PROVISIONING REGRESSION / BROADCAST POISONING TO LATERAL MOVEMENT

FOOTHOLD · 30 MIN

Transient Test Host Credential Capture to Lateral Movement to Domain Compromise

Complete control of the domain despite a mature remediation history. One provisioning gap undid fleet-wide hardening because the shared local administrator password crossed the domain boundary.

ATTACK SNAPSHOT

ENVIRONMENT
Mature internal network, long-term continuous testing client, hardened Windows Active Directory

FOOTHOLD
30 min

RESULT
Full Domain Compromise via Shared Local Administrator Reuse

CATEGORY
Provisioning Regression / Broadcast Poisoning to Lateral Movement

HOW IT WAS CONFIGURED

- Established client on a long-term continuous testing engagement with a mature remediation history across prior internal findings.
- Broadcast protocol poisoning (mDNS, LLMNR, DHCPv6) had been reported and remediated at the fleet level in a previous engagement.
- A standalone Windows host was provisioned outside the hardened configuration. Because it was never domain-joined, Group Policy never pushed the broadcast-protocol fix to it, and the local administrator account used during provisioning ended up reused across other similar hosts.

HYPOTHESIS

OBSERVATION
Pinion still saw answerable mDNS and DHCPv6 broadcasts on a segment where this attack class had been reported remediated in prior engagements.

SUSPICION
Something had regressed. Likely a host provisioned without inheriting the current Group Policy configuration.

THEORY
Capturing authentication from the regressed host would yield a local credential, and that credential would reuse across the fleet because provisioning scripts tend to carry the same seed password.

ATTACK PATH

1. POISON MDNS/DHCPV6
2. CAPTURE ADMIN HASH
3. CRACK PASSWORD
4. SPRAY ACROSS FLEET
5. DUMP DC → DOMAIN

"The vulnerability we helped them fix in a previous engagement was applied to every current device, and steps were put in place to make sure new devices received the fix as well. The newly deployed server, though, was not domain-joined, so it never received that fix. Fixing a vulnerability once does not keep it fixed if provisioning does not inherit the fix, and thankfully we were able to catch that very quickly with Pinion."

JUAN PABLO GOMEZ POSTIGO — Penetration Tester



Exploit Demonstration & Impact

EXPLOIT STEPS

1. Pinion passively observed poisonable mDNS and DHCPv6 traffic on the workstation segment.
2. Pinion poisoned mDNS and DHCPv6 responses, directing a Windows host to send authentication attempts to the testing infrastructure.
3. Captured a Net-NTLMv2 hash for the local Administrator account on a non-domain-joined Windows host answering the poisoned broadcasts.
4. Sprocket cracked the hash offline and recovered the cleartext local administrator password.
5. Sprayed the recovered password across the fleet. One standalone host plus three domain-joined hosts authenticated as local administrator with the same password.
6. On the file server, custom techniques were employed to dump sensitive registry hives.
7. Within the registry hives, Sprocket extracted a domain administrator's cached credential hash, cracked it offline, and ran `secretsdump` against the domain controller to extract password hashes for every user in the environment.

PROOF ARTIFACT

```
nxc smb <workstation-fleet> -u Administrator
-p <recovered-pwd> --local-auth
```

HOST

`<workstation-fleet>` (three domain-joined hosts)

AUTHENTICATION

local Administrator, same password as the standalone test host

RESULT

A custom technique on the file server surfaced a cached domain administrator credential, and `secretsdump` delivered the full hash set

ATTACKER GAINS

TECHNICAL

Captured authentication from poisoned broadcast protocols on a newly provisioned host, cracked its local administrator hash, and sprayed it to discover reuse across three domain-joined hosts.

CAPABILITY

Pulled sensitive registry hives from the file server, extracted a cached domain administrator credential, cracked it offline, and ran `secretsdump` against the domain controller to extract password hashes for every user in the environment.

BUSINESS IMPACT

Complete control of the domain despite a mature remediation history. One provisioning gap undid fleet-wide hardening because the shared local administrator password crossed the domain boundary.

WHY CONTINUOUS TESTING WINS

- Pinion captured the hash during passive observation, allowing a human tester to immediately focus on a revealed attack path without spending time setting up tooling.
- The regressed host did not exist during a legacy pentest and would have sat untested until the following year, long enough for the shared credential to spread further.
- Even when LAPS is provisioned and unique local administrator credentials are enforced going forward, previously used local administrator accounts can persist on hosts. Continuous testing surfaces those lingering accounts before they become part of a usable chain.

WHY TRADITIONAL TESTING MISSED THIS

- An annual retest would check the hardened fleet and record mDNS and DHCPv6 as fixed.
- A standalone host that is never domain-joined inherits no Group Policy, so the fleet-level fix never reaches it.

Automation breaks on real-world complexity, human expertise doesn't.

THREATS DON'T CLOCK OUT. NEITHER DO WE.