33-Hardening Active Directory

Let's take some time to look at a few hardening measures that can be put in place to stop common TTPs like those we utilized in this module from being successful or providing any helpful information. Our goal as penetration testers is to help provide a better operational picture of our customers' network to their defenders and help improve their security posture. So we should understand some of the common defense tactics that can be implemented and how they would affect the networks we are assessing. These basic hardening steps will do much more for an organization (regardless of size) than purchasing the next big EDR or SIEM tool. Those extra defensive measures and equipment only help if you have a baseline security posture with features like logging enabled and proper documentation and tracking of the hosts within the network.

Step One: Document and Audit

Proper AD hardening can keep attackers contained and prevent lateral movement, privilege escalation, and access to sensitive data and resources. One of the essential steps in AD hardening is understanding everything present in your AD environment. An audit of everything listed below should be done annually, if not every few months, to ensure your records are up to date. We care about:

Things To Document and Track

- `Naming conventions of OUs, computers, users, groups`
- `DNS, network, and DHCP configurations`
- `An intimate understanding of all GPOs and the objects that they are applied to`
- `Assignment of FSMO roles`
- `Full and current application inventory`
- `A list of all enterprise hosts and their location`
- `Any trust relationships we have with other domains or outside entities`
- `Users who have elevated permissions`

People, Processes, and Technology

AD hardening can be broken out into the categories *People*, *Process,* and *Technology*. These hardening measures will encompass the hardware, software, and human aspects of any network.

People

In even the most hardened environment, users remain the weakest link. Enforcing security best practices for standard users and administrators will prevent "easy wins" for pentesters and malicious attackers. We should also strive to keep our users educated and aware of threats to themselves. The measures below are a great way to start securing the Human element of an AD environment.

- The organization should have a strong password policy, with a password filter that disallows the use of common words (i.e., welcome, password, names of months/days/seasons, and the company name). If possible, an enterprise password manager should be used to assist users with choosing and using complex passwords.
- Rotate passwords periodically for **all** service accounts.
- Disallow local administrator access on user workstations unless a specific business need exists.
- Disable the default `RID-500 local admin` account and create a new admin account for administration subject to LAPS password rotation.
- Implement split tiers of administration for administrative users. Too often, during an assessment, you will gain access to Domain Administrator credentials on a computer that an administrator uses for all work activities.
- Clean up privileged groups. `Does the organization need 50+ Domain/Enterprise Admins?` Restrict group membership in highly privileged groups to only those users who require this access to perform their day-to-day system administrator duties.
- Where appropriate, place accounts in the `Protected Users` group.
- Disable Kerberos delegation for administrative accounts (the Protected Users group may not do this)

Protected Users Group

The Protected Users group first appeared with Window Server 2012 R2. This group can be used to restrict what members of this privileged group can do in a domain. Adding users to Protected Users prevents user credentials from being abused if left in memory on a host.

Viewing the Protected Users Group with Get-ADGroup

```
PS C:\Users\htb-student> Get-ADGroup -Identity "Protected Users" -Properties
Name,Description,Members



Description       : Members of this group are afforded additional
protections against authentication security threats.
                    See http://go.microsoft.com/fwlink/?LinkId=298939 for
more information.
DistinguishedName : CN=Protected Users,CN=Users,DC=INLANEFREIGHT,DC=LOCAL
GroupCategory     : Security
GroupScope        : Global
Members           : {CN=sqlprod,OU=Service
Accounts,OU=IT,OU=Employees,DC=INLANEFREIGHT,DC=LOCAL, CN=sqldev,OU=Service
                    Accounts,OU=IT,OU=Employees,DC=INLANEFREIGHT,DC=LOCAL}
Name              : Protected Users
ObjectClass       : group
ObjectGUID        : e4e19353-d08f-4790-95bc-c544a38cd534
```

```
SamAccountName     : Protected Users
SID                : S-1-5-21-2974783224-3764228556-2640795941-525
```

The group provides the following Domain Controller and device protections:

- Group members can not be delegated with constrained or unconstrained delegation.
- CredSSP will not cache plaintext credentials in memory even if Allow delegating default credentials is set within Group Policy.
- Windows Digest will not cache the user's plaintext password, even if Windows Digest is enabled.
- Members cannot authenticate using NTLM authentication or use DES or RC4 keys.
- After acquiring a TGT, the user's long-term keys or plaintext credentials are not cached.
- Members cannot renew a TGT longer than the original 4-hour TTL.

Processes

Maintaining and enforcing policies and procedures that can significantly impact an organization's overall security posture is necessary. Without defined policies, it is impossible to hold an organization's employees accountable, and difficult to respond to an incident without defined and practiced procedures such as a disaster recovery plan. The items below can help to define processes, policies, and procedures.

- Proper policies and procedures for AD asset management.
  - AD host audit, the use of asset tags, and periodic asset inventories can help ensure hosts are not lost.
- Access control policies (user account provisioning/de-provisioning), multi-factor authentication mechanisms.
- Processes for provisioning and decommissioning hosts (i.e., baseline security hardening guideline, gold images)
- AD cleanup policies
  - `Are accounts for former employees removed or just disabled?`
  - `What is the process for removing stale records from AD?`
  - Processes for decommissioning legacy operating systems/services (i.e., proper uninstallation of Exchange when migrating to 0365).
  - Schedule for User, groups, and hosts audit.

Technology

Periodically review AD for legacy misconfigurations and new and emerging threats. As changes are made to AD, ensure that common misconfigurations are not introduced. Pay attention to any vulnerabilities introduced by AD and tools or applications utilized in the environment.

- Run tools such as BloodHound, PingCastle, and Grouper periodically to identify AD misconfigurations.
- Ensure that administrators are not storing passwords in the AD account description field.
- Review SYSVOL for scripts containing passwords and other sensitive data.
- Avoid the use of "normal" service accounts, utilizing Group Managed (gMSA) and Managed Service Accounts (MSA) where ever possible to mitigate the risk of Kerberoasting.
- Disable Unconstrained Delegation wherever possible.
- Prevent direct access to Domain Controllers through the use of hardened jump hosts.
- Consider setting the `ms-DS-MachineAccountQuota` attribute to `0`, which disallows users from adding machine accounts and can prevent several attacks such as the noPac attack and Resource-Based Constrained Delegation (RBCD)
- Disable the print spooler service wherever possible to prevent several attacks
- Disable NTLM authentication for Domain Controllers if possible
- Use Extended Protection for Authentication along with enabling Require SSL only to allow HTTPS connections for the Certificate Authority Web Enrollment and Certificate Enrollment Web Service services
- Enable SMB signing and LDAP signing
- Take steps to prevent enumeration with tools like BloodHound
- Ideally, perform quarterly penetration tests/AD security assessments, but if budget constraints exist, these should be performed annually at the very least.
- Test backups for validity and review/practice disaster recovery plans.
- Enable the restriction of anonymous access and prevent null session enumeration by setting the `RestrictNullSessAccess` registry key to `1` to restrict null session access to unauthenticated users.

Protections By Section

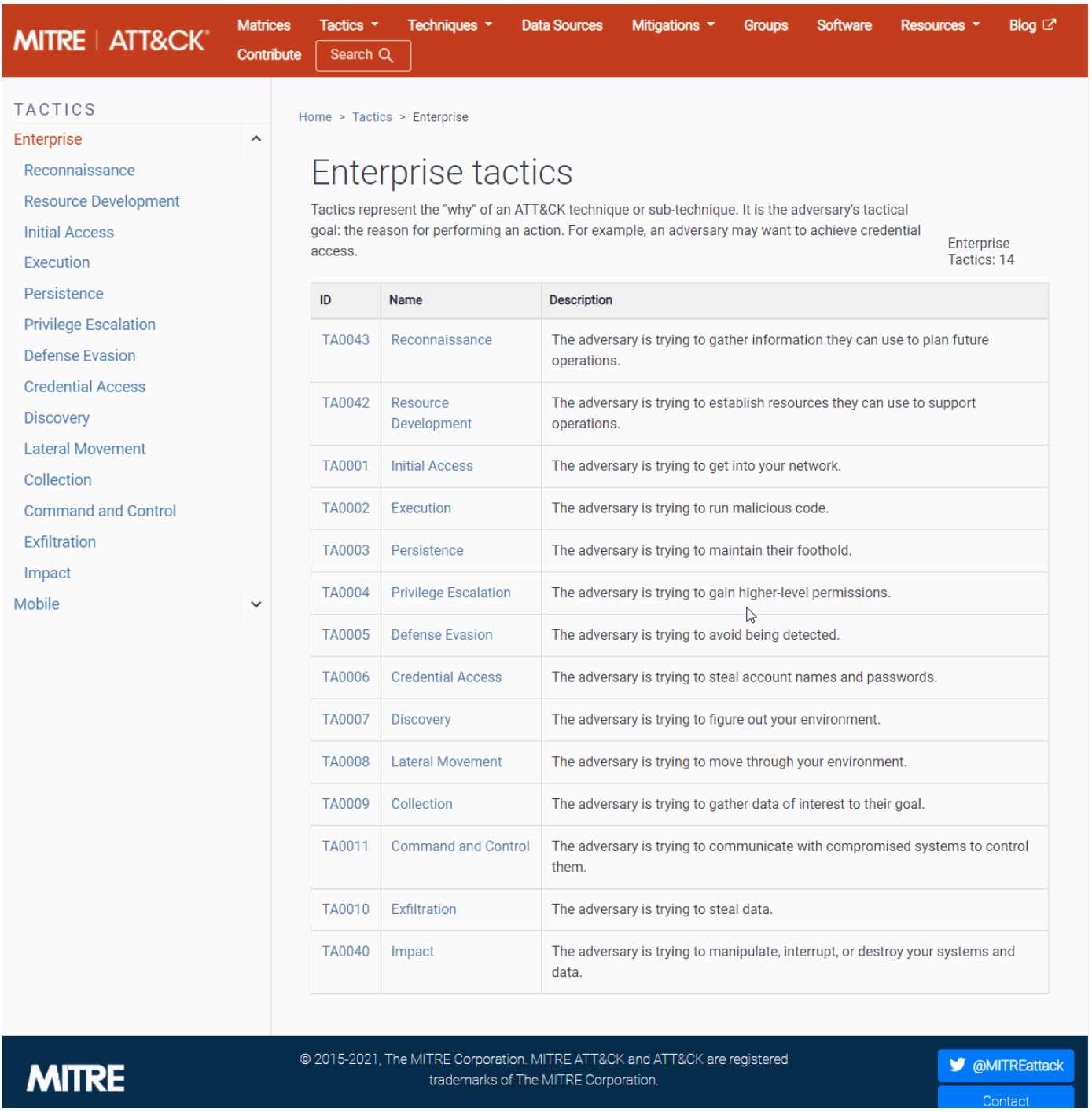
As a different look at this, we have broken out the significant actions by section and correlated controls based on the TTP and a MITRE tag. Each tag corresponds with a section of the Enterprise ATT&CK Matrix found here. Any tag marked as `TA` corresponds to an overarching tactic, while a tag marked as `T###` is a technique found in the matrix under tactics.

TTP	MITRE Tag	Description
`External Reconnaissance`	`T1589`	This portion of an attack is extremely hard to detect and defend against. An attacker does not have to interact with

TTP	MITRE Tag	Description
		your enterprise environment directly, so it's impossible to tell when it is happening. What can be done is to monitor and control the data you release publically to the world. Job postings, documents (and the metadata left attached), and other open information sources like BGP and DNS records all reveal something about your enterprise. Taking care to `scrub` documents before release can ensure an attacker cannot glean user naming context from them as an example. The same can be said for not providing detailed information about tools and equipment utilized in your networks via job postings.
`Internal Reconnaissance`	`T1595`	For reconnaissance of our internal networks, we have more options. This is often considered an active phase and, as such, will generate network traffic which we can monitor and place defenses based on what we see. `Monitoring network traffic` for any suspicious bursts of packets of a large volume from any one source or several sources can be indicative of scanning. A properly configured `Firewall` or `Network Intrusion Detection System` (`NIDS`) will spot these trends quickly and alert on the traffic. Depending on the tool or appliance, it may even be able to add a rule blocking traffic from said hosts proactively. The utilization of network monitoring coupled with a SIEM can be crucial to spotting reconnaissance. Properly tuning the Windows Firewall settings or your EDR of choice to not respond to ICMP traffic, among other types of traffic, can help deny an attacker any information they may glean from the results.
`Poisoning`	`T1557`	Utilizing security options like `SMB message signing` and `encrypting traffic` with a strong encryption mechanism will go a long way to stopping poisoning & man-in-the-middle attacks. SMB signing utilizes hashed authentication codes and verifies the identity of the sender and recipient of the packet. These actions will break relay attacks since the attacker is just spoofing traffic.
`Password Spraying`	`T1110/003`	This action is perhaps the easiest to defend against and detect. Simple logging and monitoring can tip you off to password spraying attacks in your network. Watching your logs for multiple attempts to login by watching `Event IDs 4624` and `4648` for strings of invalid attempts can tip you off to password spraying or brute force attempts to access the host. Having strong password policies, an account lockout policy set, and utilizing two-factor or multi-factor authentication can all help prevent the success of a password spray attack. For a deeper look at the recommended policy settings, check out this article and the NIST documentation.
`Credentialed Enumeration`	`TA0006`	There is no real defense you can put in place to stop this method of attack. Once an attacker has valid credentials, they effectively can perform any action that the user is allowed to do. A vigilant defender can detect and put a stop to this, however. Monitoring for unusual activity such as issuing commands from the CLI when a user should not

TTP	MITRE Tag	Description
		have a need to utilize it. Multiple RDP requests sent from host to host within the network or movement of files from various hosts can all help tip a defender off. If an attacker manages to acquire administrative privileges, this can become much more difficult, but there are network heuristics tools that can be put in place to analyze the network constantly for anomalous activity. Network segmentation can help a lot here.
`LOTL`	N/A	It can be hard to spot an attacker while they are utilizing the resources built-in to host operating systems. This is where having a `baseline of network traffic` and `user behavior` comes in handy. If your defenders understand what the day-to-day regular network activity looks like, you have a chance to spot the abnormal. Watching for command shells and utilizing a properly configured `Applocker policy` can help prevent the use of applications and tools users should not have access to or need.
`Kerberoasting`	`T1558/003`	Kerberoasting as an attack technique is widely documented, and there are plenty of ways to spot it and defend against it. The number one way to protect against Kerberoasting is to `utilize a stronger encryption scheme than RC4` for Kerberos authentication mechanisms. Enforcing strong password policies can help prevent Kerberoasting attacks from being successful. `Utilizing Group Managed service accounts` is probably the best defense as this makes Kerberoasting no longer possible. Periodically `auditing` your users' account permissions for excessive group membership can be an effective way to spot issues.

MITRE ATT&CK Breakdown



I wanted to take a second to show everyone how it appears when exploring the ATT&CK framework. We will use the example above of `Kerberoasting` to look at it through the lens of the framework. Kerberoasting is a part of the larger `Tactic tag TA0006 Credential Access` (Green square in the image above). Tactics encompass the overall goal of the actor and will contain various techniques which map to that goal. Within this scope, you will see all manner of credential-stealing techniques. We can scroll down and look for `Steal or Forge Kerberos Tickets`, which is `Technique Tag T1558` (blue square in the image above). This technique contains four sub-techniques (indicated by the `.00#` beside the technique name) Golden Ticket, Silver Ticket, Kerberoasting, and AS-REP Roasting. Since we care about Kerberoasting, we would select the sub-technique `T1558.003` (orange box in the image above), and it will take us to a new page. Here, we can see a general explanation of the technique, the information referencing the ATT&CK platform classification on the top right, examples of its use in the real world, ways to mitigate and detect the tactic, and finally, references for more information at the bottom of the page.

So our technique would be classified under `TA0006/T1558.003`. This is how the Tactic/Technique tree would be read. There are many different ways to navigate the framework. We just wanted to provide some clarification on what we were looking for and how we were defining tactics versus techniques when talking about MITRE ATT&CK in this module. This framework is great to explore if you are curious about a `Tactic` or `Technique` and want more information about it.

These are not an exhaustive list of defensive measures, but they are a strong start. As attackers, if we understand the potential defensive measures we can face during our assessments, we can plan for alternate means of exploitation and movement. We won't win every battle; some defenders may have their environments locked down tight and see every move you make, but others may have missed one of these recommendations. It is important to explore them all, and help provide the defensive team with the best results possible. Also, understanding how the attacks and defenses work will make us improve cybersecurity practitioners overall.