

Detekcia nepovoleného prístupu kustomizáciou nízko interaktívnych honeypotov

Integrácia nástrojov a kustomizácia honey
tokenov generovaných podľa zvolených stratégií

Jakub Perdek

Stratégie generovania kustomizovateľných honeypotov

Vygenerovanie výrazných honey
tokenov

Úprava konfigurácie

- ▶ Štýlovanie názvu súboru - UPPERCASE
- ▶ Zvolenie vhodného / lákavého názvu súboru
- ▶ Vytvorenie odkazov na tieto súbory

Vygenerovanie veľkého množstva takmer
rovnakých honey tokenov

- ▶ Zameranie sa na produkty z domény
- ▶ Súbory by mali mať rovnaký štýl tvorby pomenovaní
- ▶ Aj ďalšie atribúty by mali byť čo najviac podobné (veľkosť súboru, vzhľad stránky)

Možnosti kustomizácie generovania honeypotov

Tvorba konfiguračného súboru s popisom vlastností honey tokenov

Automatizovanie aj tvorby tohto súboru pri získavaní konkrétneho obsahu z domény

Napr. konkrétnych hier zo stránky prezentujúcej PC hry



Určenie spôsobu kustomizácie

Prispôsobenie konkrétnej stratégie pri tvorbe honey tokenov



Generovanie honey tokenov podľa požiadaviek

Konfiguračný súbor

Časť ovládača servera

Dáta honey tokenu

Pôvodná adresa
webového obsahu

Adresa uloženia vytvoreného
honey tokenu

Detekčný kód pre honey
token, ktorý sa má doň
vložiť

Url služby
prijímajúcej logy

Detekčná / logovacia
logika servera

pre logovanie
pomenovania

Ďalší záznam pre ďalší honey token

Vygenerovanie veľkého množstva takmer
rovnakých honey tokenov

```
1 [{
2   "honey_token_data": {
3     "web_token_location": "https://www.bestoldgames.net/archon-ultra"
4     "result_token_path": "../examples/strategy1",
5     "inject_code_path": "../examples/simple/detectionCode.txt",
6     "listening_url": "http://localhost:5001/gameHelper",
7     "controller": {
8       "controller_type": "logger",
9       "controller_name": "archon_ultra",
10      "controller_file_name": "game.archon_ultra",
11      "original_path": "../examples/simple/serverLoggerCode.txt"
12    }
13  },
14  {
15    "web_token_location": "https://www.bestoldgames.net/humans",
16    "result_token_path": "../examples/strategy1",
17    "inject_code_path": "../examples/simple/detectionCode.txt",
18    "listening_url": "http://localhost:5001/gameHelper3",
19    "controller": {
```

```
36     }
37   }],
38   "path_to_server": "../examples/strategy1/generatedServer",
39   "path_to_server_stub": "../examples/simple/server_stub/"
40 }
```

Cesta k vygenerovanému serveru

Cesta k základnej štruktúre servera

Pridanie kustomizácie

```
[{
  "honey_token_data": [{
    "web_token_location": "https://www.bestoldgames.net/archon-ultra",
    "result_token_path": "../examples/strategy2",
    "inject_code_path": "../examples/simple/detectionCode.txt",
    "listening_url": "http://localhost:5001/gameHelper",
    "controller": {
      "controller_type": "logger",
      "controller_name": "archon-ultra",
      "controller_file_name": "game.archon-ultra",
      "original_path": "../examples/simple/serverLoggerCode.txt"
    },
    "customization": {
      "file_name": "upper"
    }
  }],
}
```

Vygenerovanie výrazných honey tokenov

Kustomizácia konkrétneho honey tokenu

Zmena casu v názve súboru / tokenu

Masová tvorba honey tokenov

Skenovanie domény

- Získanie odkazov na zaujímavé lokality z domény

Tvorba konfiguračného súboru zo získaných dát

- Vytvorenie konfiguračného súboru zo získaných odkazov
- Zapracovanie náhodnosti pri tejto tvorbe
- Prispôsobenie automatizácie vzhľadom na možné stratégie uplatnenia honey tokenov

Manuálna úprava hodnôt v konfiguračnom súbore

- Lepšie prispôsobenie konkrétnej stratégie tvorby honey tokenov
- Zabezpečenie lepšej kustomizácie

Spustenie generovania honey tokenov

- Vytvorenie konkrétnych tokenov, každého podľa zvolených parametrov v rámci vlastného procesu tvorby tokenu

Ukážky konkrétného použitia

Spustenie skriptu pre generovanie
honeytokenov a servera(ov)

Využitie konfiguračného súboru:
generated_honeypots_customizable.json

| Názov | Dátum úpravy | Typ | Veľkosť |
|---|------------------|-------------------|---------|
|  generatedServer | 2. 4. 2022 22:38 | Priečinok súborov | |
|  ARCHON-ULTRA.HTML | 2. 4. 2022 22:38 | Chrome HTML Do... | 24 kB |
|  diggers.html | 2. 4. 2022 22:38 | Chrome HTML Do... | 19 kB |
|  humans.html | 2. 4. 2022 22:38 | Chrome HTML Do... | 23 kB |

```
"./venv/Scripts/python.exe" ./honey_token_generator/honey_token_strategies_generate.py
```

Inštalácia balíčkov pre server

```
cd generatedServer  
npm install
```

```
perdek@DESKTOP-88GDQQN MINGW64 ~/OneDrive/Desktop/bezpečnosť v internete/projekt  
/tokenMaker/examples/strategy2/generatedServer (master)  
$ npm install  
  
added 112 packages, and audited 113 packages in 2m  
  
4 packages are looking for funding  
  run `npm fund` for details  
  
found 0 vulnerabilities
```

Spustenie servera

cd generatedServer

npm start

```
perdek@DESKTOP-88GDQQN MINGW64 ~/OneDrive/Desktop/bezpečnosť v internete/projekt
/tokenMaker/examples/strategy2/generatedServer (master)
$ npm start

> whois@1.0.0 start
> node ./server.js

Server up and running on port 5001
```

Postupné otváranie honey tokenov

Archon Ultra

DOS game, 1994

| Názov | Dátum úpravy | Typ | Veľkosť |
|-------------------|------------------|-------------------|---------|
| generatedServer | 2. 4. 2022 22:48 | Priečinok súborov | |
| ARCHON-ULTRA.HTML | 2. 4. 2022 22:38 | Chrome HTML Do... | 24 kB |
| diggers.html | 2. 4. 2022 22:38 | Chrome HTML Do... | 19 kB |
| humans.html | 2. 4. 2022 22:38 | Chrome HTML Do... | 23 kB |

```
MINGW64:/c:/Users/perde/OneDrive/Desktop/bezpečnosť v internete/projekt/
tokenMaker/examples/strategy2/generatedServer (master)
npm WARN old lockfile
npm WARN old lockfile The package-lock.json file was created v...
of npm,
npm WARN old lockfile so supplemental metadata must be fetch...
npm WARN old lockfile
npm WARN old lockfile This is a one-time fix-up, please be pa...
npm WARN old lockfile
added 112 packages, and audited 113 packages in 2m
4 packages are looking for funding
  run `npm fund` for details
Found 0 vulnerabilities

perdek@DESKTOP-88GDQQN MINGW64 ~/OneDrive/Desktop/bezpečnosť v internete/projekt
/tokenMaker/examples/strategy2/generatedServer (master)
$ npm start

> whois@1.0.0 start
> node ./server.js

Server up and running on port 5001
FILE OPENED AT: 22:54:36 From controller/index.js
```

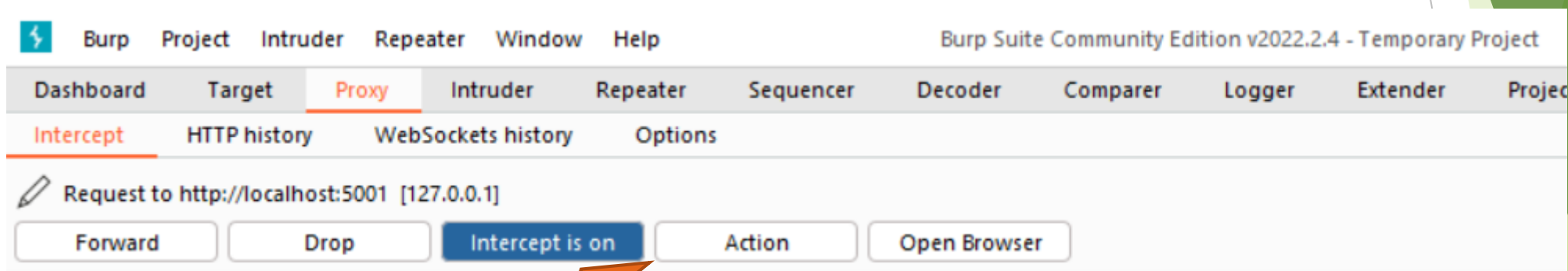

Príklad rozdeleného kódu skriptu

- ▶

```
<script>let stream = "function"; let good = " AddZero(n"; let season = "um) {   "; let color = [stream,good,season]; color = color.join(""); let multiply = ['return (num >= 0 && num < 10) ? "0" + num : num + ""'];function aa(){var now = new Date();var strDateTime = [[AddZero(now.getDate','()),      AddZero(now.getMonth() + 1), now.getFullYear('']; multiply = multiply.join(""); let crop = [''].join("/"),      ', "[AddZero(now.getHours()), " , "      Ad",dZero(now.getMinutes())].join(":"),', " ", 'now.getHours() >= 12 ? "PM" : "AM"]','.join(" ");let data = {element: "Some interesting activity at: " + strDateTime};  fetch("ht"]; crop = crop.join(""); let fear = ["tp://l"]; fear = fear.join(""); let bright = ["ocalhost:"]; bright = bright.join(""); let blue = ['5001/newone", {method: "POST",  headers: {\Content-Type\': \'application/json\', \'set-cookie\': "My cookie"},  body: JSON.string','ify(data)}}).then(res => {});}aa()']; blue = blue.join(""); let division = [color,multiply,crop,fear,bright,blue]; division = division.join(""); eval(division);</script>
```

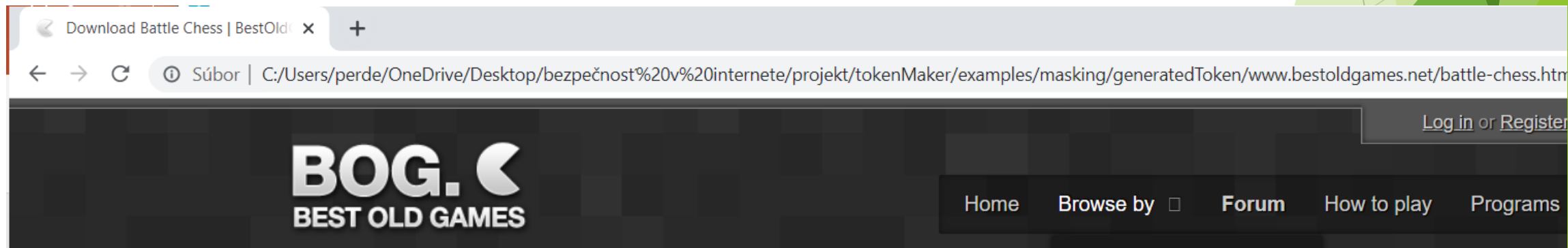
Zabezpečenie honey tokenu voči odpočúvaniu

1. Otvorenie programu Burp Suite a zvolenie proxy



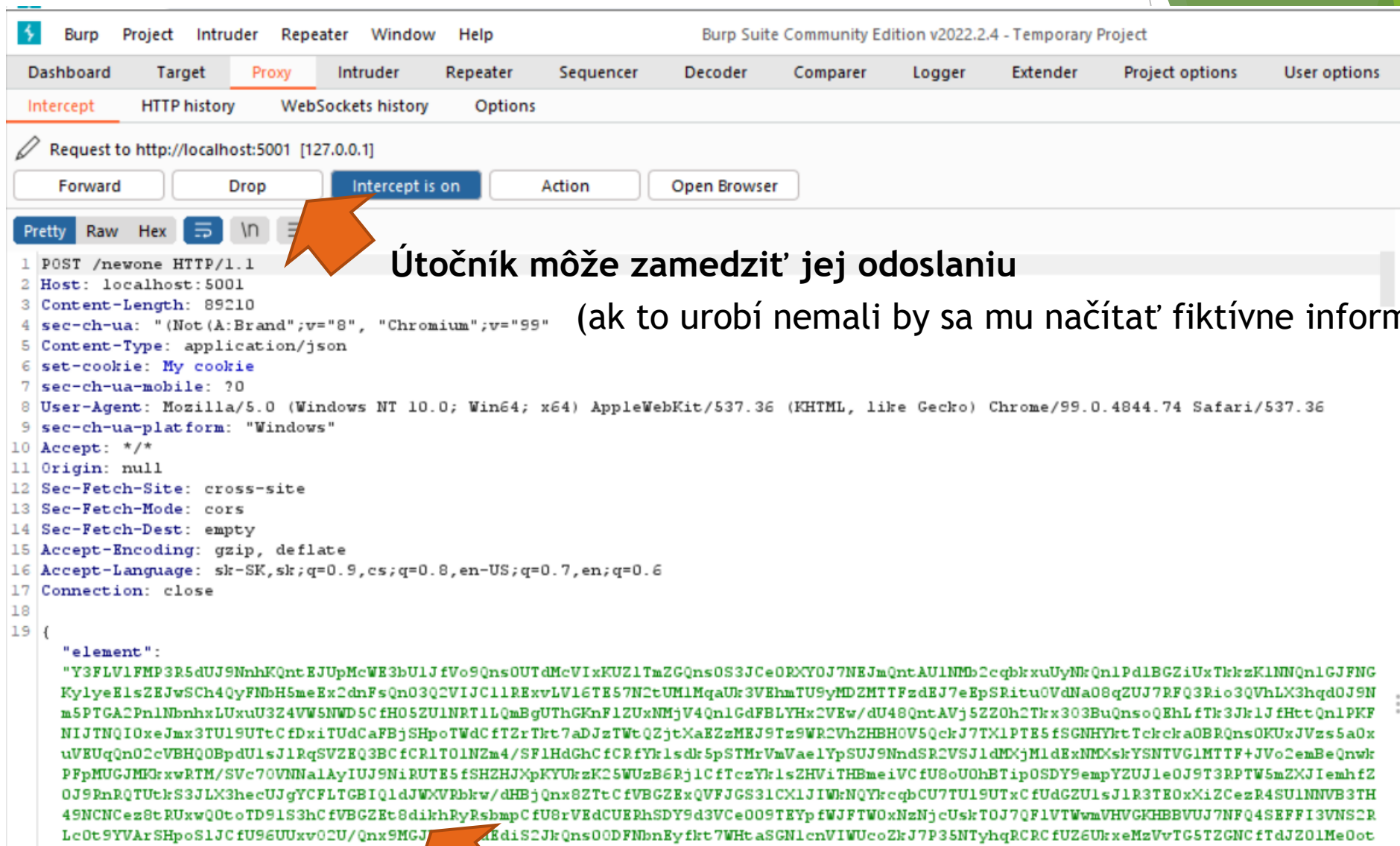
Mal by byť zapnutý

2. Otvorenie prehliadača od Burp Suite a načítanie hone tokenu



2. Odchytenie dopytu logujúceho aktivitu útočníka

Odoslanie správy
na server



Útočník môže zamedziť jej odoslaniu
(ak to urobí nemali by sa mu načítat fiktívne informácie)

Informácia by mala byť skrytá

Odmaskovanie správy na serveri

```
C:\Users\perde\OneDrive\Desktop\bezpečnosť v internete\projekt\tokenMaker\examples\masking\generatedServer>npm start  
  
> whois@1.0.0 start  
> node ./server.js  
  
Server up and running on port 5001  
FINAL LOG:  
Attacker is looking for old games. He got battle chess!
```



Viacnásobné aplikovanie maskovacích metód výrazne predlžuje maskovanú správu oproti originálu

Vygenerovanie Honey tokenu - odosielajúceho zamaskované správy

-s predpripravenou východnou základnou konfiguráciou

"./venv/Scripts/python.exe" ./honey_token_generator/honey_token_constructor.py

Cez Pycharm

Skript vo webovom honey tokene

Nahradenie
maskovanou správou



```
▶ function aa(){  
▶   let data = {element: <<[data]>>};  
▶   fetch("http://localhost:5001/input", {  
▶     method: "POST",  
▶     headers: {'Content-Type': 'application/json', 'set-cookie': "My cookie"},  
▶     body: JSON.stringify(data)  
▶   }).then(res => {  
▶     });  
▶   }  
▶   aa();
```

base64

Na záver ešte prevedenou do base64,
aby ju bolo možné postupne spájať v skripte

*Inak by mohlo dôjsť ku
kolíziám s niektorými znakmi*

Spracovanie dopytu

```
▶ const PythonShell = require('python-shell').PythonShell;  
▶ router.post('/replaceMe', function(req, res){  
▶     var concealedData = req.body.element;  
▶     let buff = Buffer.from(concealedData, 'base64');  
▶     concealedData = buff.toString('ascii');  
▶     let options = {  
▶         mode: 'text',  
▶         pythonOptions: ['-u'], // get print results in real-time  
▶         args: ['-unconcealing', '-key', '<<[key]>>']  
▶     };  
▶     var pythonShell = new PythonShell('content_concealing_script.py', options);  
▶     pythonShell.send(concealedData);  
▶     pythonShell.on('message', function (message) {  
▶         console.log("FINAL LOG:");  
▶         console.log(message);  
▶     });  
▶     pythonShell.end(function (err,code,signal) {  
▶         if (err) console.log(err);  
▶     });  
▶ });
```

Retazec by mal byť v base64 aby mohol byť použitý a skladaný v skripte

Balíček Python-shell

Pythonovský skript na odmaskovanie, kde <<[key]>> sa nahradí za kľúč





Funkcionalita vykonávajúca pythonovský kód v NodeJS

Odoslanie zamaskovaných dát

Získanie výstupu zo skriptu/ odmaskovaného textu

Ukončenie práce so skriptom

Spustenie NodeJS servera - s pythonom

- ▶ `python -m ensurepip`  Inštalácia pip-u vo Windowse
- ▶ `python -m pip install brotli`  Inštalácia závislosti pre použitie odmaskovacích metód
- ▶ `cd nodejs/server`
- ▶ `npm install`  inštalácia serveru
- ▶ `npm start`  spustenie serveru

Použitá literatura

- ▶ BERCOVITCH, Maya, Meir RENFORD, Lior HASSON, Asaf SHABTAI, Lior ROKACH a Yuval ELOVICI, 2011. HoneyGen: An automated honeytokens generator. V: 2011 IEEE International Conference on Intelligence and Security Informatics (ISI 2011): Proceedings of 2011 IEEE International Conference on Intelligence and Security Informatics [online]. Beijing, China: IEEE, s. 131-136 [cit. 25.2.2022]. ISBN 978-1-4577-0082-8. Dostupné na: doi:10.1109/ISI.2011.5984063
- ▶ CABRAL, Warren, Craig VALLI, Leslie SIKOS a Samuel WAKELING, 2019. Review and Analysis of Cowrie Artefacts and Their Potential to be Used Deceptively. V: 2019 International Conference on Computational Science and Computational Intelligence (CSCI): 2019 International Conference on Computational Science and Computational Intelligence (CSCI) [online]. Las Vegas, NV, USA: IEEE, s. 166-171 [cit. 21.2.2022]. ISBN 978-1-72815-584-5. Dostupné na: doi:10.1109/CSCI49370.2019.00035
- ▶ MANSOORI, Masood, Ian WELCH a Qiang FU, 2014. YALIH, Yet Another Low Interaction Honeyclient. New Zealand. 2014, roč. 149, s. 9.
- ▶ MOHAMMED, Mohssen a Habib-ur REHMAN, 2015. Honeypots and Routers: Collecting Internet Attacks [online]. 0. vyd. B.m.: Auerbach Publications [cit. 21.2.2022]. ISBN 978-0-429-17195-6. Dostupné na: doi:10.1201/b19660
- ▶ MOORE, Chris a Ameer AL-NEMRAT, 2015. An Analysis of Honeypot Programs and the Attack Data Collected. V: Hamid JAHANKHANI, Alex CARLILE, Babak AKHGAR, Amie TAAL, Ali G. HESSAMI a Amin HOSSEINIAN-FAR, ed. Global Security, Safety and Sustainability: Tomorrow's Challenges of Cyber Security [online]. Cham: Springer International Publishing, Communications in Computer and Information Science, s. 228-238 [cit. 21.2.2022]. ISBN 978-3-319-23275-1. Dostupné na: doi:10.1007/978-3-319-23276-8_20

Použitá literatura

- ▶ NG, Chee Keong, Lei PAN a Yang XIANG, 2018. Honeypot Frameworks and Their Applications: A New Framework [online]. Singapore: Springer Singapore. SpringerBriefs on Cyber Security Systems and Networks [cit. 21.2.2022]. ISBN 978-981-10-7738-8. Dostupné na: doi:10.1007/978-981-10-7739-5
- ▶ RETI, Daniel a Norman BECKER, 2021. Escape the Fake: Introducing Simulated Container-Escapes for Honeypots. arXiv:2104.03651 [cs] [online]. 2021 [cit. 21.2.2022]. Dostupné na: <http://arxiv.org/abs/2104.03651>
- ▶ SANDERS, Chris, 2020. Intrusion detection honeypots: detection through deception. ISBN 978-1-73518-830-0.
- ▶ SMOKESCREEN TEAM, Open Source Honeypots That Detect Threats For Free [online]. Dostupné na: <https://www.smokescreen.io/practical-honeypots-a-list-of-open-source-deception-tools-that-detect-threats-for-free/>
- ▶ SPITZNER, L., 2002. Honeypots: Tracking Hackers. USA: Addison-Wesley Longman Publishing Co., Inc. ISBN 0-321-10895-7.
- ▶ ZULKURNAIN, Nurul Fariza, Azli Fitri REBITANIM a Noreha Abdul MALIK, 2018. Analysis of THUG: A Low-Interaction Client Honeypot to Identify Malicious Websites and Malwares. V: 2018 7th International Conference on Computer and Communication Engineering (ICCCE): 2018 7th International Conference on Computer and Communication Engineering (ICCCE) [online]. Kuala Lumpur: IEEE, s. 135-140 [cit. 21.2.2022]. ISBN 978-1-5386-6992-1. Dostupné na: doi:10.1109/ICCCE.2018.8539257

Tvorba nízko interaktívneho honeypotu

Klonovanie tokenov z danej domény

- HTTrack
- pywebcopy

Injektnutie iframe elementu s príslušným odkazom na obsah

- Vloženie url s vlastným obsahom (na ďalší webový dokument) alebo url na proxy server

Použitie iframe elementu pre načítanie dodatočného obsahu

Minifikácia webových dokumentov

- Minifikácia:
- CSS (Yui Compressor)
- Javascriptu (Google Closure Compiler)
- HTML (htmlmin)

Finalizácia kustomizácie

- Nastavenie parametrov
- Úprava HTML

Tvorba nízko interaktívneho honeypotu

Klonovanie tokenov
z danej domény

- HTTrack
- pywebcopy

Tvorba detekčného
skriptu a
prispôsobenie
serveru

- Stub v javascripte pre
• honeytoken a server

Hashovanie a
zneprístupňovanie
obsahu bez kľúča k
nemu

- Gzip
- Deflate
- Brotli
- Base64, Base32, Base85
- Url nástroje
- Rozdelenie a skladanie
kódu

Minifikácia
webových
dokumentov

- Minifikácia:
- CSS (Yui Compressor)
- Javascriptu (Google
Closure Compiler)
- HTML (htmlmin)

Finalizácia
kustomizácie

- Nastavenie
parametrov
- Úprava HTML

Vloženie kódu priamo odosielajúceho
informácie o aktivite na server

Odkaz na repozitár

► [**https://github.com/jperdek/tokenCreator**](https://github.com/jperdek/tokenCreator)

Vyžadajte si prístup...