Matt Ziegler

MBA, CISSP, CISA, QSA
Director of Advisory Services
Novacoast

Pedro Sosa

Penetration Tester
Director of Security Services
Novacoast

Tyler Johnson

CISSP, CISA, QSA
Directory of Advisory Services
Novacoast

PCI Security Standards Council

Beyond the Checkbox

Uncovering Hidden Risks in PCI DSS Compliance

Agenda

- Why compliance ≠ security
- The attacker’s perspective
- Four real world hidden risk examples:
  - IPv6 DNS Spoofing
  - Password Reuse & Credential Stuffing
  - ADCS Misconfigurations
  - Dual-Homed Machines
- Key lessons and takeaways
- Q&A

Compliance vs. Security

Compliance is the start, not the end, of your journey

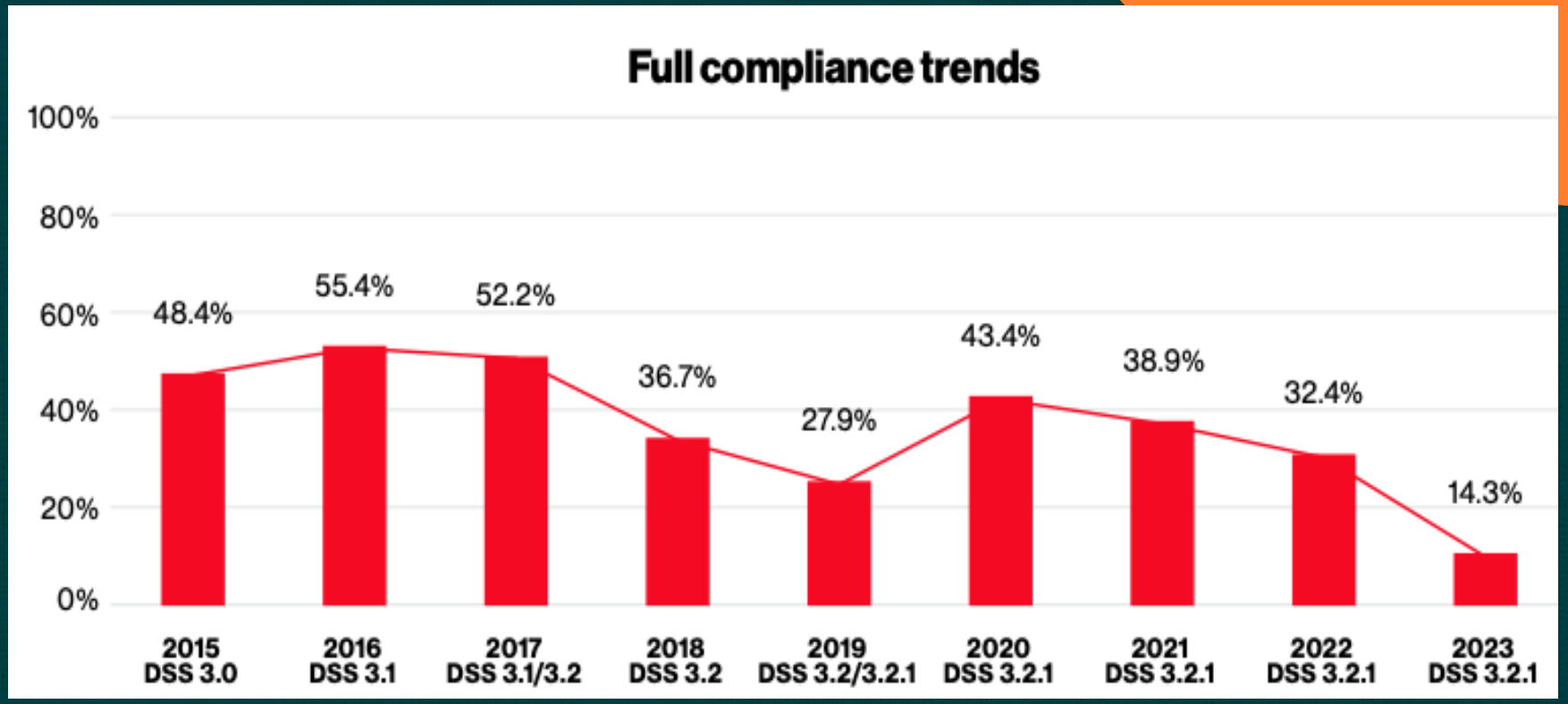
Receiving a “Compliant” Assessment Result, or that a Requirement is “In Place” means you’ve met the minimum baseline.

- Attackers do not care if you’re compliant
- Attackers care if you’re vulnerable
- An assessment is a point in time measurement
    - While some controls require periodic review, most are an annual evaluation
- Gaps between policy, process, and real-world configurations create hidden risks
- In 2019, only 27.9% of organizations maintained their compliance throughout the year*
- In 2023, this dropped to 14.3% of organizations maintaining their compliance throughout the year**
- In 2025, only 54% of perimeter-device vulnerabilities were fully remediated in the past year. ***

*Source: Verizon 2020 Payment Security Report
**Source: Verizon 2024 Payment Security Report
***Source: Verizon 2025 Data Breach Investigations Report

Maintained Compliance

Maintaining is hard



Source: Verizon 2024 Payment Security Report

43% of Breaches from Three Vectors

Stolen/Compromised Credentials

16%

Accounting for an average of $4.81M per breach

Phishing Attacks

15%

Accounting for an average of $4.88M per breach

Cloud Misconfiguration

12%

Accounting for an average of $3.98M per breach

Source: IBM – Cost of a Data Breach Report 2024

Compliance vs. Effectiveness, Adequacy & Completeness

Compliance

Meets the Requirements *as written.*

Effectiveness

Actually works as intended in your environment.

Adequacy

Is strong enough to handle the threats and risks.

Completeness

Covers the entire relevant scope. No hidden gaps.

The Attacker's Perspective

Compliance

Meets the Requirements *as written.*

Effectiveness

Actually works as intended in your environment.

An attacker only needs one control to be ineffective, inadequate, or incomplete. It doesn't matter how many boxes are checked, and the attacker doesn't care about "defined scope."

Adequacy

Is strong enough to handle the threats and risks.

Completeness

Covers the entire relevant scope. No hidden gaps.

Hidden Risk #1: IPv6 DNS Spoofing

The Invisible IPv6 Path

How attackers pivot using IPv6 to spoof DNS and exfiltrate.

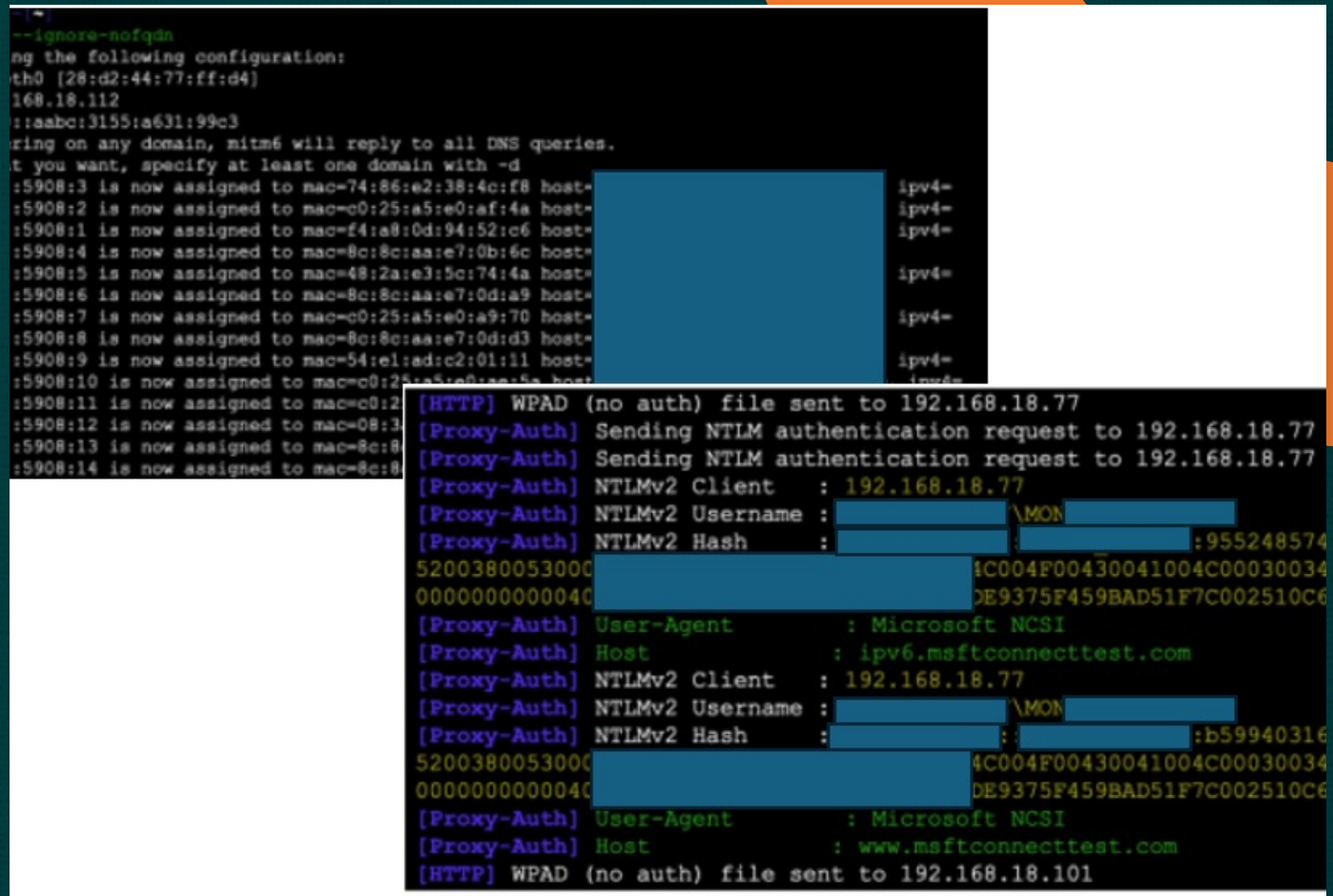
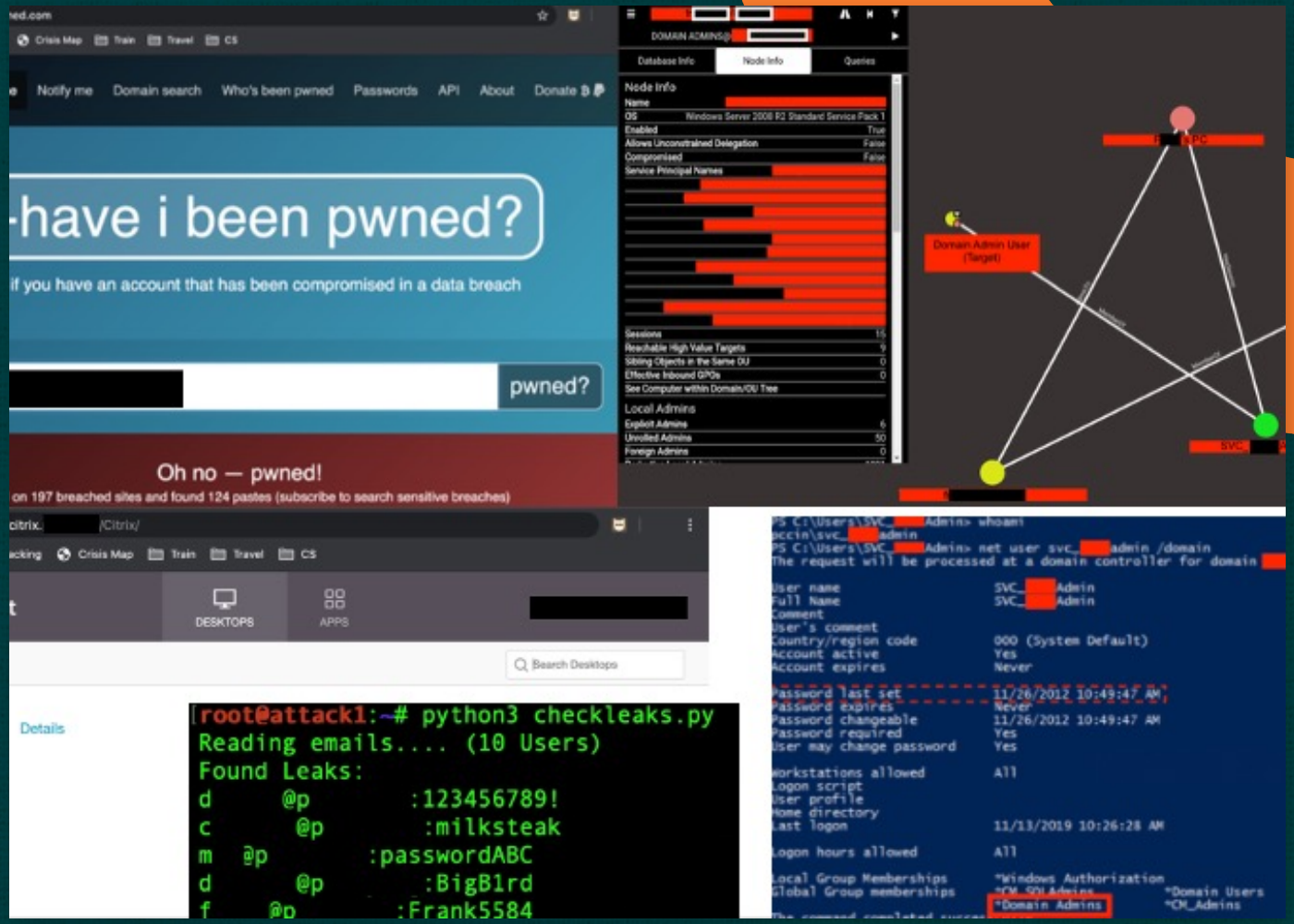


Figure #23: Capturing Proxy-Authentication from Malicious WPAD file.

Hidden Risk #2: Password Reuse & Credential Stuffing

The Human Factor

Even with a compliant password policy, and strict enforcement, credential reuse outside your environment is a massive potential gap.



Hidden Risk #3: ADCS Misconfiguration

The Escalation Trap

Active Directory Certificate Services are rarely in scope, but impact the CDE when exploited.

```
Client Authentication                : True
Enrollment Agent                     : False
Any Purpose                          : False
Enrollee Supplies Subject            : True
Certificate Name Flag                : EnrolleeSuppliesSubject
Enrollment Flag                      : PublishToDs
                                       IncludeSymmetricAlgorithms
Private Key Flag                     : ExportableKey
Extended Key Usage                   : Client Authentication
                                       Secure Email
                                       Encrypting File System
Requires Manager Approval            : False
Requires Key Archival                : False
Authorized Signatures Required       : 0
Validity Period                      : 1 year
Renewal Period                       : 6 weeks
Minimum RSA Key Length               : 2048
Permissions
  Enrollment Permissions
    Enrollment Rights                : [redacted].COM\Enterprise Admins
                                       [redacted].COM\[redacted] - Domain Admin
                                       S-1-5-21-[redacted]
                                       [redacted].COM\[redacted]
                                       [redacted].COM\Domain Admins
                                       [redacted].COM\Domain Users
```

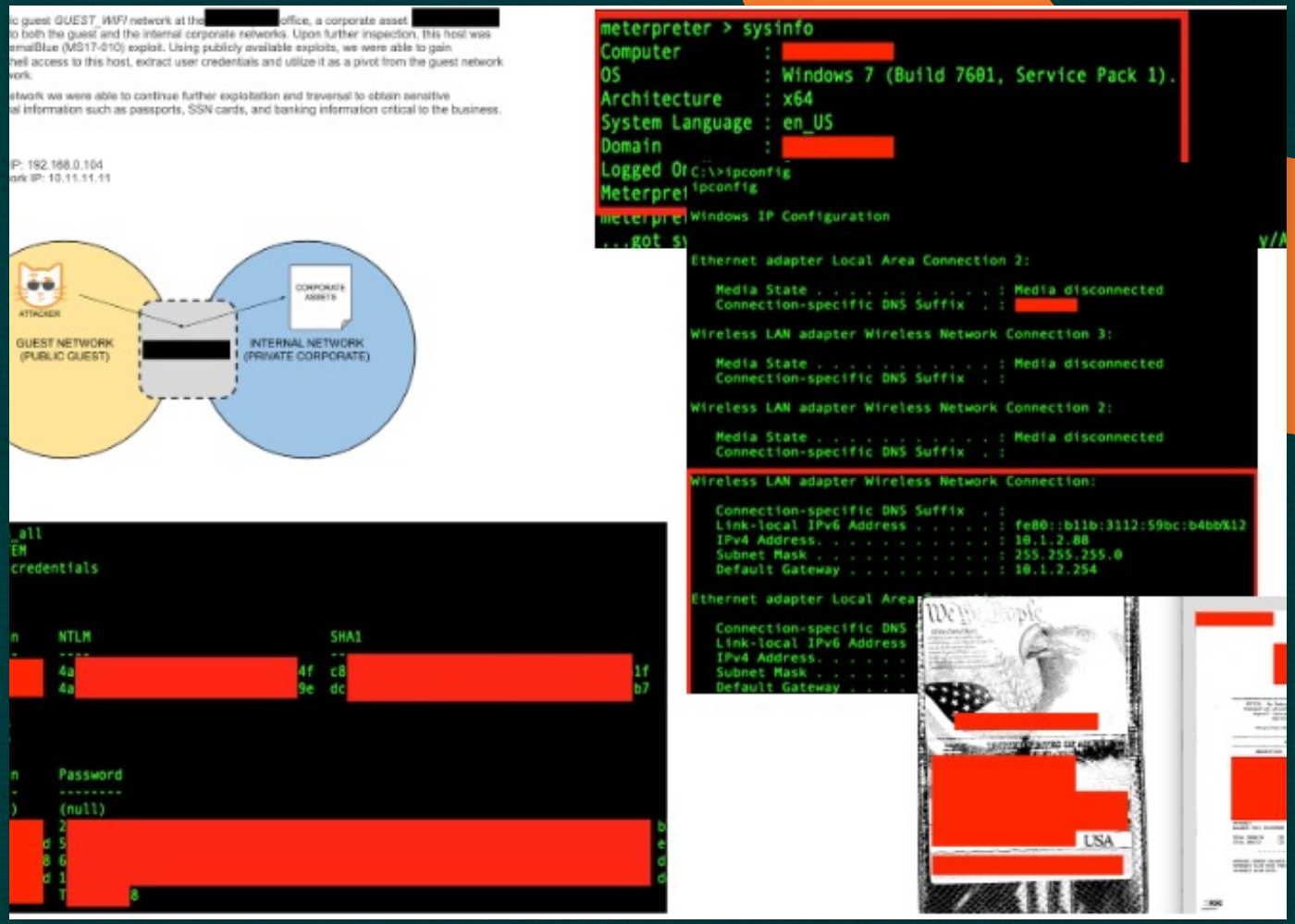
Figure #17: Misconfigured Template.

```
┌──(root㉿ scdata1)-[~]
└─# certipy-ad req -target [redacted] -ca [redacted] -upn [redacted].COM -u [redacted].com
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 188084
[*] Got certificate with UPN [redacted].COM'
[*] Certificate has no object SID
[*] Saved certificate and private key to [redacted]

┌──(root㉿ scdata1)-[~]
└─# certipy-ad auth -pfx sasccmclientpush.pfx
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: [redacted].com
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to [redacted]
```

Hidden Risk #4: Dual-Homed Systems

The Open Door

Scope creep and poor segmentation can lead to system misconfiguration and dual-homed systems.



Lessons Learned

What We See Too Often

Performing hundreds of penetration tests, security audits, system evaluations, and incident responses we've learned each of the following lessons:

- Compliance is a snapshot, Security is continuous
- Configuration drift happens – trust but verify
- People are your first AND last line of defense
- Always test your segmentation
- Add threat-based testing (beyond just ASVs and Penetration Testing)
  - Red Teams
  - Purple Teams

Practical Takeaways

Beyond the Checkbox: What to do Next

So, what should you do next?

- Treat PCI DSS as a starting point, not a destination
- Validate controls with regular penetration testing, red teaming, purple teaming
- Monitor for legacy protocols, configuration drift, and system modifications
- Implement real-time detection & response
- Educate your staff, and then test them
  - Run contests, engage your corporate staff
  - Perform more than annual training
  - Integrate training into your annual review processes
  - Include both technical and non-technical staff

Thank You!

Come visit us at Booth #23

PCI Security Standards Council®

2025 NORTH AMERICA COMMUNITY MEETING