RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

CHANGE

Challenge today's security thinking

SESSION ID: SPO-R05B

Security Issues that deserve a logo

Gavin Millard

EMEA Technical Director
Tenable
@gmillard

New Threats Discovered Every Day

HEARTBLEED

90M

network devices vulnerable

SHELLSHOCK

70%

of all Internet-facing machines exposed

STAGEFRIGHT

Billion

Android devices possibly affected by major flaw in Media Library

GHOST

Almost every Linux system vulnerable due to glibc flaw

FLASH

Multiple zero days leveraged by exploit kits

SCADA

Numerous remote code execution vulnerabilities discovered

WINDOWS

Numerous remote code execution vulnerabilities discovered

LOGOS LEAD TO
KNEE JERK REACTIONS
NOT IMPROVEMENTS

tenable®

The biggest issue we face in security today isn't

APT

IT'S APATHY

Many Old Issues Still Linger

GLIMPSE

Lack of visibility due to large compound annual growth rates

INVADER

Inability to identify attack path to defend against breach

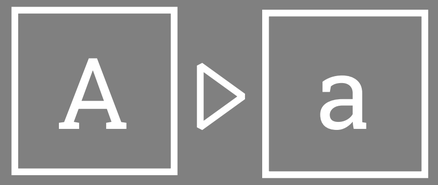
STUTTER

Communication failure between security staff and the business

BANDIT

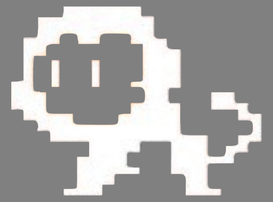
Buying expensive bandaids for massive bullet holes

ROT26



Data is not encrypted... Why is the data not encrypted?!

SHAKESPEARE



Given a few tries, a chimp banging on a keyboard would guess your password

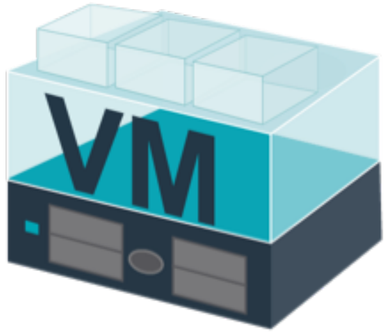
GLIMPSE

Lack of visibility due to large compound annual growth rates

MOST ORGANISATIONS LACK VISIBILITY

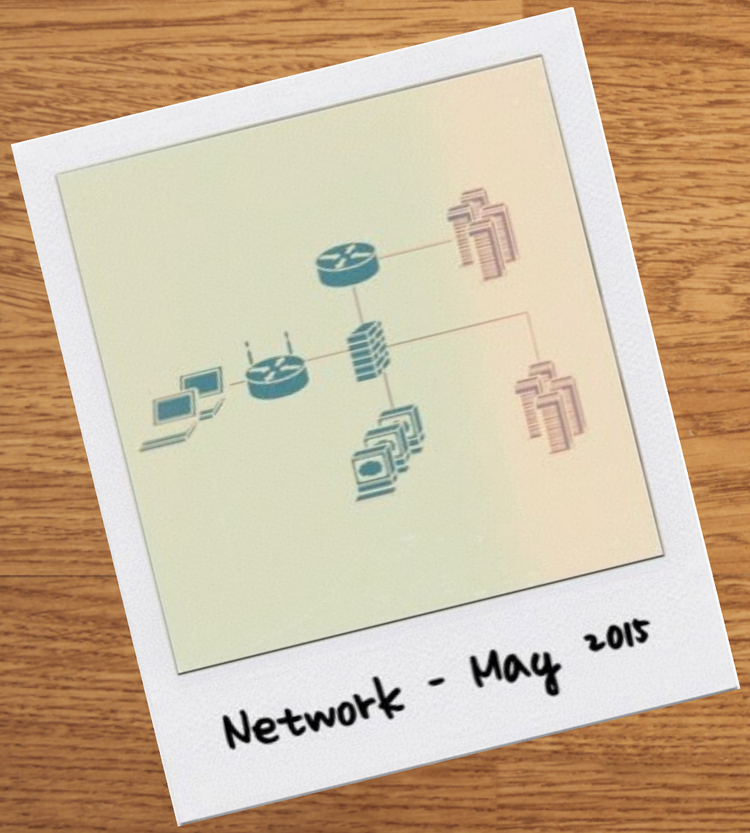
tenable®

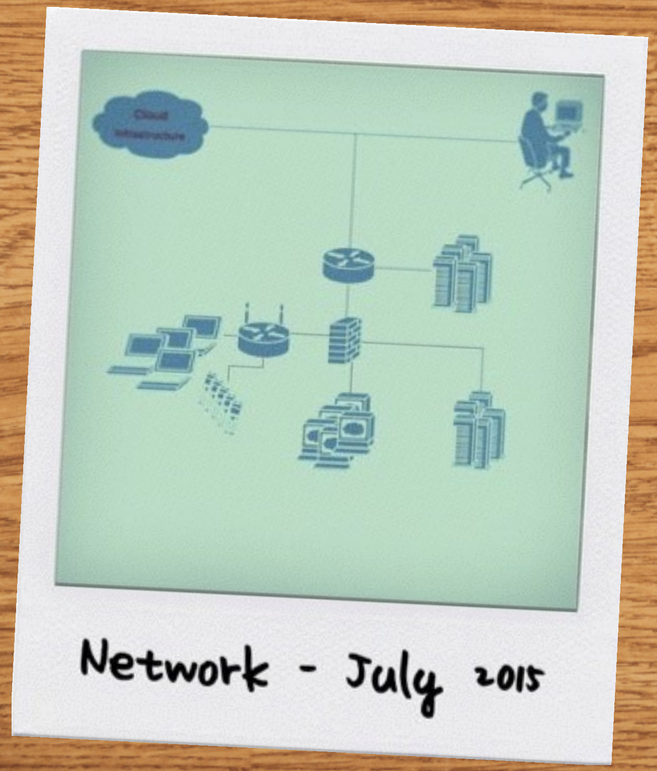
RSA® Conference 2015
Abu Dhabi


VM

EMBRACE OR BE CIRCUMVENTED

Using a 20th Century approach to try and fix a 21st Century problem





SNAPSHOTS ARE NOT ENOUGH

1

What assets, data and vulnerabilities reside on the network?

GLIMPSE

Lack of visibility due to large compound annual growth rates

INVADER

Inability to identify attack path to defend against breach

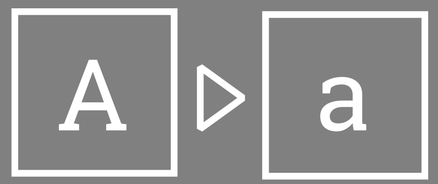
STUTTER

Communication failure between security staff and the business

BANDIT

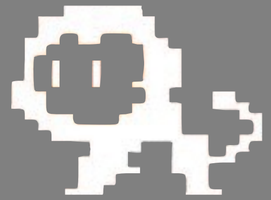
Buying expensive bandaids for massive bullet holes

ROT26



Data is not encrypted… Why is the data not encrypted?!

SHAKESPEARE



Given a few tries, a chimp banging on a keyboard would guess your password

BANDIT

Buying expensive bandaids for massive bullet holes

The Almighty Security Vendors Will Save Us!


Security isn’t about spending a portion of the annual budget on tools - it’s about doing the right activities to reduce risk

PRACTICE THE FUNDAMENTALS FIRST

tenable®

RSA Conference 2015
Abu Dhabi

2

What controls need to be implemented to continuously protect and monitor the assets?

tenable®

RSA® Conference 2015
Abu Dhabi

GLIMPSE

Lack of visibility due to large compound annual growth rates

INVADER

Inability to identify attack path to defend against breach

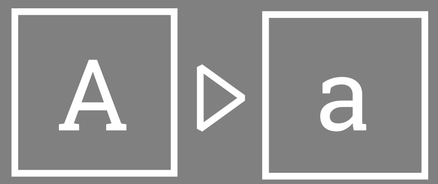
STUTTER

Communication failure between security staff and the business

BANDIT

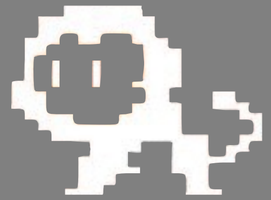
Buying expensive bandaids for massive bullet holes

ROT26



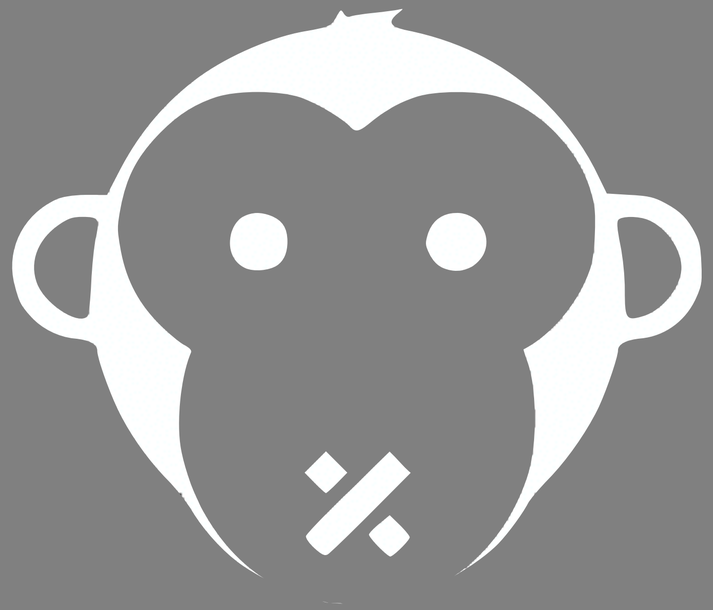
Data is not encrypted… Why is the data not encrypted?!

SHAKESPEARE



Given a few tries, a chimp banging on a keyboard would guess your password

STUTTER



Communication failure between security staff and the business

MANY SECURITY TEAMS LACK

CREDIBILITY

AT THE BUSINESS LEVEL

3

How do I communicate the effectiveness of security and demonstrate value to the business?

tenable®

RSA Conference 2015
Abu Dhabi

Bits and bytes don’t belong in the boardroom

Metrics are the language of Business

EFFECTIVENESS METRICS

tenable®

RSA® Conference 2015
Abu Dhabi

ALIGN SECURITY ISSUES to the BUSINESS RISK

tenable®

RSA® Conference 2015
Abu Dhabi

GLIMPSE

Lack of visibility due to large compound annual growth rates

INVADER

Inability to identify attack path to defend against breach

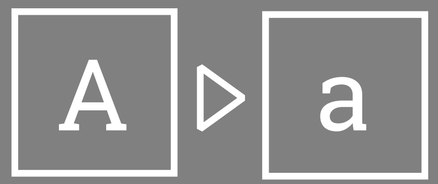
STUTTER

Communication failure between security staff and the business

BANDIT

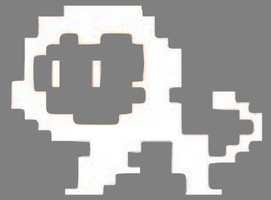
Buying expensive bandaids for massive bullet holes

ROT26



Data is not encrypted… Why is the data not encrypted?!

SHAKESPEARE

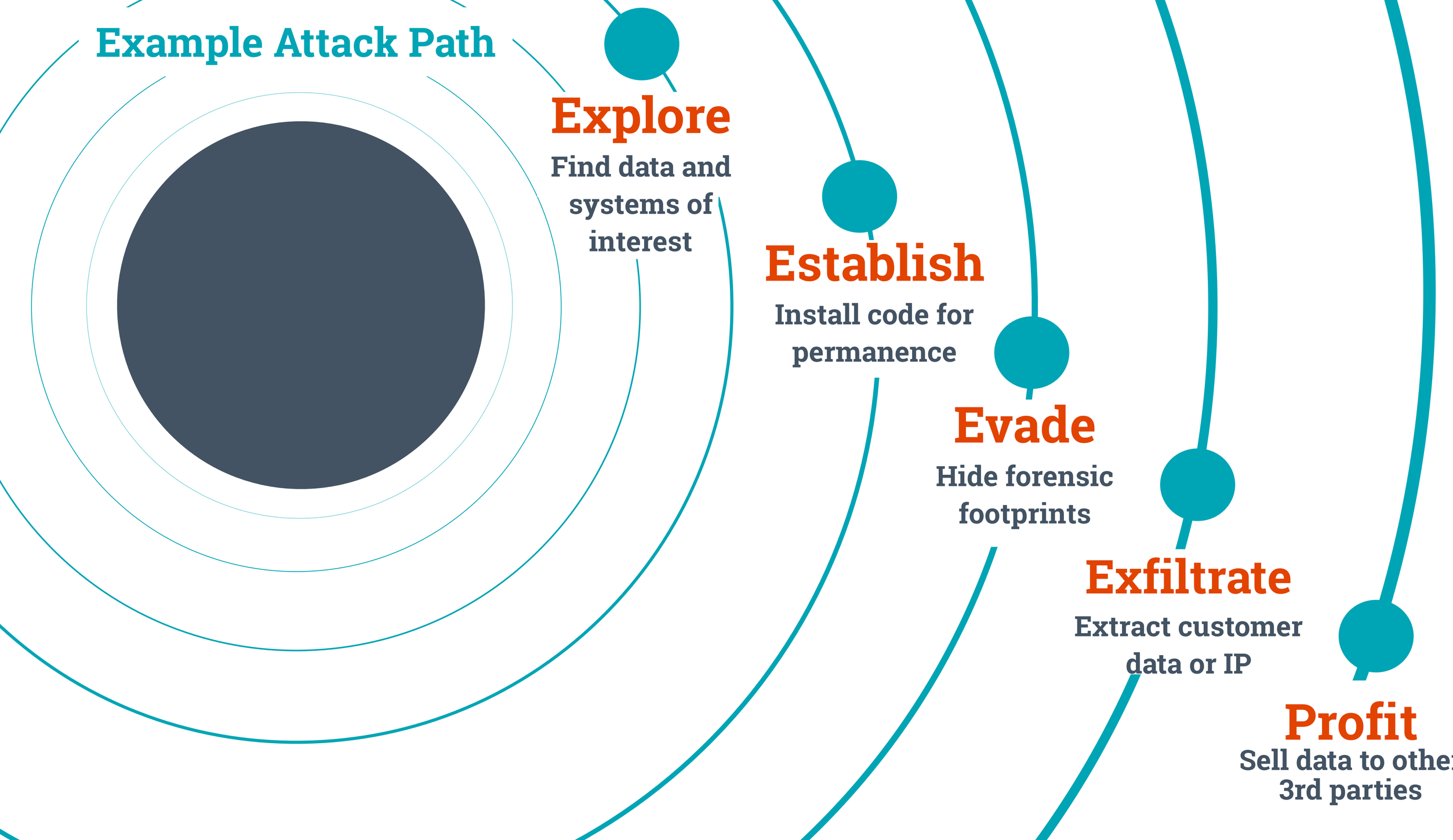


Given a few tries, a chimp banging on a keyboard would guess your password

INVADER

Inability to identify attack path to defend against breach

Example Attack Path



Explore

Find data and systems of interest

Establish

Install code for permanence

Evade

Hide forensic footprints

Exfiltrate

Extract customer data or IP

Profit

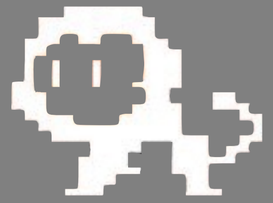
Sell data to other 3rd parties

FOCUSING ON FIXING THE FOUNDATIONAL

GLIMPSE

Lack of visibility due to large compound annual growth rates

SHAKESPEARE



Given a few tries, a chimp banging on a keyboard would guess your password

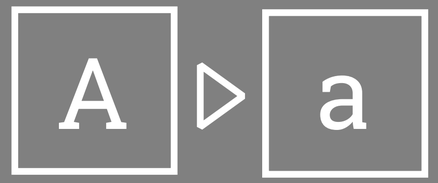
INVADER

Inability to identify attack path to defend against breach

BANDIT

Buying expensive bandaids for massive bullet holes

ROT26



Data is not encrypted... Why is the data not encrypted?!

STUTTER

Communication failure between security staff and the business

Organisations need to stop focusing on the

0 DAY

AND FIX THE +100 DAY

tenable®

RSA Conference 2015
Abu Dhabi

Follow me on Twitter

@gmillard

Email me

gmillard@tenable.com

Website

tenable.com

tenable®

RSA® Conference 2015

Abu Dhabi