RAPID7

Hunting the White Whale

Andrew Whitaker

Sr. Manager, Global Services Penetration Testing

April, 2016

Punk in training

What stopped me was not a sophisticated lock, a high fence, or a gated community. What stopped me was the risk of getting caught.

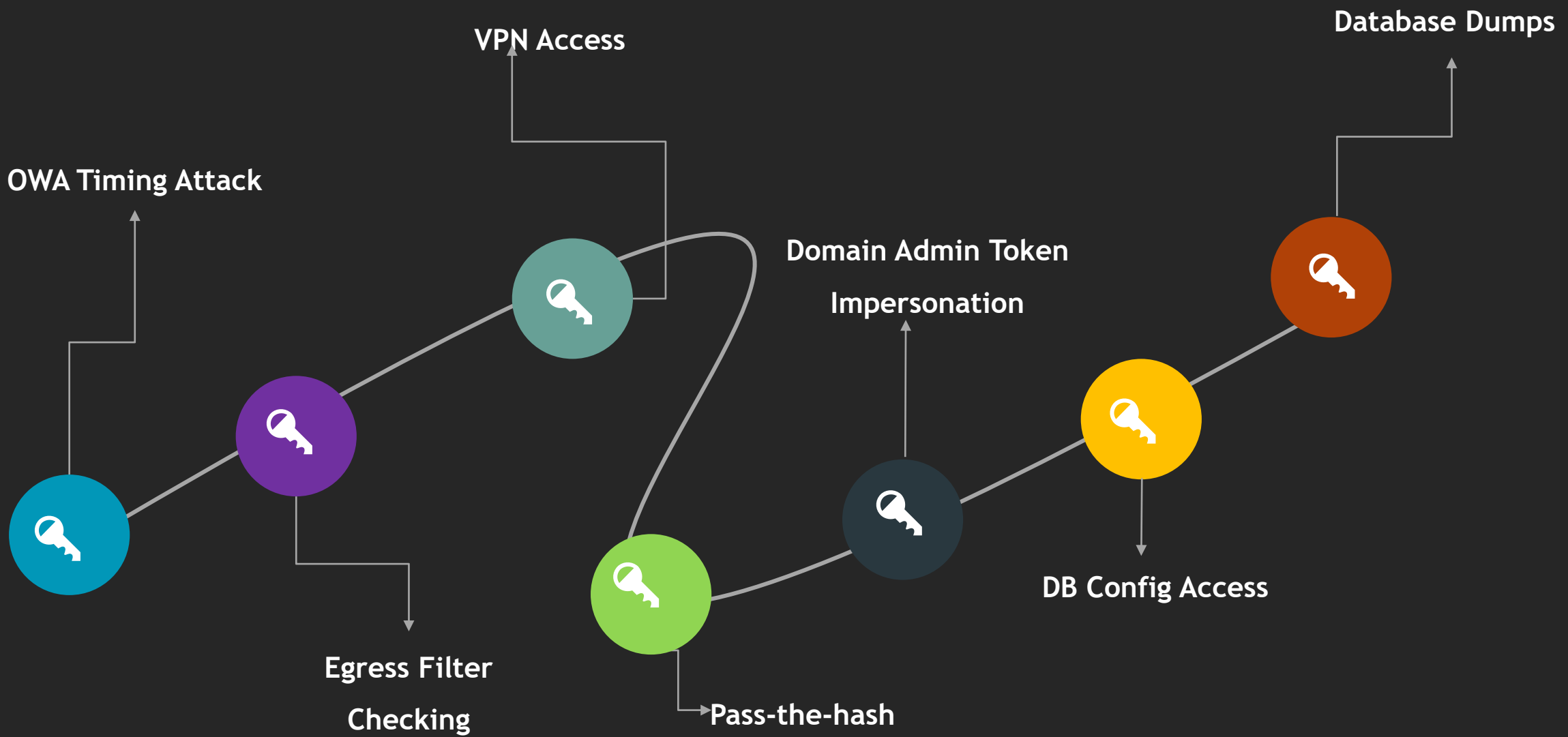
Fast forward a few years

Professional Hacker

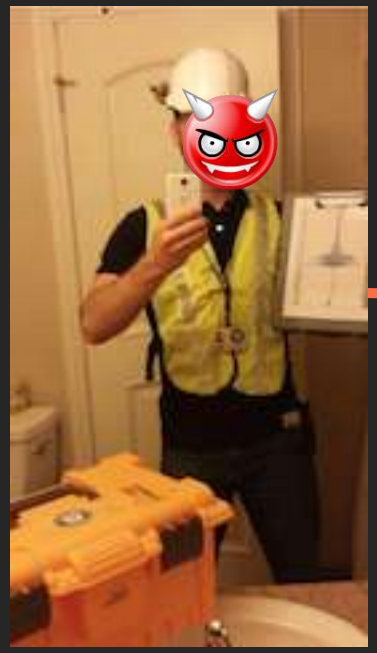
With a big antenna

How are we compromising networks today?

War Stories


VPN Access
Database Dumps
OWA Timing Attack
Domain Admin Token
Impersonation
Egress Filter
Checking
Pass-the-hash
DB Config Access

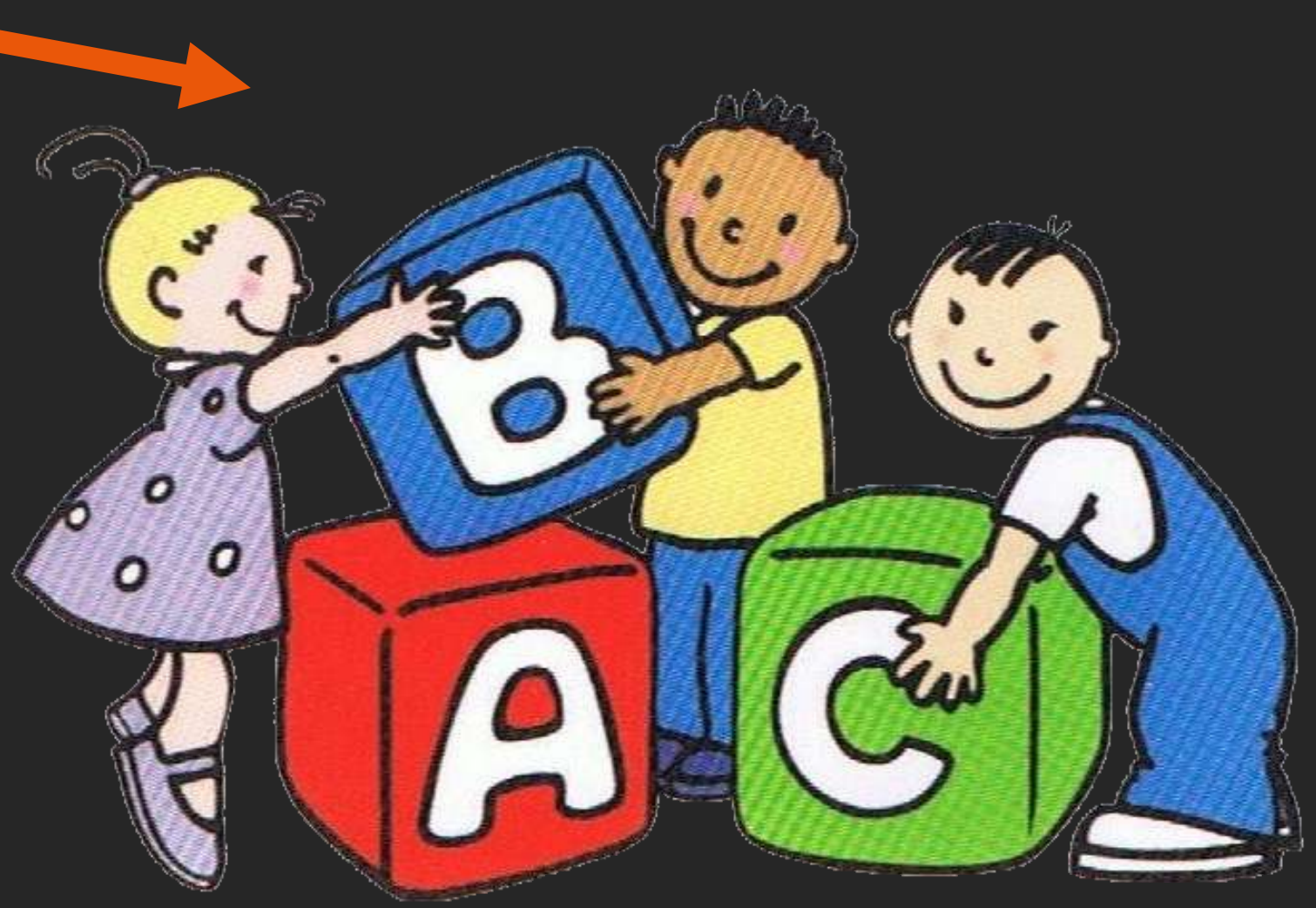
RAPID7



RAPID7


OPEN
CLEAR

Pwned



RAPID7

96% of companies fail phishing campaigns

Of those that fail, 28% of users will give up credentials when asked

93% of companies have exploitable vulnerabilities.

On average, an attacker can get sensitive data in just a few minutes. An attacker can obtain domain admin privileges in less than an hour.

80% of companies have cryptographic and configuration flaws with their digital certificates.

64% of companies are susceptible to NULL session enumeration.

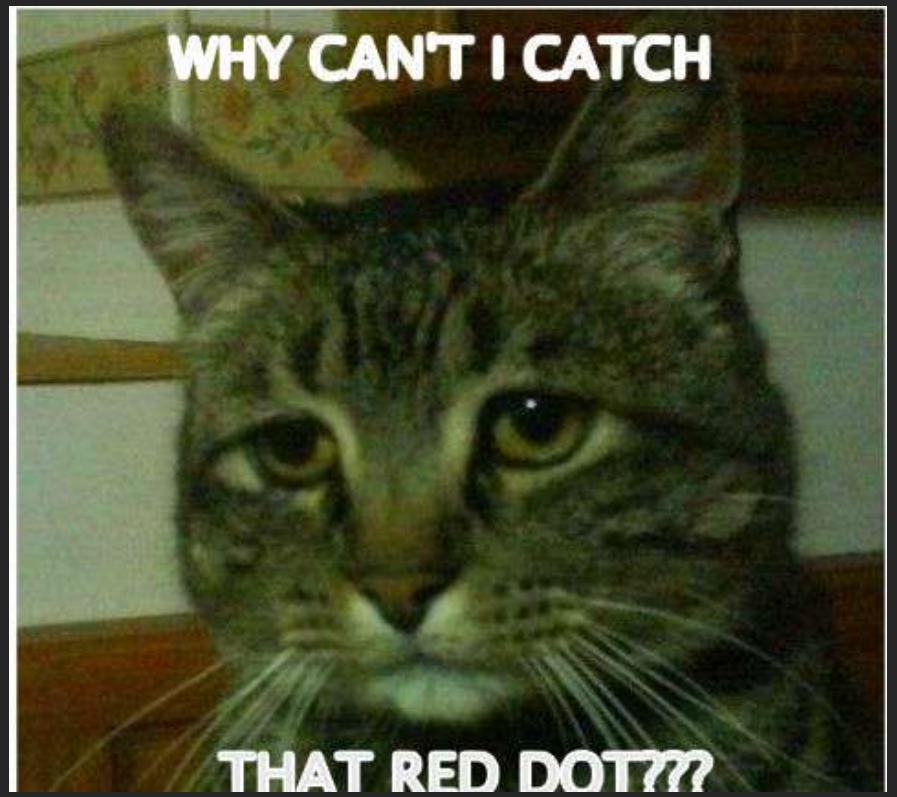
41% of companies are using weak or default SNMP community strings.

59% of companies have technologies using default passwords.

1 out of 10 public facing websites can be hacked using SQL injection.

73% of companies are vulnerable to session hijacking via Cross-Site Scripting.

Depressed yet?



“Everybody has a plan until they get punched in the face”.

Emerging Threat Landscape

10 Years Ago

- “It’s not a matter of if you are going to be hacked, it’s a matter of when.”

Today

- “You’re being hacked.”

Emerging Threat Landscape

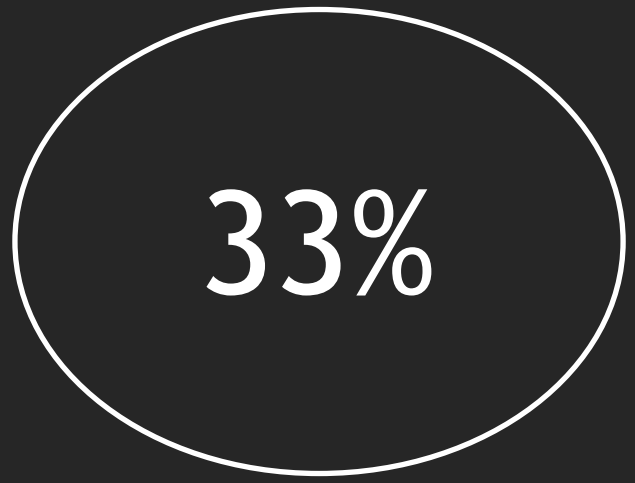
10 Years Ago

- Black market focused on financial data

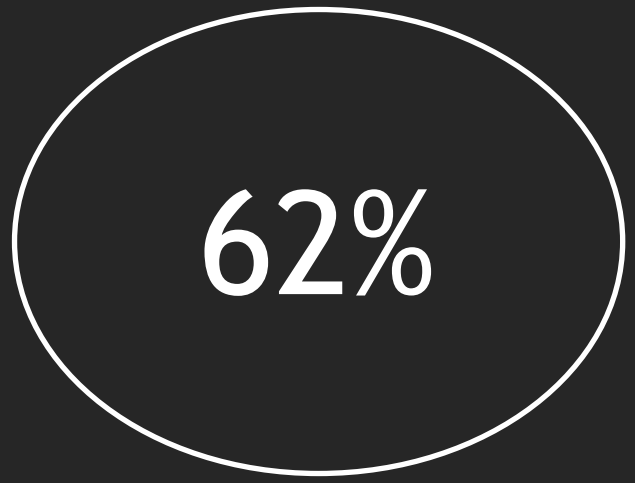
Today

- Black market focused on financial data, PII, PHI, computing resources, intellectual property, brand destruction, doxing

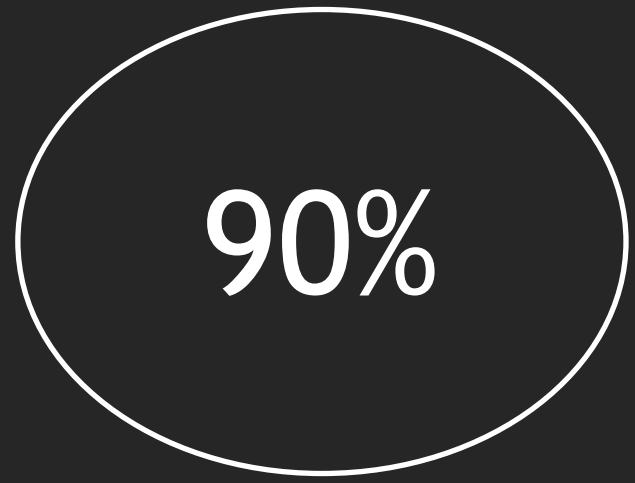
The Challenge



33% of all reported incidents take more than a month and up to a year to discover.
-Verizon Data Breach Report



62% of all organizations are receiving more alerts than they can handle.
- Rapid7 2015 IDR Survey



90% of malware samples are unique to an organization, making signature based endpoint solutions no longer effective.
-Verizon Data Breach Report


WANT TO KNOW A
SECRET?

We use existing processes, channels, and accounts to compromise your network.

Verizon Data Breach Report

Compromised credentials were the most common way for attackers to breach a network in 2013-2014.

The next most common attack vectors were targeted malware and phishing.

71% of attacks and breaches involved compromised end-user devices.

Incident Detection and Response Today

- Organizations are recognizing that they must evolve their detection and response capabilities to combat these threats.

- Rapid7's IDR survey showed that 44% of companies would be spending more in 2016 on IDR than they had in 2015.

- Gartner predicts that by 2020, 60% of enterprise infosec budgets will be allocated to rapid detection and response approaches.

Implementing Detection and Response is proactive, not reactive.

Mature IDR Programs

- Quick Response – you can’t afford to wait 200+ days
- Eliminate the noise – focus on alerts that matter
- Adaptable – look for deviations
- Deception – traps and distractions
- Endpoint and Behavior Analysis – watch what the hackers watch
- Rehearsal drills – tabletop exercises, red team/blue team penetration tests

The Attacker's Perspective

No other mechanism has been more effective at stopping our attacks during penetration tests than intelligent, rapid, endpoint detection and response.

Hunting the “White Whale”

“I know not all that may be coming, but be it what it will, I’ll go to it laughing.”

Herman Melville

Moby Dick

In Conclusion