Would Your Organization Fail the Active Directory Security Assessment?

Presented by:
Ran Harel—Principal Security Product Manager, Semperis
Darren Mar-Elia—VP of Products, Semperis (@grouppolicyguy)
Some Context

- Active Directory is often ignored from a security perspective despite,
  - It’s a key target for attackers
  - Most AD implementations we see have holes big enough to drive a truck through
  - It is increasingly being used as a platform to gain access to cloud resources (e.g. SolarWinds attack)
Active Directory – a lucrative target

Initial foothold → AD → Persistence
- Misconfigurations
- Vulnerabilities
- Stale accounts
- Complexity!!

Privilege Escalation → Lateral Movement

Impact
- Data theft
- Ransomware / Cryptolockers
- Backdoors
Informed by Our Experiences with Purple Knight

A point-in-time snapshot of AD security posture

https://www.purple-knight.com
What are the common weak spots?

- **Account Security**
  - Weak account security setting (e.g. passwords, guest accounts left on, etc.)

- **Account Delegation**
  - Poor management of AD delegation—who can do what against privileged accounts

- **AD Infrastructure Security**
  - AD infrastructure settings that leave you open to attack

- **Kerberos Security**
  - Sophisticated Kerberos-based attacks that take advantage of weak Kerberos delegation

- **Group Policy**
  - Group Policy delegation and management blind spots that lead to take over
Account Security--Password Policies: The Risks

- Admin accounts whose passwords are not sufficiently complex or don’t change frequently
- Service accounts that have old passwords and access to critical applications/data
- Admins who are not required to use MFA
- Krbtgt password is not rotated every 180 days (at least)
- Users whose password never expire
- Users who don’t require passwords
Attack example – password spray

Attacker goal: take over an account with a common / insufficiently complex password

• This attack is also called “low and slow” as opposed to traditional “brute-force” attacks
• Entails using a small number of frequently used passwords against a large number of accounts
• Avoids detection by slowly attempting authentication on each separate account – thereby avoiding lockout
Account Security--Password Policies: Mitigations

- Ensure password policies are sufficiently strong, esp. for privileged accounts
  - Look at Fine-Grained Password Policy to have different password policies for privileged accounts
- Rotating passwords on a regular basis, esp. for privileged and service accounts
- MFA should be a must for privileged users.
  - Consider Adaptive MFA to reduce impact on users
Account Security-Accounts with Elevated Privileges: The Risks

- User and service accounts that may have privileges beyond what are really needed
  - “Privilege creep”
  - Stale accounts
  - Temporary accounts that weren’t removed
- Also, normal user accounts whose privileges were elevated
Attack example – “Shadow Admins”

2017 Oracle Solaris vulnerability enabled the infamous “Shadow Brokers” group to implant malicious code at many victims sites that elevated normal users to admins that went undetected.
Account Security-Accounts with Elevated Privileges: Mitigations

- The first step is identifying the privileged accounts
  - “Privileged” has different meanings in different environments.
  - Not just members of Domain Admins
  - Smart solutions to scan AD and identify hidden admins
- Ensure that they are securely managed/delegated in AD
- Monitor critical users & groups for changes in ACLs
AD Delegation—the Risks

- Excessive or inappropriate permissions on “sensitive objects”
  - Sensitive objects include:
    - AdminSDHolder container
    - Domain NC Head
    - Containers where GPOs are linked (esp. when those GPOs are processed by DCs)
    - “Cross-tier” delegation (e.g. Help Desk group that has full control over DC admins group)
Attack example – DC Sync / DCShadow

- An attacker that controls a user with DC Sync rights can force changes into AD to create their own accounts and backdoors or retrieve credentials.
AD Delegation—Mitigations

• Again, discovery is key—AD delegation is complex and, over time, grows more complex and often contradictory

• Lock down the sensitive objects—take a least privilege approach here

• Enforce Admin Tiering on management of AD objects relevant to each tier
  • e.g. Tier 2 Admins should not have Full Control/Write over Tier 1 or Tier 0 AD objects, etc.
Kerberos Security – The Risks

• Totally securing Kerberos is hard—it's distributed nature makes it hard to completely protect

• Lots of different types of attacks, with supporting tooling:
  • Golden Ticket
  • Silver Ticket
  • Kerberoasting
  • Resource-based Constrained Delegation

• Many (Most?) Kerberos attacks start with credential theft—this is a key area to protect
Attack example – Kerberos Golden Ticket

Attacker forges TGT with the \textit{krbtgt} hash

TGT

Presents forged TGT to a DC

TGS

Attacker receives TGS to any service

Impact
Kerberos Security – Mitigations*

- Avoid unconstrained delegation in all cases
- Rotate passwords regularly on all “Kerber-ized” services
- Avoid defining SPNs on privileged accounts and/or
- Make privileged accounts ineligible for delegation

* This is just a start—lots to do here to protect against Kerberos attacks. **Purple Knight** has some indicators that can help here.
Group Policy Security—The Risks

- Why Abuse Group Policy?
  - If compromised, it's the perfect malware delivery and privilege escalation vehicle
- Common types of abuse:
  - Weak delegation on critical GPOs leads to injecting malware payloads into SYSVOL for delivery to endpoints
  - Weak delegation on linking of containers leads to GPOs being used to weaken or adjust security hardening
- GPO Content Weaknesses
  - GPP Preferences Passwords still lingering in GPOs
Attack example – GPO Linking at the Domain level

- A configuration risk that allows users to apply policies to the entire domain

- Attacker gets credentials to user with Write permissions on GPLink
- Finds a GPO that lowers security
- Weakened GPO
- Links that GPO to the entire domain
- Impact
Bonus attack – Passwords in SYSVOL

• An old vulnerability from 2014

Impact

These passwords were encrypted using a known global key. This makes it trivial to decrypt them.
Group Policy Security – Mitigations

- Keep tight delegation on who can edit GPOs
- This is especially true for GPOs that are linked to containers processed by DCs
- Keep control over GP linking delegation on sensitive containers:
  - Domain
  - Domain Controllers OU
  - AD sites that contain DCs
- Monitor GPOs for changes, esp. critical GPOs that deliver security settings or those linked to sensitive containers
Know thy enemy and know yourself.

Purple Knight is an Active Directory security assessment tool built and managed by an elite group of Microsoft identity experts.

www.purple-knight.com
Monitor, detect, & respond

- Continuous vulnerability assessment
- Tamperproof tracking
- Real-time security alerts
- Auto-remediation (malicious change rollback)
- Compliance reporting
Shorten forest recovery by 90%

- Clean restore (malware free)
- Rapid recovery
- Advanced automation
- Anywhere recovery
- Post-attack forensics (AD anti-virus)
Questions?