Carnegie Mellon University

Daedalus Network: Adaptive Cyber Deception

APRIL 23, 2024

Pau Balcells Sanchez & Adam Hunt
+ our heros Yinuo + Fei!

Motivation

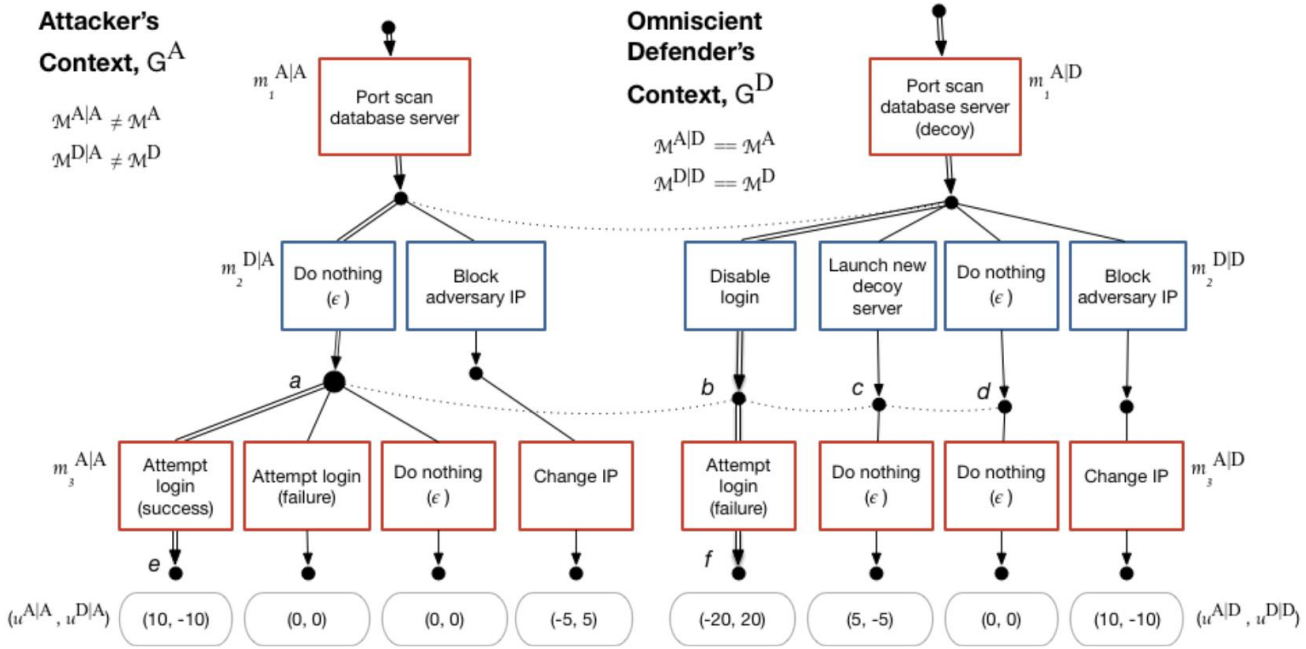
- Networks are constantly under attack
- Defenders face significant disadvantages

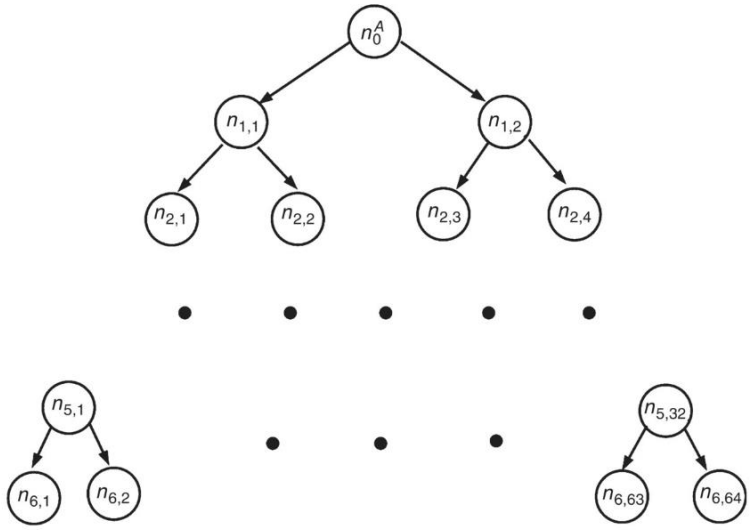
Domain Description

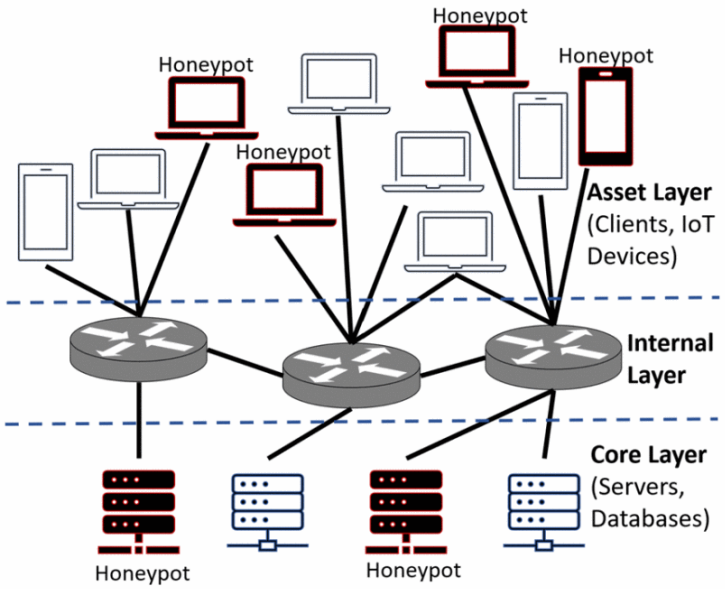
- Cyber Deception
- Active Engagment
- Learn about attacker

Related Work

- Similar methods
- Lack large-scale deployment



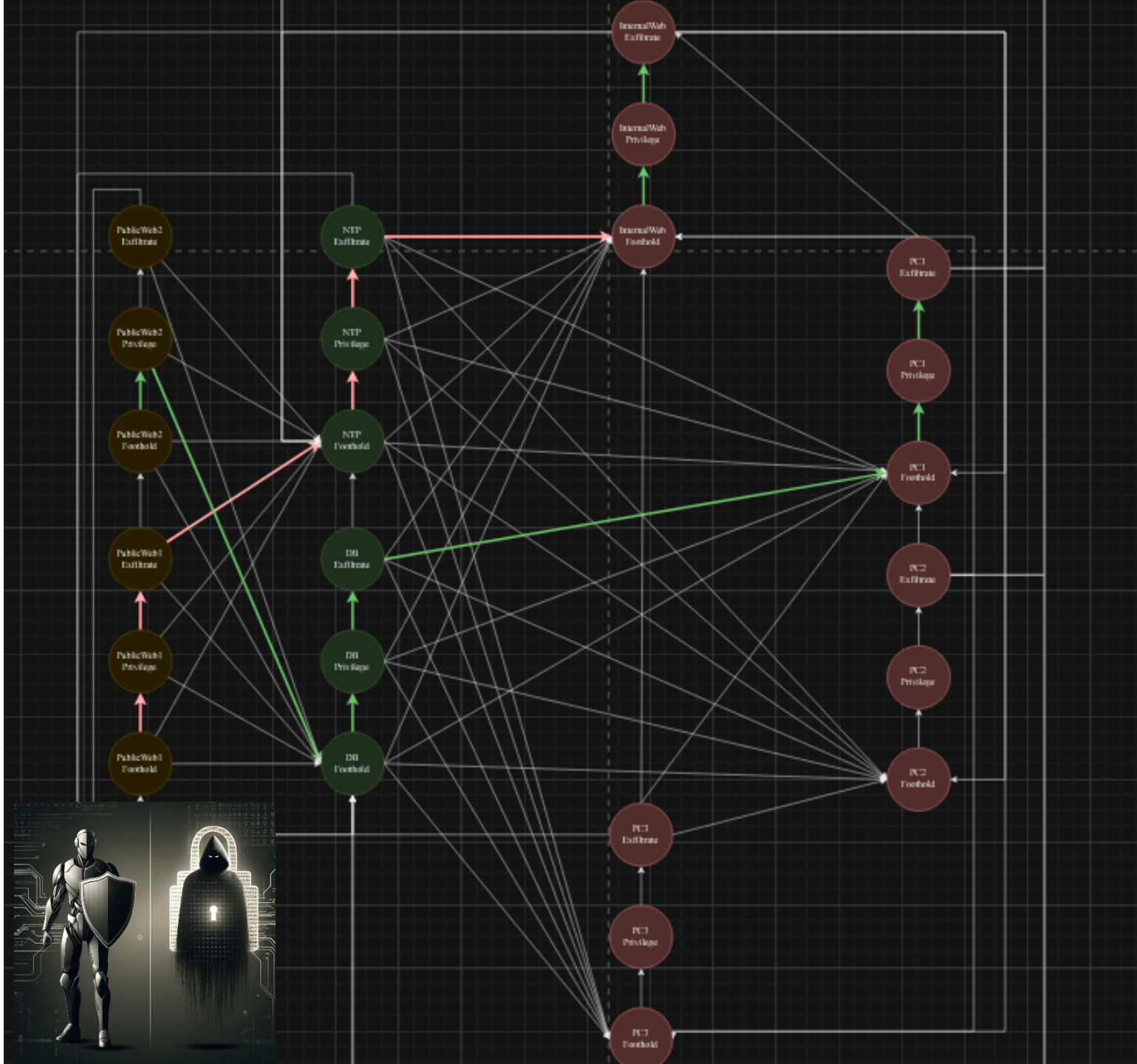




Contributions

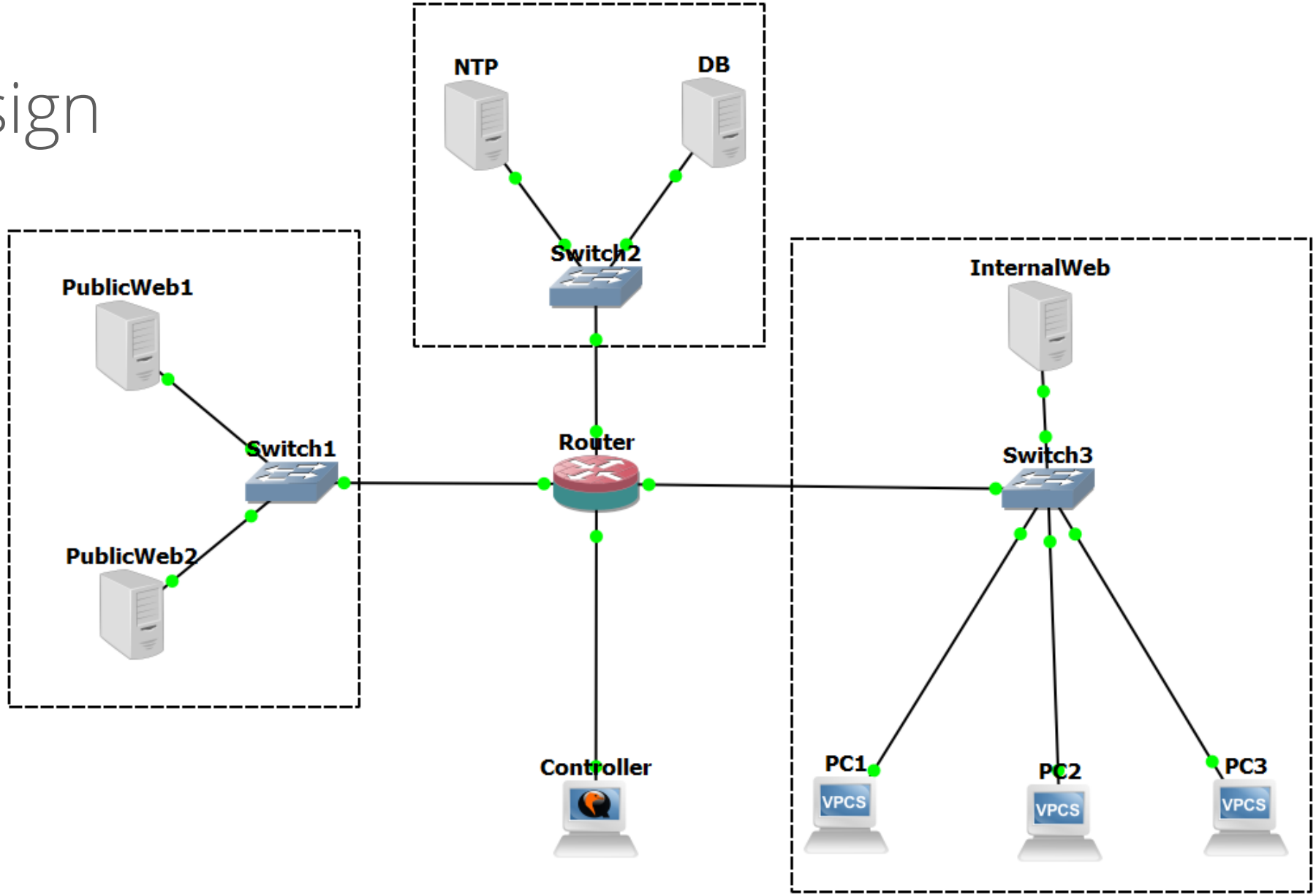
Refined Game Model

- Attack Graph
- Attacker
- Defender



System Design

- Layered Enterprise Network
- Command and Control
- Sensors and Actuators



Deployment

- Amazon Web Services
- Virtual Private Cloud
- EC2 Instances

Instances (11) Info

Find Instance by attribute or tag (case-sensitive)

Instance state = running | Clear filters

Name	Instance ID	Instance state
Public Server 1	i-0019dc99bc9bb85ea	Running
HoneyPot-Pub...	i-0f4012cd80d740b2c	Running
HoneyPot-NTP...	i-04a94d6d7fb9d3066	Running
PC1-WEB	i-07804fd9a42c65b49	Running
PC2-WEB	i-0013de65425006ac3	Running
PC3-WEB	i-0728c5e8f73936f4c	Running
Controller	i-04790eba4bba6c27a	Running
Public Server 2	i-031de534e971284af	Running
WEB	i-065a8db824659ae77	Running
NTP	i-0cf451c097f950db6	Running
DB	i-07ab0dcafa14c9bcc	Running

DEMO TIME!!!

Scenario

rapid7/metasploit-framework

#18621 Add module t
Backup Migration Wl
plugin (CVE-2023-...

2 comments

jheysel-r7 opened on December 15, 2023

Scenario

product.name="WordPress"

Query

ALL WEB NON-WEB

Results 7,665,785 Filter: Past month

54.230.253.3 / 80 / bien-dans-son-ventre.com View Detail

Location: United States
Web Title: bien-dans-son-ventre.com
Protocol: http
Trans Protocol: tcp

Header App/Product 200 2024-04-22 G

```
HTTP/1.1 200 OK
Pragma: no-cache
Content-Type: text/html; charset=UTF-8
Age: 24747
X-Amz-Cf-Id: bloGeYO3kpNjjCMi941H0xX_0b3nU8NNAS8psG3F1ihzpeDef68ERA==
Link: <https://bien-dans-son-ventre.com/wp-json/>; rel="https://api.w.org/",<https://bien-dans-son-
ventre.com/wp-json/wp/v2/pages/71>; rel="alternate"; type="application/json",<https://bien-dans-so
```

50.87.224.250 / 443 / www.newsite.dandscpas.com View Detail

Location: United States
Web Title: Del Sesto & Sterrett, LLP
Protocol: https
Trans Protocol: tcp

Header App/Product 200 2024-04-22 G

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Host-Header: c2hhcmVkLmJsdWVob3N0LmNvbQ==
X-Proxy-Cache: EXPIRED
Server: nginx/1.21.6
Vary: Accept-Encoding
Cache-Control: max-age=300
```

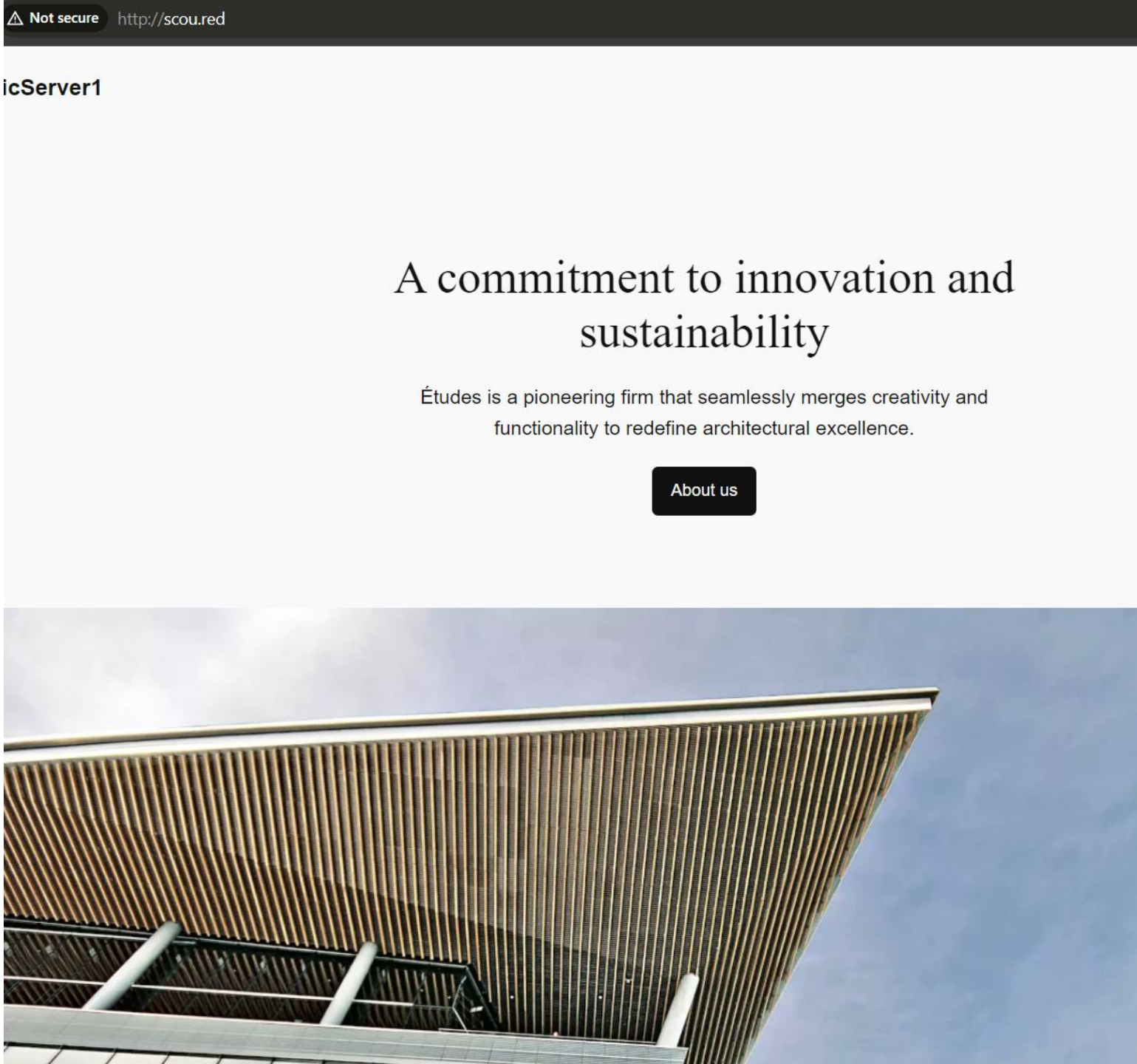
50.87.224.250 / 443 / theedifyingmom.com View Detail

Location: United States
Web Title: Home - theEdifyingMom
Protocol: https
Trans Protocol: tcp

Header App/Product 200 2024-04-22 G

```
HTTP/1.1 200 OK
Server: nginx/1.21.6
X-Endurance-Cache-Level: 2
X-Newfold-Cache-Level: 2
Cookie: nfdbrandname=bluehost; expires=Mon, 17 Apr 2034 18:47:47 GMT; Max-Age=315360000;
path=/
X-Nginx-Cache: WordPress
```

Scenario


Not secure
http://scou.red
icServer1
A commitment to innovation and sustainability
Études is a pioneering firm that seamlessly merges creativity and functionality to redefine architectural excellence.
About us

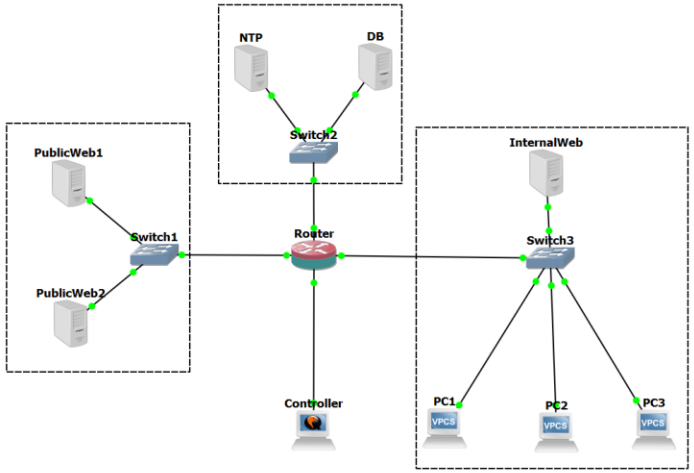
Evaluation

- Effectiveness of the defender
  - Ability to engage a diversity of attackers
  - Reduce detection time
  - Mitigate damage caused

Future Work

- RL-based Defender
- Multi-Attacker
- Deployment Automation

Terraform



Questions?

References

- Kimberly Ferguson-Walter, Sunny Fugate, Justin Mauger, and Maxine Major. 2019. Game theory for adaptive defensive cyber deception. In Proceedings of the 6th Annual Symposium on Hot Topics in the Science of Security (HotSoS '19). Association for Computing Machinery, New York, NY, USA, Article 4, 1–8. https://doi.org/10.1145/3314058.3314063

- A. H. Anwar, M. Zhu, Z. Wan, J. -H. Cho, C. A. Kamhoua and M. P. Singh, "Honeypot-Based Cyber Deception Against Malicious Reconnaissance via Hypergame Theory," GLOBECOM 2022 - 2022 IEEE Global Communications Conference, Rio de Janeiro, Brazil, 2022, pp. 3393-3398, doi: 10.1109/GLOBECOM48099.2022.10000813. keywords: {Knowledge engineering;Uncertainty;Reconnaissance;Numerical models;Delays;Complexity theory;Global communication},

- Xi, B. and Kamhoua, C.A. (2020). A Hypergame-Based Defense Strategy Toward Cyber Deception in Internet of Battlefield Things (IoBT). In Modeling and Design of Secure Internet of Things (eds C.A. Kamhoua, L.L. Njilla, A. Kott and S. Shetty). https://doi.org/10.1002/9781119593386.ch3