AUTONOMOUS RECON / BACKUP EXPOSURE TO CREDENTIAL CHAIN

FOOTHOLD · 20 MIN

Backup Appliance Exposure to Hypervisor Takeover and Domain Compromise

Full control of Active Directory from a single unauthenticated foothold. Through the vSphere Client pivot, every virtual machine the hypervisor fleet manages becomes reachable, including systems that are not routable from the attacker's starting segment.

ATTACK SNAPSHOT

ENVIRONMENT	FOOTHOLD	RESULT	CATEGORY
First internal pentest, new client, mid-size Active Directory environment	20 min	Full Domain Compromise via Exposed Hypervisor Backups	Autonomous Recon / Backup Exposure to Credential Chain

HOW IT WAS CONFIGURED

- First internal engagement for this client, no prior pentest on record, no prior remediation cycle.
- Multiple internal IP ranges in scope, representative of a growing enterprise environment.
- Pinion, Sprocket's AI testing agent, ran in parallel with human tester planning on day one.

HYPOTHESIS

OBSERVATION

A backup appliance on the internal network accepted a NULL SMB session and enumerated six shares holding virtual machine images and system backups. The same appliance also exported one of those directories over NFS to any host with read-write permissions.

SUSPICION

The host's DNS record, the backup-related services exposed, and the share names themselves led Pinion to flag the enumerated contents as likely to carry configuration snapshots and SQL dumps with credential material intended for operators, not attackers.

THEORY

Reading the backup catalog would surface stored credentials for a hypervisor or administrative platform, and that pivot would reach the domain controllers directly.

ATTACK PATH

1. RECON FLAGS APPLIANCE
2. NULL SMB + NFS MOUNT
3. LOOT VSPHERE CREDS
4. SNAPSHOT DC MEMORY
5. DUMP HASHES → DOMAIN

"Pinion identified this attack path before recon was even halfway finished. On a traditional pentest the customer waits while we grind through enumeration before any value lands. Here the path was in front of us early enough to spend the rest of the first day proving it out instead of hunting for it."

PETER CIPOLONE — Penetration Tester



Exploit Demonstration & Impact

EXPLOIT STEPS

1. Pinion observed a backup appliance at `<backup-host>` accepting a NULL SMB session and raised the finding to critical severity based on the enumerated share names and service identity before human review.
2. Sprocket authenticated with a NULL SMB session and enumerated six exposed shares holding full-system images, host-level backups, failover copies, and virtualization recovery data: `nxc smb <backup-host> -u '' -p '' --shares`.
3. Confirmed the appliance also exported the same `backups/samba` directory over NFS and recovered cleartext vSphere service account credentials from a SQL dump unpacked out of a backup archive.
4. Logged into the vSphere Client with the recovered credentials and identified the domain controller virtual machines across the managed ESXi hosts.
5. Triggered memory snapshots on each domain controller virtual machine from the vSphere Client and downloaded the resulting snapshot files to a tester-controlled host.
6. Parsed the SAM, SYSTEM, and SECURITY registry hives out of the captured memory, recovered a domain controller machine account hash, and ran `secretsdump` against the domain controller to extract password hashes for every user in the environment.

PROOF ARTIFACT

```
nxc smb <backup-host> -u '' -p '' --shares
```

HOST

`<backup-host>` (backup appliance)

AUTHENTICATION

NULL SMB session; same directory also exported over NFS to any host

SHARES EXPOSED

six shares holding full-system images, host-level backups, failover copies, and virtualization recovery data

ATTACKER GAINS

TECHNICAL

Unauthenticated foothold on a backup appliance via NULL SMB session and anonymous NFS mount, with cleartext vSphere credentials recovered from a SQL dump granting access to the vSphere Client.

CAPABILITY

Control of the domain controller virtual machines at the hypervisor level, access to every machine the hypervisor fleet manages, and the full set of Active Directory credentials needed to impersonate any user in the environment.

BUSINESS IMPACT

Full control of Active Directory from a single unauthenticated foothold. Through the vSphere Client pivot, every virtual machine the hypervisor fleet manages becomes reachable, including systems that are not routable from the attacker's starting segment.

WHY CONTINUOUS TESTING WINS

- Pinion prioritized this exposure above other findings on day one, allowing a human tester to immediately focus on a revealed attack path.
- Even when a client removes anonymous access on this specific appliance, embedded credentials inside archived backups can persist in other backup locations. Continuous testing surfaces those lingering credentials before they become part of a usable chain.

WHY TRADITIONAL TESTING MISSED THIS

- Annual pentest cadence leaves backup appliances unchecked between engagements, and backup contents drift as retention policies change.
- Share name semantics are invisible to vulnerability scanners, which flag unauthenticated SMB but not what the shares are likely to contain.
- Credentials embedded inside SQL backup files are invisible to configuration audits and only surface once the archive is actually mounted and parsed.