SECURING SENSITIVE DATA

A STRANGE GAME

THE ONLY WAY TO WIN…

SECURING SENSITIVE DATA

A STRANGE GAME

THE ONLY WAY TO WIN…
IS NOT TO PLAY

Bio

Jeff Elliot, TLA’s, 4LA’s, 5LA’s

Associate Director, Protiviti

8 years PCI QSA

The Fine Print

- Try the things I am going to recommend at your own risk. They are expensive. Do it right, you're a hero. Do it wrong, you're fired.
- All products listed are only representative samples. Choose the product or service that works best in your environment.
- I am not a lawyer, I am a consultant.
- I might not be YOUR consultant…

THE ISSUE

THE ISSUE

THE ISSUE

$

CREDIT CARDS *ARE* $

THE ISSUE

CREDIT CARDS *ARE* $

CRIMINALS WANT $

THE ISSUE

CREDIT CARDS *ARE* $

CRIMINALS WANT $

MERCHANTS SPEND $ TO TRY AND ACHIEVE “COMPLIANCE”

Compliance Math

$$\sum \binom{Compliance}{Cost,\ Pain}! = SECURITY$$

THE ISSUE

BUT WE STILL HAVE DATA BREACHES…

THE ISSUE

BUT WE STILL HAVE DATA BREACHES…

FAR TOO OFTEN

TALES FROM THE QSA TRENCHES

- GOOD CRYPTO IS DIFFICULT
  - Stream ciphers hate key reuse

TALES FROM THE QSA TRENCHES

SEGMENTATION

=

ISOLATION

!=

CONTROLLED ACCESS

TALES FROM THE QSA TRENCHES

- PCI DSS 1.1: “Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment”. 9/2006
- PCI DSS 1.2, 1.2.1, 2.0, 3.0: “Network segmentation of, or isolating (segmenting), the cardholder data environment from the remainder of the corporate network…” 10/2008+

Jericho was right

attrition.org
@attritionorg

Follow

@Wh1t3Rabbit what a colossal waste of time and energy. no matter how you scope a PCI assessment, it is *always* smaller than attacker scope

TALES FROM THE QSA TRENCHES

- SEGMENTATION = ISOLATION != CONTROLLED ACCESS
  - Jericho was right
  - An Outside Job

[redacted]

Subject: RE: [redacted] External Pen Test

Actually, db below is qa, but it's part of pci and contains credit card info according to our sysadmins [redacted].

So, we can consider that you've reached your goal.

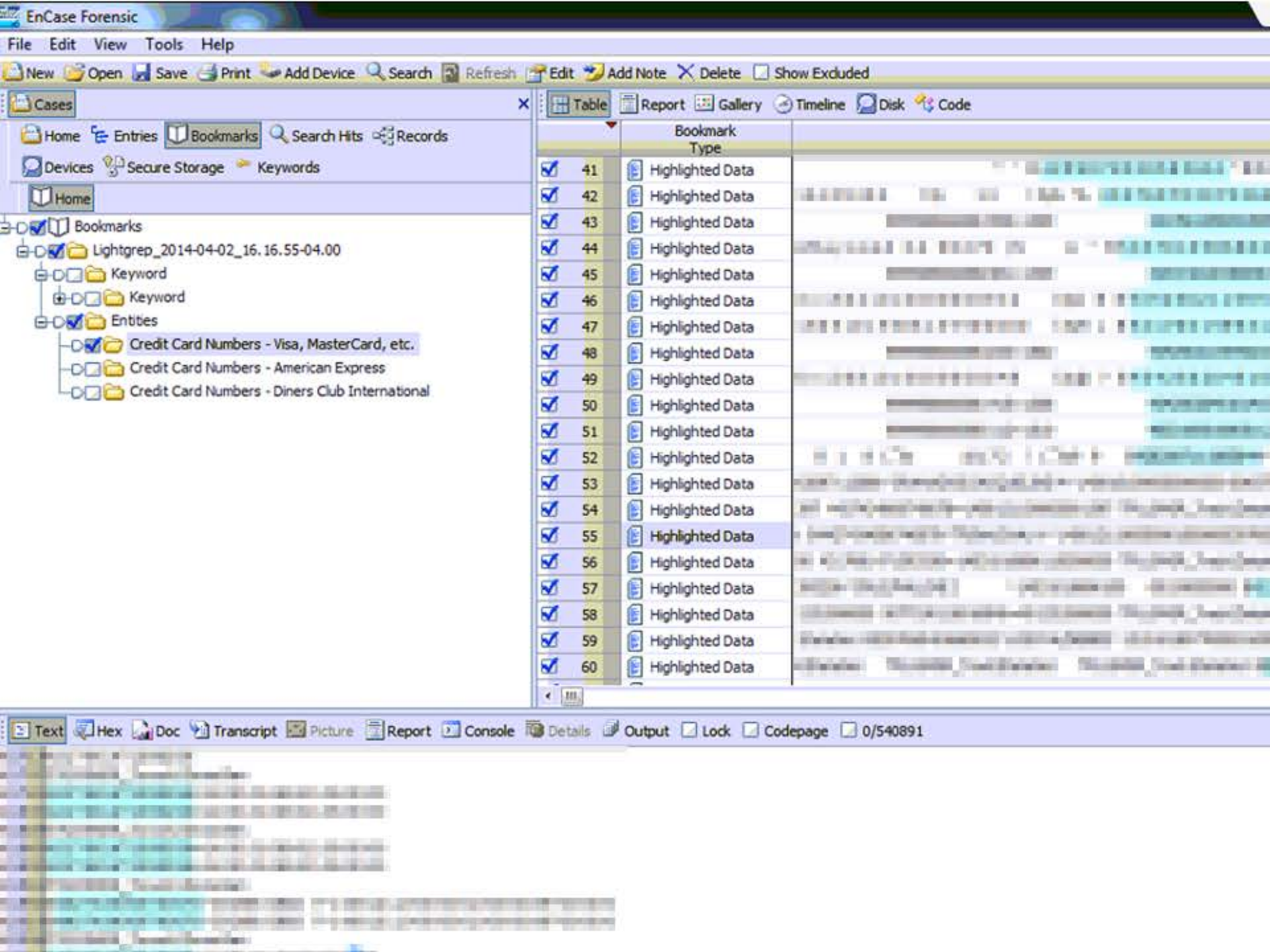
We'll wait for your report.

Another Pen Test

- Compromised a DA account
- Pivoted from their SCCM(which has 2FA) over SMB to CDE systems.
- Added that account to the ESXi Admins group.
- Login using vSphere client that manages all of the CDE systems.
- Logged into the Console for those systems since 2FA was not enforced at that level.

TALES FROM THE QSA TRENCHES

HUMANS!


EnCase Forensic
File Edit View Tools Help
New Open Save Print Add Device Search Refresh Edit Add Note Delete Show Excluded
Cases
Home Entries Bookmarks Search Hits Records
Devices Secure Storage Keywords
Home
Bookmarks
Lightgrep_2014-04-02_16.16.55-04.00
Keyword
Keyword
Entities
Credit Card Numbers - Visa, MasterCard, etc.
Credit Card Numbers - American Express
Credit Card Numbers - Diners Club International
Table Report Gallery Timeline Disk Code
Bookmark Type
41 Highlighted Data
42 Highlighted Data
43 Highlighted Data
44 Highlighted Data
45 Highlighted Data
46 Highlighted Data
47 Highlighted Data
48 Highlighted Data
49 Highlighted Data
50 Highlighted Data
51 Highlighted Data
52 Highlighted Data
53 Highlighted Data
54 Highlighted Data
55 Highlighted Data
56 Highlighted Data
57 Highlighted Data
58 Highlighted Data
59 Highlighted Data
60 Highlighted Data
Text Hex Doc Transcript Picture Report Console Details Output Lock Codepage 0/540891

TALES FROM THE QSA TRENCHES

HUMANS!

"But I needed to debug a production problem"

TALES FROM THE QSA TRENCHES

HUMANS!

"But I needed to debug a production problem…"

"…and I forgot to turn it off when I was done"

THE POTENTIAL SOLUTION

THE POTENTIAL SOLUTION
P2PE
(POINT TO POINT ENCRYPTION)
+
TOKENIZATION

THE POTENTIAL SOLUTION
P2PE
(POINT TO POINT ENCRYPTION)
+
TOKENIZATION

PCI SSC FAQ #1086: "Is encrypted cardholder data in scope for PCI DSS?"

"It is possible that encrypted data may potentially be out of scope for a particular entity *if, and only if,* it is validated (for example, by a QSA or ISA) that the entity in possession of the encrypted data does not have access to the cleartext cardholder data or the encryption process, nor do they have the ability to decrypt the encrypted data. This means the entity does not have cryptographic keys anywhere in their environment, and that none of the entity's systems, processes or personnel have access to the environment where cryptographic keys are located, nor do they have the ability to retrieve them."

https://www.pcisecuritystandards.org/faq/

KEY (get it?) ELEMENTS of P2PE

- tl;dr: https://www.pcisecuritystandards.org/documents/P2PE_v1_1_FAQs_Aug2012.pdf et al

- No keys in the merchant environment
- Encrypt at POI using a TRSM / HSM
- Decrypt only at the bank or service provider

KEY (get it?) ELEMENTS of P2PE

- tl;dr: https://www.pcisecuritystandards.org/documents/P2PE_v1_1_FAQs_Aug2012.pdf et al

- No keys in the merchant environment
- Encrypt at POI using a TRSM / HSM
- Decrypt only at the bank or service provider

BREAKING NEWS!

BREAKING NEWS!

Validated P2PE Solutions

- You should use a PCI validated P2PE Solution
- There's a list here: https://www.pcisecuritystandards.org/approved_companies_providers/validated_p2pe_solutions.php

BUT THERE ARE ONLY 10 !?!?!?111

https://www.pcisecuritystandards.org/approved_companies_providers/validated_p2pe_solutions.php Retrieved July 26, 2014

A TALE OF TWO CONTRACTS

"Merchants using encryption solutions that are not included on the Council's List of Validated P2PE Solutions should consult with their acquirer or payment brand about use of these solutions."

PAYMENT BRANDS -> CONTRACT WITH -> ACQUIRING BANKS

ACQUIRING BANKS -> CONTRACT WITH -> MERCHANTS

https://www.pcisecuritystandards.org/documents/P2PE_v1_1_FAQs_Aug2012.pdf

Acquiring banks enforce compliance requirements on merchants

Acquiring banks enforce compliance requirements on merchants

and…

Acquiring banks enforce compliance requirements on merchants

and…

Acquiring banks are accepting alternative solutions.

Acquiring banks enforce compliance requirements on merchants

and…

Acquiring banks are accepting alternative solutions (and sometimes selling them).

THERE ARE FAR MORE THAN 3

PayMetric	CardVault	FutureX
SafeNet	Thales e-Security	Voltage
Bluefin PayConex	EPS Total Care	Solve Data Shield
Chase PaymentTech Orbital	First Data TransArmor	Protegrity
MerchantLink	RSA	Element

AND TOO MANY MORE TO LIST

https://www.google.com/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=list+of+tokenization+solutions Retrieved July 26, 2014

BUT MY DATABASE ONLY TAKES NUM*16

Doesn’t crypto make big ugly strings?

FORMAT PRESERVING ENCRYPTION

THE POTENTIAL DRAWBACKS

THE POTENTIAL DRAWBACKS

$

THE POTENTIAL DRAWBACKS

$

DATA JAIL

THE POTENTIAL DRAWBACKS

$

DATA JAIL

INFORMATION SECURITY BUDGET

THE POTENTIAL DRAWBACKS

$

DATA JAIL

INFORMATION SECURITY BUDGET

THE POTENTIAL DRAWBACKS

$

DATA JAIL

INFORMATION SECURITY
BUDGET

THE POTENTIAL DRAWBACKS

$

DATA JAIL

INFORMATION SECURITY
BUDGET

Other Potential Issues

- Implementation Issues
  - Whitelists
  - Manual Entry
  - Gift Card Entry
  - Black Boxes are Black Boxes

So What?

- Thieves can’t steal what you don’t have
- Auditors can’t audit what you don’t have
- No breach fines if there is no breach

So What?

- Thieves can’t steal what you don’t have
- Auditors can’t audit what you don’t have
- No breach fines if there is no breach
- No CIO’s / CEO’s / CISO’s have to get fired if there is no breach