes data
- turris package: ludus

https://github.com/stratosphereips/Ludus
Q&A
Thanks for your attention!

@ondrej_lukas
lukasond@fel.cvut.cz

@RealKalin
ivanokal@fel.cvut.cz

https://www.stratosphereips.org/ludus