What I’ve Learned

Stories from 30 years of hacking

Anthony S. Clark

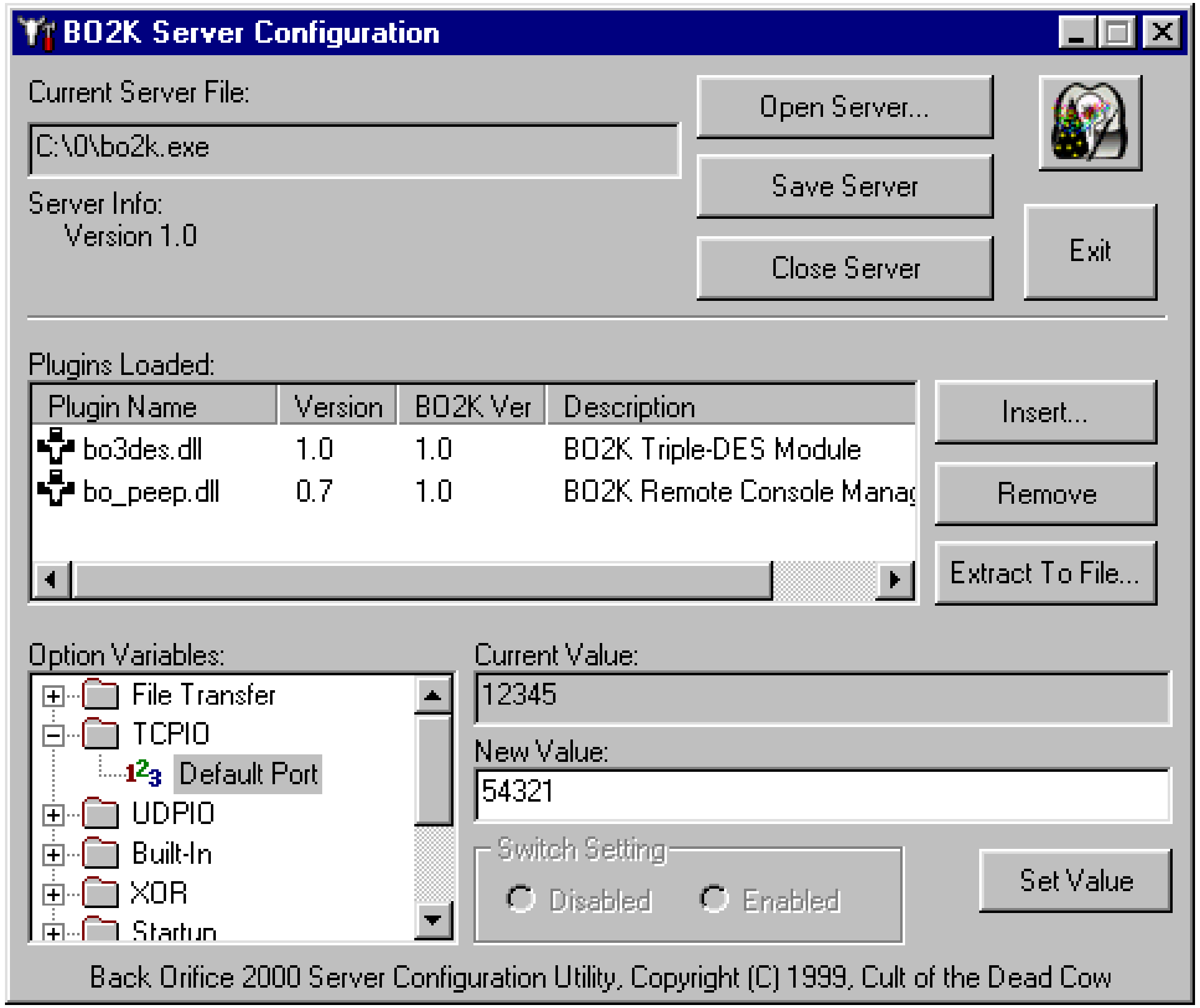
Who am I?

- Anthony S. Clark
  - **Work:**
    - Boldend, CTO
    - Attack Research, Owner & formerly CEO
    - Audeo Technical Advisors, President/Owner
  - **Speaker**:
    - Blackhat
    - Defcon
    - Source
    - B-Sides

Cult of the Dead Cow

One of the first RATs

- Remote control
  - GUI
- Camera capture
- Encryption



Current Server File: C:\0\bo2k.exe

Server Info:
Version 1.0

Plugins Loaded:

Plugin Name	Version	BO2K Ver	Description
bo3des.dll	1.0	1.0	BO2K Triple-DES Module
bo_peep.dll	0.7	1.0	BO2K Remote Console Manag

Option Variables:

```
⊞ File Transfer
⊟ TCPIO
    Default Port
⊞ UDPIO
⊞ Built-In
⊞ XOR
⊞ Startup
```

Current Value: 12345

New Value: 54321

Switch Setting: ○ Disabled ○ Enabled

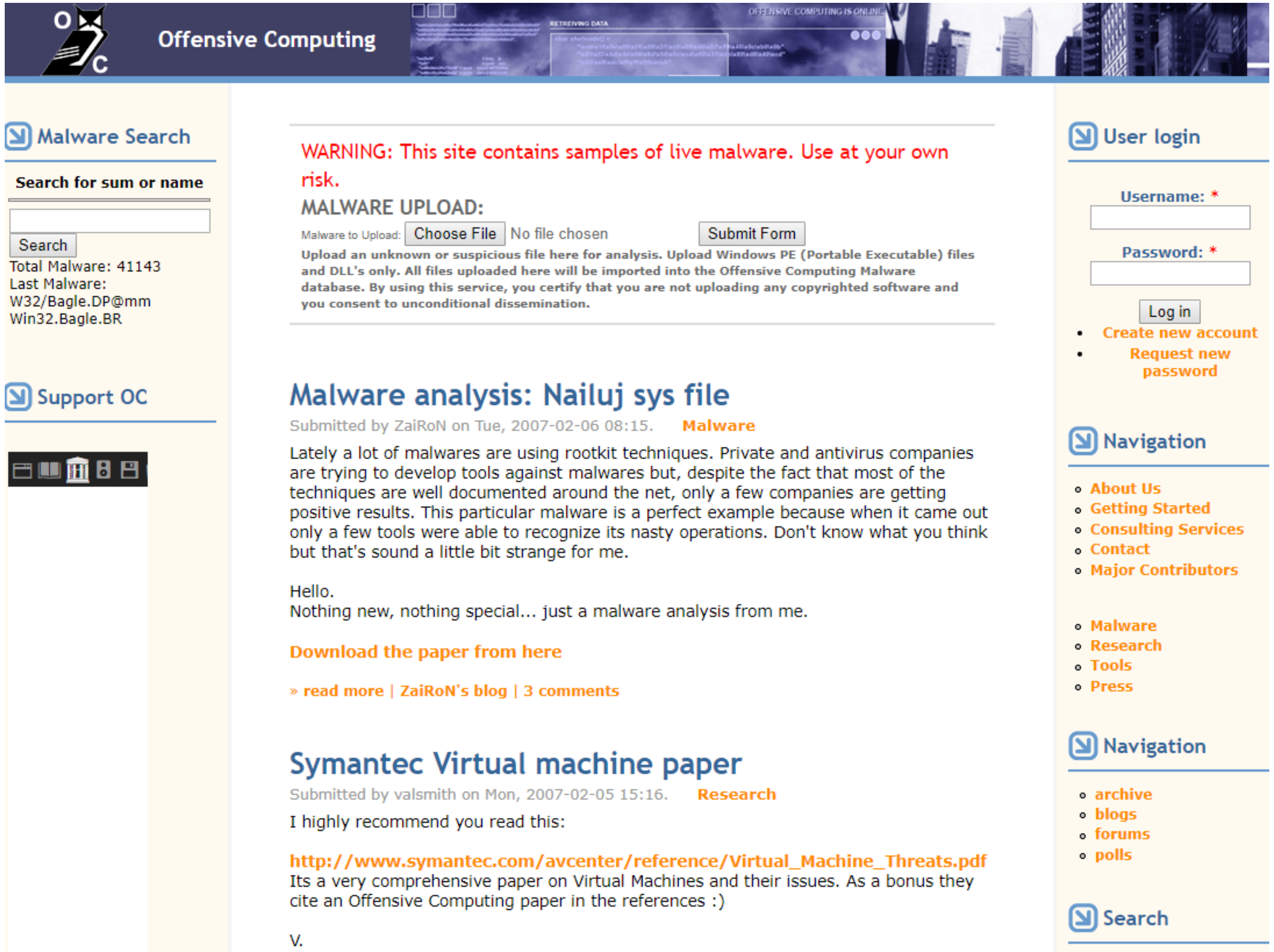
Back Orifice 2000 Server Configuration Utility, Copyright (C) 1999, Cult of the Dead Cow

Metasploit

Premier Pen Testing Tool:

- Exploits for tons of platforms
- Meterpreter
- Encoders
- Evasions

Offensive Computing



Malware Search

Search for sum or name

Total Malware: 41143
Last Malware:
W32/Bagle.DP@mm
Win32.Bagle.BR

Support OC

WARNING: This site contains samples of live malware. Use at your own risk.

MALWARE UPLOAD:

Malware to Upload: No file chosen

Upload an unknown or suspicious file here for analysis. Upload Windows PE (Portable Executable) files and DLL's only. All files uploaded here will be imported into the Offensive Computing Malware database. By using this service, you certify that you are not uploading any copyrighted software and you consent to unconditional dissemination.

Malware analysis: Nailuj sys file

Submitted by ZaiRoN on Tue, 2007-02-06 08:15. Malware

Lately a lot of malwares are using rootkit techniques. Private and antivirus companies are trying to develop tools against malwares but, despite the fact that most of the techniques are well documented around the net, only a few companies are getting positive results. This particular malware is a perfect example because when it came out only a few tools were able to recognize its nasty operations. Don't know what you think but that's sound a little bit strange for me.

Hello.
Nothing new, nothing special... just a malware analysis from me.

Download the paper from here

» read more | ZaiRoN's blog | 3 comments

Symantec Virtual machine paper

Submitted by valsmith on Mon, 2007-02-05 15:16. Research

I highly recommend you read this:

http://www.symantec.com/avcenter/reference/Virtual_Machine_Threats.pdf
Its a very comprehensive paper on Virtual Machines and their issues. As a bonus they cite an Offensive Computing paper in the references :)

V.

User login

Username: *

Password: *

- Create new account
- Request new password

Navigation

- About Us
- Getting Started
- Consulting Services
- Contact
- Major Contributors

- Malware
- Research
- Tools
- Press

Navigation

- archive
- blogs
- forums
- polls

Search

One of the first:

- Automated Malware Analysis
- Sandbox
- Shared disassembly
- Multiple AV scanner
- Collaborative RE

Los Alamos National Laboratory

- Research Scientist 4
  - Nuclear Weapons Division
  - CSIRT/Red Team
  - Non-Proliferation

Attack Research

Published Research

- Tactical Exploitation
- Tactical Response
  MetaPhish, PDF Infection, & Tor Backdoor
- Balancing the Pwn Trade Deficit
- Carnal0wnage Blog
- Blackhats Always Win
- From Internet to SCADA
- Dissecting Web Attacks
- ERP Forgotten Worlds
- Wolves Still Among Us
- The Internet
- The Nuclear Option
- Meta-Post Exploitation
- Inside the World of Malicious Blog Spam
- Legacy Systems (DARPA)

Beginning

- 1982 Tandy Color Computer
  - 7th Birthday
  - No storage allowed
  - 2000 lines of code
  - Start over on power off

Would you like to play a game?

- 1983 Wargames came out
  - Emulated it on the Tandy
  - No modem
  - Pretended to launch missiles
  - Scared the hell out of my friends
  - Parents freaked out
  - Grounded

1st Lesson

Human Psychology is a Vulnerability

(& adults don’t understand computers)

External Hacking

- Radio Shack display computers
  - Autoexec.bat
    - 10 PRINT “HACKED!”
    - 20 GOTO 10
- Walmart display computers
  - Security software
  - Bad directory permissions
  - Safe mode
  - Delete & Reboot

2nd Lesson

If you don’t physically control the computer, you can’t expect security

(even if you purchase a product to do so)

Imposter Syndrome

- Got a job at the Lab
  - Was like winning the lottery
  - No formal education
  - Surrounded by PHDs
  - Assumed I was too dumb
  - Terrified I'd get fired
  - Took on projects I didn't know how to do
    - Crypto
    - De-obfuscation
    - Supercomputers & Genome
  - Worked 8 hours every night
  - Became a research scientist

3rd Lesson

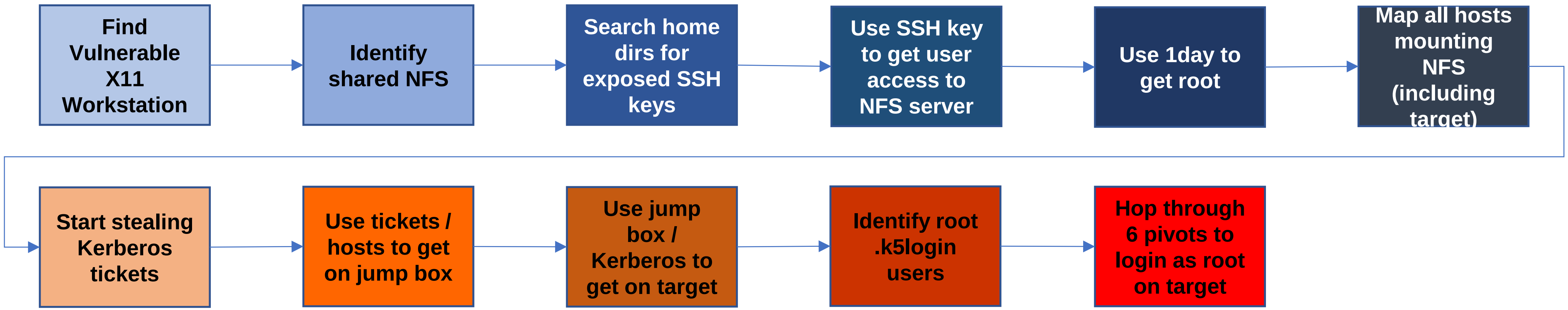
Take the opportunity & work hard

(everyone is winging it)

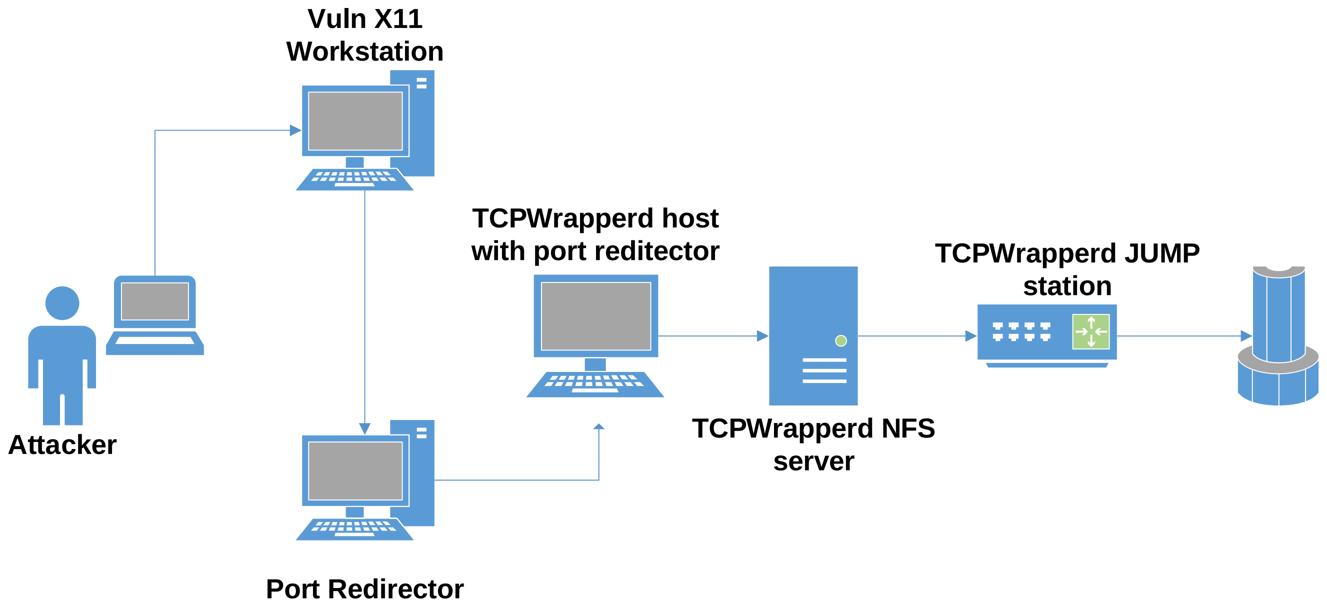
Hard Hacks – Super Computer

- **Task**:
  - Try to hack the fastest computer in the world
- **Protections:**
  - TCPWrappers
  - Kerberos
  - Log aggregation & analysis
  - SSH
  - Jump stations
  - 2FA

Hard Hacks – Super Computer



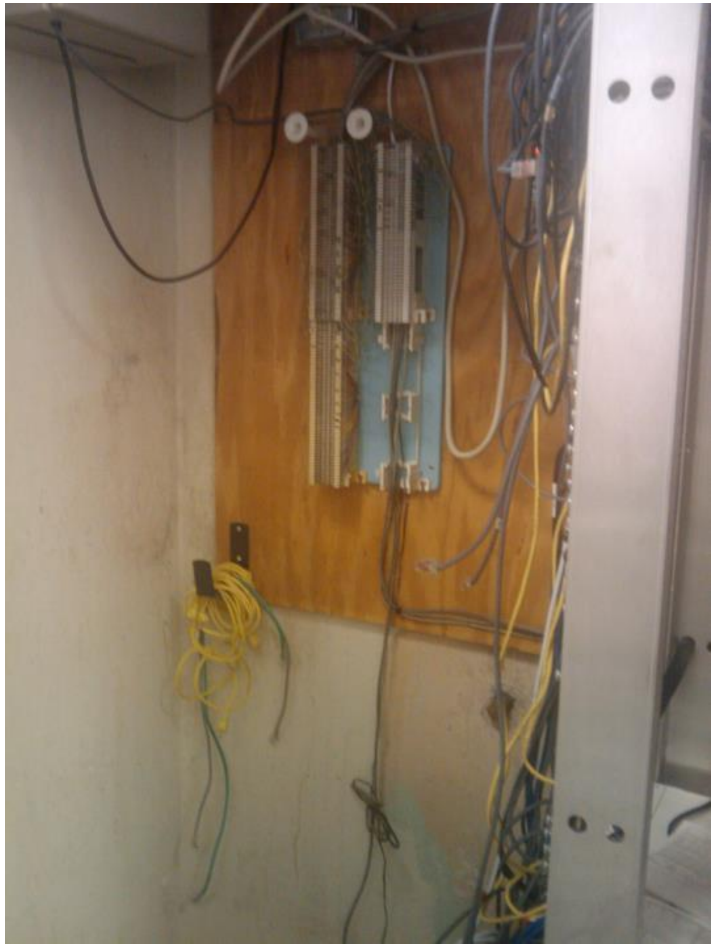
1. Find Vulnerable X11 Workstation
2. Identify shared NFS
3. Search home dirs for exposed SSH keys
4. Use SSH key to get user access to NFS server
5. Use 1day to get root
6. Map all hosts mounting NFS (including target)
7. Start stealing Kerberos tickets
8. Use tickets / hosts to get on jump box
9. Use jump box / Kerberos to get on target
10. Identify root .k5login users
11. Hop through 6 pivots to login as root on target

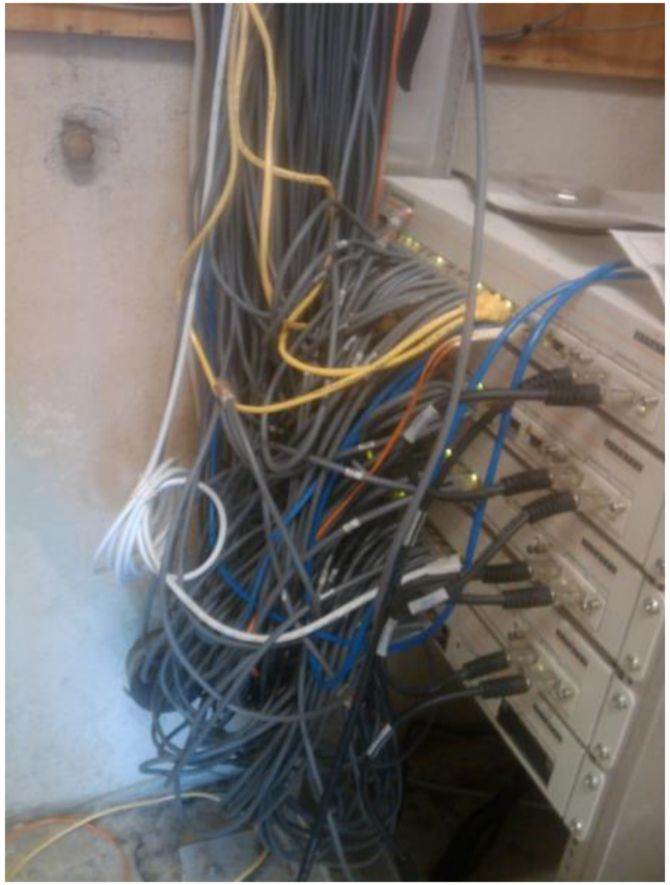


Hard Hacks - SCADA

- **Task**:
  - Hack “air-gapped” SCADA systems
- **Protections:**
  - Physical Security
  - “Air-gapped”
  - Not well known technology
  - Firewalls
  - Atypical network protocols

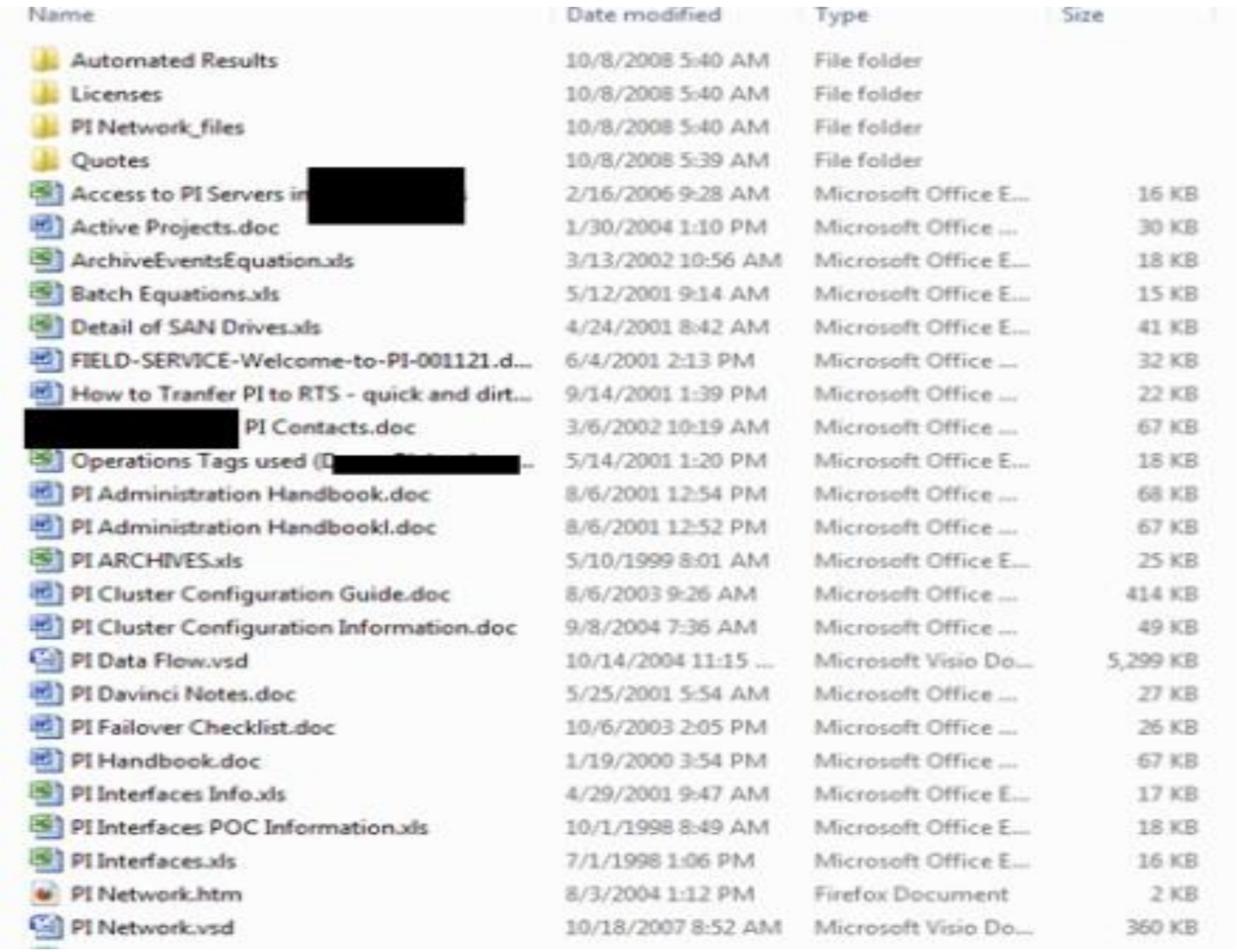
Hard Hacks - SCADA





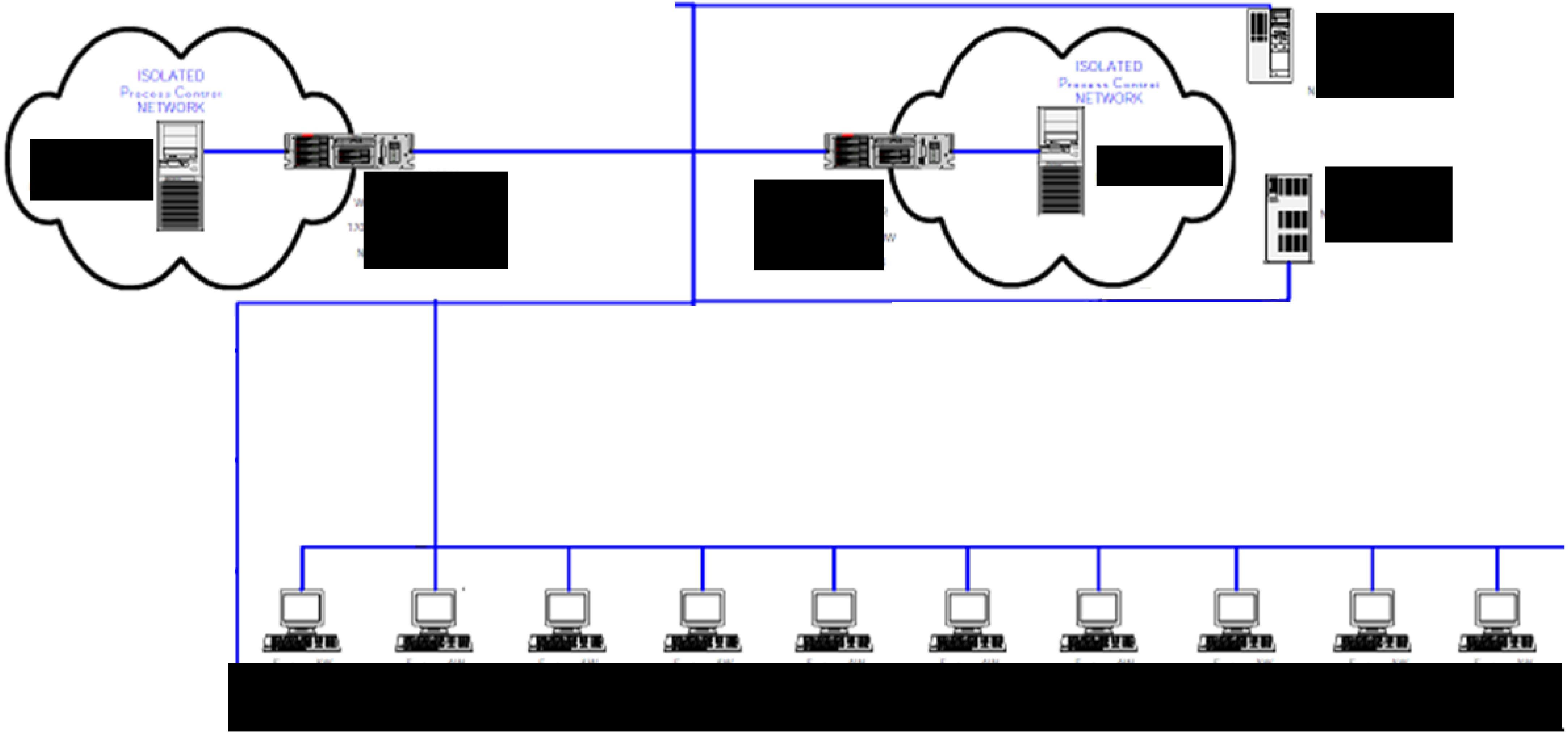
Hard Hacks - SCADA

SCADA system manuals, procedures, and access info on a compromised hosts desktop



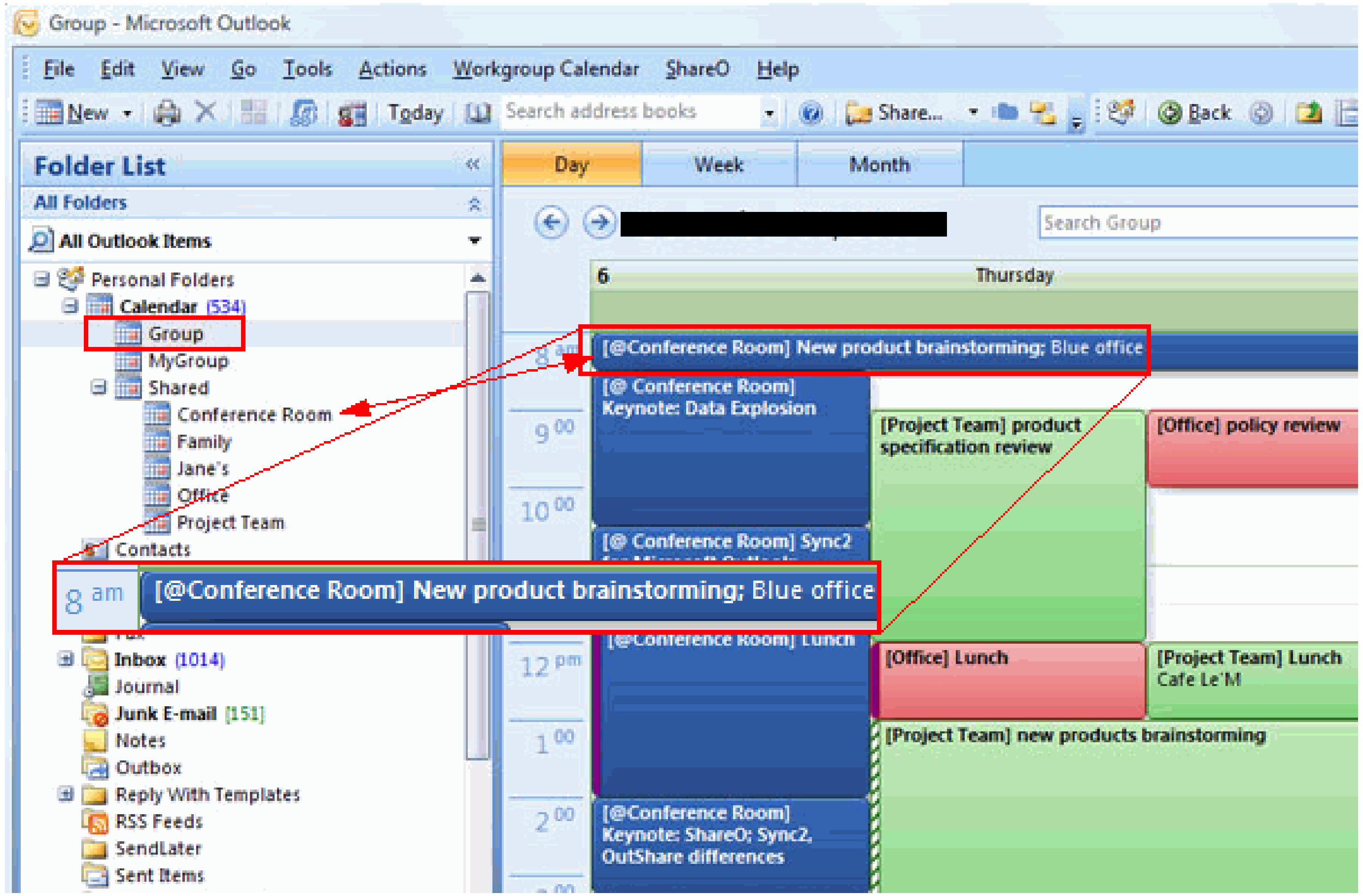
Name	Date modified	Type	Size
Automated Results	10/8/2008 5:40 AM	File folder	
Licenses	10/8/2008 5:40 AM	File folder	
PI Network_files	10/8/2008 5:40 AM	File folder	
Quotes	10/8/2008 5:39 AM	File folder	
Access to PI Servers i[redacted]	2/16/2006 9:28 AM	Microsoft Office E...	16 KB
Active Projects.doc	1/30/2004 1:10 PM	Microsoft Office ...	30 KB
ArchiveEventsEquation.xls	3/13/2002 10:56 AM	Microsoft Office E...	18 KB
Batch Equations.xls	5/12/2001 9:14 AM	Microsoft Office E...	15 KB
Detail of SAN Drives.xls	4/24/2001 8:42 AM	Microsoft Office E...	41 KB
FIELD-SERVICE-Welcome-to-PI-001121.d...	6/4/2001 2:13 PM	Microsoft Office ...	32 KB
How to Tranfer PI to RTS - quick and dirt...	9/14/2001 1:39 PM	Microsoft Office ...	22 KB
[redacted] PI Contacts.doc	3/6/2002 10:19 AM	Microsoft Office ...	67 KB
Operations Tags used (D[redacted]..	5/14/2001 1:20 PM	Microsoft Office E...	18 KB
PI Administration Handbook.doc	8/6/2001 12:54 PM	Microsoft Office ...	68 KB
PI Administration Handbookl.doc	8/6/2001 12:52 PM	Microsoft Office ...	67 KB
PI ARCHIVES.xls	5/10/1999 8:01 AM	Microsoft Office E...	25 KB
PI Cluster Configuration Guide.doc	8/6/2003 9:26 AM	Microsoft Office ...	414 KB
PI Cluster Configuration Information.doc	9/8/2004 7:36 AM	Microsoft Office ...	49 KB
PI Data Flow.vsd	10/14/2004 11:15 ...	Microsoft Visio Do...	5,299 KB
PI Davinci Notes.doc	5/25/2001 5:54 AM	Microsoft Office ...	27 KB
PI Failover Checklist.doc	10/6/2003 2:05 PM	Microsoft Office ...	26 KB
PI Handbook.doc	1/19/2000 3:54 PM	Microsoft Office ...	67 KB
PI Interfaces Info.xls	4/29/2001 9:47 AM	Microsoft Office E...	17 KB
PI Interfaces POC Information.xls	10/1/1998 8:49 AM	Microsoft Office E...	18 KB
PI Interfaces.xls	7/1/1998 1:06 PM	Microsoft Office E...	16 KB
PI Network.htm	8/3/2004 1:12 PM	Firefox Document	2 KB
PI Network.vsd	10/18/2007 8:52 AM	Microsoft Visio Do...	360 KB

Hard Hacks - SCADA



Hard Hacks - SCADA

- Access to victim Outlook
  - Including Calendar
  - Engineers used VNC to connect to SCADA systems
    - (and left them connected)
  - Wait for PLC engineer to go to a meeting
  - Take over his box and use his GUI SCADA apps to cause havoc



[redacted]

[@Conference Room] New product brainstorming; Blue office

[@ Conference Room] Keynote: Data Explosion

[Project Team] product specification review

[Office] policy review

[@ Conference Room] Sync2

8 am [@Conference Room] New product brainstorming; Blue office

[@Conference Room] Lunch

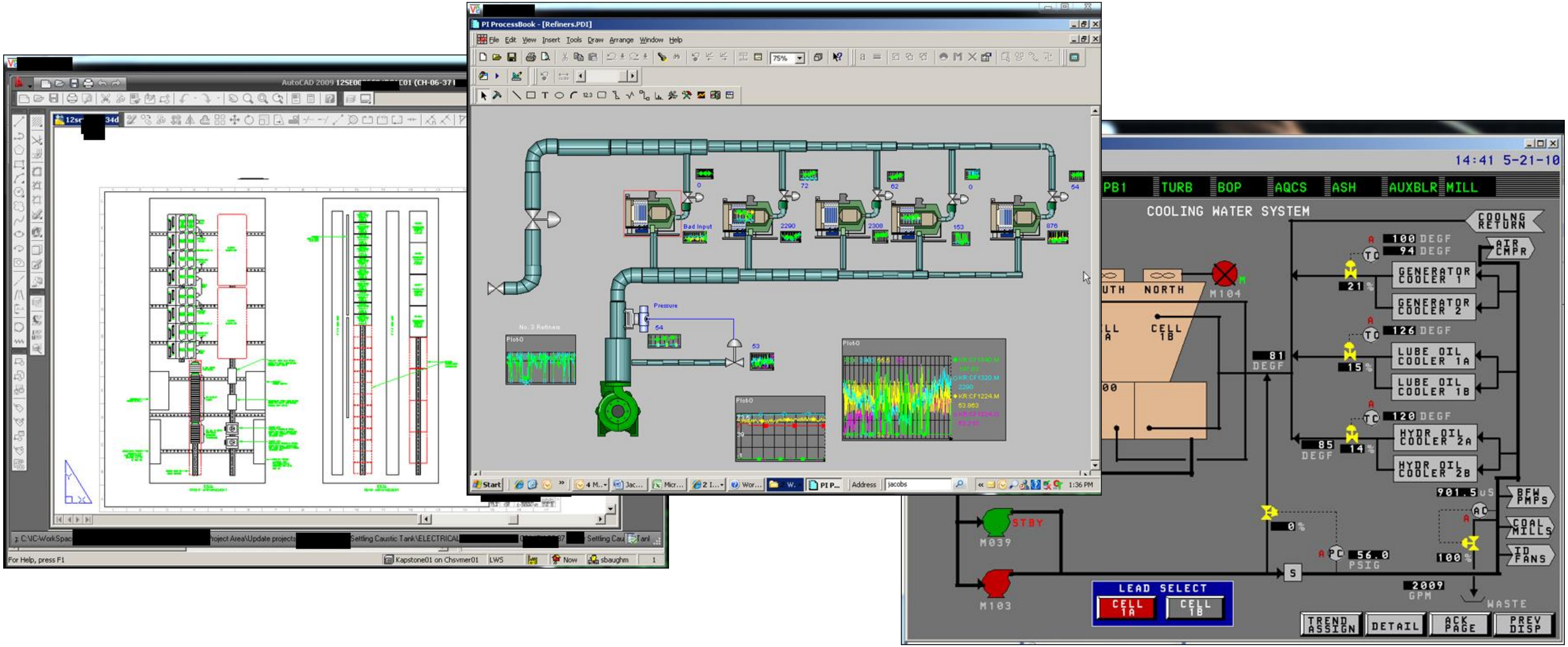
[Office] Lunch

[Project Team] Lunch Cafe Le'M

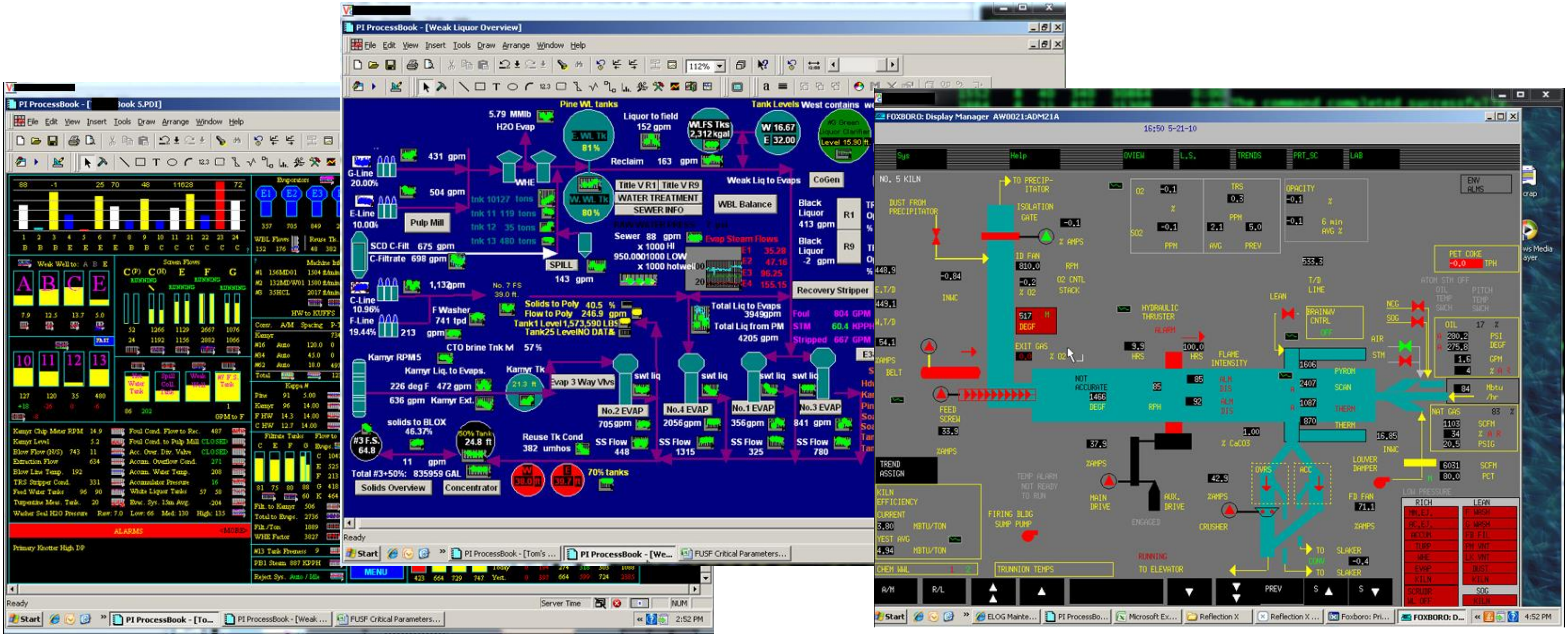
[Project Team] new products brainstorming

[@Conference Room] Keynote: ShareO; Sync2, OutShare differences

Hard Hacks - SCADA



Hard Hacks - SCADA



4th Lesson

Everything is hackable

(no matter how crazy)

I Want to be a Pen Tester

- Well over 200,000 computers compromised
- Hack once, come back the next year, same vulnerabilities exist
- Problems never change
  - Bad IT operations
  - Weak passwords
  - Unpatched systems
- Could write the report without doing the test and be 90% right
- Basically patch management validation
- Good pentesters always win

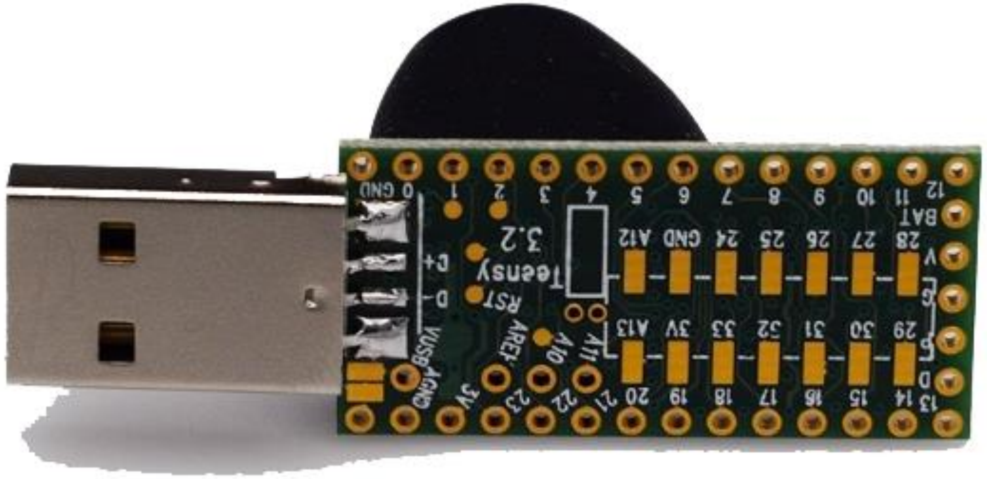
5th Lesson

Many Organizations Don’t Benefit from Penetration Testing

(and the market devoured itself)

Ethics & Business Decisions

- Individual stole sensitive info using USB
- We investigated
- Built a tool to detect where key had been used
  - And if others had
- Were told to delete the tool
- Protect Business Interests

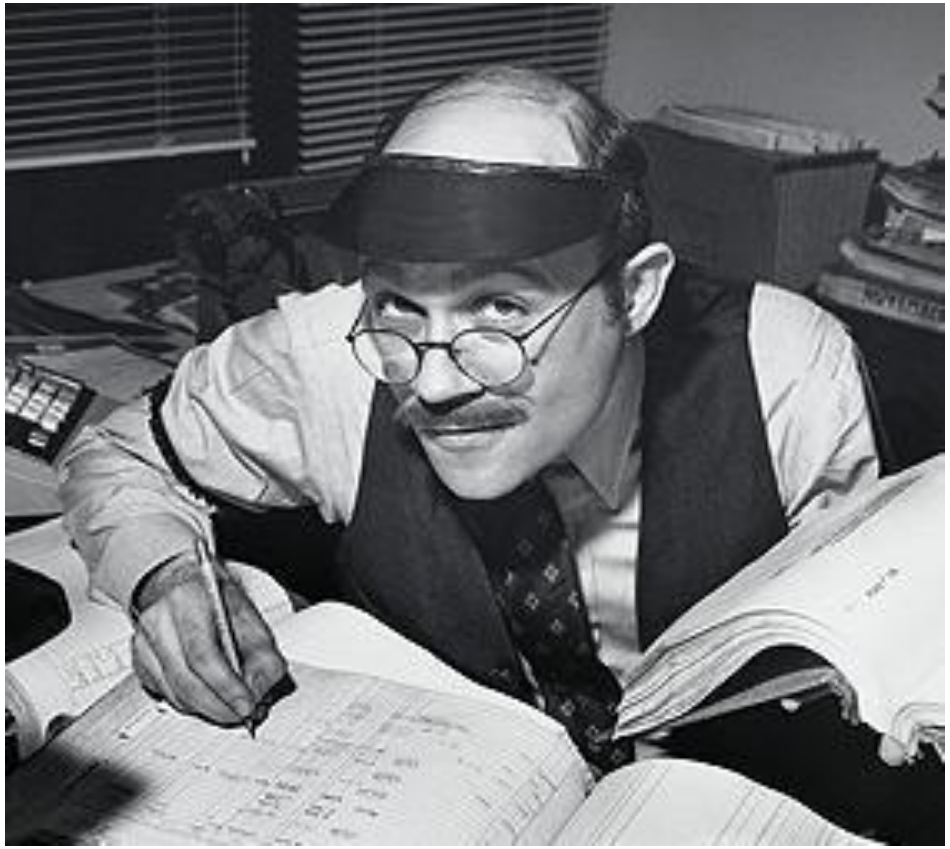


Ethics & Business Decisions

- High revenue customer
- InfoSec vs Management
  - **InfoSec**: “Our mission is to protect company data”
  - **Management**: “We need them to provide metrics for acquisition’s due diligence, but not find too much”
- Management thought they had 15 security people
  - 1 EA, 1 Sr. Advisor, 1 DBA, 3 SysAdmins, 2 managers, 1 DevOps, 1 Coder, etc.
  - 1 Sr. security engineer (quitting), 1 Jr. security engineer

Ethics & Business Decisions

- Transportation Technology Customer
  - PCI requirements didn't fit
  - Still had to be compliant
  - "Enabled" audit passing
  - Put real focus into product security
  - Provided actual security value to customers while working around PCI requirements



Ethics & Business Decisions

- Energy customer
- Multiple compromises
- We put advanced IR / RE in place
    - Expensive with low value return
    - What does attribution buy you?
- Instead, they ensured they could completely rebuild any system, anywhere in the world, in less than 4 hours
    - Requires strong inventory / architecture

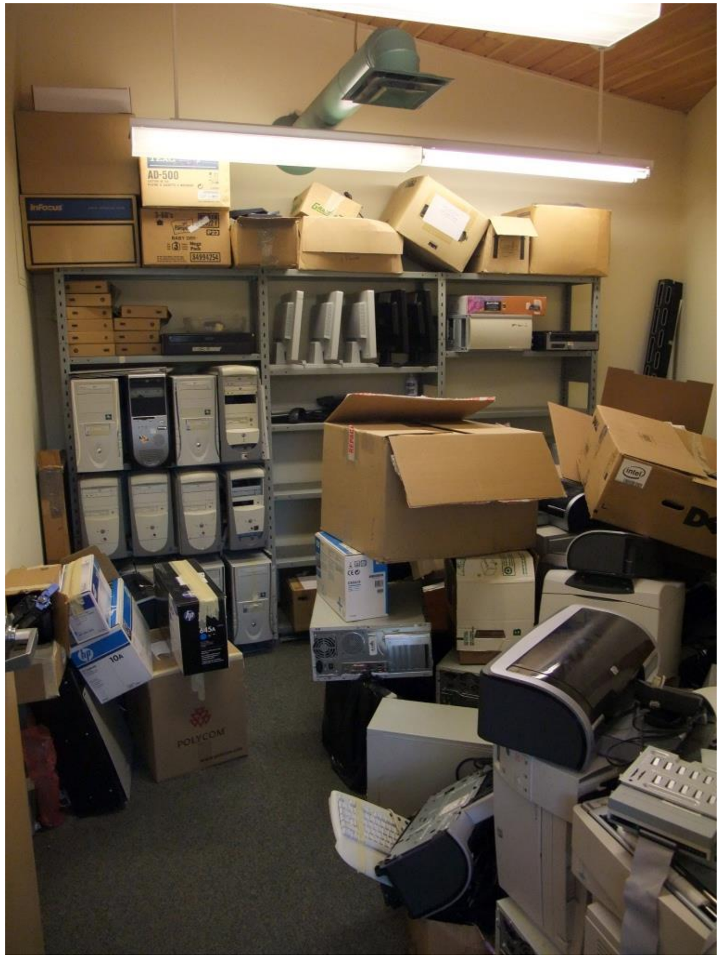
6th Lesson

Valid Business Decisions Can Contradict Conventional Security Wisdom

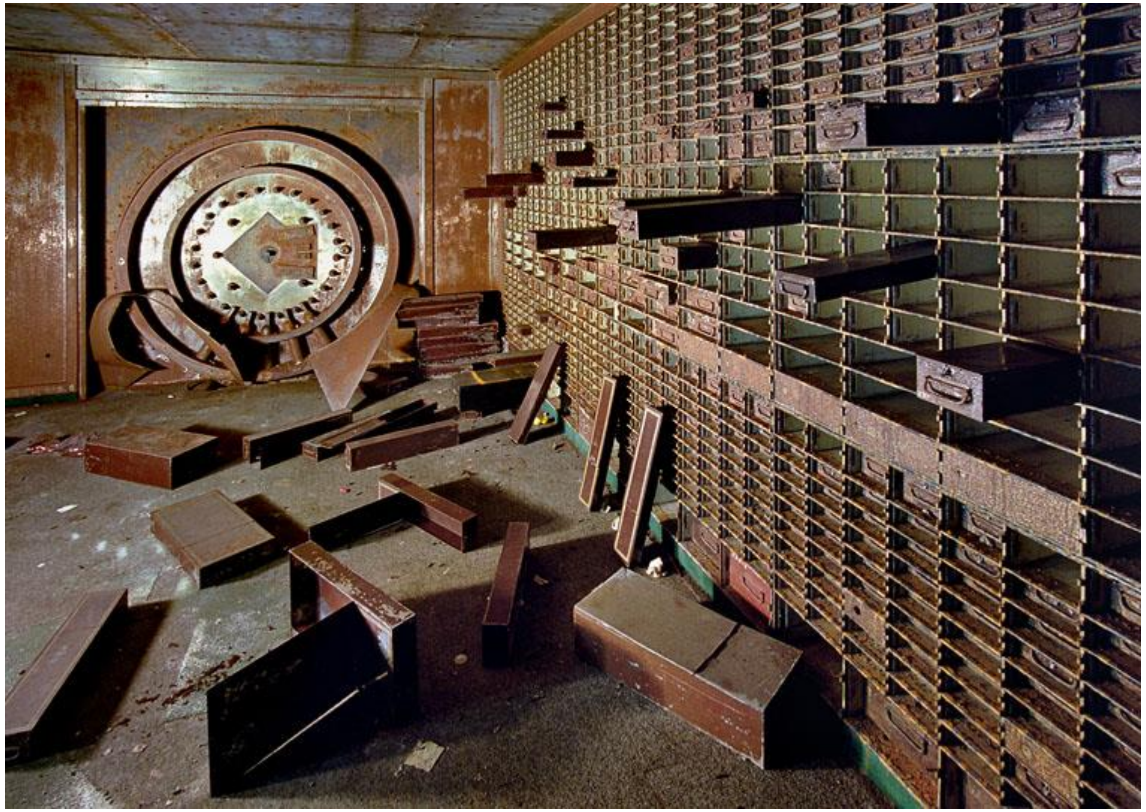
(I didn’t know everything)

Stacks of Security Products

- Transportation Tech Client
  - Purchased all kinds of security products
    - AV
    - IPS/IDS
    - Firewalls
    - Anti-malware
    - Log Aggregation / SEIM
    - Threat Intelligence
  - Not enough staff to deploy / monitor
  - Appliances sat stacked in boxes for years
  - Still got hacked multiple times



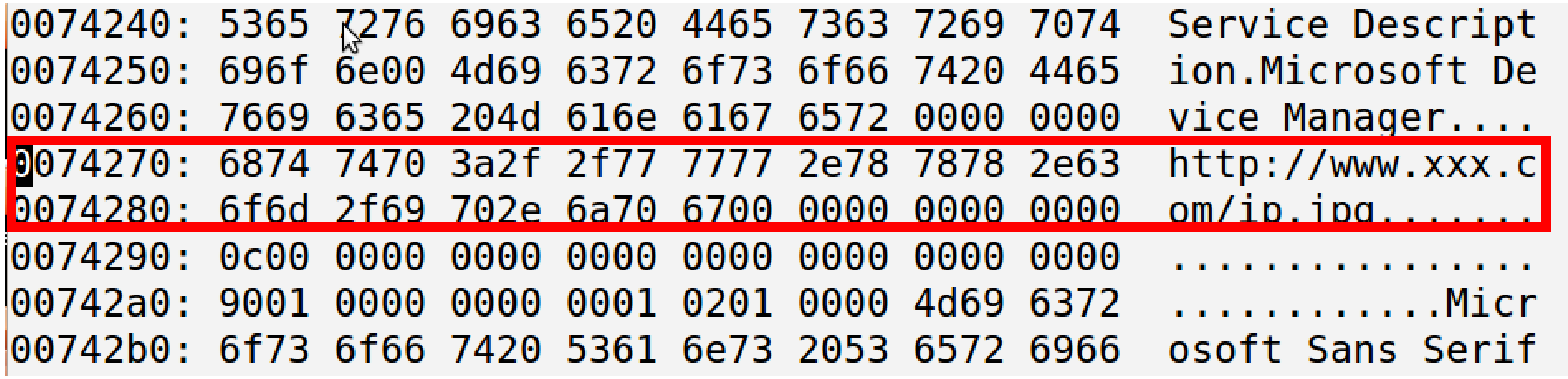
DLP



- Large Hedge Fund
- **Task**:
  - Test several top DLP products
- **Protections**:
  - Keyword detection & alerting
  - Network protocol analysis
  - “Secret” endpoint agents
  - Traffic monitoring
- Every single one was compromised / bypass in 1 day

An Inconvenient AV Truth

- **How to most AV’s work?**
  - Disclaimer: This is an over-simplification
  - OP Code / Hex Byte Signature matching
    - Each file is read on disk (not executed)
    - The file is parsed
    - The AV searches for a known sequence of bytes



```
0074240: 5365 7276 6963 6520 4465 7363 7269 7074  Service Descript
0074250: 696f 6e00 4d69 6372 6f73 6f66 7420 4465  ion.Microsoft De
0074260: 7669 6365 204d 616e 6167 6572 0000 0000  vice Manager....
0074270: 6874 7470 3a2f 2f77 7777 2e78 7878 2e63  http://www.xxx.c
0074280: 6f6d 2f69 702e 6a70 6700 0000 0000 0000  om/ip.jpg.......
0074290: 0c00 0000 0000 0000 0000 0000 0000 0000  ................
00742a0: 9001 0000 0000 0001 0201 0000 4d69 6372  ............Micr
00742b0: 6f73 6f66 7420 5361 6e73 2053 6572 6966  osoft Sans Serif
```

An Inconvenient AV Truth

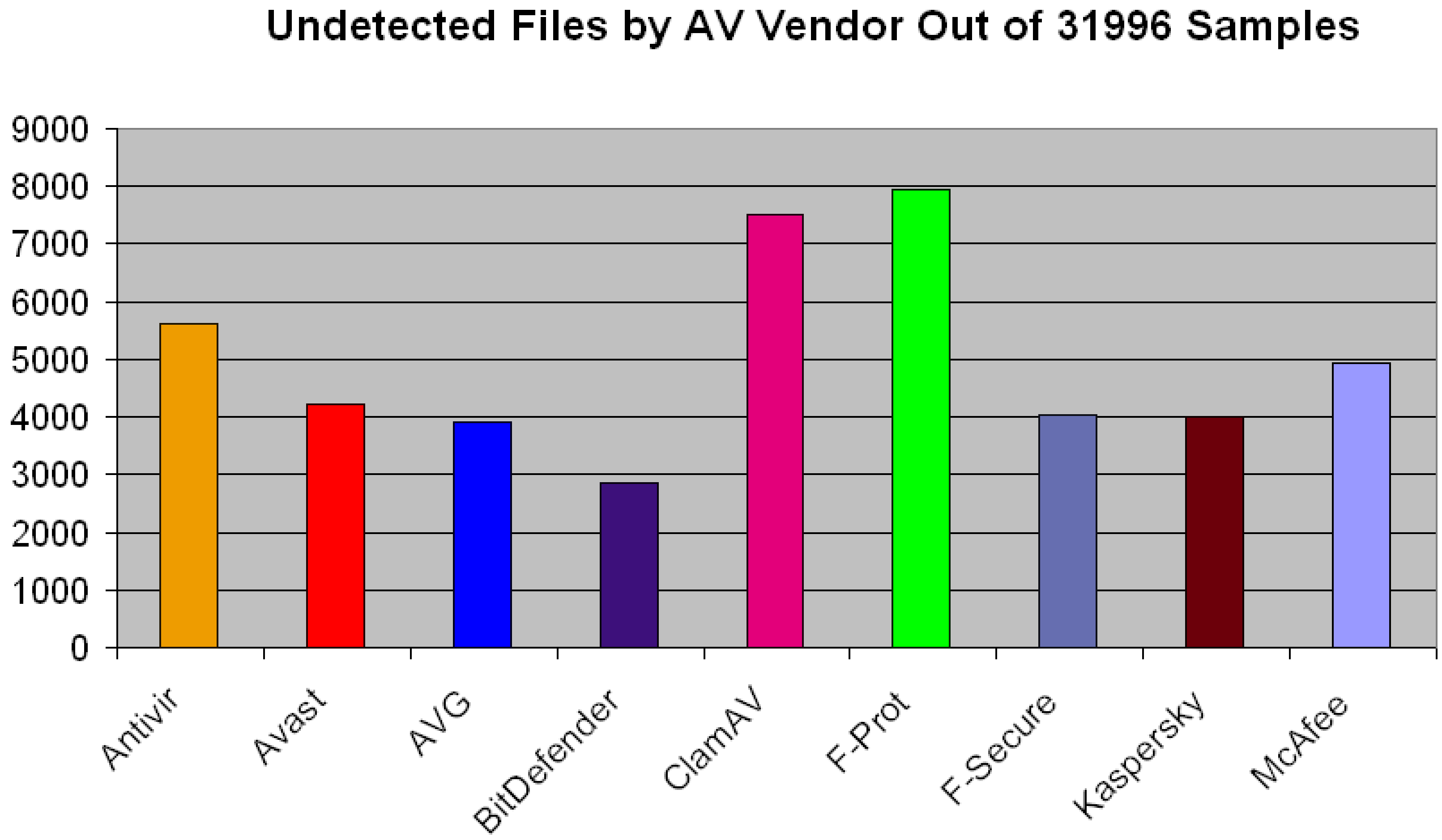
- **Evasion Example Part 1**
  - Example string in a file used by AV for detection:
    - “fatal: cracking requires a username”
  - String in bytes, aka rough AV signature:

    66 61 74 61 6C 3A 20 63 72 61 63 6B 69 6E 67 20 72 65 71 75 69 72 65 73 20 61 20 75 73 65 72 6E 61 6D 65 0A 00
  - Attacker changes a few bytes to change the string and evade the signature using a binary / hex editor

    66 61 74 61 6C 3A 20 **63 72 61 63** 6B 69 6E 67 20 72 65 71 75 69 72 65 73 20 61 20 75 73 65 72 6E 61 6D 65 0A 00
  - Becomes:

    66 61 74 61 6C 3A 20 **62 72 65 62** 6B 69 6E 67 20 72 65 71 75 69 72 65 73 20 61 20 75 73 65 72 6E 61 6D 65 0A 00

An Inconvenient AV Truth



40% efficacy rate common

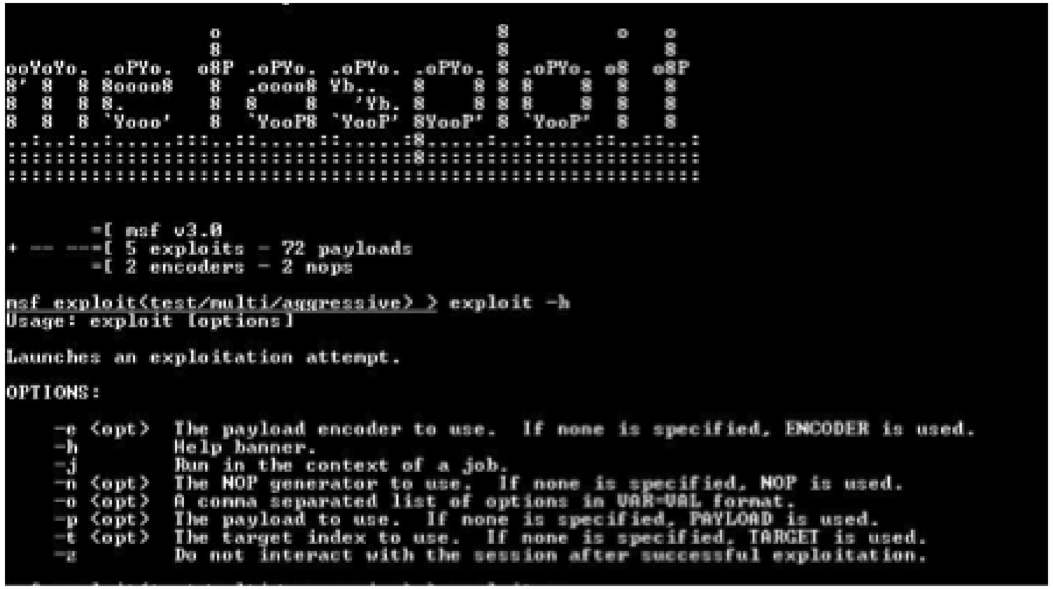
7th Lesson

Security Products Don’t Work

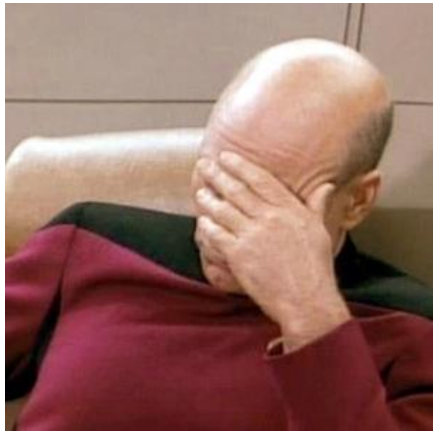
(but you still probably need them)

Metasploit

- Framework for Exploit Dev:
  - Shellcode library
  - Network protocol handlers
  - Encoders
  - Opcode searcher
  - Can write exploits in a couple of lines
  - Super powerful for exploit dev
- How did everyone use it?
  - As a pentesting tool

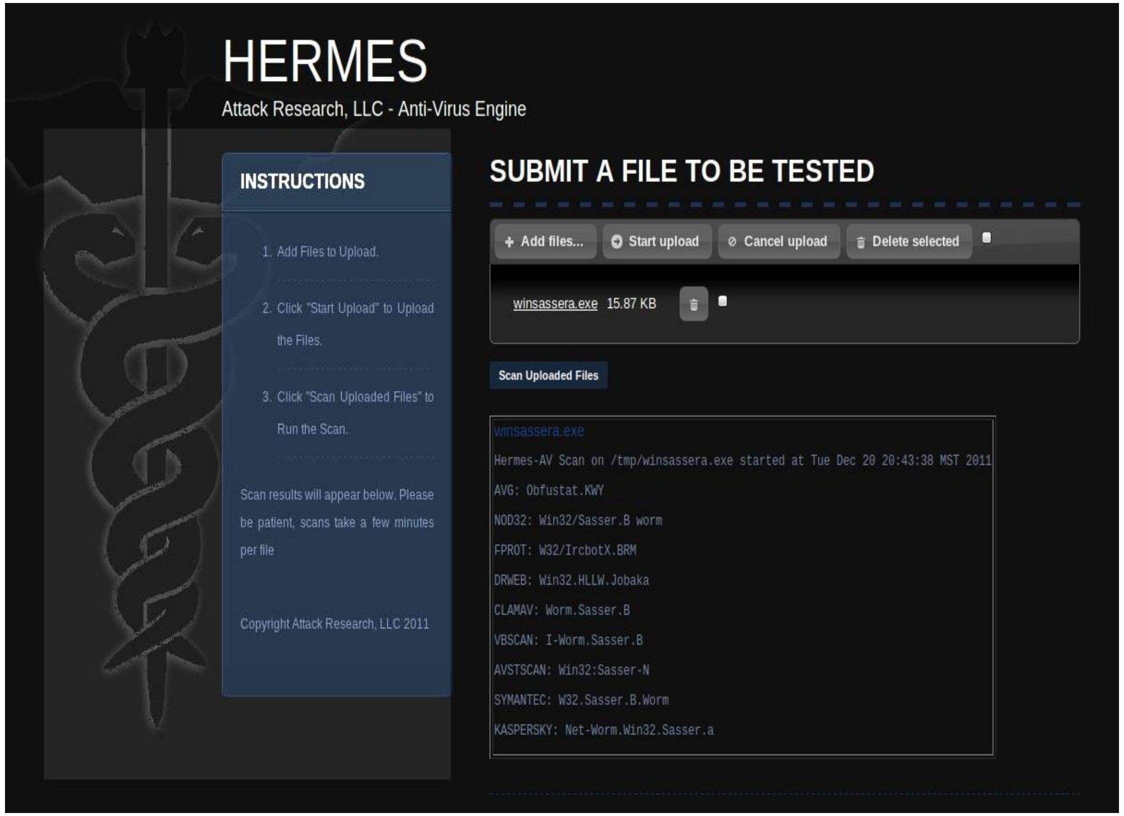


```
                     o                          8         o   o
                     8                          8             8
ooYoYo. .oPYo.  o8P .oPYo. .oPYo. .oPYo. 8 .oPYo. o8   o8P
8' 8  8 8oooo8   8  .oooo8 Yb..   8    8 8 8    8  8    8
8  8  8 8.       8  8    8   'Yb. 8    8 8 8    8  8    8
8  8  8 `Yooo'   8  `YooP8 `YooP' 8YooP' 8 `YooP'  8    8
..:..:..:.....:::..::.....::.....:8.....:..:.....::..::..:
::::::::::::::::::::::::::::::::::8:::::::::::::::::::::::::
::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::


       =[ msf v3.0
+ -- --=[ 5 exploits - 72 payloads
       =[ 2 encoders - 2 nops

msf exploit(test/multi/aggressive) > exploit -h
Usage: exploit [options]

Launches an exploitation attempt.

OPTIONS:

    -e <opt>  The payload encoder to use.  If none is specified, ENCODER is used.
    -h        Help banner.
    -j        Run in the context of a job.
    -n <opt>  The NOP generator to use.  If none is specified, NOP is used.
    -o <opt>  A comma separated list of options in VAR=VAL format.
    -p <opt>  The payload to use.  If none is specified, PAYLOAD is used.
    -t <opt>  The target index to use.  If none is specified, TARGET is used.
    -z        Do not interact with the session after successful exploitation.
```



Malware Analysis

- I developed, built, submitted patent for a RE replacement
  - Dynamic / Static analysis
  - Machine Learning
  - Multi-AV Scanner
  - IOC extraction
  - Imports extraction
  - Anti-anti-analysis
- Several years of development
- ~100 customer max market



HERMES

Attack Research, LLC - Anti-Virus Engine

INSTRUCTIONS

1. Add Files to Upload.
2. Click "Start Upload" to Upload the Files.
3. Click "Scan Uploaded Files" to Run the Scan.

Scan results will appear below. Please be patient, scans take a few minutes per file

Copyright Attack Research, LLC 2011

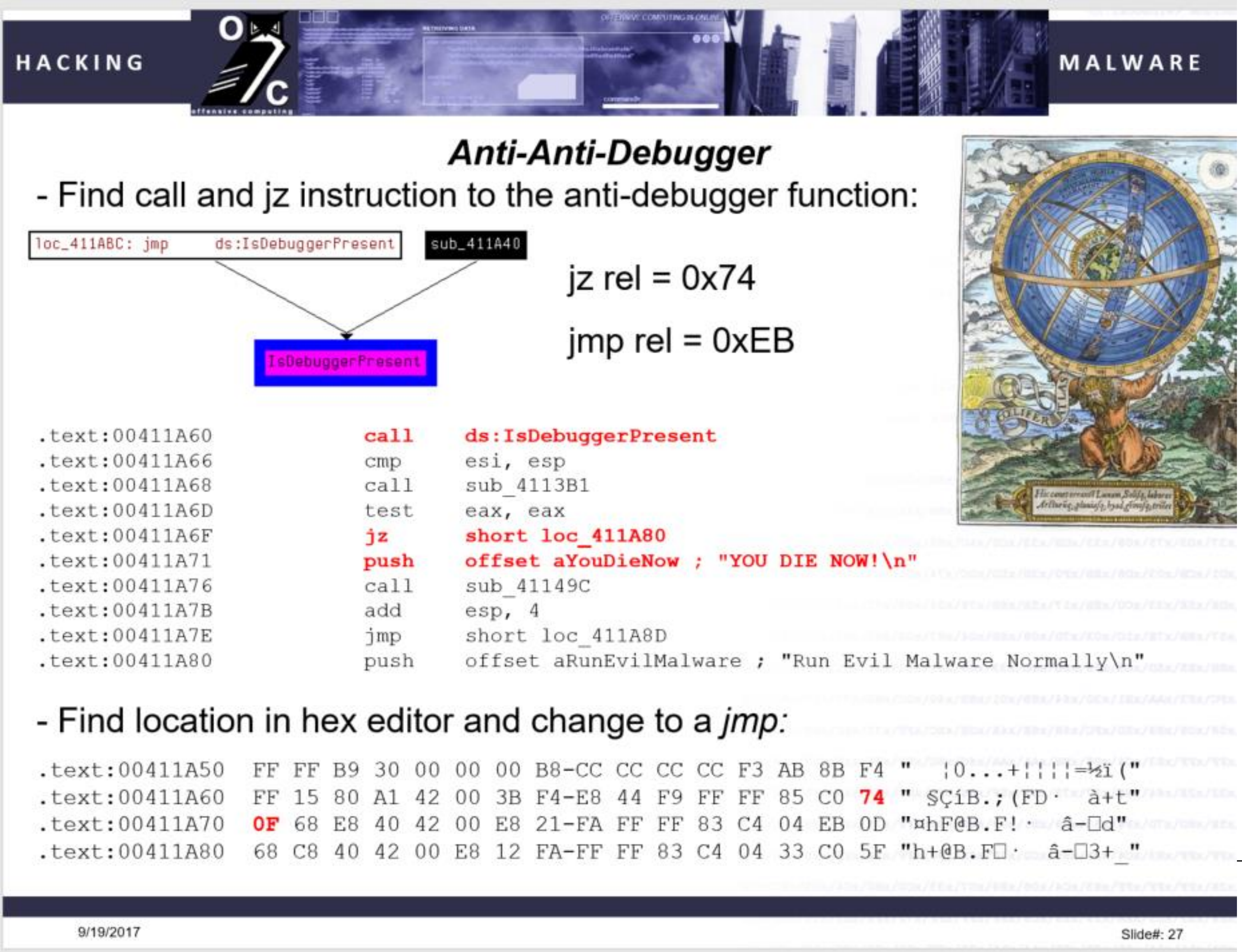
SUBMIT A FILE TO BE TESTED

winsassera.exe 15.87 KB

```
winsassera.exe
Hermes-AV Scan on /tmp/winsassera.exe started at Tue Dec 20 20:43:38 MST 2011
AVG: Obfustat.KWY
NOD32: Win32/Sasser.B worm
FPROT: W32/IrcbotX.BRM
DRWEB: Win32.HLLW.Jobaka
CLAMAV: Worm.Sasser.B
VBSCAN: I-Worm.Sasser.B
AVSTSCAN: Win32:Sasser-N
SYMANTEC: W32.Sasser.B.Worm
KASPERSKY: Net-Worm.Win32.Sasser.a
```

Con Talks

- One of my first con talk slides



Anti-Anti-Debugger

- Find call and jz instruction to the anti-debugger function:

jz rel = 0x74

jmp rel = 0xEB

```
.text:00411A60          call    ds:IsDebuggerPresent
.text:00411A66          cmp     esi, esp
.text:00411A68          call    sub_4113B1
.text:00411A6D          test    eax, eax
.text:00411A6F          jz      short loc_411A80
.text:00411A71          push    offset aYouDieNow ; "YOU DIE NOW!\n"
.text:00411A76          call    sub_41149C
.text:00411A7B          add     esp, 4
.text:00411A7E          jmp     short loc_411A8D
.text:00411A80          push    offset aRunEvilMalware ; "Run Evil Malware Normally\n"
```

- Find location in hex editor and change to a *jmp:*

```
.text:00411A50  FF FF B9 30 00 00 00 B8-CC CC CC CC F3 AB 8B F4 "   ¦0...+¦¦¦¦=½ï("
.text:00411A60  FF 15 80 A1 42 00 3B F4-E8 44 F9 FF FF 85 C0 74 " §ÇíB.;(FD·  à+t"
.text:00411A70  0F 68 E8 40 42 00 E8 21-FA FF FF 83 C4 04 EB 0D "¤hF@B.F!·  â-□d"
.text:00411A80  68 C8 40 42 00 E8 12 FA-FF FF 83 C4 04 33 C0 5F "h+@B.F□·  â-□3+_"
```

9/19/2017

Slide#: 27

Con Talks

- One of my last con talk slides

THESE GUYS

Slide: 6

Con Talks

- Guess which one was more popular / higher rated?
  - Other researchers (maybe 20-40 people?) liked and respected the first set of slides
  - Everyone else assumed I was smart, but couldn’t really take my research back to work with them and apply it on real business security problems
  - Other researchers didn’t care about my last set of slides
  - Most of the audience found real value in the material
  - I learned to simplify and speak about concepts with broad impact rather than highly technical niche hacks

8th Lesson

What You Think is Cool is Not Necessarily What Everyone Thinks is Cool

(and there may be no market for it)

((but it still may have value in ways you never considered))

Program Death

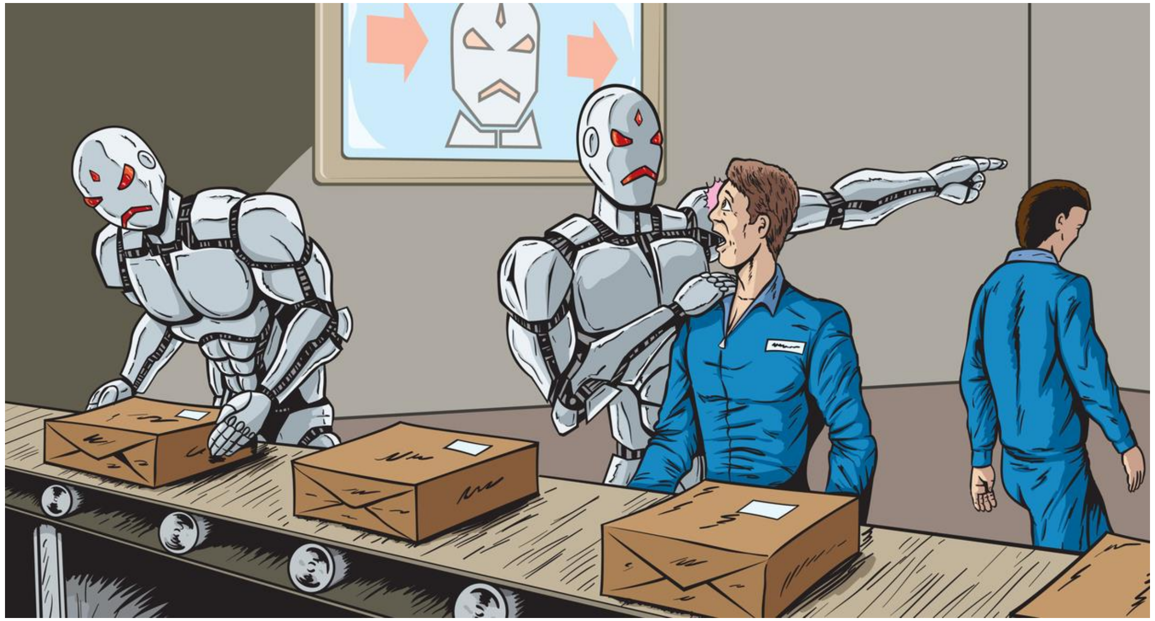
- Worked in a 30mil $ security program
  - Massive morale problems, non-competitive pay, no internal capability investment
  - Four core staff proposed program restructuring and solutions
  - CEO: “I couldn’t fix this if I wanted to, not a business priority”
  - Top management: “Deal with it, you won’t go anywhere, do more with less”
  - All four staff left and within one year the program completely collapsed
  - Massive unintended consequences
  - Organization is now desperately trying to rebuild it

Most Secure Client Ever

- Major Social Media client had a best-in-class security team of over 20 people
- We conducted a 6 week attack simulation using 0days, C2 in China, hardware implants, custom tools
  - We got caught (we never get caught)
  - Within 4 hours of detection they knew everything we had done
  - Tons of custom, in-house written tools, effectively deployed products, training, monitoring staff, etc.
- A competitor hired away the entire team
- We went back three years later and they couldn’t detect or stop us, nor could they determine what we had done

Outsourcing FTW

- Major Oil Client
  - Security team of 15 people
  - Paid us for 1 year to build and automate security processes
  - The whole team quit
  - Monitoring and maintenance of what we built was outsourced to 3rd world country for 15$ an hour
  - They have not been hacked



Outsourcing FTW

- Large Hedge Fund
  - IT team of 100s
  - Very high standards for all groups (except IT)
  - Hacked everything
  - Vulnerabilities found were due to IT’s failures
  - They fired and replaced ALL of IT in 1 year
  - Security increased 10x

9th Lesson

Good Security Programs Depend on People and Can Die Quickly

(Hold on to your key, linchpin staff)

((With deep enough pockets and strong IT, people can be replaced))

(((be careful what you recommend, they might listen to you)))

Putting It Together

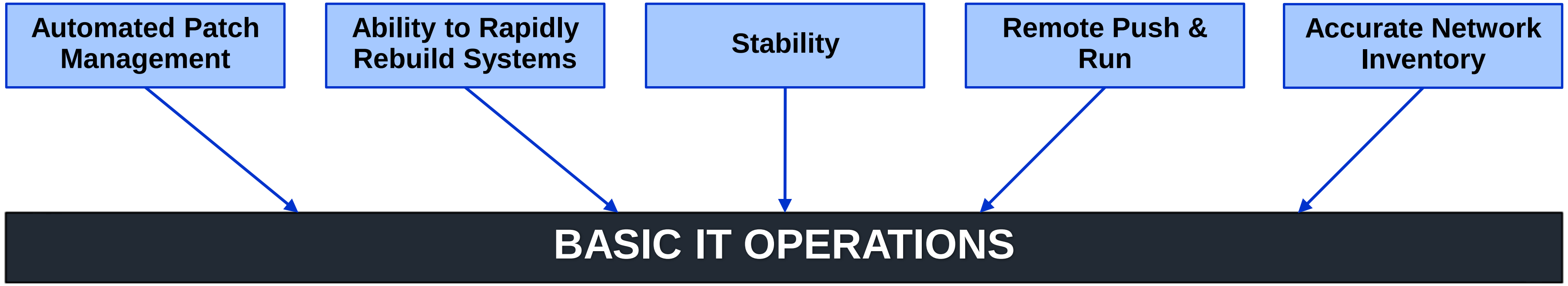
- I have founded and run multiple security companies
- Built and operated enterprise security programs
- Consulted for Fortune 10 clients
- Reverse engineered, tracked, and analyzed countless APT and criminal attacks
- Penetrated 100’s of 1000’s of computers
- Built and tried to sell security products
- Trained 100s of security professionals
- What is the main lesson I have learned?

10th Lesson

Strong Basic IT Operations Matter More Than Almost Any Other Security Factor

(getting the basics done is more important than “cool”)

Security Pyramid



Automated Patch Management

Ability to Rapidly Rebuild Systems

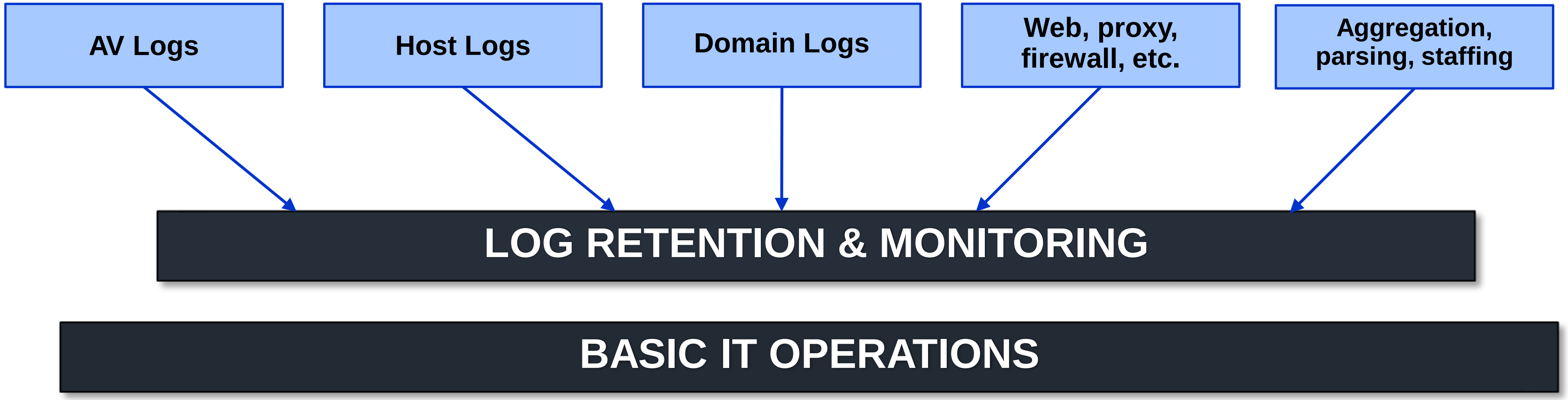
Stability

Remote Push & Run

Accurate Network Inventory

BASIC IT OPERATIONS

Security Pyramid



AV Logs

Host Logs

Domain Logs

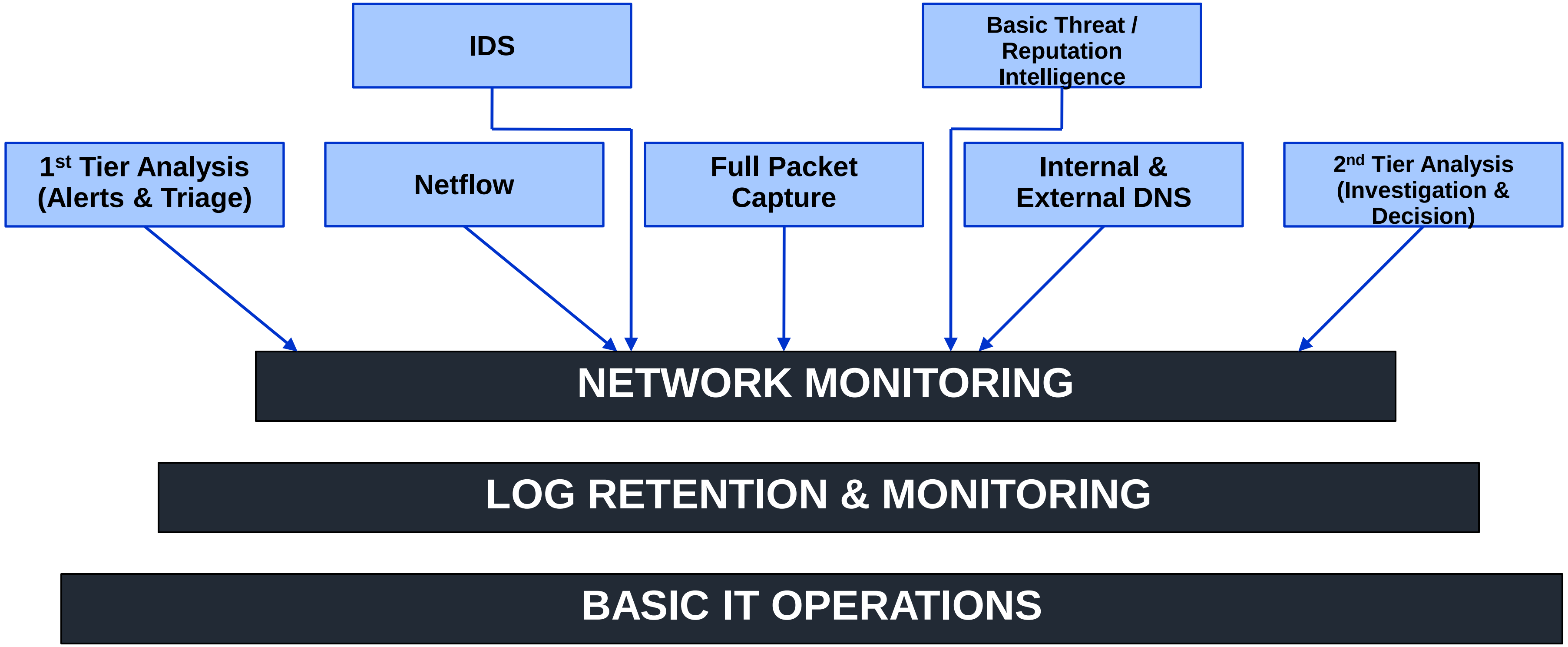
Web, proxy, firewall, etc.

Aggregation, parsing, staffing

LOG RETENTION & MONITORING

BASIC IT OPERATIONS

Security Pyramid



IDS

Basic Threat / Reputation Intelligence

1st Tier Analysis (Alerts & Triage)

Netflow

Full Packet Capture

Internal & External DNS

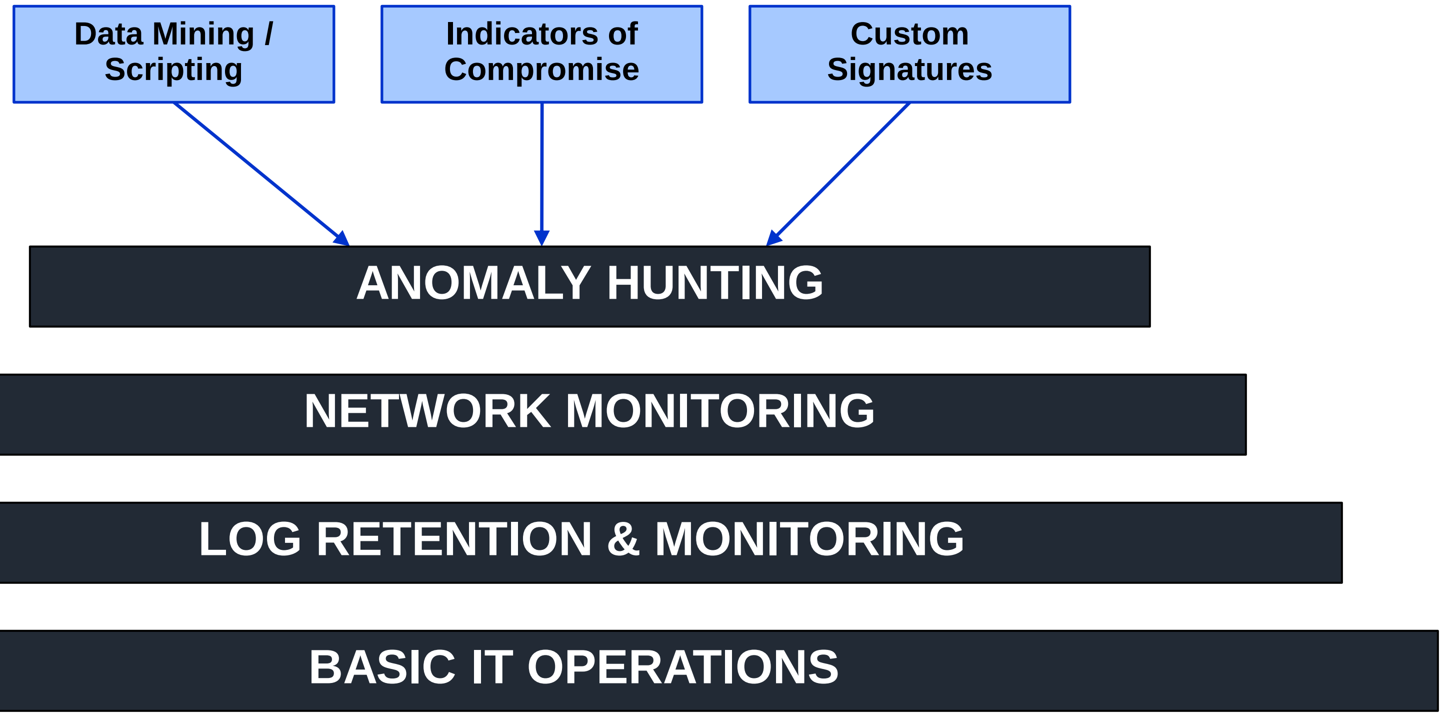
2nd Tier Analysis (Investigation & Decision)

NETWORK MONITORING

LOG RETENTION & MONITORING

BASIC IT OPERATIONS

Security Pyramid



Data Mining / Scripting

Indicators of Compromise

Custom Signatures

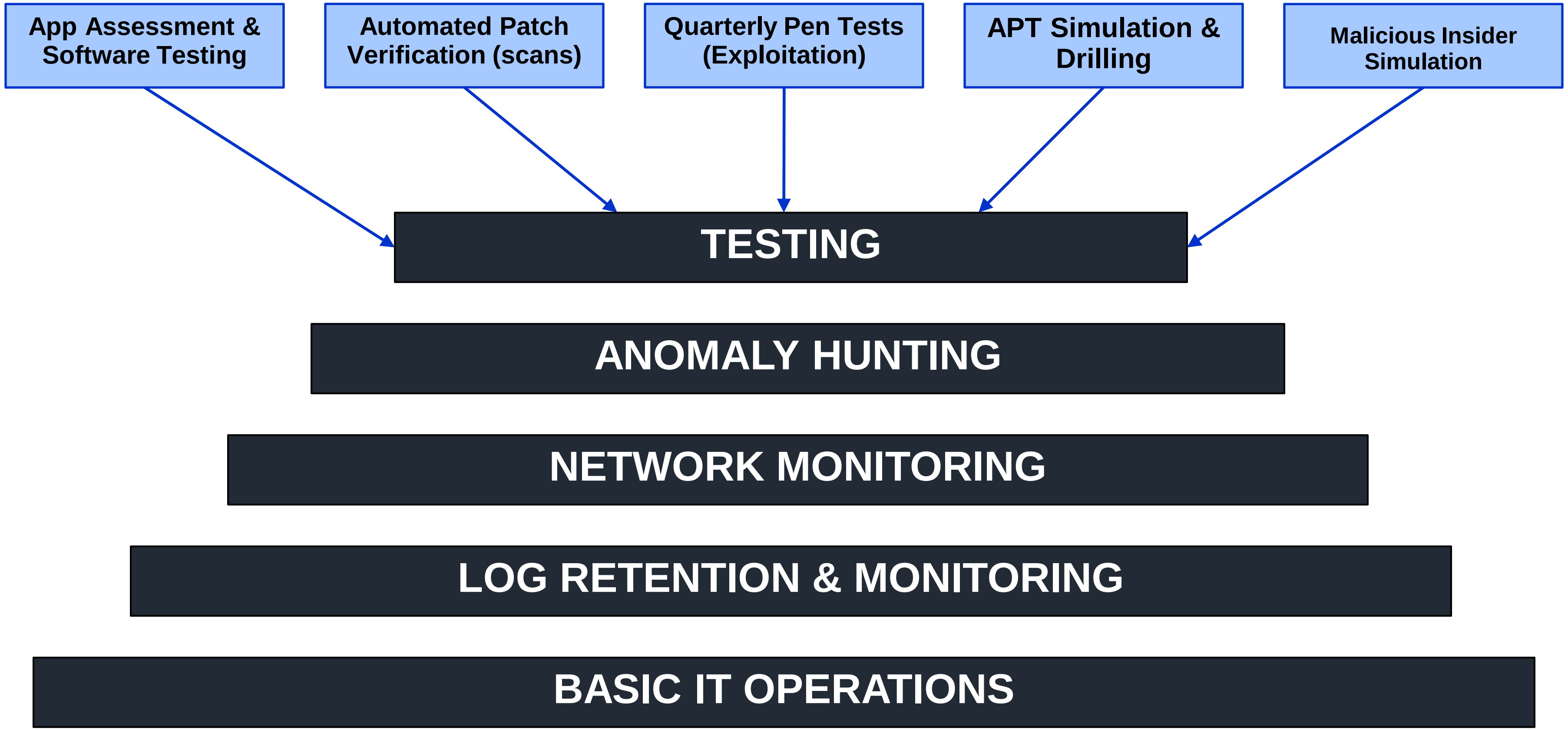
ANOMALY HUNTING

NETWORK MONITORING

LOG RETENTION & MONITORING

BASIC IT OPERATIONS

Security Pyramid



(may belong lower down if you are a product company)

App Assessment & Software Testing

Automated Patch Verification (scans)

Quarterly Pen Tests (Exploitation)

APT Simulation & Drilling

Malicious Insider Simulation

TESTING

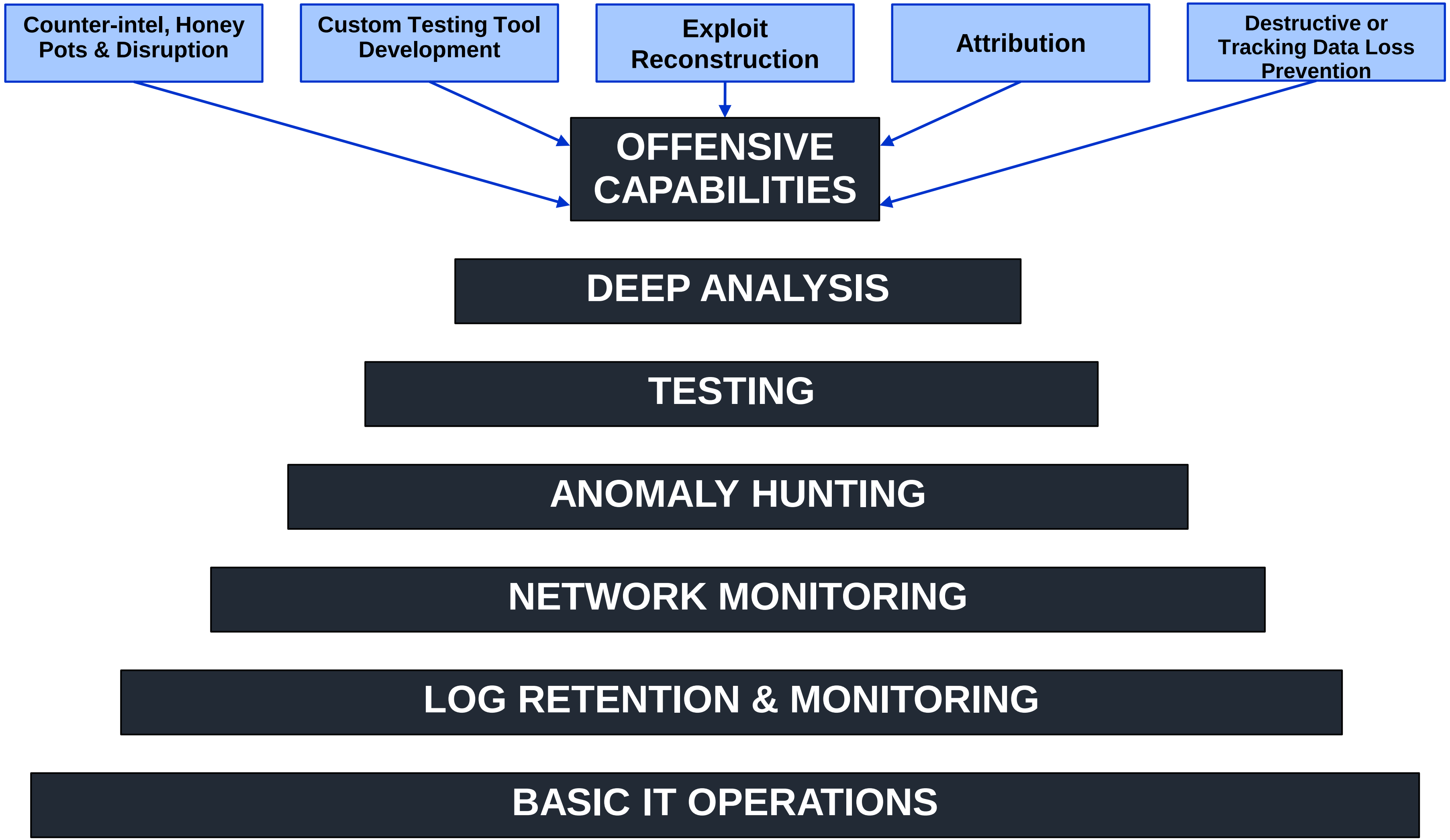
ANOMALY HUNTING

NETWORK MONITORING

LOG RETENTION & MONITORING

BASIC IT OPERATIONS

Security Pyramid



Counter-intel, Honey Pots & Disruption

Custom Testing Tool Development

Exploit Reconstruction

Attribution

Destructive or Tracking Data Loss Prevention

OFFENSIVE CAPABILITIES

DEEP ANALYSIS

TESTING

ANOMALY HUNTING

NETWORK MONITORING

LOG RETENTION & MONITORING

BASIC IT OPERATIONS

Lessons Recap

1. **Human Psychology is a Vulnerability**
2. **If you don’t physically control the computer, you can’t expect security**
3. **Take the initiation & work hard**
4. **Everything is hackable / hacked**
5. **Many Organizations Don’t Benefit from Penetration Testing**
6. **Valid Business Decisions Can Contradict Conventional Security Wisdom**
7. **Security Products Don’t Work**
8. **What You Think is Cool is Not Necessarily What Everyone Thinks is Cool**
9. **Good Security Programs Depend on People and Can Die Quickly**
10. **Strong Basic IT Operations Matter More Than Almost Any Other Security Factor**

Additional Lessons

- Not all security companies / researchers are ethical
- Publicity and cons can be overrated
- Exploits / 0day are a bad return on investment
- Threat intelligence is mostly snake oil unless it includes a human component
  - Threat reduction is where its at
- Everybody is hacked but its not the end of the world (usually)
- Don’t beat up security companies that get hacked too hard, there are reasons for certain vulnerabilities (ex. Lack of email encryption)
- Sales and project manager staff translate to more revenue than technical staff
- Security researchers aren’t finishers
- Hire / surround yourself with people smarter than you
- IR should be drilled and treated like a routine job (3 shifts, no freakout emergencies)

Questions?