# LARES

**Continuous Defensive Improvement Through Adversarial Simulation and Collaboration**

# TOP 10 PENETRATION FINDINGS

## Executive Overview

Lares® encounters a seemingly endless number of vulnerabilities and attack vectors when we conduct a penetration test or red team engagement, regardless of organization size or maturity. Though not every engagement is identical, we have analyzed the similarities between hundreds of engagements throughout 2019 and the following list represents the most frequently observed penetration test findings we encountered.

## *Top 10 Penetration Test Findings*

- Brute Forcing Accounts With Weak and Guessable Passwords
- Kerberoasting
- Excessive File System Permissions
- WannaCry/EternalBlue
- WMI Lateral Movement
- Inadequate Network Segmentation
- Inappropriate Access Control
- Post-Exercise Defensive Control Tuning
- Malicious Multifactor Enrollment or MFA Bypass
- Phish-in-the-Middle (PiTM)

It should be noted that the Top 10 discussed within this paper does not pretend to emphasize the findings as being the most severe, but rather, the most frequently encountered during engagements for the time period. We hope you enjoy the report and please reach out via email, sales@lares.com, or phone, (720) 600-0329, should you have any additional questions, comments, or concerns

**Lares**
2311 Champa Street
Denver, CO 80205

Phone: (720) 600-0329
Twitter: @Lares_

Email: sales@lares.com
www.lares.com


# Brute Forcing Accounts With Weak and Guessable Passwords

The use of multifactor authentication is recommended and provides a higher level of security than usernames and passwords alone. However, organizations that have not implemented multi-factor authentication should be aware that adversaries may target accounts where users have selected weak or guessable passwords (e.g. the names of local sports teams, their company, pets, or some combination of the season or year) in order to gain access to systems, services, and network resources.

## Detection

Monitor authentication logs for system and application login failures of valid accounts. If authentication failures are high, then there may be a brute force attempt to gain access to a system using legitimate credentials.

Also, monitor for many failed authentication attempts from a single source across numerous accounts that may result from password spraying attempts.

- For password spraying consider enabling the following via Domain Controller Group Policy located in `Policies > Windows Settings > Security Settings > Local Policy > Audit Policy:Domain Controllers:` "Audit Logon" (Success & Failure) for event ID 4625.
- Domain Controllers: "Audit Kerberos Authentication Service" (Success & Failure) for event ID 4771.
- All systems: "Audit Logon" (Success & Failure) for event ID 4648.
- Instrument client-facing applications such as web site authentication portals to log and alert on authentication successes and failures.
- Ensure logging is available from all affected hosts

Once auditing has been enabled, the Security Event Log should be forwarded to a central log repository for correlation and alerting.

## Mitigation

Set account lockout policies after a certain number of failed login attempts to prevent passwords from being guessed, however, consider that brute force activity may lock accounts unexpectedly and cause a Denial of Service and increase service desk calls. Consider the use of multifactor authentication, but limit the new user enrollment period window to ensure adversaries aren't able to enroll their own devices. Password vaulting, blacklisting and regular audits can help combat weak passwords in use.

Never reuse passwords between user accounts, service accounts, and administrative accounts and consider using a Local Administrator Password Solution (LAPS) for the management of local account passwords of domain joined computers.

### References


- https://attack.mitre.org/techniques/T1110/
- https://attack.mitre.org/techniques/T1111/

# Kerberoasting

Kerberos Service Principal Names (SPNs) are used to uniquely identify each instance of a Windows service configured to accept Kerberos Tickets for authentication. Kerberos authentication requires that SPNs be associated with at least one service account (an account specifically tasked with running a service).

Adversaries possessing a valid Kerberos Ticket-Granting Ticket (TGT) may request one or more Kerberos Ticket-Granting Server (TGS) Service Tickets for any service with an SPN configured from a Key Distribution Server, typically the Domain Controller (DC) in Windows Active Directory. Adversaries can request a service ticket be encrypted with the legacy RC4 algorithm which uses the NT LanManager (NTLM) hash of the service account associated with the SPN.

This Service Ticket can be taken offline and a brute-force attack can be used to recover the plain-text credentials of the account. In many environments, the Service Account has administrative permissions to the server where the SPN is configured. This same attack could be executed using service tickets captured from network traffic, however, newer operating systems request Service Tickets encrypted with the AES algorithm.

## Detection

Enable Audit Kerberos Service Ticket Operations to log Kerberos TGS service ticket requests. Particularly investigate irregular patterns of activity (e.g accounts making numerous requests, Event ID 4769, within a small time frame, especially if they also request RC4 encryption).

Additionally, a “canary” account can be created and configured with an SPN. This account should not be used so that when a ticket is requested (4769) for the “canary” account, it would warrant further investigation by the organization’s security team as immediate suspicious behavior.

## Mitigation

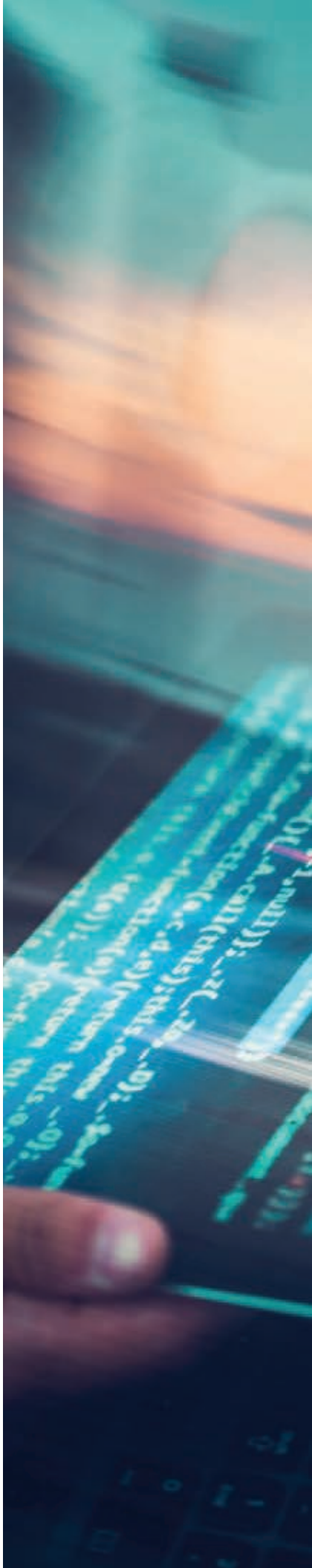
Ensure strong password length (ideally 15+, random characters leveraging multicase alphanumeric and special characters) and complexity for service accounts. Also, ensure that the passwords for these accounts periodically expire. Consider using Group Managed Service Accounts or another third party product such as password vaulting to reduce the overall exposure.

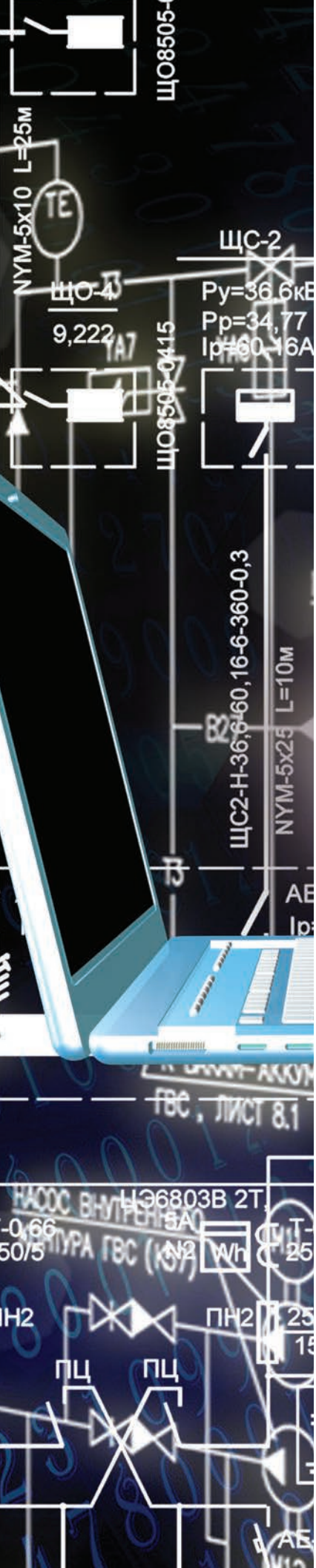
Ensure that regular users within your infrastructure are not running with Administrative privileges on their own machines and limit service accounts to minimal required privileges, including membership in privileged groups such as Domain Administrators. Perform routine audits of all SPNs to ensure only those required are enabled within the Domain.

Where possible, enable AES Kerberos encryption (or another stronger encryption algorithm), rather than RC4.

### References


- https://attack.mitre.org/techniques/T1208/




# Excessive File System Permissions

Processes may automatically execute specific binaries as part of their functionality or to perform other actions. Improperly set permissions on the binary or directory in which it resides may allow an attacker to replace the legitimate binary with a file of their choosing. If the legitimate binary was previously configured to execute under higher-level permissions (such as the SYSTEM account, commonly used to run Services), then the newly replaced binary will run with those same elevated permissions.

Adversaries may use this technique to replace legitimate pre-existing binaries or DLLs with their own malicious ones in order to execute subversive, or potentially disruptive code with a much higher permission level than that of their current user permissions. This technique can also be used as a means to establish persistence if the executing process is set to run at a specific time or during a certain event like system startup).

## Detection

If an executable is written, renamed, and/or moved to match an existing service executable, it could be detected and correlated with other suspicious behavior. The use of traditional file integrity monitoring (FIM) tools in conjunction with the hashing of binaries and service executables could be used to detect replacement or modification against historical data.

Monitor the process execution tree for abnormal process calls from well-known processes and services, and for the execution of other commands in addition to new network-based connections to unfamiliar IP addresses or domains.

## Mitigation

Use auditing tools, such as a File Integrity Monitoring (FIM) tool, capable of detecting file system permissions abuse opportunities on systems within an enterprise and correct them. Limit privileges of user accounts and groups. Ensure that only authorized administrators can change services and other system-level functionality.

Identify and block potentially malicious software that may be executed through abuse of file, directory, and service permissions. Tools like AppLocker are capable of auditing and/or blocking unknown programs and should be utilized. Deny the execution of binaries from user directories, temp directories, and other non-standard or approved directories, where able. Also consider periodic testing of the server and desktop “Gold Images” used within the environment to prevent systemic weakness from affecting a significant number of systems at once.

## References


- https://attack.mitre.org/techniques/T1044/

# WannaCry/EternalBlue

Remote code execution vulnerabilities exist in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests. An attacker who successfully exploited the vulnerabilities could gain the ability to execute code on the target server. Though this vulnerability was resolved in MS17-010, many organizations have yet to deploy this patch or disable SMBv1 within their organization.

The EternalBlue and EternalRomance exploits were leaked by "The Shadow Brokers" group on April 14, 2017. The included tools targeted multiple vulnerabilities in the Windows implementation of the SMB protocol as outlined in MS17-010.

The EternalBlue exploit was also leveraged by WannaCry ransomware to compromise Windows machines, load malware, and propagate to other machines in a network.

## Detection

Look for SMBv1 protocols communicating on your network by reviewing stateful firewall logs, intrusion detection/protection system logs, or network traffic analysis. Microsoft has also released scripts and guidance to detect and disable SMBv1 on systems.

## Mitigation

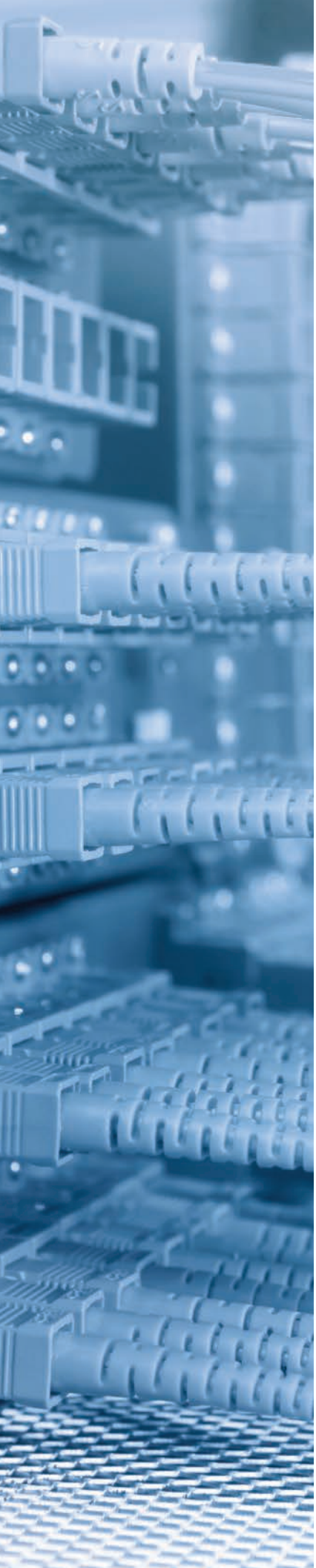
Patches for this vulnerability were released in March of 2017. A periodic patch review process should be developed to ensure applicable, critical patches are identified and deployed in a timely manner.

Microsoft also recommends disabling SMBv1 in favor of newer, more secure versions. SMBv1 can be disabled via Group Policy and its state validated using the guidance provided in the *References* section.

Consider enabling host-based firewalls on clients and servers to minimize the exposure of sensitive ports such as 445/TCP used by SMB. By enabling a host-based firewall, organizations can prevent adversary lateral movement as well as minimize the impact of an automated worm in case of infection.

### References


- https://research.checkpoint.com/eternalblue-everything-know/
- https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010
- https://support.microsoft.com/en-us/help/2696547/detect-enable-disable-smbv1-smbv2-smbv3-in-windows-and-windows-server
- https://blogs.technet.microsoft.com/staysafe/2017/05/17/disable-smb-v1-in-managed-environments-with-ad-group-policy/
- https://attack.mitre.org/techniques/T1210/

# WMI Lateral Movement

Lateral movement is a critical phase in any attack targeting more than a single computer. Is it not a vulnerability, but rather, a technique employed by attackers to interact with or gain access to, a system other than the current system upon which they are operating.

Lateral movement techniques usually abuse existing mechanisms often leveraged by legitimate systems administrators, assuming the attacker has the right credentials. The Windows Management Instrumentation system allows for a structured approach to communicating with a remote computer and exposes system monitoring and configuration capabilities to a remote machine. An adversary can use this native functionality to execute malicious code, modify system settings such as adding a user or changing a password, or disabling security tools before performing other activities.

## Detection

Consider enabling WMI Tracing on servers and workstations within your environment, and centrally monitor or correlate these events. The process execution tree can be monitored for processes spawning from the WMI parent process of WMIPRVSE.EXE.

## Mitigation

By default, only administrators are allowed to connect remotely using WMI. Restrict other users who are allowed to connect, or disallow all users to connect remotely to WMI.

In many cases, disabling WMI or RPCS may cause system instability. It is recommended that you evaluate and test the impact to your infrastructure before disabling.

### References


- https://attack.mitre.org/techniques/T1047/
- https://redcanary.com/blog/lateral-movement-winrm-wmi/
- https://www.cybereason.com/blog/wmi-lateral-movement-win32

# Inadequate Network Segmentation

Most corporate networks are largely flat, meaning there are often no firewalls or other access control devices between endpoints. This allows an attacker to enumerate remote services on servers or workstations that normally do not communicate with each other, providing an attacker additional targets to potentially compromise.

Typical end-user workstations in an enterprise environment rarely need to communicate with each other and most end-user workstations don't need to communicate directly with back-end database systems.

Consider how broad the access is for remote users on client VPN solutions or virtualized environments. Often organizations focus heavily on technologies to restrict and monitor end user systems when connected to the internal network but overlook the broad access available when that same end user system is connected to the VPN for remote access.

## Detection

Without properly implemented network-based and host-based technical controls, detecting inadequate network segmentation is quite difficult. Endpoint agents can typically alert on initiated connection attempts from unauthorized (or unexpected) clients. Similarly, network-based IDS, IPS, or deep packet inspection technologies can be used to detect repeated connection attempts to and from systems within your environment.

## Mitigation

Organizations should consider segmenting their networks into zones based on security risk and exposure, and implement logical separation using VLANs and stateful firewalls. Internet-accessible zones should be isolated from the rest of the environment and be behind a default-deny access control list or firewall rule with heavy monitoring. This should also be the case with other untrusted networks such as the organization's Guest wireless.

Carving up an existing network may feel like a daunting task at first, but is much easier when broken down and accomplished in smaller chunks. If a full network redesign isn't possible, consider implementing host-based firewalls on all workstations and servers during the system design phase and architect proper segmentation as new systems are introduced and legacy systems are retired.

This methodology also applies to cloud-hosted resources, and can be implemented through multiple subscriptions and network security groups. If your organization is considering a "push to the cloud," it's best to consider network segmentation based on risk from the beginning and incorporating lessons learned from legacy on-premise infrastructure.

### References


- https://attack.mitre.org/mitigations/M1030/
- https://attack.mitre.org/techniques/T1133/
- https://attack.mitre.org/techniques/T1046/


# Inappropriate or Ineffective Access Control

Just like network endpoints, user access permissions should be segmented based on risk and exposures. Authentication and Authorization are two separate topics, and bring up two distinct issues. In Active Directory environments, by default, all users are allowed to authenticate to every other system even though they may not have the appropriate authorization to access services hosted on that system.

This default authentication configuration allows for unrestricted configuration and service enumeration that can allow an attacker the ability to gather enough information to further their foothold in the environment. Tools like Bloodhound take advantage of this configuration and can help attackers build a map of which systems to target next.

## Detection

Effective audit logging should help indicate if users are attempting to access resources that they should not have access to. Behavior anomaly detection tools could also shine the light on users attempting to access something that they have never attempted to access before, which could be cause for alarm.

## Mitigation

Organizations should consider implementing a policy of least privilege approach, and specifically for Windows environments, hardening systems by implementing the Group Policy option of *"Deny access to this computer from the network."*

Organizations should also consider investigating which users may be unexpectedly authorized to access certain services. Tools, such as the previously mentioned BloodHound, can identify where users have administrative permissions, Remote Desktop (RDP) access, and access to SQL Servers.

This information may be useful to uncover unexpected group memberships or misconfigured permissions. Data discovery and data classification tasks are also extremely useful when undertaking access control efforts. By identifying and classifying data, weak permissions that break the corporate access control model can be more easily identified, and may lead to less broad-access permissions on file shares and database servers.

## References


- https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn221954(v%3Dws.11)
- https://github.com/BloodHoundAD/BloodHound
- https://attack.mitre.org/tactics/TA0004/

# Post-Exercise Defensive Control Tuning

Organizations expend enormous time and financial resources on the operationalization of modern security platforms without first allocating the necessary time and people to effectively tune these controls. These systems are just that: a **platform** on which other pieces of a fully functioning security system has to be built.

Most organizations we interact with have the appropriate visibility and logging capabilities, such as a Security Information Event Management (SIEM), but the logging and alerting processes aren't appropriately tuned to generate meaningful alerts for the assigned security analysts to respond. The information stored in these SIEMs are good for forensics after a breach, but many businesses want to be more proactive in their Incident Response activities.

## Detection

Purple team exercises will help organizations better understand the types of events, alerts, and incidents that currently deployed tools may be missing. Similarly, formal Table Top exercises, emulating specific attack methodologies, should be conducted, and results reviewed, to ensure effective monitoring throughout the organization's security ecosystem.

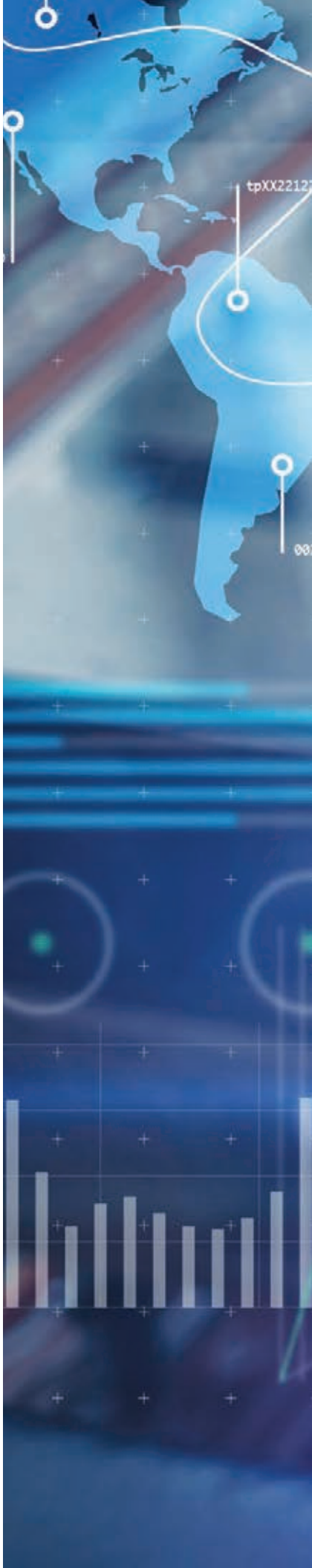
## Mitigation

Organizations should become familiar with common attacker techniques and strive to operationalize this knowledge within their security teams. Security teams can then prioritize which techniques they may experience based on the attack groups most likely to target their vertical, and build prevention and detection strategies to better identify potentially malicious activity within their environment.

A maturity model should be adopted to provide a path to a successful control tuning program. This model can help drive current detection gaps as well as provide a roadmap for future security tool funding requests, along with providing valuable information for an organization's security stack.

### References


- https://www.malwarearchaeology.com/cheat-sheets/
- https://car.mitre.org/

# Malicious Multifactor Enrollment or MFA Bypass

Malicious Multifactor Enrollment refers to an attacker's ability to enroll themselves into an organization's multifactor authentication system. Organizations typically allow for self-enrollment in multifactor authentication systems to ease load on the helpdesk. As user's may be off-site when they're required to enroll, these systems are typically deployed as Internet-facing, and always accessible, systems. A malicious attacker can take advantage of these systems by identifying which accounts are not yet enrolled and can enroll on the user's behalf using the attacker's own information.

If the self-enrollment period has no expiration date, attackers may attempt to enroll additional devices in an attempt to assume control of the user's previously authorized account. Often these systems allow for additional (rogue) devices to be enrolled even after the authorized corporate device is enrolled.

## Detection

Effective detection is only made easier through the use of properly configured audit logs. An increase in the amount of enrollments, over a short period of time, may be indicative of an attacker attempting to maliciously enroll themselves. Multiple enrollment attempts from the same source IP address or registered phone number should be suspect as should additional enrollment attempts to previously authorized accounts using new devices. Registrations outside of regular business hours could also point towards suspicious activity.

## Mitigation

Organization's should limit the amount of time that newly created accounts are eligible for self-enrollment and a second factor of authorization should also be required during the enrollment process. An infinite amount of time for enrollment dramatically increases the risk for abuse.

All user accounts should not be granted inclusion in the organization's VPN or remote access group by default. These users should only be moved into the group after they have successfully completed their self-enrollment and the enrollment window has expired.

Utilize a Mobile Device Management (MDM) solution to authorize and monitor devices approved to enroll. Do not allow multiple additional devices to be enrolled if the user already has successfully enrolled a device in the past.

Conduct routine audits on all accounts that have not yet been enrolled during the approved window and restrict access to the non-compliant account forcing enrollment or notifying the user of their required actions.

### References


- https://attack.mitre.org/techniques/T1047/
- https://redcanary.com/blog/lateral-movement-winrm-wmi/
- https://www.cybereason.com/blog/wmi-lateral-movement-win32

# Phish-in-the-Middle (PiTM)

"Phish in the Middle" or (PiTM) is a technique used to hijack the trust of an email recipient by replying to an ongoing email thread. An attacker who is able to gain access to a user's mailbox by recovering their password via phishing, brute force, or other means, can simply reply to an existing email in the user's inbox with a malicious payload or requesting the recipient to perform some action.

This technique bypasses all known phishing training and email security controls as:

- The email comes from someone they know,
- The body, signature, and text of the message are relevant to an ongoing conversation,
- The email bypasses perimeter security spanning gateways such as anti-spam and anti-phishing, and
- The document in the email comes from someone they already have a relationship with.

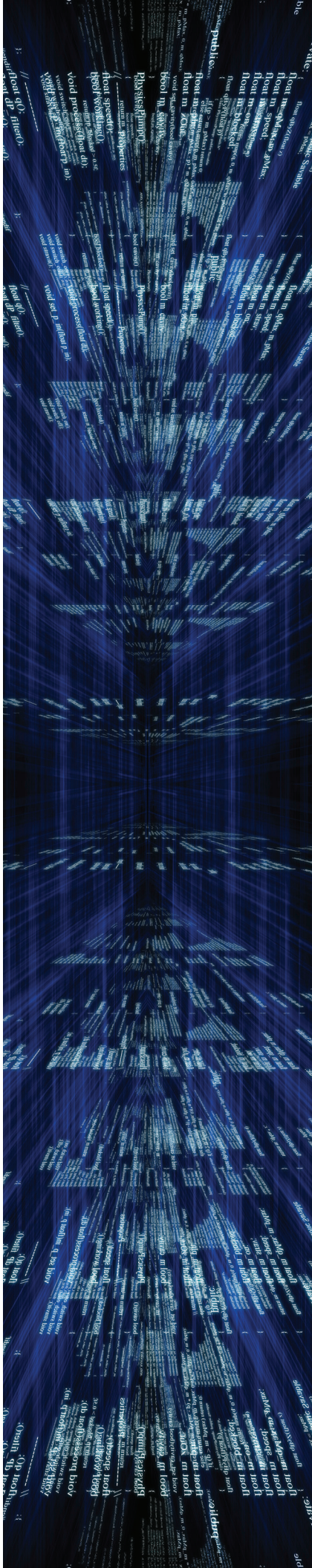
In most scenarios, the unsuspecting user will open an attachment or perform a requested action as the credibility with the sender is already established from the ongoing conversation thread. This increases the likelihood for success as the attacker does not need to coerce the recipient and they have real time feedback during the attack, unlike conventional phishing where the attacker is blind to the victim's actions in most cases.

## Detection

Detection capabilities depend on the type of attack the adversary may be attempting. If malicious payloads are inserted into an active message thread, host based and inline controls could increase the likelihood for detection. Is the payload safe on disk? Is the endpoint security product effective in detecting and stopping execution?

In some scenarios, the attacker may request the targeted user to visit an external website to attempt other client side attacks. Outbound web proxies and content inspection filters can help to identify when a user attempts to visit a malicious or untrusted external website. These solutions are also effective in detecting when malicious files are attempted to be downloaded.

*Continued on the next page*



*Continued from previous page*

## Mitigation

As with any Social Engineering tactic, the best defense is on-going training coupled with adequate technologies to help defend the user population and their corporate assets. Ensure that users are trained on the various types of Social Engineering techniques they may be exposed to when using their devices. While conventional training often focuses on common phishing methods, techniques such as PiTM should be incorporated into training modules to ensure users are comfortable in detecting and responding to suspicious requests, even in trusted and active on-going conversations. As the creative methods of attackers continue to evolve, so should the training and topics that are being delivered to your staff.

Defensive controls must also be tested through simulated exercises. Routine purple teaming (collaborative) workshops can help to measure how effective your defensive technologies are in stopping attacks such as PiTM. Various payloads, command and control transports, content inspection and web filtering can all be measured and tuned through coordinated attack simulations.

### References


- https://attack.mitre.org/techniques/T1189/
- https://attack.mitre.org/techniques/T1192/
- https://attack.mitre.org/techniques/T1193/
- https://attack.mitre.org/techniques/T1043/

# Conclusion

At first, we were surprised at how many times the above Top 10 findings were found during our penetration test and red team engagements. As we wrapped up 2019, however, the surprise gave way to expectation and we found ourselves genuinely surprised if one or all of the Top 10 were not found on the engagement.

Every single vulnerability described in this paper can be avoided or eliminated through better cybersecurity hygiene practices. Table 1 provides a final reminder on the mitigation suggestions for each of the Top 10 penetration test findings detailed within this paper.

**Table 1 - Top 10 Penetration Test Findings: Mitigations**

| Finding | Mitigations |
|---|---|
| **Brute Forcing Accounts With Weak Passwords Provided During Open Enrollment** | • Account lockout policies after a certain number of failed login attempts (prevents passwords guessing).<br>• Utilize password complexity standards.<br>• Use multifactor authentication.<br>• Limit the new user enrollment period window. |
| **Kerberoasting** | • Ensure strong password length and complexity for service accounts.<br>• Expire passwords periodically.<br>• Use Group Managed Service Accounts or third-party password vaults.<br>• Limit service account access, and group membership, to what is required.<br>• Enable AES Kerberos encryption rather than RC4. |
| **Excessive File System Permissions** | • Use tools to detect file permissions abuse.<br>• Limit privileges of user accounts and groups.<br>• Whitelist legitimate executables.<br>• Deny execution from user directories (e.g. download directories and temp directories).<br>• Turn off UAC's privilege elevation for standard users to automatically deny elevation requests.<br>• Enable installer detection for all users. |
| **WannaCry/EternalBlue** | • Apply MS17-010 patches from Microsoft.<br>• Disable SMBv1<br>• Block inbound SMB at your perimeter.<br>• Disallow endpoints from communicating via SMB. |
| **WMI Lateral Movement** | • Evaluate disabling WMI or RPCS.<br>• Restrict non-administrator users from connecting remotely to WMI.<br>• Prevent credential overlap across systems of administrator and privileged accounts. |
| **Inadequate Network Segmentation** | • Segment networks into zones based on security risk and exposure.<br>• Internet-accessible zones should be isolated and subject to a 'default-deny' access control rule.<br>• Implement host-based firewalls on all workstations and servers. |

*Continued on the next page*

*Continued from previous page*

| Finding | Mitigations |
|---|---|
| **Inappropriate or Ineffective Access Control** | • Deploy *"Deny access to this computer from the network."* Group Policy option.<br>• Identify and classify sensitive data within the organization.<br>• Audit for weak permissions that break the corporate access control model. |
| **Post-Exercise Defensive Control Tuning** | • Become familiar with common attacker techniques and operationalize learned knowledge.<br>• Prioritize techniques applicable to your environment and tune accordingly.<br>• Adopt a maturity model to provide a path to a successful control tuning program. |
| **Malicious Multifactor Enrollment or MFA Bypass** | • Limit the amount of time that newly created accounts are eligible for self-enrollment.<br>• Utilize a second factor of authorization during the enrollment process.<br>• Leverage MDM solutions to authorize and monitor devices approved to enroll. |
| **Phish-in-the-Middle (PiTM)** | • On-going training coupled with adequate technologies to defend corporate assets.<br>• Defensive controls must be tested through simulated exercises.<br>• Routine purple teaming (collaborative) workshops help measure effectiveness. |

Addressing the issues disclosed in this paper not only makes your organization a more difficult target for attackers, it also challenges your penetration testers to become more creative during their engagements - something that may lead to previously undiscovered vulnerabilities or attackable threat vectors..

We encourage you to contact Lares today to schedule a quick Security Health Check, penetration test, or full defensive review of your infrastructure to validate if these findings exist within your organization.

# ABOUT LARES

Lares® (Lar-Res) is a Denver, CO cybersecurity consulting company that prides itself on its ability to provide continuous defensive improvement through adversarial simulation and collaboration. Lares can help your organization validate its security posture through offensive security-focused services such as complex adversarial simulations, network penetration testing, application security assessments, insider threat assessments, vulnerability research, continuous security testing, virtual Chief Information Security Officer (CISO) services, and coaching.

## *Why the Industry Looks to Lares for Leadership*

Historically, industry assessments focus on the negative aspects of your organization's security program. Lares is committed to highlighting where gaps may exist and working closely with you to build a mature security program capable of defending against any adversary you may face.

The team at Lares:

- Created the Penetration Testing Execution Standard (PTES), the global industry-standard of effective penetration testing.
- Founded the Security BSides international information security conference organization to make security education available, accessible, and affordable to individuals, regardless of budget.
- Team is a founding member of the National Collegiate Cyber Defense Competitions (NCCDC) that oversees all 10 regional Collegiate Cyber Defense Competitions (CCDC) to mentor the next generation of offensive security experts.

Here at Lares, we want to help you make the most informed security decisions you can for your organization by giving you confidence. Confidence to defend against attackers with the tools at hand, address security and compliance concerns, and pass audits and assessments.

# LARES

**Continuous Defensive Improvement Through Adversarial Simulation and Collaboration**

**Lares**
2311 Champa Street
Denver, CO 80205

Phone: (720) 600-0329
Twitter: @Lares_

Email: sales@lares.com
www.lares.com

# LARES

**Continuous Defensive Improvement Through Adversarial Simulation and Collaboration**


**Lares**
**2311 Champa Street**
**Denver, CO 80205**

**Phone:**
**(720) 600-0329**
**Twitter: @Lares_**

**Email:**
**sales@lares.com**
**www.lares.com**