SANS | Research Program

Continuous Penetration Testing: Closing the Gaps Between Threat and Response

SPONSORED BY

Sprocket Security

A SANS First Look

Written by **Chris Dale** | September 2025

Introduction: Leading a Needed Change in Penetration Testing

Sometimes we need to pause and ask the most fundamental question: What is the purpose of penetration testing? Not just in theory, but in real-world practice. Because if we don't understand why we're doing it, how can we ever do it well?

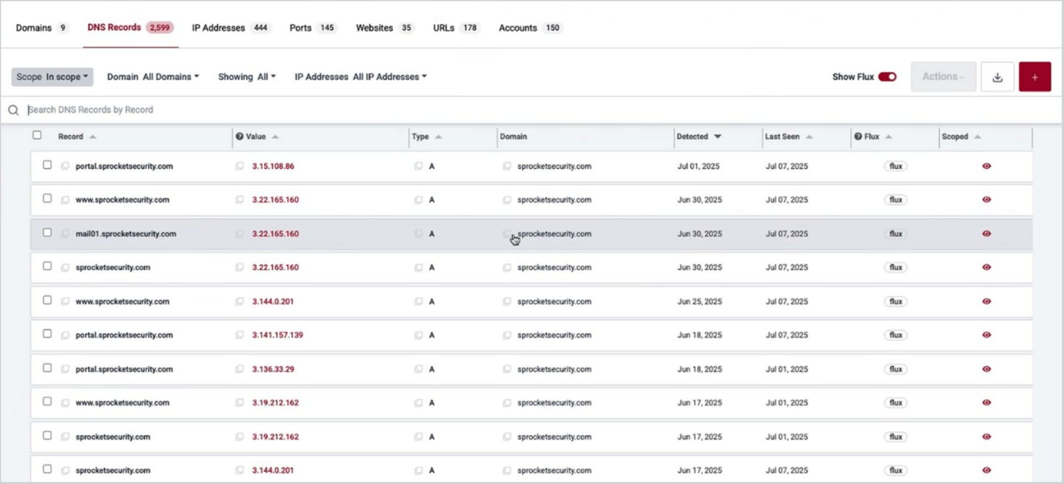
Penetration testing should bring one clear outcome to mind: hardening your business against real threats. It's not just about finding vulnerabilities. It's about proactively ensuring that threat actors stay out. That's the true value of effective penetration testing.

IT is a moving target. Systems, configurations, and threat models shift constantly. A penetration test report, no matter how thorough, captures only a moment in time. By the time the ink dries or the PDF lands in someone's inbox, parts of that report may already be outdated. Services get patched, often exposing new attack surfaces. Firewalls and infrastructure evolve, driven by internal DevOps changes or third-party updates. New vulnerabilities are discovered daily. This ongoing flux underscores the need for continuous assessment and adaptive security strategies, rather than relying on static, point-in-time evaluations.

What Does Continuous Penetration Testing Look Like?

Asset inventory has been a persistent challenge for organizations over the decades. A fast-evolving technology, attack surface management (ASM), has emerged to address the problem. By continuously discovering and assessing assets, ASM provides defenders with much-needed visibility and control.

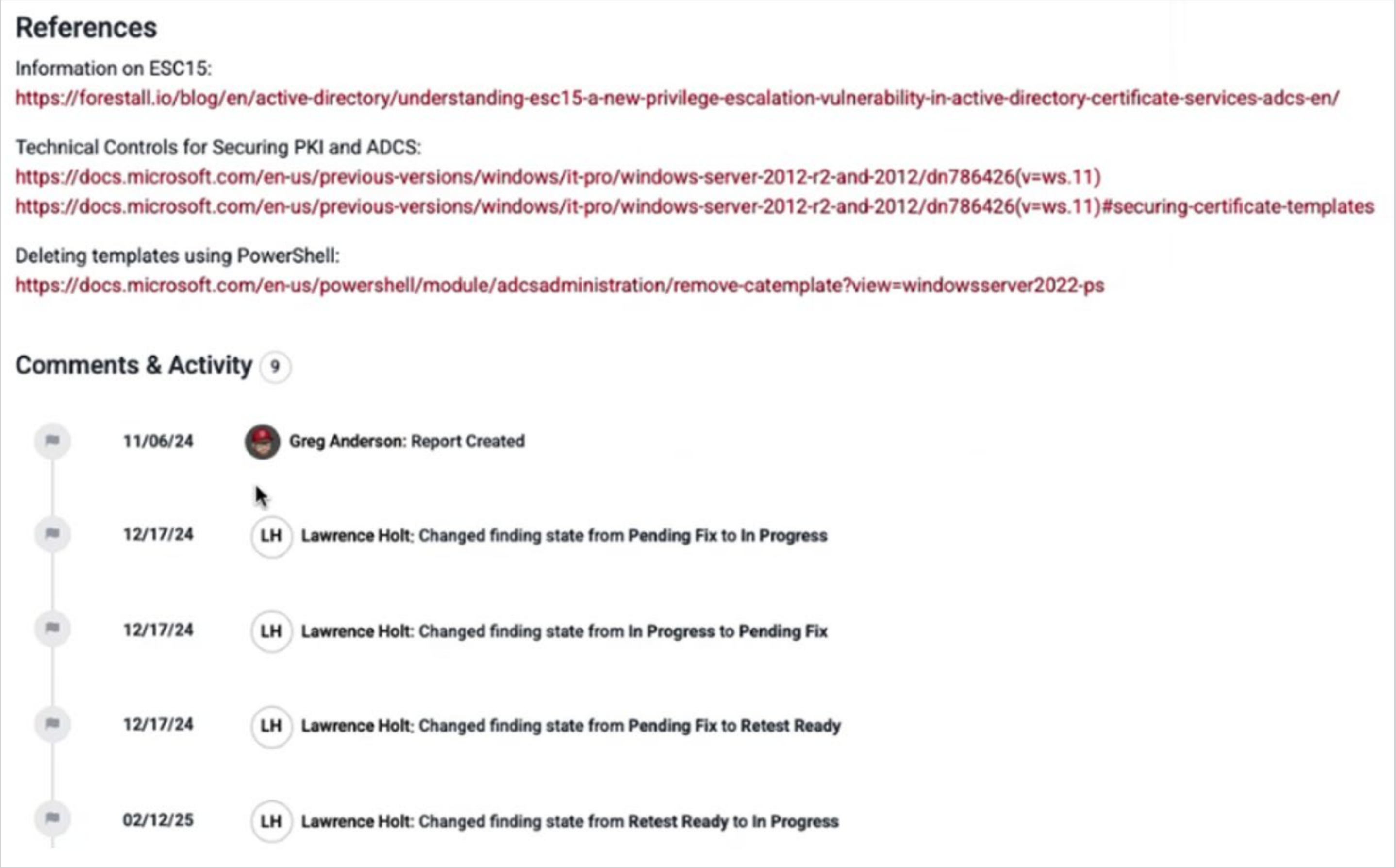
In this SANS First Look, we examine an example of this approach from Sprocket Security, a tool with continuous discovery capabilities that not only supports blue teams in managing exposure but also provides penetration testers with critical input for discovering real risks. In this way, a single capability can serve two purposes—effectively acting as a purple team tool (see Figure 1).



☐	Record	Value	Type	Domain	Detected	Last Seen	Flux	Scoped
☐	portal.sprocketsecurity.com	3.15.108.86	A	sprocketsecurity.com	Jul 01, 2025	Jul 07, 2025	flux	👁
☐	www.sprocketsecurity.com	3.22.165.160	A	sprocketsecurity.com	Jun 30, 2025	Jul 07, 2025	flux	👁
☐	mail01.sprocketsecurity.com	3.22.165.160	A	sprocketsecurity.com	Jun 30, 2025	Jul 07, 2025	flux	👁
☐	sprocketsecurity.com	3.22.165.160	A	sprocketsecurity.com	Jun 30, 2025	Jul 07, 2025	flux	👁
☐	www.sprocketsecurity.com	3.144.0.201	A	sprocketsecurity.com	Jun 25, 2025	Jul 07, 2025	flux	👁
☐	portal.sprocketsecurity.com	3.141.157.139	A	sprocketsecurity.com	Jun 18, 2025	Jul 07, 2025	flux	👁
☐	portal.sprocketsecurity.com	3.136.33.29	A	sprocketsecurity.com	Jun 18, 2025	Jul 01, 2025	flux	👁
☐	www.sprocketsecurity.com	3.19.212.162	A	sprocketsecurity.com	Jun 17, 2025	Jul 01, 2025	flux	👁
☐	sprocketsecurity.com	3.19.212.162	A	sprocketsecurity.com	Jun 17, 2025	Jul 01, 2025	flux	👁
☐	sprocketsecurity.com	3.144.0.201	A	sprocketsecurity.com	Jun 17, 2025	Jul 07, 2025	flux	👁

Figure 1. Sprocket Security ASM Asset Inventory

The fusion of red and blue is vital. We need to bridge the gap between attack and defense with more intention. Less of "us vs. them" and more of "us *and* them" working together toward a shared goal. Figure 2 shows how Sprocket Security provides the much-needed collaboration between offense and defense. This drives knowledge transfer, rapid response, and actionable insights that accelerate remediation.



References

Information on ESC15:
https://forestall.io/blog/en/active-directory/understanding-esc15-a-new-privilege-escalation-vulnerability-in-active-directory-certificate-services-adcs-en/

Technical Controls for Securing PKI and ADCS:
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn786426(v=ws.11)
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn786426(v=ws.11)#securing-certificate-templates

Deleting templates using PowerShell:
https://docs.microsoft.com/en-us/powershell/module/adcsadministration/remove-catemplate?view=windowsserver2022-ps

Comments & Activity 9

11/06/24 Greg Anderson: Report Created

12/17/24 LH Lawrence Holt: Changed finding state from Pending Fix to In Progress

12/17/24 LH Lawrence Holt: Changed finding state from In Progress to Pending Fix

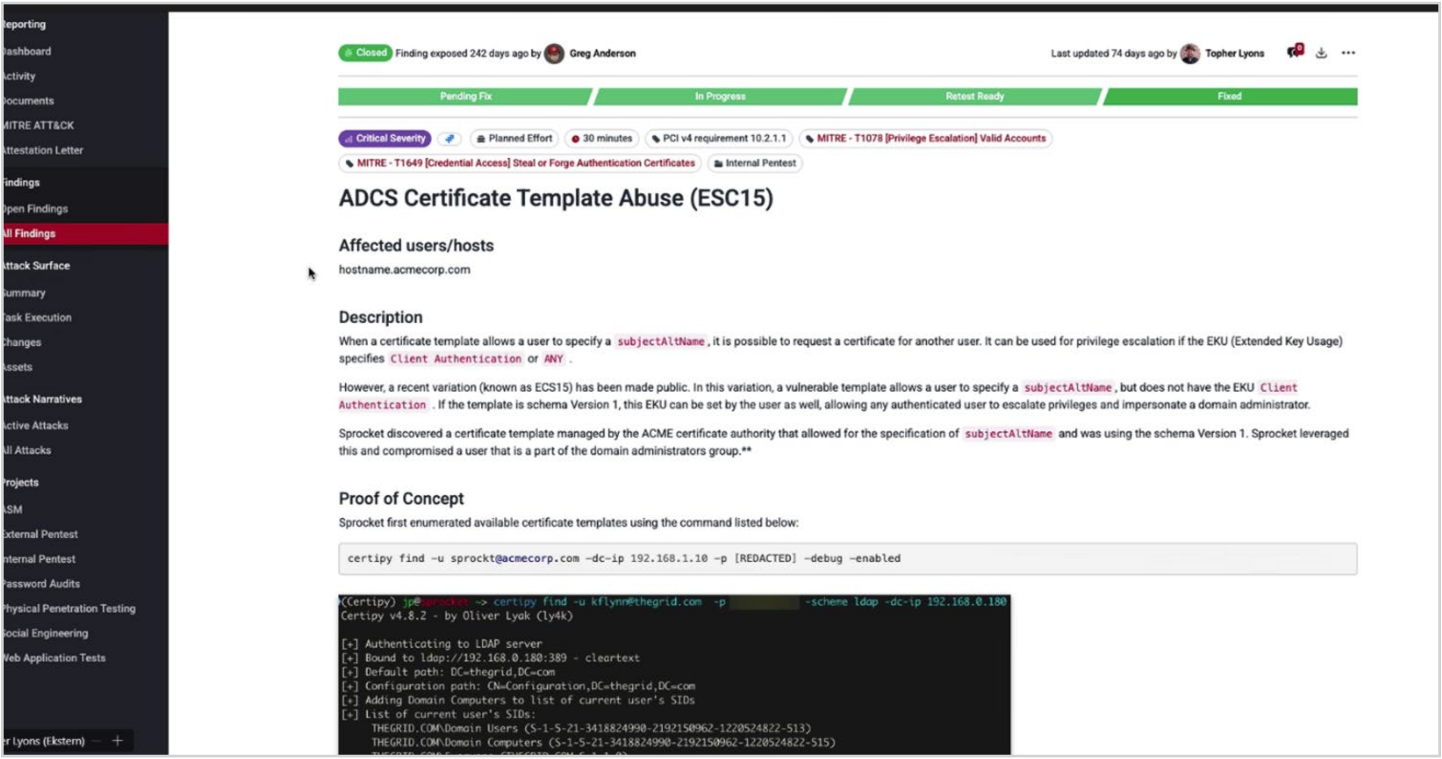
12/17/24 LH Lawrence Holt: Changed finding state from Pending Fix to Retest Ready

02/12/25 LH Lawrence Holt: Changed finding state from Retest Ready to In Progress

Figure 2. Collaboration Between Offense and Defense

As a customer, it is reassuring to know that a continuous penetration test is running against your assets. Someone has your back. When your environment changes or the industry shifts, you can trust that skilled eyes are watching. The penetration testers are always looking, always assessing, ready to identify risks as they emerge.

Getting insights into the ongoing campaigns against your company not only is useful for compliance but also helps drive insights and understanding for you and the teams defending your attack surfaces. Sprocket Security provides the technical details and evidence of vulnerabilities that need remediation from the customer, as shown in Figure 3.



Finding exposed 242 days ago by Greg Anderson

Last updated 74 days ago by Topher Lyons

ADCS Certificate Template Abuse (ESC15)

Affected users/hosts

hostname.acmecorp.com

Description

When a certificate template allows a user to specify a `subjectAltName`, it is possible to request a certificate for another user. It can be used for privilege escalation if the EKU (Extended Key Usage) specifies `Client Authentication` or `ANY`.

However, a recent variation (known as ECS15) has been made public. In this variation, a vulnerable template allows a user to specify a `subjectAltName`, but does not have the EKU `Client Authentication`. If the template is schema Version 1, this EKU can be set by the user as well, allowing any authenticated user to escalate privileges and impersonate a domain administrator.

Sprocket discovered a certificate template managed by the ACME certificate authority that allowed for the specification of `subjectAltName` and was using the schema Version 1. Sprocket leveraged this and compromised a user that is a part of the domain administrators group.**

Proof of Concept

Sprocket first enumerated available certificate templates using the command listed below:

```
certipy find -u sprockt@acmecorp.com -dc-ip 192.168.1.10 -p [REDACTED] -debug -enabled
```

```
(Certipy) jp@[redacted] -> certipy find -u kflynn@thegrid.com  -p [redacted] -scheme ldap -dc-ip 192.168.0.180
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[+] Authenticating to LDAP server
[+] Bound to ldap://192.168.0.180:389 - cleartext
[+] Default path: DC=thegrid,DC=com
[+] Configuration path: CN=Configuration,DC=thegrid,DC=com
[+] Adding Domain Computers to list of current user's SIDs
[+] List of current user's SIDs:
     THEGRID.COM\Domain Users (S-1-5-21-3418824990-2192150962-1220524822-513)
     THEGRID.COM\Domain Computers (S-1-5-21-3418824990-2192150962-1220524822-515)
```

Figure 3. Sprocket Security's Technical Details and Vulnerability Evidence

Security That Delivers Actionable Results

Compliance is important, but meaningful impact from your cybersecurity initiatives is what truly matters. Without real results and ongoing traction, are these efforts paying off, or could they be doing more harm than good? This is especially critical when security initiatives must be prioritized in real time and executed under urgent conditions, which unfortunately has often been the case in the modern IT landscape.

Continuous penetration testing draws practical security results in a continuous and evolving IT landscape.

Bottom Line: IT Is Changing, and So Should Your Security

Security is not a solo mission. Blue teams need reinforcement, and the red team is not the enemy. They are the missing pieces. When offensive and defensive efforts combine, they build a more complete view of the threat landscape. This collaboration turns theory into action and response into prevention.

Pentesters cannot afford to be the boy who cried wolf. Vague findings, theoretical risks, and shallow noise only waste time. A red team must prove what matters by showing real impact, with context and clarity. On the other hand, defenders must patch what truly matters. When both sides focus on what is real, measurable, and relevant, the result is trust, not fatigue. That trust is the foundation for security decisions that *actually* work.

Some risks demand action in less than 24 hours. When the environment shifts or new exposure appears, waiting for the next test cycle is not good enough. If your penetration testing is not continuous, then the gaps are real. You are vulnerable between the scans and the reports. Modern threat landscapes require constant visibility, fast feedback loops, and the ability to react in real time. That is not a luxury—it is survival.

Sprocket
Security