Enterprise Wi-Fi Recon - rEAPing the benefits

LUKE MCDONNELL
(intrepid)

Disclaimer

All views, ideas and opinions shared are my own. Unless they are quotes, pictures, links, or technical looking information, which is most likely copied from search engine results.

Anything I say or express are my own views and not the views, opinions of, or in any way related to the company I work for or its affiliates.

Agenda

- About me
- What this talk isn’t about
- What this talk is about
- Good content (hopefully)
  - Various stages of enterprise wireless maturity
  - Recon
  - Harvesting
  - Probes
- How/where to apply it
- Recap

About me

- 9+ years as sysadmin in payments and defence type companies
- Pentesting for about a year
- Got a few certs including
  - Some SANS certs
  - OSWP

About me

- Play hard, work hard
  - Surfing
  - Mountain biking
- Pentest like I ride…

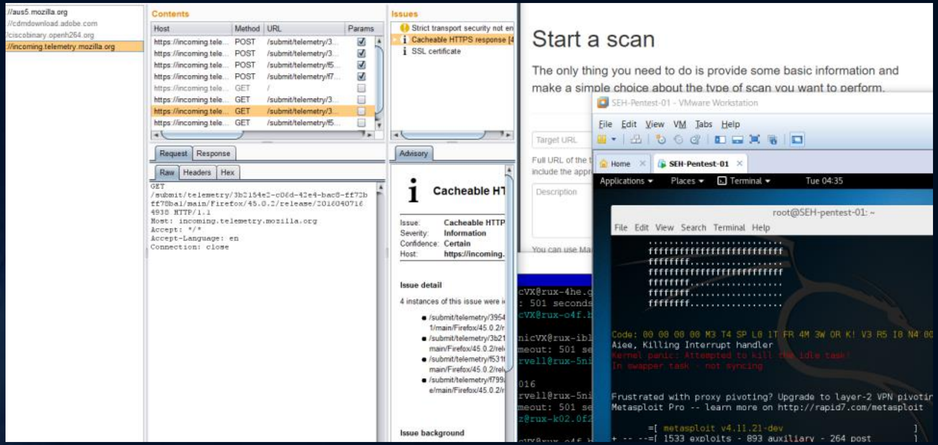
About me

- Riding

- Crashing

About me

- Testing



Host	Method	URL	Params
https://incoming.tele...	POST	/submit/telemetry/3...	☑
https://incoming.tele...	POST	/submit/telemetry/3...	☑
https://incoming.tele...	POST	/submit/telemetry/f5...	☑
https://incoming.tele...	POST	/submit/telemetry/f7...	☑
https://incoming.tele...	GET	/	□
https://incoming.tele...	GET	/submit/telemetry/3...	□
https://incoming.tele...	GET	/submit/telemetry/3...	□
https://incoming.tele...	GET	/submit/telemetry/f5...	□

Strict transport security not en

Cacheable HTTPS response [4

SSL certificate

```
GET
/submit/telemetry/3b2154e2-c06d-42e4-bac8-ff72b
ff78ba1/main/Firefox/45.0.2/release/2016040716
4938 HTTP/1.1
Host: incoming.telemetry.mozilla.org
Accept: */*
Accept-Language: en
Connection: close
```

Cacheable HT

Issue: Cacheable HTTP
Severity: Information
Confidence: Certain
Host: https://incoming.

Issue detail

4 instances of this issue were i

- /submit/telemetry/3954 1/main/Firefox/45.0.2/r
- /submit/telemetry/3b21 main/Firefox/45.0.2/rel
- /submit/telemetry/f531 main/Firefox/45.0.2/rel
- /submit/telemetry/f799 e/main/Firefox/45.0.2/r

Issue background

Start a scan

The only thing you need to do is provide some basic information and make a simple choice about the type of scan you want to perform.

Full URL of the t include the appr

You can use Ma

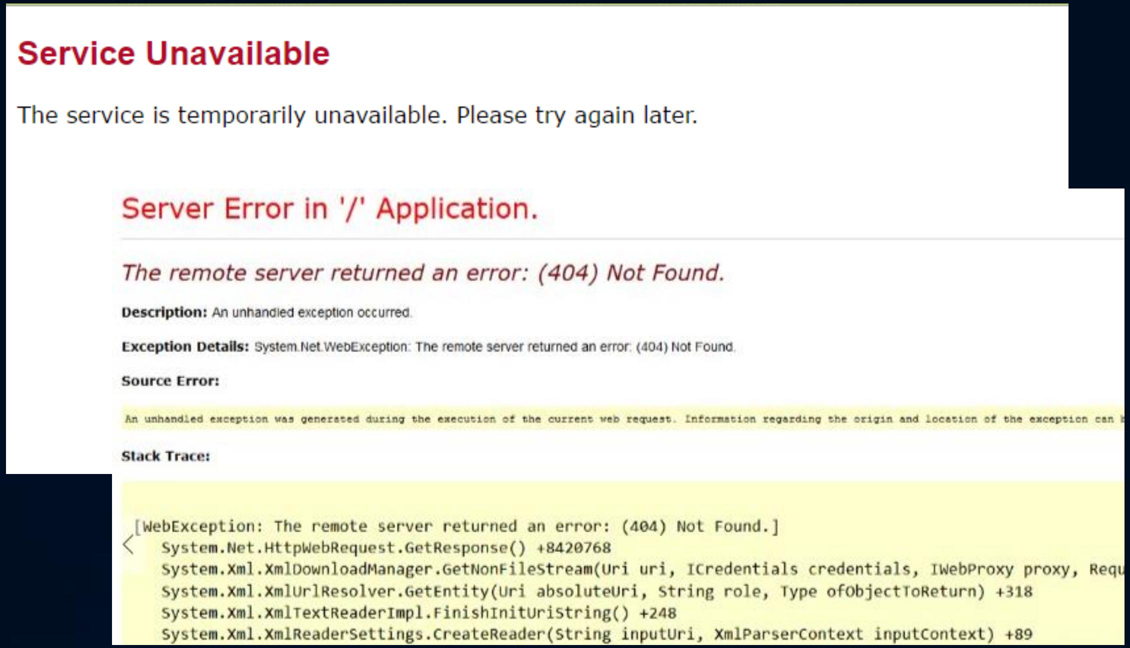
SEH-Pentest-01 - VMware Workstation

root@SEH-pentest-01: ~

```
cVX@rux-4he.g
: 501 seconds
cVX@rux-o4f.h

nicVX@rux-ibl
meout: 501 se
rvell@rux-5ni

016
rvell@rux-5ni
meout: 501 se
z@rux-k02.0f2
```

```
        ...........................
        ffffffffffffffffffffffffff
        ffffffff..................
        ffffffffffffffffffffffffff
        ffffffff..................
        ffffffff..................
        ffffffff..................


Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N4 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing


Frustrated with proxy pivoting? Upgrade to layer-2 VPN pivotin
Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.21-dev                         ]
+ -- --=[ 1533 exploits - 893 auxiliary - 264 post        ]
```

- Crashing



Service Unavailable

The service is temporarily unavailable. Please try again later.

Server Error in '/' Application.

The remote server returned an error: (404) Not Found.

Description: An unhandled exception occurred.

Exception Details: System.Net.WebException: The remote server returned an error: (404) Not Found.

Source Error:

```
An unhandled exception was generated during the execution of the current web request. Information regarding the origin and location of the exception can b
```

Stack Trace:

```
[WebException: The remote server returned an error: (404) Not Found.]
   System.Net.HttpWebRequest.GetResponse() +8420768
   System.Xml.XmlDownloadManager.GetNonFileStream(Uri uri, ICredentials credentials, IWebProxy proxy, Requ
   System.Xml.XmlUrlResolver.GetEntity(Uri absoluteUri, String role, Type ofObjectToReturn) +318
   System.Xml.XmlTextReaderImpl.FinishInitUriString() +248
   System.Xml.XmlReaderSettings.CreateReader(String inputUri, XmlParserContext inputContext) +89
```

Generic enterprise wireless pentest

- Wireless scanning
- Find SSIDs in range
- Walk around, searching for rogue devices
- Identify Security protocols (WPA/WEP/EAP)
  - Crack/Brute force
- FakeAP/Evil Twin etc…

- Everything this talk is NOT about

Enterprise Recon

- What else is there?
- What/how can it be applied?

Various stages of enterprise wireless maturity

Stages of enterprise wireless maturity

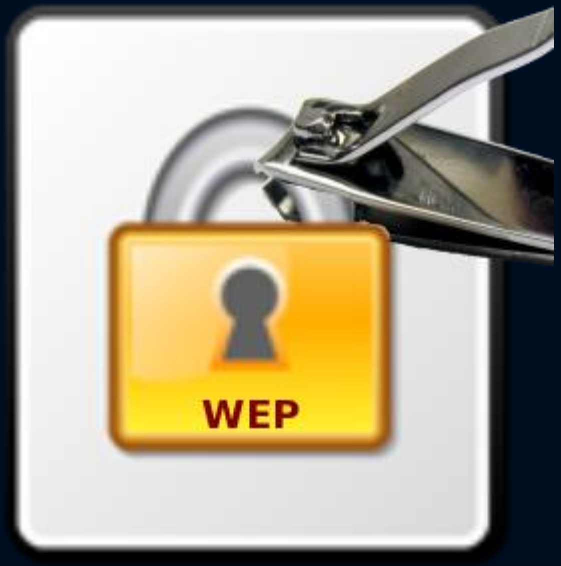
Open network wireless as only Wi-Fi network	Cowboys – no idea on wireless security
WEP	Same
WPA single network	Small company/low budget
WPA multiple network	Growing company some good security
OPEN/WPA/EAP multiple networks	Mature, large company with a good budget, some security knowledge
	Good security consultant

Open networks

- All size businesses use open
  - Small businesses open only
  - Large enterprise incorporate open as part of their solution
- Cowboys/Use case
- Open slather/Locked down
- If not air gapped no excuse

WEP networks

- Small businesses
- Zero idea on security
- Zero budget
- No excuse for this in 2016



WPA/2 networks

- Small - Mid sized business
- Growing Business
  - Some idea of security
  - Low budget
  - Low resources

EAP networks

- Large enterprise
- More advanced life forms
  - Good security team
  - Good wifi security
  - Good security consultant/contractor

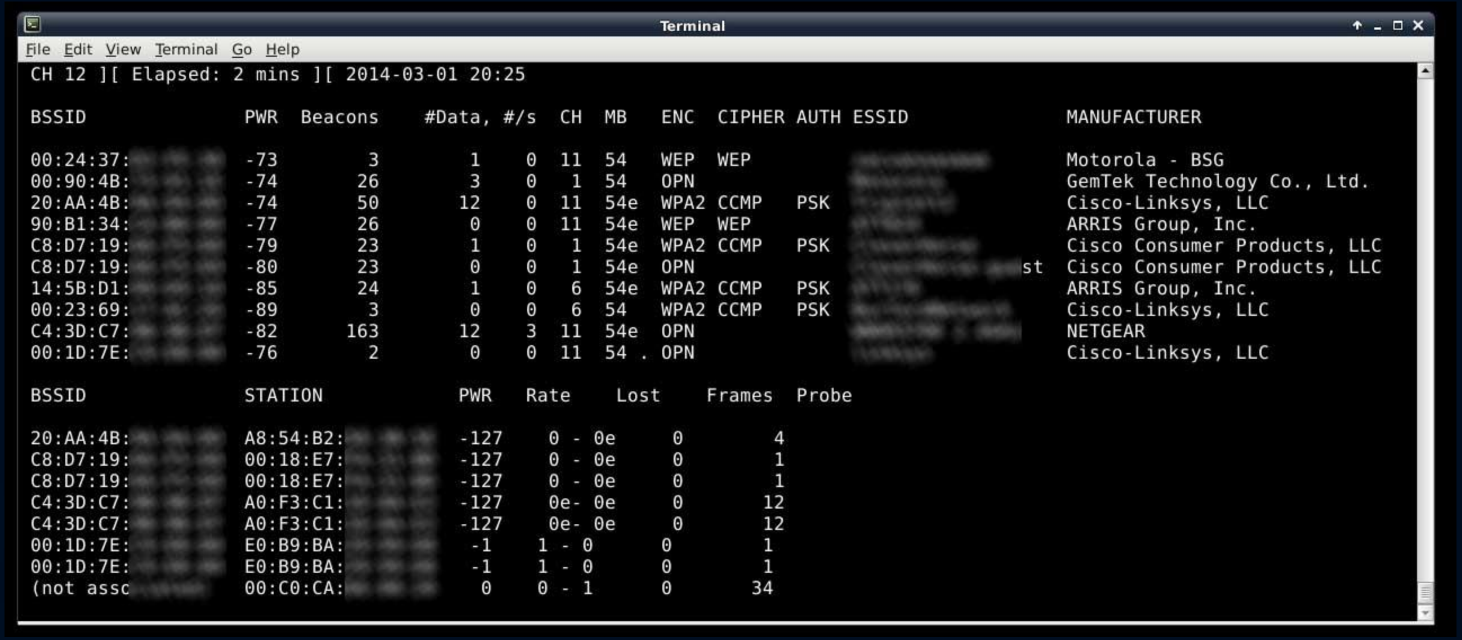
Applying this information

- Size of the company
  - Complexity or size of actual scope compared to agreed scope
- Maturity of security within the company
  - Do they apply similar security to the rest of the business?
    - If WEP is being used, they probably don't care about SSLv2
  - Expect that if they are using certs for Wi-Fi they probably have good knowledge of certs elsewhere

Recon

Manufacturer

- airodump –manufacturer
  - show what kit is being used



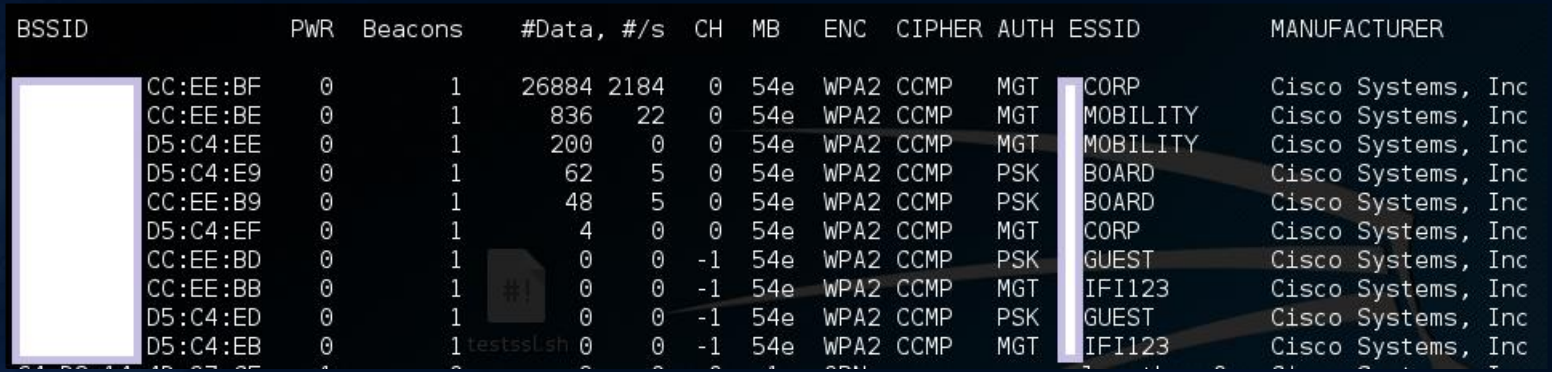
```
CH 12 ][ Elapsed: 2 mins ][ 2014-03-01 20:25

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID              MANUFACTURER

00:24:37:[redacted]  -73        3        1    0  11  54   WEP  WEP         [redacted]         Motorola - BSG
00:90:4B:[redacted]  -74       26        3    0   1  54   OPN              [redacted]         GemTek Technology Co., Ltd.
20:AA:4B:[redacted]  -74       50       12    0  11  54e  WPA2 CCMP   PSK  [redacted]         Cisco-Linksys, LLC
90:B1:34:[redacted]  -77       26        0    0  11  54e  WEP  WEP         [redacted]         ARRIS Group, Inc.
C8:D7:19:[redacted]  -79       23        1    0   1  54e  WPA2 CCMP   PSK  [redacted]         Cisco Consumer Products, LLC
C8:D7:19:[redacted]  -80       23        0    0   1  54e  OPN              [redacted]st       Cisco Consumer Products, LLC
14:5B:D1:[redacted]  -85       24        1    0   6  54e  WPA2 CCMP   PSK  [redacted]         ARRIS Group, Inc.
00:23:69:[redacted]  -89        3        0    0   6  54   WPA2 CCMP   PSK  [redacted]         Cisco-Linksys, LLC
C4:3D:C7:[redacted]  -82      163       12    3  11  54e  OPN              [redacted]         NETGEAR
00:1D:7E:[redacted]  -76        2        0    0  11  54 . OPN              [redacted]         Cisco-Linksys, LLC

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

20:AA:4B:[redacted]  A8:54:B2:[redacted]  -127    0 - 0e     0        4
C8:D7:19:[redacted]  00:18:E7:[redacted]  -127    0 - 0e     0        1
C8:D7:19:[redacted]  00:18:E7:[redacted]  -127    0 - 0e     0        1
C4:3D:C7:[redacted]  A0:F3:C1:[redacted]  -127    0e- 0e     0       12
C4:3D:C7:[redacted]  A0:F3:C1:[redacted]  -127    0e- 0e     0       12
00:1D:7E:[redacted]  E0:B9:BA:[redacted]    -1    1 - 0     0        1
00:1D:7E:[redacted]  E0:B9:BA:[redacted]    -1    1 - 0     0        1
(not assc[redacted]  00:C0:CA:[redacted]     0    0 - 1     0       34
```

Use of multiple SSIDs

- This can also show the maturity of the wireless solution
  - eg ‘**mobility’** network, ‘corp’ network, ‘guest’ network

Use of multiple SSIDs

- Businesses really don’t know what wireless networks they have
  - can use "next in line mac" to identify other SSIDs
  - Not in scope != company doesn’t want it included
  - DEV networks



```
BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID          MANUFACTURER

[redacted]CC:EE:BF    0        1    26884 2184   0  54e  WPA2 CCMP   MGT  [redacted]CORP         Cisco Systems, Inc
[redacted]CC:EE:BE    0        1      836   22   0  54e  WPA2 CCMP   MGT  [redacted]MOBILITY     Cisco Systems, Inc
[redacted]D5:C4:EE    0        1      200    0   0  54e  WPA2 CCMP   MGT  [redacted]MOBILITY     Cisco Systems, Inc
[redacted]D5:C4:E9    0        1       62    5   0  54e  WPA2 CCMP   PSK  [redacted]BOARD        Cisco Systems, Inc
[redacted]CC:EE:B9    0        1       48    5   0  54e  WPA2 CCMP   PSK  [redacted]BOARD        Cisco Systems, Inc
[redacted]D5:C4:EF    0        1        4    0   0  54e  WPA2 CCMP   MGT  [redacted]CORP         Cisco Systems, Inc
[redacted]CC:EE:BD    0        1        0    0  -1  54e  WPA2 CCMP   PSK  [redacted]GUEST        Cisco Systems, Inc
[redacted]CC:EE:BB    0        1        0    0  -1  54e  WPA2 CCMP   MGT  [redacted]IFI123       Cisco Systems, Inc
[redacted]D5:C4:ED    0        1        0    0  -1  54e  WPA2 CCMP   PSK  [redacted]GUEST        Cisco Systems, Inc
[redacted]D5:C4:EB    0        1        0    0  -1  54e  WPA2 CCMP   MGT  [redacted]IFI123       Cisco Systems, Inc
```

Applying this information

- Manufacturer
  - Identify preferred vendor
  - Make assumptions on security decisions
    - Cisco – Old school "no-one got fired for buying cisco"
    - Aruba – Cutting edge, better security?
    - Mixed kit – Legacy? Slow to decommission?
  - Unidentified firewall on external? Try the identified Wi-Fi vendor

- Use of multiple SSIDs
  - Mobility – Use lootybooty
  - DEV networks
    - Open access
    - Easy password
  - Finding more SSIDs than specified in scope
    - If Wi-Fi pentest, shows you're doing your job!

Harvesting

Open Wi-Fi

- Internal DNS server
- Sniff DNS lookups, internal hostnames

WPA/2

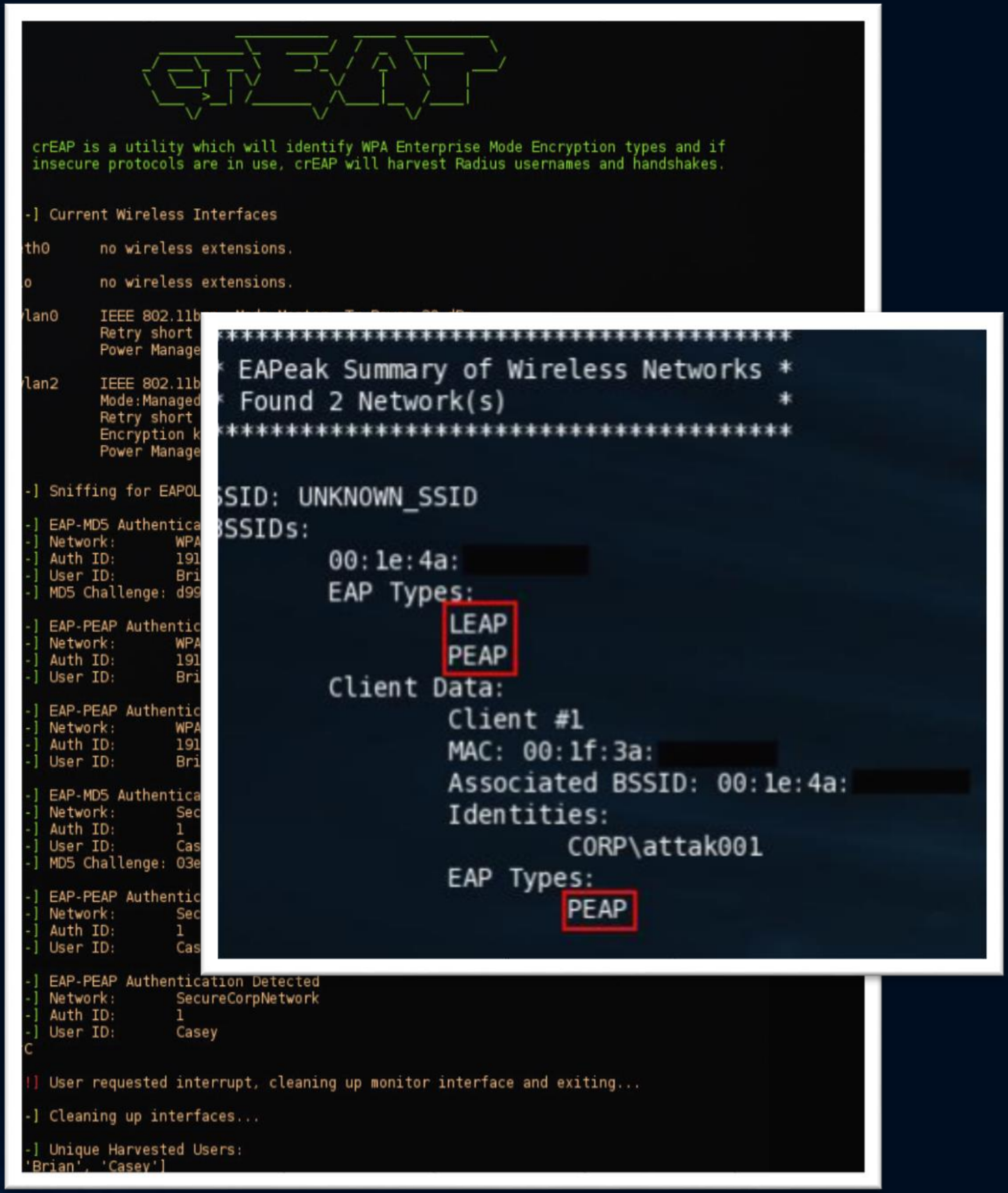
- Dependant on password list
  - Scrape the website for words, add ‘guest’ or ‘123’ and bam, password found.

(not really harvesting, more of a tip)

EAP/PEAP

- Harvest domain and usernames

- crEAP
- EAPeak



```
crEAP is a utility which will identify WPA Enterprise Mode Encryption types and if
insecure protocols are in use, crEAP will harvest Radius usernames and handshakes.

-] Current Wireless Interfaces

th0      no wireless extensions.

o        no wireless extensions.

lan0     IEEE 802.11b
         Retry short
         Power Manage

lan2     IEEE 802.11b
         Mode:Managed
         Retry short
         Encryption k
         Power Manage

-] Sniffing for EAPOL

-] EAP-MD5 Authentica
-] Network:        WPA
-] Auth ID:        191
-] User ID:        Bri
-] MD5 Challenge:  d99

-] EAP-PEAP Authentic
-] Network:        WPA
-] Auth ID:        191
-] User ID:        Bri

-] EAP-PEAP Authentic
-] Network:        WPA
-] Auth ID:        191
-] User ID:        Bri

-] EAP-MD5 Authentica
-] Network:        Sec
-] Auth ID:        1
-] User ID:        Cas
-] MD5 Challenge:  03e

-] EAP-PEAP Authentic
-] Network:        Sec
-] Auth ID:        1
-] User ID:        Cas

-] EAP-PEAP Authentication Detected
-] Network:        SecureCorpNetwork
-] Auth ID:        1
-] User ID:        Casey
C

!] User requested interrupt, cleaning up monitor interface and exiting...

-] Cleaning up interfaces...

-] Unique Harvested Users:
'Brian', 'Casey']
```

```
****************************************
 EAPeak Summary of Wireless Networks *
 Found 2 Network(s)                  *
****************************************

SSID: UNKNOWN_SSID
BSSIDs:
        00:1e:4a:[redacted]
        EAP Types:
                LEAP
                PEAP
        Client Data:
                Client #1
                MAC: 00:1f:3a:[redacted]
                Associated BSSID: 00:1e:4a:[redacted]
                Identities:
                        CORP\attak001
                EAP Types:
                        PEAP
```

Applying this information

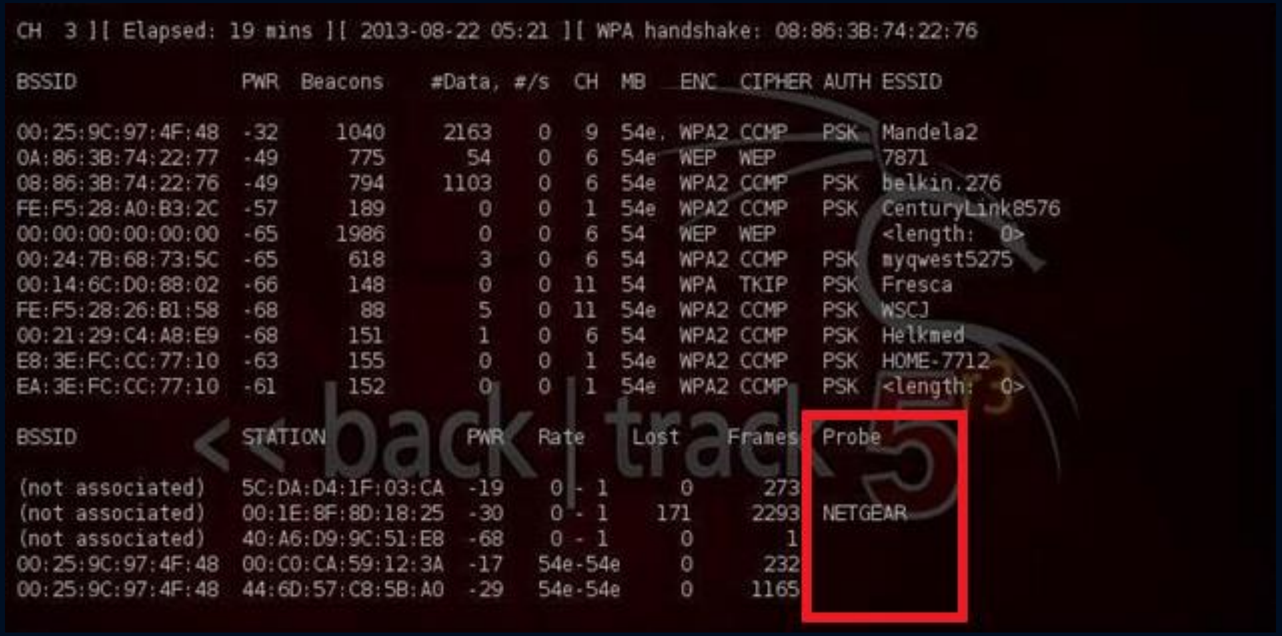
- List of internal hostnames and IP addresses
  - Useful for internal pentests
- Valid domain and usernames
  - Well.. Urgh
    - VPN
    - Internal pentest
    - External webapps
    - Anything that uses same auth mechanism
  - Scrape websites for Director names and other logins

Probes

Probes

- Even if a client is connected, it will still probe for previously associated Wi-Fi networks

- Airodump-ng



```
CH  3 ][ Elapsed: 19 mins ][ 2013-08-22 05:21 ][ WPA handshake: 08:86:3B:74:22:76

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:25:9C:97:4F:48  -32     1040     2163    0   9  54e. WPA2 CCMP   PSK  Mandela2
0A:86:3B:74:22:77  -49      775       54    0   6  54e  WEP  WEP         7871
08:86:3B:74:22:76  -49      794     1103    0   6  54e  WPA2 CCMP   PSK  belkin.276
FE:F5:28:A0:B3:2C  -57      189        0    0   1  54e  WPA2 CCMP   PSK  CenturyLink8576
00:00:00:00:00:00  -65     1986        0    0   6  54   WEP  WEP         <length:  0>
00:24:7B:68:73:5C  -65      618        3    0   6  54   WPA2 CCMP   PSK  myqwest5275
00:14:6C:D0:88:02  -66      148        0    0  11  54   WPA  TKIP   PSK  Fresca
FE:F5:28:26:B1:58  -68       88        5    0  11  54e  WPA2 CCMP   PSK  WSCJ
00:21:29:C4:A8:E9  -68      151        1    0   6  54   WPA2 CCMP   PSK  Helkmed
E8:3E:FC:CC:77:10  -63      155        0    0   1  54e  WPA2 CCMP   PSK  HOME-7712
EA:3E:FC:CC:77:10  -61      152        0    0   1  54e  WPA2 CCMP   PSK  <length:  0>

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   5C:DA:D4:1F:03:CA  -19    0 - 1      0      273
(not associated)   00:1E:8F:8D:18:25  -30    0 - 1    171     2293  NETGEAR
(not associated)   40:A6:D9:9C:51:E8  -68    0 - 1      0        1
00:25:9C:97:4F:48  00:C0:CA:59:12:3A  -17   54e-54e     0      232
00:25:9C:97:4F:48  44:6D:57:C8:5B:A0  -29   54e-54e     0     1165
```

Probes

Company assets are probing for “Maccas free wifi” and every other coffee shop

- Assumption of policies and policy adherence
  - Machines are not locked down to specific SSIDs
  - Running evil twin of hostapd-wpe is going to be easy
  - Shows what the users think of network policies and what is ‘cyber safety’
    - More likely to have rogue APs

Probes

- Find rogue access points

  - PC1 is connected to ‘easywifi123’

    But is also probing for ‘CORP’

  We could assume that either there is a 3G device or a rogue access point

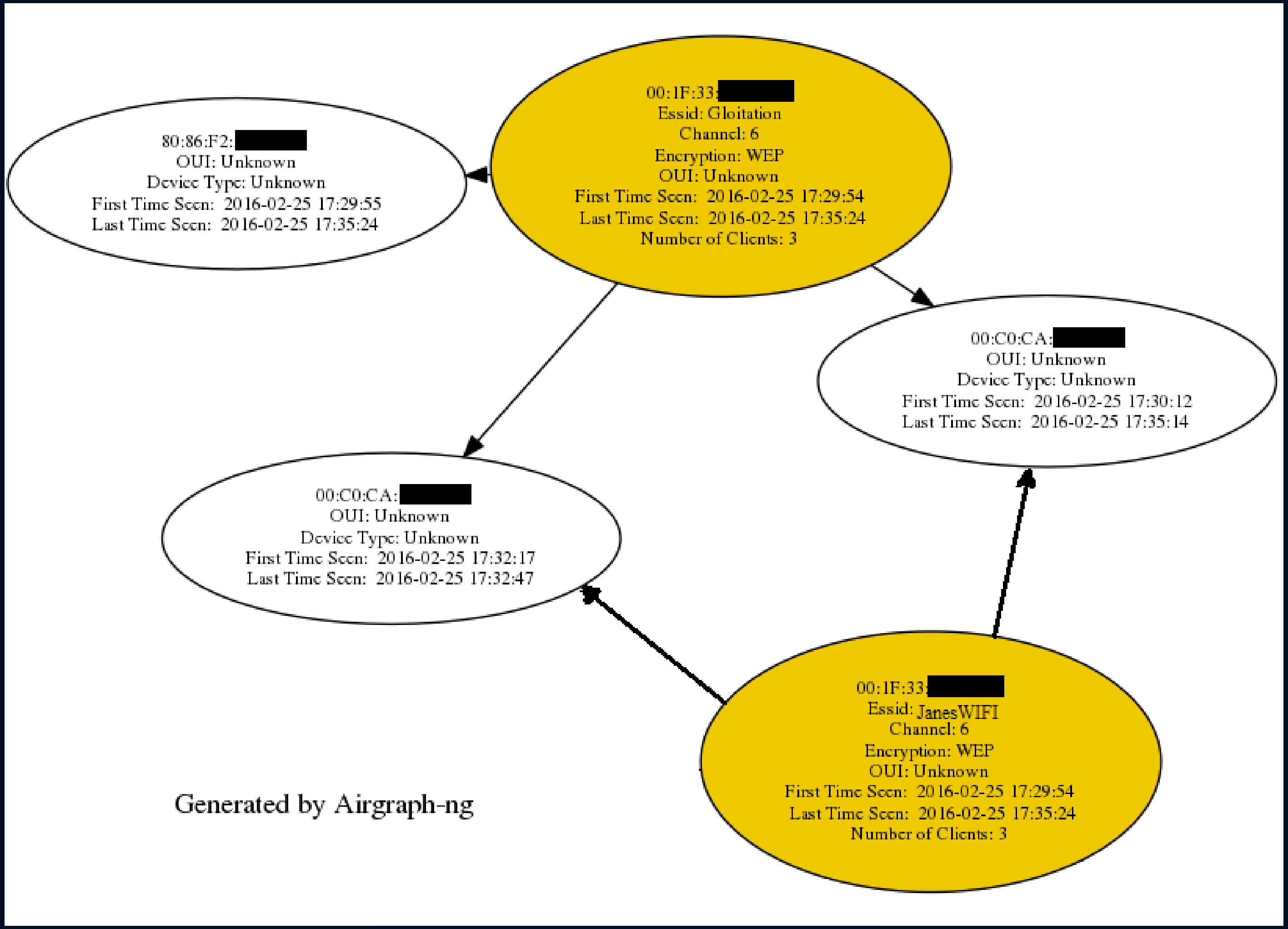
Probes

- Find out about office romances
  - PC1 probe: JanesWIFI

  Credentials: John director
  - PC2 probe: JanesWIFI

  Credentials: Jane PA

- Airgraph-ng



00:1F:33:[redacted]
Essid: Gloitation
Channel: 6
Encryption: WEP
OUI: Unknown
First Time Seen: 2016-02-25 17:29:54
Last Time Seen: 2016-02-25 17:35:24
Number of Clients: 3

80:86:F2:[redacted]
OUI: Unknown
Device Type: Unknown
First Time Seen: 2016-02-25 17:29:55
Last Time Seen: 2016-02-25 17:35:24

00:C0:CA:[redacted]
OUI: Unknown
Device Type: Unknown
First Time Seen: 2016-02-25 17:30:12
Last Time Seen: 2016-02-25 17:35:14

00:C0:CA:[redacted]
OUI: Unknown
Device Type: Unknown
First Time Seen: 2016-02-25 17:32:17
Last Time Seen: 2016-02-25 17:32:47

00:1F:33:[redacted]
Essid: JanesWIFI
Channel: 6
Encryption: WEP
OUI: Unknown
First Time Seen: 2016-02-25 17:29:54
Last Time Seen: 2016-02-25 17:35:24
Number of Clients: 3

Generated by Airgraph-ng

Applying this information

- An idea of security awareness level of the employees
  - What level of response to expect from the rest of the employees for the rest of the engagement/s
- List of probed SSIDs
  - Useful for Hostapd-wpe or evil twin attacks
- Rogue access point SSID
  - Easy entry into the corp network

Recap

What do we have

- An idea of the security posture of the company
- Possible preferred manufacturer/vendor
- List of internal hostnames and IP addresses
- Valid domain and usernames
- Possible entry point into the network via rogue APs or with credentials
- Proof that the CEO spends time at his personal assistant's house which will help to blackmail more pentesting work out of the company…

And we haven’t even walked into the building…

Links

- crEAP
  https://github.com/ShellIntel/scripts/blob/master/crEAP.py
- Aircrack suite
  http://www.aircrack-ng.org/
- EAPeak
  https://github.com/securestate/eapeak
- Lootybooty
  https://github.com/Torinson/lootbooty
- Hostapd-wpe
  https://github.com/OpenSecurityResearch/hostapd-wpe
- Evil twin
  http://www.aircrack-ng.org/doku.php?id=airbase-ng

Questions?