Microsoft

POP - Securing Lateral Account Movement (SLAM) *Credential Theft Mitigation*

POPSLAM

Target Audience:

This course is an advanced course for implementing lateral movement mitigations from Microsoft's Pass the Hash Whitepaper. The specific tasks discussed in this POP includes:

Enforce local account restrictions for remote access.

Deny network logon to local accounts

Create unique passwords for local privileged accounts

Overview

As the tools and techniques for credential theft and reuse attacks like the Pass-the-Hash (PtH) attack improve, malicious users are finding it easier to achieve their goals through these attacks. The PtH attack is one of the most popular types of credential theft and reuse attack seen by Microsoft to date. This Proactive Operations Program is part of the Credential Theft Mitigations suite and provides defenses for lateral traversal, a key aspect of this attack technique.

Key Features and Benefits

In many organizations, the local administrator username and password are shared among many machines, creating a risk of lateral movement if any machine is compromised. This Proactive Operations Program is designed to provide your organization with advanced skills and tools to increase the difficulty for an attacker to move between machines while maintaining manageability.

Technical Highlights

After completing this course, you will be able to:

- Understand the tools that are used to exploit "Pass the Hash (PtH)
- Understand the breadth of related credential theft risks
- Understand the specific risks of shared passwords and available mitigations
- Enforce local account restrictions for remote access
- Deny network logon for remote access to all local accounts
- In a lab environment, practice implementation steps to create unique passwords for local privileged accounts on all machines.
- Overview and practice of automated password changes for privileged local accounts.
- Implement recovery procedures of the password for these privileged local accounts.

Focus Areas

Environment Requirements:

Customer will need to provide a lab Active Directory environment. This will require at a minimum the following: 1 Domain Controller, 1 system for each member operating system currently used in the environment.

The POP - Securing Lateral Account Movement is scheduled for 3 days with a Microsoft Premier Field Engineer working alongside the customer's Security and Active Directory Staff. The deliverable will consist of training, knowledge transfer and implementation of the discussed topics in a customer provided lab. Optionally, a customer may choose to perform a basic implementation in their production environment after testing in a lab environment.

Module 1: Overview of Pass the Hash: Module will cover the Pass the Hash credential reuse. Will also discuss system architecture regarding NT Hash, LM Hash, and clear-text passwords to prime the participants on the issues being mitigated.

Module 2: Pass the Hash Mitigations: This module covers different mitigations to reduce the risk of Pass the Hash. This will include all current Microsoft recommended mitigations and begin focusing specifically on the topics that will be used for mitigating Lateral Traversal.

Module 3: Enforce Local Account Restrictions for Remote Access: This module covers a number of GPO settings that will be implemented to ensure that local system accounts are not allowed to connect to other client systems in the environment.

Module 4: Enabling the local firewall: Discussion around using the local firewall on client machines to ensure that client systems do not have connectivity to each other unless specifically allowed. Will focus on using the Windows Firewall however the topics covered could be used with any client firewall vendor.

Module 5: Randomizing Local Administrator Passwords: This module covers a solution for randomizing the local administrator passwords and storing these passwords in Active Directory in a secure fashion.

Module 6: Putting it all together : Conclusion of delivery will test the implemented mitigations. Steps included password randomization and retrieval, ensuring clients cannot connect to each other using local accounts and that firewall rule sets prevent unnecessary client to client communications.