Privileged Account Insecurity: The Target of All Exploitive Attacks

Presented by: Vishal Patel, CISSP
An Attacker Must Obtain Insider Credentials

“…100% of breaches involved stolen credentials.”

“APT intruders…prefer to leverage privileged accounts where possible, such as Domain Administrators, service accounts with Domain privileges, local Administrator accounts, and privileged user accounts.”

Mandiant, M-Trends and APT1 Report
The privileged pathway of insider attacks

Typically done via **spear phishing or social engineering**.

**Search** machine for credentials; **capture** passwords and/or hashes.

Locate desired data or systems to accomplish goal.

---

Unintentional insiders typically stop here with unintentional exposure of data.

Execute **pass-the-hash** to move to new systems under the guise of authorized privileged users.
Typical processes that attackers expose...

- Local admin accounts set to the same password
- Separate, named domain accounts created for each admin
- Non-expiring passwords for critical accounts
- Hard-coded credentials for applications in code, scripts and appliances
- Unmanaged SSH Keys used for interactive sessions and applications
- Workstation users granted local admin rights
- Standing Access – network, access and authentication
- Excessive Permissions for specific roles, like; DBA, Developers, etc.
- Lack of visibility around who, why and is it legitimate access
Make the attacker’s job as difficult as possible

- Control applications, and detect and block credential theft attempts
- Secure, rotate and control access to privileged credentials
- Detect and alert on anomalous and high-risk activity

- Reduce the attack surface
- Lock down credentials
- Limit lateral movement
- Detect, block and alert on threats

- Apply least privilege policies at the end point
- Isolate critical systems and protect sensitive credentials
- Monitor and record sessions

Break Through Perimeter
Use Inside Access
Disrupt Business
Exfiltrate Data
Steal Money
Next steps

Lock Down Credentials
Secure, rotate and control access to privileged passwords and SSH keys

Isolate & Control Sessions
Prevent direct access to critical systems and enforce least privileges

Continuously Monitor
Continuously monitor privileged user and account activity
AD User Audit – Low Hanging Fruit

```powershell
Set-ExecutionPolicy -ExecutionPolicy Unrestricted

$ADSearh.SearchRoot = "LDAP://$Domain"
$ADSearh.SearchScope = "subtree"
$ADSearh.PageSize = 100
$ADSearh.Filter = "(objectClass=user)"
$ADSearh.PropertiesToLoad.Add("distinguishedName")
$ADSearh.PropertiesToLoad.Add("SAMAccountName")
$ADSearh.PropertiesToLoad.Add("lastLogonTimeStamps")
$ADSearh.PropertiesToLoad.Add("pwdLastSet")
$ADSearh.PropertiesToLoad.Add("userAccountControl")
$userObjects = $ADSearh.FindAll()
Foreach ($user in $userObjects) {
    $dn = $user.Properties.Item("distinguishedName")
    $sam = $user.Properties.Item("SAMAccountName")
    $logon = $user.Properties.Item("lastLogonTimeStamps")
    if($logon.Count -eq 0) {
        $lastlogon = "Never"
    } else {
        $lastlogon = [DateTime]$logon[0].AddYears(1600)
    }
}
```

"CN=Charlie Pace,OU=iSeries Admins,OU=Users,OU=cyberArk,DC=cyberArk,DC=local", Charlie, Never, 04/27/2015 16:19:03, Enabled-password never expires
"CN=Clarie Littleton,OU=iSeries Admins,OU=Users,OU=cyberArk,DC=cyberArk,DC=local", Clarie, Never, 04/27/2015 16:20:16, Enabled-password never expires
"CN=Cindy Schumaker,OU=IT Auditors,OU=Users,OU=cyberArk,DC=cyberArk,DC=local", Cindy, 06/29/2016 19:07:01, 04/27/2015 16:24:15, Enabled-password never expires
"CN=Hugo Reyes,OU=IT Auditors,OU=Users,OU=cyberArk,DC=cyberArk,DC=local", Hugo, Never, 04/27/2015 16:25:51, Enabled-password never expires
"CN=Judy Fleming,OU=IT Auditors,OU=Users,OU=cyberArk,DC=cyberArk,DC=local", Judy, Never, 04/27/2015 16:26:48, Enabled-password never expires
"CN=Chris Bracket,OU=Security Admins,OU=Users,OU=cyberArk,DC=cyberArk,DC=local", Chris, Never, 04/27/2015 16:54:43, Enabled-password never expires
"CN=James Ford,OU=Security Admins,OU=Users,OU=cyberArk,DC=cyberArk,DC=local", James, Never, 04/27/2015 17:01:06, Enabled-password never expires
"CN=Ben Love,OU=All Users,OU=Users,OU=cyberArk,DC=cyberArk,DC=local", Ben, 03/03/2017 21:58:46, 04/27/2015 17:13:40, Enabled-password never expires
Framework for Privileged Access Behavior – Alerting and Remediation

Is it normal for:
- **User X** to access **Asset Y** at **Time Z**

Is it normal for:
- **Command X** to be executed at **Rate Y** from **Location Z**
Thank You!

- Q&A