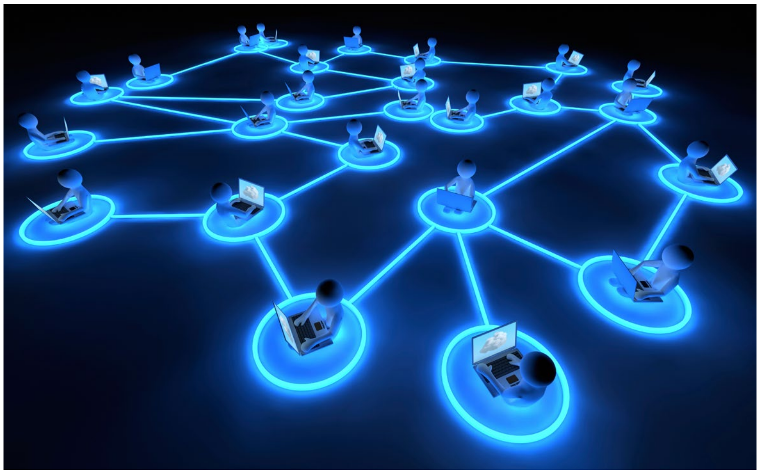
Limiting Workstation-to-Workstation Communication

Compromise of just one user workstation can lead to the loss of an entire network. All it takes is an unsuspecting user to click on a malicious email attachment or visit an infected website for an adversary to obtain access to a single workstation. Once the workstation is compromised, the attacker uses the newly gained privileges to scan and traverse the network. This leads to additional accesses and the attacker moving from one workstation to another obtaining intellectual property, critical information, and user credentials along the way. Once privileged credentials are obtained, the attacker has full control over the network and the sensitive information it contains.

Network security professionals must assume that a determined adversary will eventually breach a workstation on the network. Therefore, preventing the spread and extent of compromise by limiting workstation-to-workstation communication is a critical component of a defense-in-depth strategy.



Why Is Workstation-to-Workstation Communication a Problem?

In the early days of computer networking, files were often shared directly from one workstation to another, but modern networks leverage the power and processing capabilities of network servers. These systems serve files faster and more securely than sharing files directly between workstations. Therefore, within most enterprise environments, workstation-to-workstation communication is rarely used and does not provide any significant benefit.

In fact, workstation-to-workstation communication actually creates serious vulnerabilities. Enabling workstation-to-workstation communication can allow a network intruder to easily spread to multiple systems and establish an effective “beach head” within the network. Once a beach head is established the attackers can setup multiple communication paths out or backdoors into the network to maintain persistence.

High-value systems may be more secure and harder to access and exploit, so the attacker will then attempt to move laterally (hop from one workstation to the next within a network) to find an avenue to these targets Attackers can move laterally through the network using a variety of methods, for example by connecting to open, or poorly protected shared directories on workstations, or, more commonly for Microsoft® Windows® networks, via a particularly damaging method called pass-the-hash (PtH)[1].

PtH and other forms of legitimate credential reuse are serious vulnerabilities existing in all environments that implement Single Sign-on whether, it is Windows, Linux®, or Mac®[2]. PtH allows an attacker to reuse legitimate administrator or user credentials to move from system to system on a network without ever having to crack a password. Once an attacker compromises a single host, he will typically reuse stolen hashed credentials to spread to other systems on the network, gain access to a privileged user’s workstation, grab domain administrator credentials, and subsequently take control of the entire environment.

The threat of a PtH attack is real. PtH automation tools are publicly available on the Internet, making this attack as easy as a few button clicks. Microsoft recently emphasized that the ability to steal and reuse credentials can be utilized repeatedly to compromise entire network infrastructures within minutes.

Recommended Mitigations

Limiting workstation-to-workstation communication will severely restrict attackers' freedom of movement via techniques such as PtH. In general, limiting the number and type of communication flows between systems also aids in the detection of potentially malicious network activity. Because there are fewer allowed communication paths, abnormal flows become more apparent to attentive network defenders.

The following mitigations focus on Windows networks, but the concepts apply to other operating systems.

Restrict Communications with Firewall Rules

Prevent workstation-to-workstation communication by setting Windows Firewall rules, preferably via Group Policy so as to reach all workstations within a domain. If workstations need to communicate with each other via a particular service, configure the firewall to allow only that service-specific traffic. This simple, yet effective mitigation should have little to no impact on users and will greatly reduce the network's attack surface.

Deny Logon Across the Network

Microsoft Windows provides the ability for administrators to grant or deny users or groups of users certain privileged "user rights" on the operating system. To limit workstation-to-workstation communication, via Group Policy (preferred) or local security policy, add members of the local Administrators group to two user rights, "Deny access to this computer from the network" and "Deny log on through Remote Desktop Services" (for Windows Server® 2008R2 and later)[3].

Control Administrative Privileges

Lateral movement is most successful when conducted with privileged credentials. Therefore, controlling and protecting privileged accounts is critical. Implement a least-privilege administrative model, only granting users those privileges needed to do their jobs, and protect privileged credentials by restricting how and where they can be used.

Logically Segregate Segments by Using Private VLANs

Implement private VLANs with port restriction. Unlike traditional virtual LANs (VLANs) that can be circumvented, private VLANs prevent hosts on the same subnet from communicating with other hosts on the same subnet.

Additional Information

- Reducing the Effectiveness of Pass-the-Hash
http://www.nsa.gov/ia/_files/app/Reducing_the_Effectiveness_of_Pass-the-Hash.pdf
- Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques, December 2012
http://www.microsoft.com/en-us/download/details.aspx?id=36036
- Windows 7 STIG Version 1, Release 11, Dated 1-APR-2013
http://iase.disa.mil/stigs/os/windows/seven.html

Disclaimer of Endorsement: Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government, and shall not be used for advertising or product endorsement purposes.

[1] Microsoft® and Windows® are registered trademarks of Microsoft Corp.

[2] Linux® is a registered trademark of Linux Foundation. Mac® is a registered trademark of Apple Inc.

[3] Windows Server® is a registered trademark of Microsoft Corp.