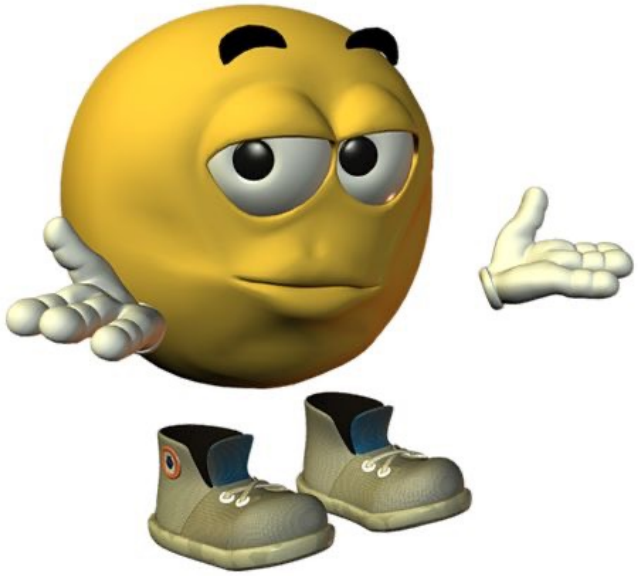
Detecting open-source honeypots

Anastasiia Dorosh



Sup, chat!

- Cybersecurity implementation lead at Labyrinth
- Have a degree in CS
- nastiadorosh.work@gmail.com

Why even think about it?

1. Open-source + and -
2. Increase credibility => gather more data
3. Know where to look during penetration testing
4. Know where the adversaries can look

Example: ZHtrap

During the login attempt, ZHtrap will ask the scanned device to execute the following command:

```
enable
linuxshell
system
bash
ls /home
ps aux
/bin/busybox ZONESEC
```

The device type is then determined based on the returned information,and the device will be regarded as a honeypot when it contains the following string.

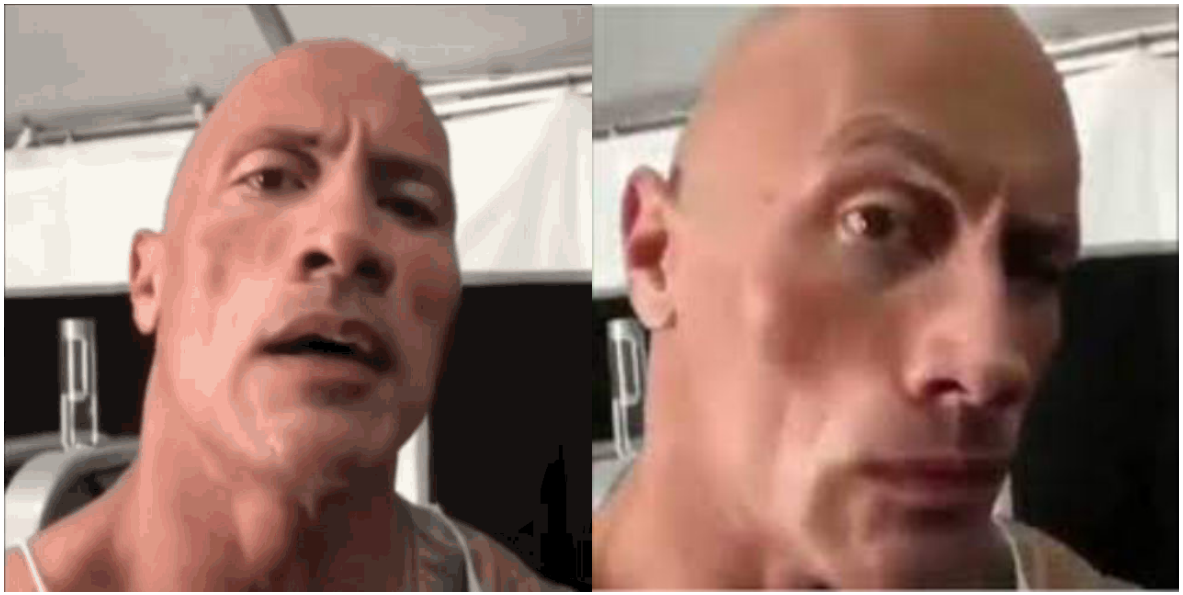
STRING	HONEYPOT
Jun22	cowrie
Jun23	cowrie
phil	cowrie
sshd:	cowrie
richard	cowrie
@LocalHost:]	cowrie
Welcome to EmbyLinux 3.13.0-24-generic	telnet-iot-honeypot

https://blog.netlab.360.com/new_threat_zhtrap_botnet_en/

How to detect them?

One basic rule:

Look for inconsistencies



Some notes

1. Decoys are investigated separately from env
2. We are okay with triggering them
3. Probabilities
4. Look at broader picture

What are we dealing with today?

Test rabbits

- Cowrie
- Conpot
- Dionaea
- Glastopf

Some basic tools

- nmap
- shodan
- telnet
- netcat
- nuclei
- tcpdump/wireshark
- etc.

Cowrie

Cowrie

Welcome to the Cowrie GitHub repository

This is the official repository for the Cowrie SSH and Telnet Honeypot effort.

What is Cowrie

Cowrie is a medium to high interaction SSH and Telnet honeypot designed to log brute force attacks and the shell interaction performed by the attacker. In medium interaction mode (shell) it emulates a UNIX system in Python, in high interaction mode (proxy) it functions as an SSH and telnet proxy to observe attacker behavior to another system.

Cowrie is maintained by Michel Oosterhof.

https://github.com/cowrie/cowrie

Test rabbit #1

This is what we are working with:

```
Nmap scan report for
Host is up (0.21s latency).

PORT      STATE    SERVICE
22/tcp    open     ssh
23/tcp    filtered telnet
80/tcp    open     http
5222/tcp  open     xmpp-client
```

Test 1: normal reaction to abnormal events

Send wrong SSH version string:

```
└─$ telnet                    22
Trying                    ...
Connected to                    .
Escape character is '^]'.
SSH-2.0-OpenSSH_6.0p1 Debian-4+deb7u2
SSH-420-OpenSSH_9.0
Protocol major versions differ.
Connection closed by foreign host.
```

Compare:

```
└─$ telnet 172.16.128.1 22
Trying 172.16.128.1...
Connected to 172.16.128.1.
Escape character is '^]'.
SSH-2.0-OpenSSH_9.7p1 Debian-5
SSH-420-OpenSSH_9.0
Invalid SSH identification string.
Connection closed by foreign host.
```

```python
    def _unsupportedVersionReceived(self, remoteVersion: bytes) -> None:
        """
        Change message to be like OpenSSH
        """
        self.transport.write(b"Protocol major versions differ.\n")
        self.transport.loseConnection()
```

https://github.com/cowrie/cowrie/blob/e7b5fc319315554d7b9adfaab3cf28246efb1df1/src/cowrie/ssh/transport.py

Test 2: basic instinct

Some dummy credentials worked

cowrie / etc / **userdb.example**

hamidmujtaba fix userdb.example (#1619) b8e69

Code Blame 22 lines (22 loc) · 589 Bytes

```
# Example userdb.txt
# This file may be copied to etc/userdb.txt.
# If etc/userdb.txt is not present, built-in defaults will be used.
#
# ':' separated fields, file is processed line for line
# processing will stop on first match
#
# Field #1 contains the username
# Field #2 is currently unused
# Field #3 contains the password
# '*' for any username or password
# '!' at the start of a password will not grant this password access
# '/' can be used to write a regular expression
#
root:x:!root
root:x:!123456
root:x:!/honeypot/i
root:x:*
tomcat:x:*
oracle:x:*
*:x:somepassword
*:x:*
```

Test 3: get hints from devs

docs/FAQ.rst

```
20
21  The default Cowrie users is called `phil` these days. Having the same
22  user always available is an easy way to identify Cowrie so it's recommend to change
29          $ bin/fsctl share/cowrie/fs.pickle
30          fs.pickle:/$ mv /home/phil /home/joe
31
```

Show 3 more matches

https://github.com/cowrie/cowrie/blob/e3df70fd9c5cfaf063258511c041c99f7ee793ea/docs/FAQ.rst

```
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
sshd:x:101:65534::/var/run/sshd:/usr/sbin/nologin
phil:x:1000:1000:Phil California,,,:/home/phil:/bin/bash
```

Test 4: simple commands

Useradd of honeypot:

```
admin@server-dev:~$ useradd catt
Adding user `catt' ...
Adding new group `catt' (1001) ...
Adding new user `catt' (1001) with group `catt' ...
Creating home directory `/home/catt' ...
Copying files from `/etc/skel' ...
Password:
Password again:

Changing the user information for catt
Enter the new value, or press ENTER for the default
        Username []:
Must enter a value!
        Username []: ll
        Full Name []: ll
        Room Number []: lll
```

Compare:

```
└─$ sudo adduser catt
info: Adding user `catt' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `catt' (1006) ...
info: Adding new user `catt' (1006) with group `catt (1006)' ...
info: Creating home directory `/home/catt' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for catt
Enter the new value, or press ENTER for the default
        Full Name []:
```

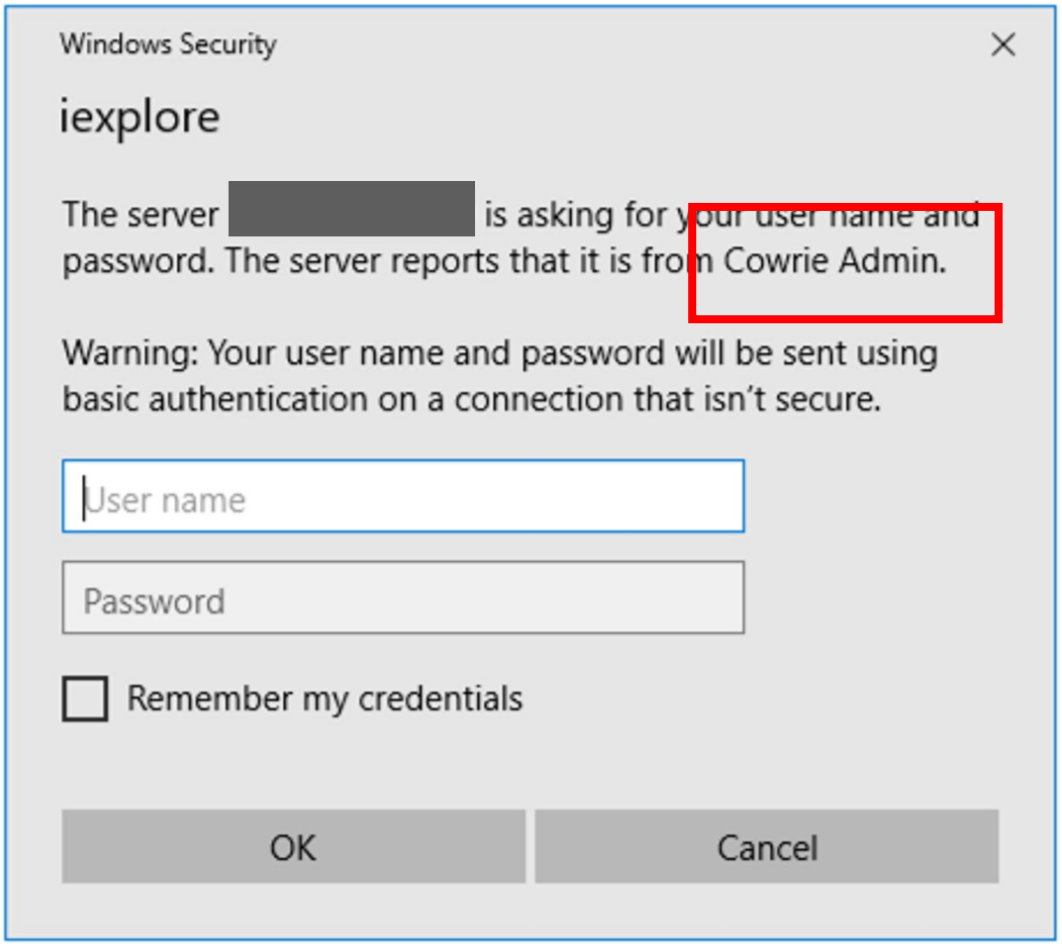
```
└─$ sudo useradd catt
```

```
99
100
101     commands["/usr/sbin/adduser"] = Command_adduser
102     commands["/usr/sbin/useradd"] = Command_adduser
103     commands["adduser"] = Command_adduser
104     commands["useradd"] = Command_adduser
```

Source: https://github.com/cowrie/cowrie/blob/e3df70fd9c5cfaf063258511c041c99f7ee793ea/src/cowrie/commands/adduser.py

Test 5: cherry on top

Check web



Conpot

Conpot

Code tests failing docs passing coverage 74% Docker Build Status

About

Conpot is an ICS honeypot with the goal to collect intelligence about the motives and methods of adversaries targeting industrial control systems.

Documentation

The documentation can be found here. If you are just checking out conpot, we suggest that you go for quick install.

If you want to tinker around and write your own template, change ports etc. We suggest that you do host install. You can find instructions on how to install conpot here and the FAQ here.

https://github.com/mushorg/conpot/tree/master

Test rabbit #2

Shodan | Maps | Images | Monitor | Developer | More...

SHODAN | Explore | Downloads | Pricing | Type / to search | Account

Regular View | Raw Data

© OpenMapTiles Satellite © MapTiler © OpenStreetMap contributors

// LAST SEEN: 2024-10-16

General Information

Hostnames	
Domains	
Cloud Provider	Google
Cloud Region	us-east5
Country	United States
City	Columbus
Organization	Google LLC
ISP	Google LLC
ASN	AS396982

Open Ports

21 22 23 80 161 502 623 2404 5900 10001 11112 44818 50100

// 21 / TCP

1124735066 | 2024-10-10T08:12:51.225876

```
200 FTP server ready.
220- Technodrome - Mouser Factory. Authorized personnel only
220
214-The following commands are recognized:
 'ABOR' 'ALLO' 'APPE' 'CDUP' 'CWD'  'DELE' 'HELP' 'LIST'
 'MDTM' 'MKD'  'MODE' 'NLST' 'NOOP' 'PASS' 'PASV' 'PORT'
 'PWD'  'QUIT' 'REIN' 'REST' 'RETR' 'RMD'  'RNFR' 'RNTO'
 'SITE' 'SIZE' 'STAT' 'STOR' 'STOU' 'STRU' 'SYST' 'TYPE'
 'USER'
214 Help command successful.
500 Command 'FEAT' not understood
```

// 22 / TCP

Test 1: Modbus

```
└$ echo -ne '\x00\x01\x00\x00\x00\x05\x01\x2B\x0E\x01\x00' | nc                    502
"+SiemensSIMATICS7-200
```

Function Code 43
(0x2B/0x0E)
Read Device Identification

> Rate

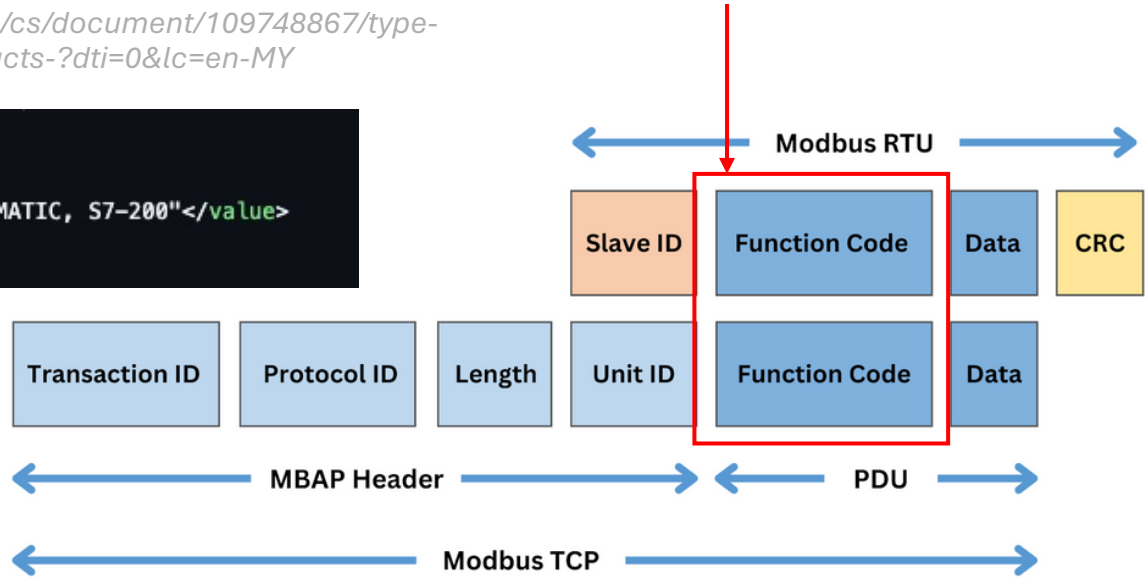
Type discontinuation SIMATIC S7-200 products

Entry | Associated product(s)

The following S7-200 products are discontinued as per Oct. 1, 2017 (milestone PM410). Thus, the stated products will be available as from Oct. 1, 2017, only as spare parts from our spare parts service.

https://support.industry.siemens.com/cs/document/109748867/type-discontinuation-simatic-s7-200-products-?dti=0&lc=en-MY

```
</key>
<key name="SystemDescription">
    <value type="value">"Siemens, SIMATIC, S7-200"</value>
</key>
<key name="Uptime">
```



https://www.wevolver.com/article/modbus-tcp

Test 1: Modbus (extra)

```
└─$ nmap --script modbus-discover.nse  -p 502 :                -d
Starting Nmap 7.94 ( https://nmap.org ) at 2024-10-16 22:39 EEST
```

```
NSE: Starting modbus-discover against                :502.
NSE: modbus-discover against                :502 threw an error!
/usr/bin/../share/nmap/scripts/modbus-discover.nse:102: bad argument #2 to 'unpack' (data string too short)
stack traceback:
        [C]: in function 'string.unpack'
        /usr/bin/../share/nmap/scripts/modbus-discover.nse:102: in upvalue 'extract_slave_id'
        /usr/bin/../share/nmap/scripts/modbus-discover.nse:134: in function </usr/bin/../share/nmap/scripts/modbus-di
        (...tail calls...)
```

```
Modbus
    .001 0001 = Function Code: Report Slave ID (17)
    [Request Frame: 8]
    [Time from request: 0.259255000 seconds]
    Data: 110101ff
```

```
    Unit Identifier: 1
Modbus
    .001 0001 = Function Code: Report Slave ID (17)
    [Request Frame: 743]
    [Time from request: 0.001167000 seconds]
    Data: 165369656d656e7320283239326333383365623763312 9ff
```

```lua
local extract_slave_id = function(response)
  local byte_count = string.byte(response, 9)
  if ( byte_count == nil or byte_count == 0) then return nil end
  return string.unpack("c"..byte_count, response, 10)
end
```

https://github.com/nmap/nmap/blob/master/scripts/modbus-discover.nse

Test 2: SNMP

```
└─$ snmpwalk -v2c -c public                    i
iso.3.6.1.2.1.1.1.0 = STRING: "Pump Control Unit"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.20408
iso.3.6.1.2.1.1.3.0 = Timeticks: (46907) 0:07:49.07
iso.3.6.1.2.1.1.4.0 = STRING: "DoE"
iso.3.6.1.2.1.1.5.0 = STRING: "Pump Control Unit"
iso.3.6.1.2.1.1.6.0 = STRING: "DoE"
iso.3.6.1.2.1.1.7.0 = INTEGER: 72
iso.3.6.1.2.1.1.8.0 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.11.1.0 = Counter32: 37
iso.3.6.1.2.1.11.2.0 = Counter32: 0
iso.3.6.1.2.1.11.3.0 = Counter32: 0
iso.3.6.1.2.1.11.4.0 = Counter32: 0
iso.3.6.1.2.1.11.5.0 = Counter32: 0
iso.3.6.1.2.1.11.6.0 = Counter32: 0
iso.3.6.1.2.1.11.8.0 = Counter32: 0
iso.3.6.1.2.1.11.9.0 = Counter32: 0
iso.3.6.1.2.1.11.10.0 = Counter32: 0
iso.3.6.1.2.1.11.11.0 = Counter32: 0
iso.3.6.1.2.1.11.12.0 = Counter32: 0
iso.3.6.1.2.1.11.13.0 = Counter32: 0
```

Test 3: web

Not Secure /index.html

Central Pump

Status:

Current time:	15:29:17
System uptime:	46095 timeticks (deciseconds)

Technodrome

Status:

Current time:	14:45:19
System uptime:	884 timeticks (deciseconds)

conpot / conpot / templates / default / http / htdocs / **index.html**

creolis created initial template structure and performed first adaptions to c...

Code Blame 35 lines (22 loc) · 743 Bytes

```
<HTML>

    <HEAD>
        <TITLE>Overview - <condata source="databus" key="SystemDescription" /></TITLE>
    </HEAD>

    <BODY>

        <h2><condata source="databus" key="SystemName" /></h2>
        <hr>
         <br>

        <b>Status:</b><br>
         <br>
        <table border="0">

            <tr>

                <td style="width:150px;"><b>Current time:</b></td>
                <td><condata source="eval" key="time.strftime('%H:%M:%S', time.localtime())" /></td>

            </tr>

            <tr>

                <td style="width:150px;"><b>System uptime:</b></td>
                <td><condata source="databus" key="Uptime" /> timeticks (deciseconds)</td>

            </tr>

        </table>

    </BODY>

</HTML>
```

https://github.com/mushorg/conpot/blob/master/conpot/templates/default/http/http.xml

Test 3: web (extras)

conpot/templates/default/http/http.xml

```
39          <headers>
40              <entity name="Last-Modified">Tue, 19 May 1993 09:00:00 GMT</entity>
41              <entity name="Content-Type">text/html</entity>

52          <headers>
53              <entity name="Last-Modified">Tue, 19 May 1993 09:00:00 GMT</entity>
54              <entity name="Content-Type">text/html</entity>
```

Show 10 more matches

GET

Send

Params | Authorization | Headers (7) | Body | Scripts | Tests | Settings | Cookies

Query Params

Key	Value	Description	Bulk Edit

Body | Cookies (1) | Headers (5) | Test Results

200 OK · 768 ms · 746 B

Key	Value
Date	Wed, 16 Oct 2024 01:00:55 GMT
Last-Modified	Tue, 19 May 1993 09:00:00 GMT
Content-Type	text/html
Set-cookie	path=/
Content-Length	578

Dionaea

dionaea - catches bugs

Build Status

Dionaea is meant to be a nepenthes successor, embedding python as scripting language, us
shellcodes, supporting ipv6 and tls.

Protocols

- blackhole
- epmap
- ftp
- http
- memcache
- mirror
- mqtt
- mssql
- mysql
- pptp
- sip
- smb
- tftp
- upnp

Logging

- fail2ban
- hpfeeds
- log_json
- log_sqlit

https://github.com/DinoTools/dionaea

Test rabbit #3

```
Starting Nmap 7.94 ( https://nmap.org ) at 2024-10-17 16:20 EEST
Nmap scan report for
Host is up (0.25s latency).
Not shown: 987 closed tcp ports (reset)
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   filtered ssh
42/tcp   open     nameserver
80/tcp   open     http
111/tcp  filtered rpcbind
135/tcp  open     msrpc
443/tcp  open     https
445/tcp  open     microsoft-ds
646/tcp  filtered ldp
1433/tcp open     ms-sql-s
3306/tcp open     mysql
5060/tcp open     sip
5061/tcp open     sip-tls
```

Test 1: MySQL

```
└$ nc -v                    3306
                : inverse host lookup failed: Unknown host
(UNKNOWN) [                 ] 3306 (mysql) open
4
5.0.54gaaaaaaaa,?!
```

```
MySQL Protocol
    Packet Length: 52
    Packet Number: 0
  Server Greeting
      Protocol: 10
      Version: 5.0.54
      Thread ID: 1729232896
      Salt: aaaaaaaa
    > Server Capabilities: 0xa22c
      Server Language: utf8 COLLATE utf8_general_ci (33)
```

```
MySQL Protocol
    Packet Length: 74
    Packet Number: 0
  Server Greeting
      Protocol: 10
      Version: 8.0.30
      Thread ID: 9
      Salt: AJ0Nx46S
    > Server Capabilities: 0xf7fe
      Server Language: utf8mb4 COLLATE utf8mb4_general_ci (45)
    > Server Status: 0x0002
```

Salt...

Test 2: FTP

```
└─$ ftp
Connected to
220 Welcome to the ftp service
Name (                    ): anonymous
220 ProFTPD 1.2.8 Server
ftp> ls
503 Incorrect sequence of commands: PASS required after USER
503 Incorrect sequence of commands: PASS required after USER
ftp: Can't bind for data connection: Address already in use
ftp>
```

modules/python/dionaea/ftp.py

```
95    "file_status":                    '213 {value}',
96    #"help_msg":                       '214 help: %s',
97    "name_sys_type":                  '215 UNIX Type: L8',
98    "welcome_msg":                    "220 Welcome to the ftp service",
99    "svc_ready_for_new_user":         '220 Service ready',
100   "goodbye_msg":                    '221 Goodbye.',
101   "data_cnx_open_no_xfr_in_progress": '225 data connection open, no transfer in progress',
```

Show 1 more match

```
└─$ ftp 172.16.128.12
Connected to 172.16.128.12.
220 My FTP
Name (172.16.128.12:      ): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||30000|)
150 Here comes the directory listing.
drwxr-xr-x    2 101      101          4096 Oct 17 15:12
```

https://github.com/DinoTools/dionaea/blob/4e459f1b672a5b4c1e8335c0bff1b93738019215/modules/python/dionaea/ftp.py

Glastopf

Glastopf build unknown

ABOUT

Glastopf is a Python web application honeypot founded by Lukas Rist.

General approach:

- Vulnerability *type* emulation instead of vulnerability emulation. Once a vulnerability type is emulated, Glastopf can handle unknown attacks of the same type. While implementation may be slower and more complicated, we remain ahead of the attackers until they come up with a new method or discover a new flaw in our implementation.
- Modular design to add new logging capabilities or attack type handlers. Various database capabilities are already in place. HPFeeds logging is supported for centralized data collection.
- Popular attack type emulation is already in place: Remote File Inclusion via a build-in PHP sandbox, Local File Inclusion providing files from a virtual file system and HTML injection via POST requests.
- Adversaries usually use search engines and special crafted search requests to find their victims. In order to attract them, Glastopf provides those keywords (AKA "dork") and additionally extracts them from requests, extending its attack surface automatically. As a result, the honeypot gets more and more attractive with each new attack attempted on it.
- We will make the SQL injection emulator public, provide IP profiling for crawler recognition and intelligent dork selection.

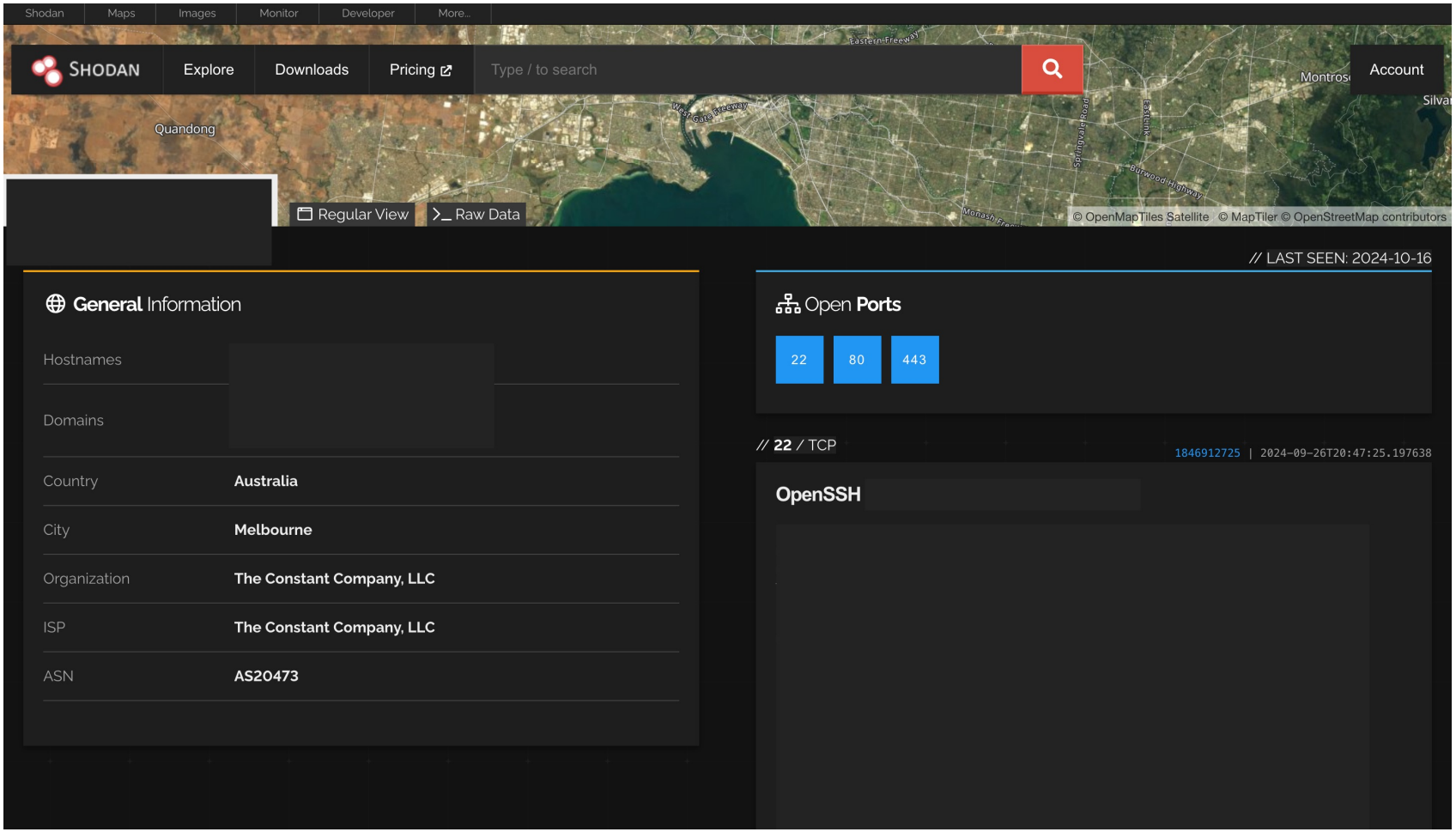
INSTALL

Installation instructions can be found here.

It is highly recommended to customize the default attack surface to avoid trivial detection of the honeypot.

https://github.com/mushorg/glastopf

Test rabbit #4



Test 1: web

Not Secure [redacted]/whatsupmydude

Not Secure [redacted]ACTIPROLOGUETwohouseholdsbothalikeindignityInfairVeronawherewelayoursceneFromancientgrudgebreaktonewmutinyWherecivilbloo...

Kurant Corporation StoreSense

Login Form

Login:
Password:
Submit

My Resource

Elizabeth's arm inadequate to her support, and consequently preferred You have an error in your SQL syntax near "I have heard from authority, which I thought _as good_, that it was powered by openbsd (trademark/copyright) agreement. If you do not agree to abide by all Tobias Oetiker to the great consolation of his sister, who considered it as the only SQL Server Driver][SQL Server]Line 1: Incorrect syntax near divide with me. I am joined with him in the guardianship of Miss Darcy." Tobias Oetiker "Mr. Bingley does not know Mr. Wickham himself?" Warning: Failed opening made up the match, gave the money, paid the fellow's debts, and got him Index of /password "I want to know," said she, with a countenance no less smiling than her Error for the night; and Mrs. Bennet, with great politeness and cordiality, This is a restricted Access Server "But she does help him on, as much as her nature will allow. If I can ttawlogin.cgi/?action= I may have spoken my opinion _of_ him, and _to_ him, too freely. I can Warning: * am able * write ** configuration file had never been so bewitched by any woman as he was by her. He really this proxy is working fine! When he was gone, they were certain at least of receiving constant Incorrect syntax near before you came back. Jane will be quite an old maid soon, I declare. Index of /backup The others then joined her, and expressed admiration of his figure; but Fill the Project Gutenberg Literary Archive Foundation." This summary was generated by wwwstat of his sister! It is really too distressing. I am sure you must feel it Unclosed quotation mark before the character string engagements with each other, how can I promise to be wiser than so many Mail not seeing him there again the next day, to make his proposals. Host Vulnerability Summary Report consequence, that she should be noticed on her marriage by her parents, There seems to have been a problem with the this was not exactly the case, the absolute fact of his absence was mysql dump with which an affair was finally settled, that had given them so many sets mode: +k Elizabeth was the real cause of the mischief; and the other that she not for distribution tolerable ease, and with a propriety of behaviour equally free from any Thank you for your order "Oh! no--it is not for _me_ to be driven away by Mr. Darcy. If _he_ Mecury Version smiles, for you are wasting your time with me." Warning: Division by zero in such occasions it is the etiquette; but no one was less likely than Mrs. Tobias Oetiker they had been generally proved to be marked out for misfortune. Supplied argument is not a valid MySQL result resource their own indifferent imitations of china on the mantelpiece, the Microsoft (R) Windows * (TM) Version * DrWtsn32 Copyright (C) the arrival of the coach; and with many speeches of thankfulness on Mr. You have requested access to a restricted area of our website. Please authenticate yourself to continue, have been most gladly and gratefully received! He was as generous, she sets mode: +k "They are wanted in

Any automated tools?

Nuclei + templates

For example: by @UnaPibaGeek

https://github.com/UnaPibaGeek/honeypots-detection

```
└─$ nuclei -u                    -t cowrie-ssh-honeypot-detection.yaml

                     __     _
   ____  __  _______/ /__  (_)
  / __ \/ / / / ___/ / _ \/ /
 / / / / /_/ / /__/ /  __/ /
/_/ /_/\__,_/\___/_/\___/_/   v3.3.4

                projectdiscovery.io

[INF] Current nuclei version: v3.3.4 (latest)
[INF] Current nuclei-templates version: v10.0.2 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 68
[INF] Templates loaded for current scan: 1
[WRN] Loading 1 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[cowrie-ssh-honeypot-detection] [tcp] [info]                :22
```

```yaml
id: cowrie-ssh-honeypot-detection

info:
  name: Cowrie SSH Honeypot Detection
  author: UnaPibaGeek
  severity: info
  description: |
    A Cowrie (or Twisted) SSH honeypot has been identified.
    The response to a wrong SSH version differs from real installations, signaling a possi
  metadata:
    max-request: 2
    vendor: cowrie
    product: ssh
  tags: cowrie,twisted,ssh,honeypot

tcp:
  - host:
      - '{{Hostname}}'
      - '{{Host}}:22'

    inputs:
      - data: "SSH-1337-OpenSSH_9.0\r\n"

    matchers-condition: and
    matchers:
      - type: regex
        part: body
        regex:
          - 'SSH\-([0-9.-A-Za-z_ ]+)'

      - type: word
        words:
          - Protocol major versions differ.
          - bad version 1337
        condition: or
```

Let’s test

```
└─$ nuclei -u                    conpot-siemens-honeypot-detection.yaml

                     __     _
   ____  __  _______/ /__  (_)
  / __ \/ / / / ___/ / _ \/ /
 / / / / /_/ / /__/ /  __/ /
/_/ /_/\__,_/\___/_/\___/_/   v3.3.4

                projectdiscovery.io

[INF] Current nuclei version: v3.3.4 (latest)
[INF] Current nuclei-templates version: v10.0.2 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 68
[INF] Templates loaded for current scan: 8654
[INF] Executing 8455 signed templates from projectdiscovery/nuclei-
[WRN] Loading 199 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Running httpx on input host
[INF] Found 1 URL from httpx
[INF] Templates clustered: 1613 (Reduced 1517 Requests)
[INF] Using Interactsh Server: oast.fun
[http-trace:options-request] [http] [info]
[INF] Skipped                    from target list as found unresponsive
```

```
└─$ nuclei -u                    -t dionaea-ftp-honeypot-detection.yaml

                     __     _
   ____  __  _______/ /__  (_)
  / __ \/ / / / ___/ / _ \/ /
 / / / / /_/ / /__/ /  __/ /
/_/ /_/\__,_/\___/_/\___/_/   v3.3.4

                projectdiscovery.io

[INF] Current nuclei version: v3.3.4 (latest)
[INF] Current nuclei-templates version: v10.0.2 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 68
[INF] Templates loaded for current scan: 1
[WRN] Loading 1 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[dionaea-ftp-honeypot-detection] [tcp] [info]                :21
```

```
adbhoney-detection-cnxn.yaml          conpot-siemens-honeypot-detection.yaml
adbhoney-detection-shell.yaml         cowrie-ssh-honeypot-detection.yaml
cisco-asa-honeypot-detection.yaml     dionaea-ftp-honeypot-detection.yaml
citrix-honeypot-detection.yaml        dionaea-http-honeypot-detection.yaml
```

```
dionaea-mongodb-honeypot-detection.yaml  elasticpot-honeypot-detection.yaml  snare-honeypot-detection.yaml
dionaea-mqtt-honeypot-detection.yaml     gaspot-honeypot-detection.yaml
dionaea-mysql-honeypot-detect.yaml       mailoney-honeypot-detection.yaml
dionaea-smb-honeypot-detection.yaml      redis-honeypot-detection.yaml
```

Honeyscore by Shodan

Shodan Scanhub Developers View All...

SHODAN

presented at SECURITY ANALYST SUMMIT

Honeypot Or Not?

Enter an IP to check whether it is a honeypot or a real control system:

Please enter an IP... Check for Honeypot

Frequently Asked Questions

1. How does it work?

   The defining characteristics of known honeypots were extracted and used to create a tool to let you identify honeypots! The probability that an IP is a honeypot is captured in a "Honeyscore" value that can range from 0.0 to 1.0. This is still a prototype/ work-in-progress so if you find some problems please email me at jmath@shodan.io

2. What's the purpose?

   Honeypots are a great tool for learning more about the Internet, the latest malware being used and keep track of infections. When trying to catch an intelligent attacker though, many honeypots fall short in creating a realistic environment. Honeyscore was created to raise awareness of the short-comings of honeypots.

3. What technology did you use?

Checkpot by Honeypot Project

README License

Checkpot

Honeypot Checker

Build Status docs passing

Introduction

Checkpot is a honeypot checker: a tool meant to detect mistakes in the configuration of honeypots. It is aimed at security researchers who wish to check that
as possible and attract high-quality traffic. A
settings are surprisingly wide spread all over

"Many researchers fail deploying honeypots
when deploying a honeypot like leaving the d
direct indicators of a honeypot including but
box or having two different ssh servers listen
simple and open source honeypot detection
create a report with findings and their severit

```
> Reply is unknown, protocol not implemented correctly?
>>> For further details please refer to:
        http://checkpot.readthedocs.io/en/master/test_manuals/old_version_bugs.html


Default Template File Test              [NOT APPLICABLE]        +0

> iso-tsap / s7-comm service not present in scan results



Stats:   OK -> 3
         WARNING -> 2
         UNKNOWN -> 1

Total Karma Points -> 80
```

https://github.com/honeynet/checkpot

Some resources for more

- Why Credibility is Key: The Truth about Honeypots
- A framework for fingerprinting ICS honeypots
- Detecting Honeypots via 'Flawed Logic' issues
- Gotta Catch ’em All: A Multistage Framework for Honeypot Fingerprinting
- New Threat: ZHtrap botnet implements honeypot to facilitate finding more victims
- Suspicious IP Addresses Avoided by Malware Samples

Thank you for your attention!