UNIVERSITY OF CAMBRIDGE

Counting Outdated Honeypots: Legal and Useful

Alexander Vetterl*, Richard Clayton* and Ian Walden‡

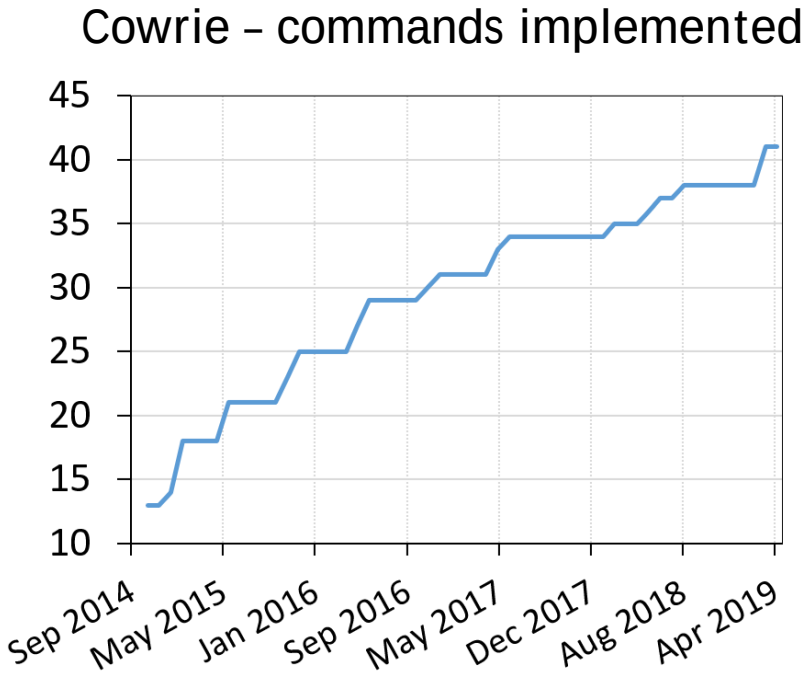
*University of Cambridge, ‡Queen Mary University of London

4th International Workshop on Traffic Measurements for Cybersecurity — May 23, 2019

Introduction

Honeypot:
A resource whose value is being attacked or compromised

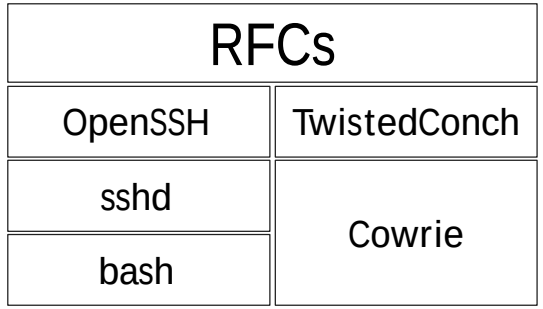
- Honeypots have been focused for years on the monitoring of human activity
- Adversaries attempt to distinguish honeypots by executing commands
- Honeypots continuously fix commands to be “more like bash”



How we currently build SSH honeypots

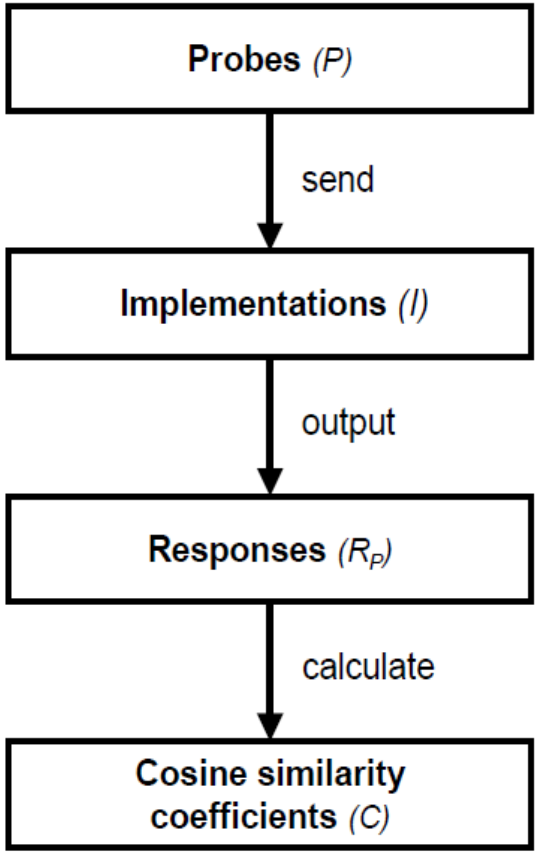
1. Find a library that implements the desired protocol (e.g. TwistedConch for SSH)
2. Write the Python program to be “just like bash”
3. Fix identity strings, error messages etc. to be “just like OpenSSH”

```
def _unsupportedVersionReceived(self, remoteVersion):
    """
    Change message to be like OpenSSH
    """
    self.transport.write(b'Protocol major versions differ.\n')
```



<u>Problem:</u>
There are lot of subtle differences between TwistedConch and OpenSSH…

Fingerprinting honeypots at internet scale



We send probes to various different implementations

- SSH honeypots (Cowrie/Kippo)
- OpenSSH, TwistedConch

We find 'the' probe that results in the most distinctive response across all implementations and perform Internet wide scans

	Date	#ACKs	Sum	Kippo	Cowrie
Scan 1 (SSH)	2017-09	18,196k	2844	906	1938
Scan 2 (SSH)	2018-01	20,586k	2779	758	2021

Login to get more details, but…

Alexander Vetterl and Richard Clayton, "Bitter Harvest: Systematically Fingerprinting Low- and Medium-interaction Honeypots at Internet Scale," in 12th USENIX Workshop on Offensive Technologies (WOOT '18). USENIX Association, Baltimore, USA

Paper was rejected due to ethical concerns

"This paper was rejected due to ethical concerns.

[...]

It was pointed out that these attempts are likely a **violation of US law**, especially the Computer Fraud and Abuse Act which prohibits accessing a computer without authorization.

The PC recommends to consult with a lawyer before trying to publish this paper a different venue."

Summary of the PC discussion

Uniformed legislation for unauthorised access

Convention on Cybercrime (“Budapest Convention”)

- States must have laws that forbit access ‘without right’
- Ratified by 62 states

EU Directive 2013/40/EU Article 3

- ‘Member states [...] shall ensure that, when committed intentionally, the **access without right**, [...] is punishable as a criminal offence where committed by infringing a security measure, at least for **cases which are not minor**.’

Legislation in the UK and USA

UK: Computer Misuse Act 1990

Access of any kind by any person to any program or data held in a computer is unauthorised if –

a) *[…]*

b) he does not have consent to access by him of **the kind in question** to the program or data.

USA: Fraud and Abuse Act 1986

'Whoever […] intentionally accesses a computer **without authorization** […] and thereby obtains […] information from any protected computer.'

Factors to consider

- No consent to access [by him] of the 'kind in question'
- Overcome some form of security mechanism
- Offences which are not minor

Legislation in the context of honeypots

In general much authorisation is implicit

- Devices and services intentionally connected to the Internet
- Web servers/ftp servers with the username ‘anonymous’ and email address as password

Our access was not unauthorised because the controller of the honeypot has –

- intentionally made available a (vulnerable) system and
- implicitly permits the access of the ‘kind of question’

Ethical considerations

- We followed our institution's ethical research policy
- We used the exclusion list maintained by DNS-OARC
- We notified all local CERTs of our scans/actions
- We respected requests to be excluded from further scanning
- We started and ended every SSH session with an explanation
- We notified the relevant honeypot and library developers of our findings

Results – Authentication configuration (1/2)

- We used the username root and initially 6 passwords, later 500 passwords
- We managed to successfully log in to about 70% of the honeypots

Outcome	6 passwords Scan 1: 2017-03		500 passwords Scan 1: 2017-03	
successful login	859	(70.9%)	794	(65.5%)
all passwords failed	110	(9.1%)	136	(11.2%)
connection timed out	49	(4.0%)	110	(9.1%)
other errors	194	(16.0%)	172	(14.2%)

Results – Authentication configuration (2/2)

- Using 500 passwords is not better than 6 passwords
- About 11% of honeypot operators do not allow logins

Outcome	500 passwords Scan 2: 2017-06		500 passwords Scan 3: 2017-09		500 passwords Scan 4: 2018-01	
successful login	1165	(66.7%)	1347	(69.5%)	1578	(78.1%)
all passwords failed	187	(10.7%)	195	(10.1%)	223	(11.0%)
connection timed out	41	(2.4%)	43	(2.2%)	7	(0.3%)
other errors	354	(20.2%)	353	(18.2%)	213	(10.6%)

Revision history for command selection

— We looked for commands in the revision history (uname -a, tftp)

Cowrie < 2016-11-02

```
root@svr04:~# tftp
-bash: tftp: command not found
root@svr04:~#
```

Cowrie ≥ 2016-11-02

```
root@svr04:~# tftp
usage: tftp [-h] [-c C C] [-l L] [-g G] [-p P] [-r R] [hostname]
root@svr04:~#
```

Results – Counting outdated honeypots (1/2)

- High market share for Kippo, which had last been updated years earlier
- Only ~25% of honeypots were up-to-date

	Scan 1: 2017-03		Scan 2: 2017-06	
Kippo $<$ 2014-05-28	1384	(42.5%)	1519	(42.8%)
Kippo $<$ 2015-05-24	659	(20.3%)	285	(8.0%)
Cowrie $<$ 2016-09-05	385	(11.8%)	392	(11.0%)
Cowrie $<$ 2016-11-02	—	—	556	(15.7%)
Cowrie $<$ 2017-06-06	—	—	—	—
Cowrie $\leq$ date of scan	827	(25.4%)	799	(22.5%)
Total	3255		3551	

Results – Counting outdated honeypots (2/2)

- The number of SSH honeypots is slightly declining (-14.6%)
- Kippo is slowly being replaced by Cowrie

	Scan 3: 2017-09		Scan 4: 2018-01	
Kippo $<$ 2014-05-28	695	(24.4%)	546	(19.6%) ⬇
Kippo $<$ 2015-05-24	211	(7.4%)	212	(7.6%)
Cowrie $<$ 2016-09-05	134	(4.7%)	147	(5.3%)
Cowrie $<$ 2016-11-02	360	(12.7%)	422	(15.2%)
Cowrie $<$ 2017-06-06	734	(25.8%)	381	(13.7%)
Cowrie $\leq$ date of scan	710	(25.0%)	1071	(38.6%) ⬆
Total	2844		2779	

Results - Set-up options

SSH Version strings

- 61 different version strings
- 72% use the default - `SSH-2.0-OpenSSH_6.0p1 Debian-4+deb7u2`

Hostname (`uname -a`)

- 3.3% use the default - `svr04`
- `debnfwmgmt-02` is used for 296 honeypots (14.6%)
  - This is the default hostname for Cowrie when it is used in T-Pot
  - T-Pot is a popular docker container and combines 16 honeypots
  - T-Pot has a significant market share

Conclusion

Many honeypots are outdated and not looked after

- Update your honeypots!

Honeypot operators do not change default configurations

- Usernames/passwords, hostnames, SSH version strings etc.

Our access to honeypots was not unauthorized

- Detailed legal analysis to enable more research in this area
- Lessons learned: Provide not only an ethical justification, but also some legal analysis

Q & A

Alexander Vetterl

alexander.vetterl@cl.cam.ac.uk