Under the Hoodie

Actionable Research from Penetration Testing Engagements

RAPID7

Webcast
NEXPOSE
Customer Testimonial
Download Nexpose Enterprise (US)
Trial
Best Practice Framework for
Vulnerability Prioritization

RAPID7

Gain the clarity, command, and confidence to embrace innovation and drive your business forward. Rapid7 transforms your data and uncertainty into answers.

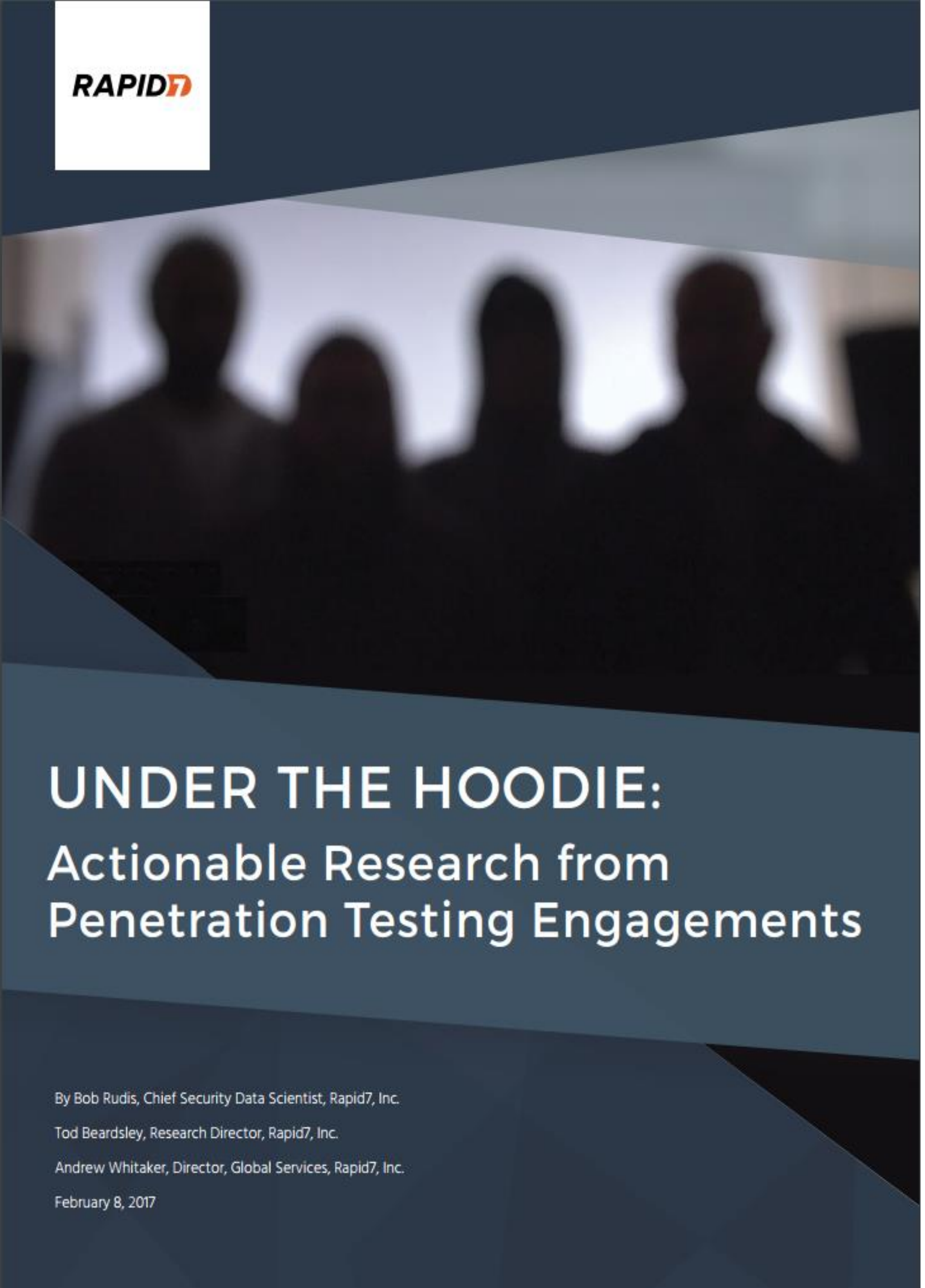
We can help you with...

- Vulnerability Management
- SIEM
- Application Security
- IT Operations
- User Behavior Analytics
- Penetration Testing
- Managed Services
- Security Advisory Services

Under the Hoodie

Tod Beardsley, Director of Research

RAPID7



RAPID7

UNDER THE HOODIE:

Actionable Research from Penetration Testing Engagements

By Bob Rudis, Chief Security Data Scientist, Rapid7, Inc.
Tod Beardsley, Research Director, Rapid7, Inc.
Andrew Whitaker, Director, Global Services, Rapid7, Inc.

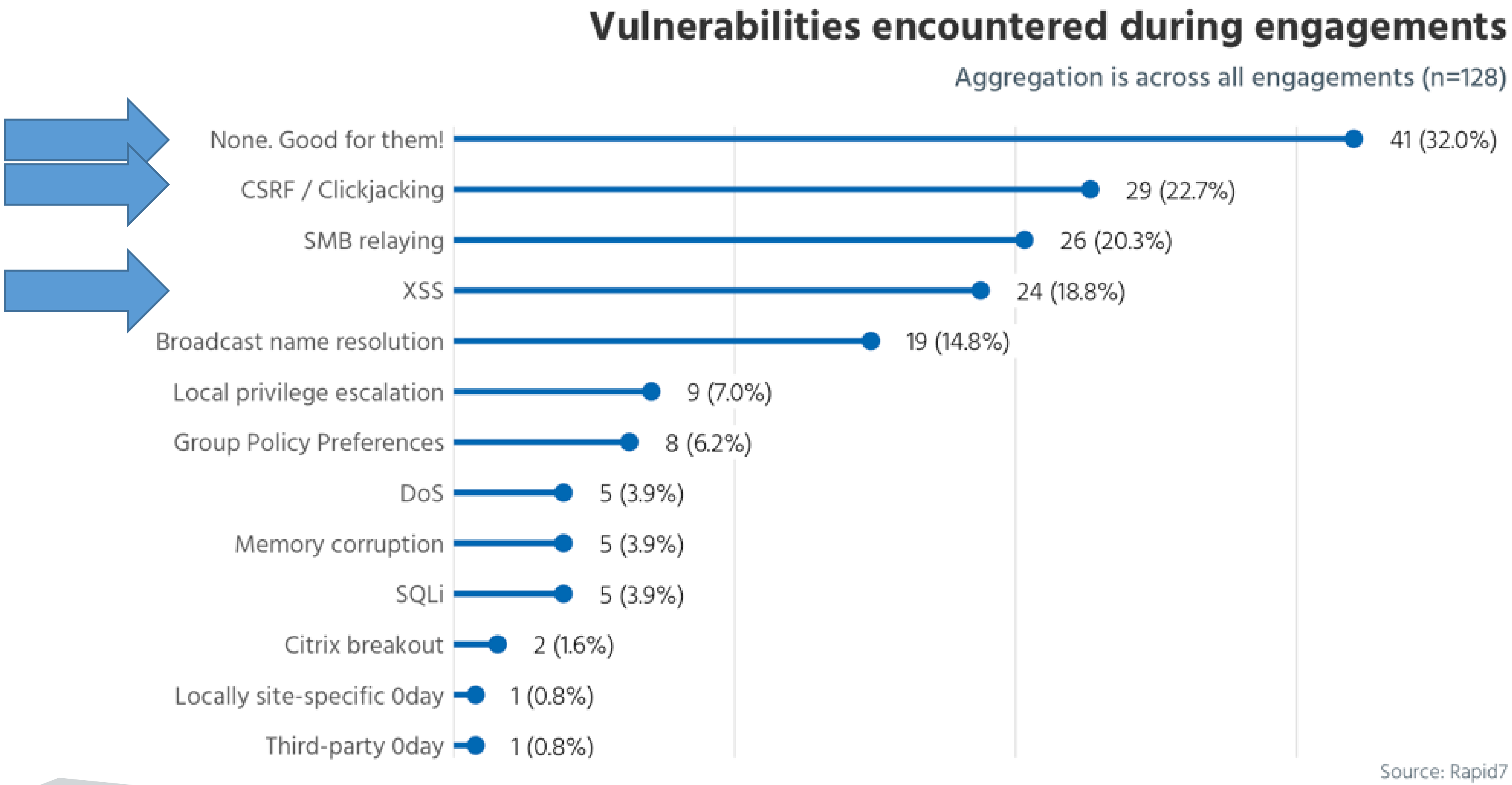
February 8, 2017

Penetration testing is routine, but occult.

- $ whoami # -> Tod Beardsley aka @todb
- https://rapid7.com/info/under-the-hoodie

Vulnerabilities and Misconfigurations

2/3rds of engagements resulted in vulnerabilities being exploited.



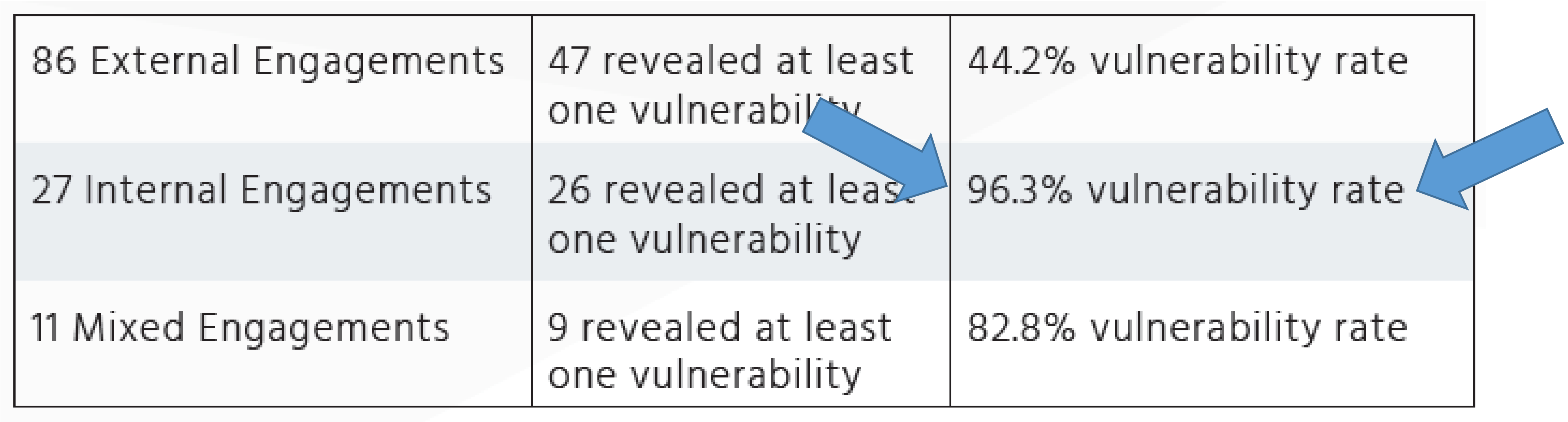
Vulnerabilities encountered during engagements

Aggregation is across all engagements (n=128)

Source: Rapid7

Internal versus external

Internal engagements, as one might expect, is full of appealing targets.



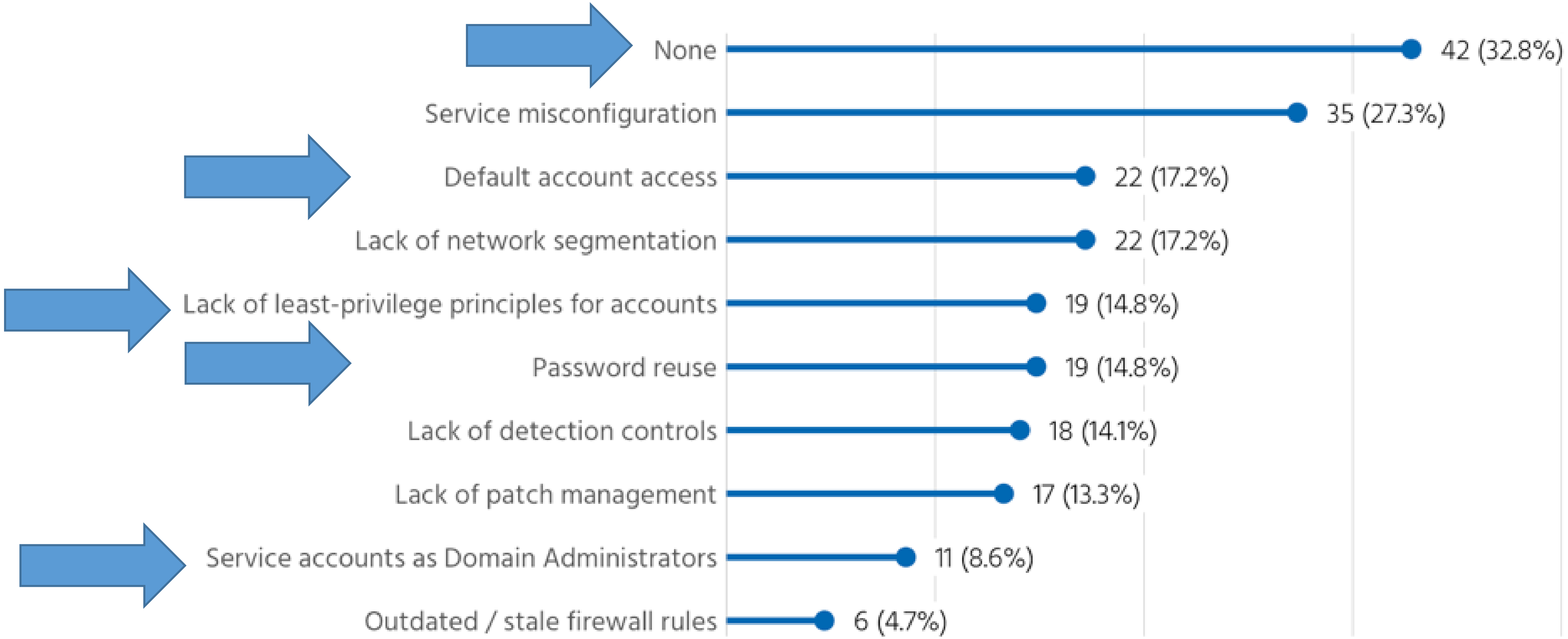
86 External Engagements	47 revealed at least one vulnerability	44.2% vulnerability rate
27 Internal Engagements	26 revealed at least one vulnerability	96.3% vulnerability rate
11 Mixed Engagements	9 revealed at least one vulnerability	82.8% vulnerability rate

About a third of the sampled engagements had an internal component.

2/3rds of engagements also uncovered network and service misconfigurations

Misconfigurations leveraged per engagement

Aggregation is across all engagements (n=128)



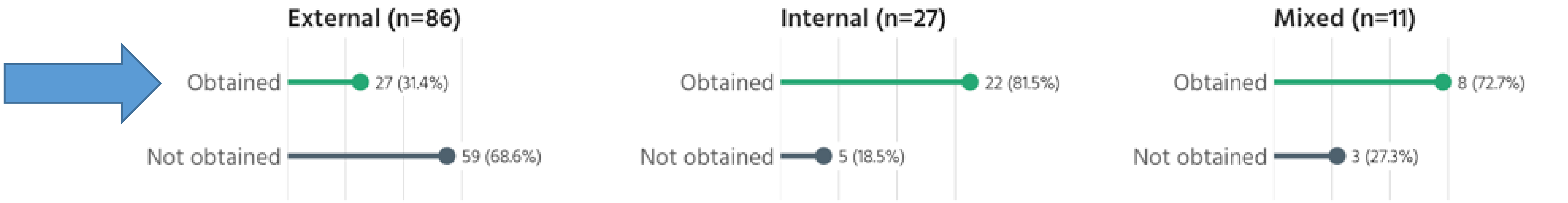
Source: Rapid7

Credentials

About 80% of internal assessments result in a credential theft.

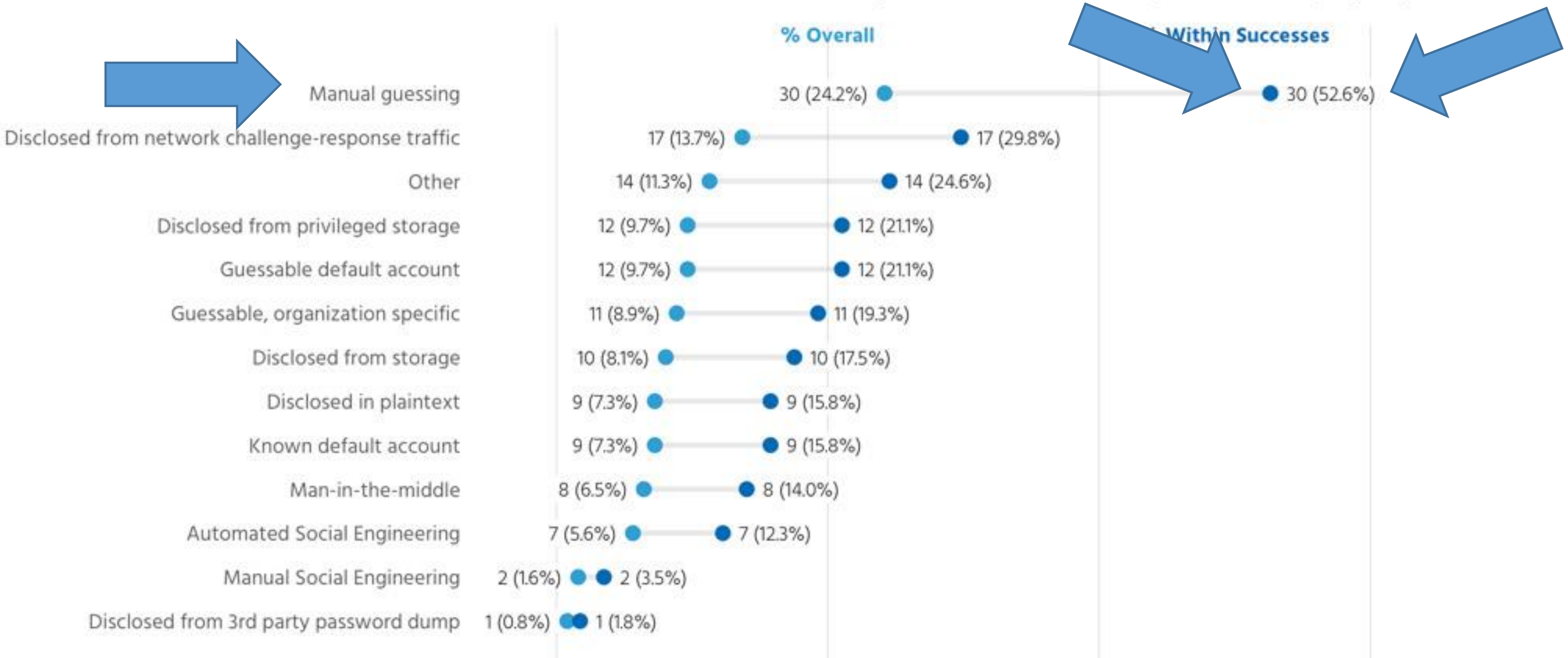
Credential capture success rates by engagement scope

Internal assessments clearly result in greater credential capture rates



Source: Rapid7

Humans: still pretty bad at passwords.



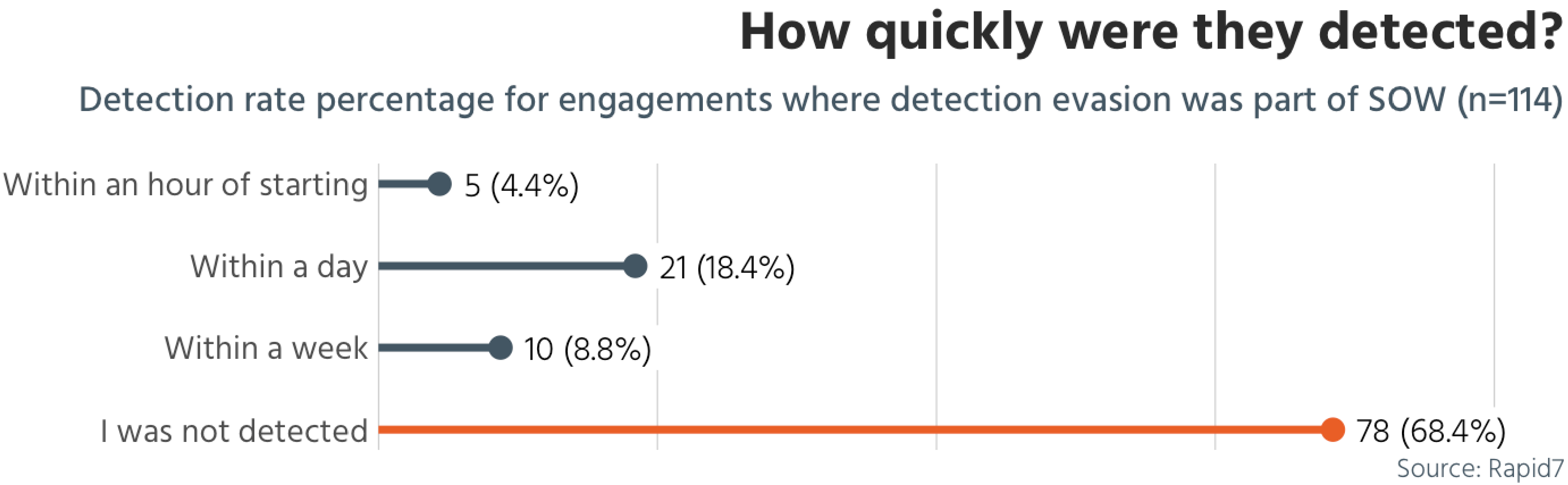
Ways passwords were discerned

This chart compares the rate across all in-scope assessments on the left (n=124) and the rate within just successful username captures on the right (n=57)

Winter2017!

Detection

2/3rds of pentesters remained undetected



Source: Rapid7

This is not good.

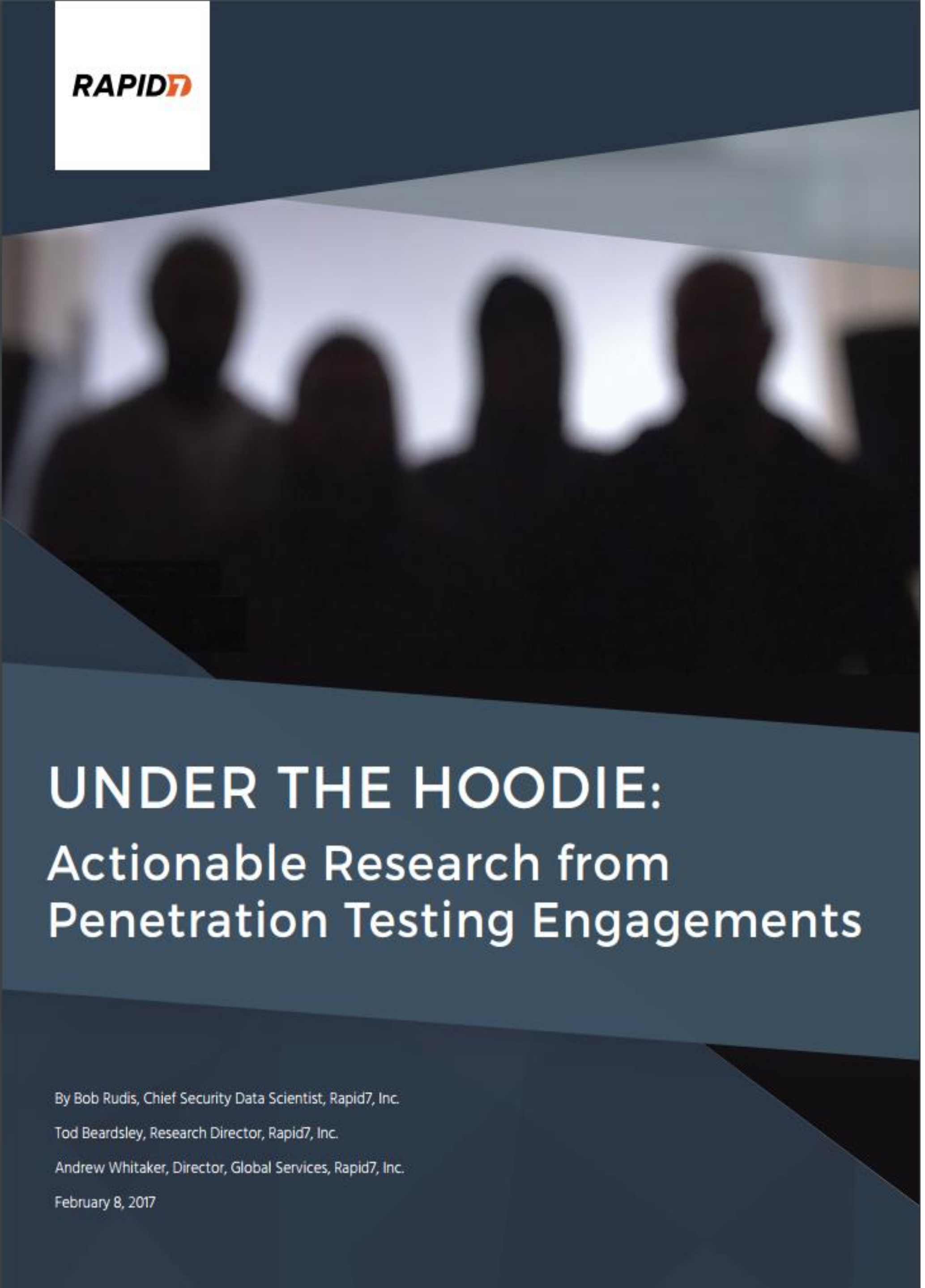
Why?

It’s not like pentesters are stealthy ninjas.

Pentesters are pretty obvious.

Detection is everything.

InsightIDR



UNDER THE HOODIE:

Actionable Research from Penetration Testing Engagements

By Bob Rudis, Chief Security Data Scientist, Rapid7, Inc.
Tod Beardsley, Research Director, Rapid7, Inc.
Andrew Whitaker, Director, Global Services, Rapid7, Inc.
February 8, 2017

Tons more to learn!

- Fun sidebar stories of pentesting in action
- Differences between industries, company size, pentest frequency, loads of juicy stats!
- “Ask a Pentester!” with Leon Johnson
- https://rapid7.com/info/under-the-hoodie