HONEYPOT

Šta je Honeypot?

"A **honeypot** is a computer system that is set up to act as a decoy to lure cyberattackers, and to detect, deflect or study attempts to gain unauthorized access to information systems." – izvor "WhatIs"

Honeypot - zamka – je računarski sistem koji je podešen tako da bude mamac za cyber napadače i tako da detektuje, odbija ili proučava pokušaje da se ostvari neautorizovani pristup IT sistemima.

Zašto honeypot?

1. Upoznavanje protivnika
2. Razumevanje napada
3. Praćenje aktuelnih trendova u napadima
4. Odvlačenje pažnje sa važnijih sistema
5. Statistika
6. Povećanje vidljivost – uvida u stvarne pokušaje upada i napada

7. Deo “**Golden Eye**” ideje - inicijative

Honeypot platforma

- ELK stack
- Modularna/docker
- Centralna kolekcija sa više honeypot tačaka
- Laka vizualizacija prikupljenih podataka
- Skalabilna

NetCC TECHNOLOGY

Demo time

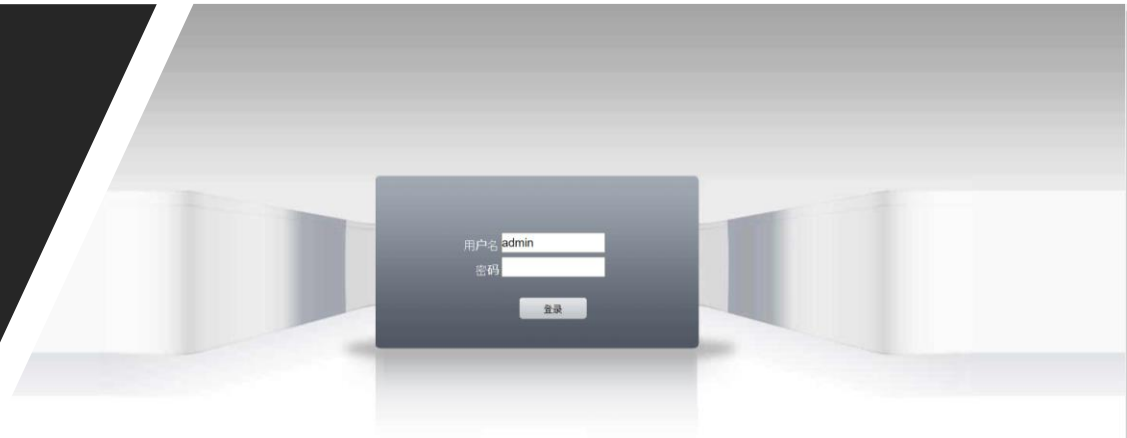
- Već 24 dana naš honeypot vredno sakuplja i prati pokušaje upada i napada na jednu našu javnu IP adresu.
- Od aktiviranja IP adrese nisu prošla ni 2 min. do prve detekcije pokušaja pristupa.
- IP adresa nikada pre toga nije korišćena...

Demo

- neočekivano veliki broj pokušaja pristupa sistemu
- Holandija među top zemljama odakle stižu napadi
- Kina, Vijetnam - očekivano
- IoT je realnost, kamere i DVR sistemi
- “brute force” napadi
- “dictionary” napadi
- najčešće kombinacije username/password

Demo – ima li šta iz Srbije?

- Sistemi inficirani sa malware-om
- IoT– kamere i DVR
- Top provajderi odakle dolaze napadi
- User/password kombinacije
- Protokoli/kanali napada



HONEYPOT

pridružite nam se!!!

Postavite senzor(e) kod vas:

- sve što je potrebno je jedna javna IP adresa
- mi obezbeđujemo Raspberry Pi ili u dogovoru koristimo vaš stari hardver
- Linux/docker sa senzorima (Windows, ind. kontroleri, web server...)

Dobijate:

- izveštaje
- lokalnu vidljivost
- mapu napada (*u pripremi)

HVALA

Pitanja?