Third Wall™ for LabTech® – Operational Considerations to Enhance Endpoint Security

Dr. Kenneth Knapp, CEO, Cyber Secure Advising
CISSP, Certified Ethical Hacker
April 2016

Although most companies these days have good firewalls and strong antivirus, the area of cybersecurity at the endpoint has become the battlefield of choice for malware and hackers. End users are, innocently or not, clicking on unsafe links and opening dangerous attachments. Employees are stealing data. And even IT professionals are leaving open protocols and services that are vulnerable – and often not even being used. The concepts of "least privilege" and "least access" are becoming ever more critical – and Third Wall is helping to address that with a technology-assisted approach.

Overview

This document will discuss a few key vulnerabilities that are addressed by Third Wall, and how you should view them in your environment. If possible, you should address these vulnerabilities, whether through Third Wall or through other means.

In general, you should implement policy changes in a business environment separately, one at a time. Local policy assignment changes should be done individually or in isolation to first assess its impact on the business networking environment. Thus, it's advisable not to make multiple changes to devices simultaneously since, if an important service becomes unstable or stops working, it's harder to isolate and troubleshoot the reason. When changes are made, it's recommended they be done individually and after waiting a sufficient amount of time. After doing so, then other changes can be made.

NIST CVSS rating legend. Most of the descriptions below make use of the National Institute of Science and Technology's National Vulnerability Database (NVD) Common Vulnerability Scoring System (CVSS). The CVSS has a scale from 0 to 10. Any score equal to or greater than 7.0 are vulnerabilities labeled as a high severity and should be given the most attention. More information about the NIST CVSS can be obtained here. The CVSS scale categories are given below.

> High - Vulnerabilities labeled High severity if they have a CVSS base score of 7.0 - 10.0
>
> Medium - Vulnerabilities labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
>
> Low - Vulnerabilities labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Select Vulnerabilities Addressed by Third Wall

Disable IGMP. Internet Group Management Protocol is used by hosts, routers and switches to establish and maintain multicast group memberships internal to a network or subnet. When a user or host joins as a member of a multicast group, IGMP is used to inform local routers to send traffic to the subscribed

host's IP address. IGMP is an integral part of IP multicast and is considered a layer 3 protocol in the OSI model.

IGMP is susceptible to a number of network attacks and can waste bandwidth and router resources if not optimally configured. IGMP vulnerabilities can allow remote attackers to cause a denial of service by using a malformed IGMP packet that is mishandled during memory allocation, causing the target to become non-responsive or unstable. Also, issues have been raised that IGMP messages could be improperly routed and launched off a local subnet to another subnet, causing authentication and authorization concerns. For a reference, one 2015 IGMP vulnerability was given a severe CVSS rating with a high level of exploitability: Vulnerability summary of CVE 2015-1414. Another authoritative report involving a 2015 Cisco IGMP vulnerability is provided here. Overall, the risk rating for IGMP in most environments is moderate.

Note that disabling IGMP may prevent some devices and applications from talking with one another such as with updating address books, using distribution lists and broadcasting streaming media (e.g. desktop conferencing). Disabling IGMP could prevent these services from working depending on the applications in your environment. IGMP is often used for online gaming applications. Moreover, IGMP can be used similarly in VLAN configurations to allow devices and applications to talk with one another. It is advised that if IGMP is turned off in any environment, it should first be done in isolation to test if any important services were negatively impacted. But if IGMP is not needed however, it can be turned off.

Disable IPv6. The IPv6 addressing protocol is designed as the successor to IPv4. IPv6 offers significantly expanded addressing capabilities, simplified header format, improved support for extensions and improved security through authentication and privacy capabilities. Over time, IPv6 will replace IPv4 on the Internet. As of June 2015, about 8% of internet addresses accessing Google use IPv6; this number grows annually. The description for IPv6 can be found in IETF RFC 2460. Like IPv4, IPv6 is a layer 3 protocol in the OSI model.

Security and administrative issues exist with the transition from IPv4 to IPv6. Depending on the environment, it can be in an organization's best interest to disable IPv6 on endpoint devices, particularly for small and medium sized organizations for the purpose of simplicity. In general, complex environments are harder to secure and manage. General security issues with IPv6 involve the large address space that may enable an attacker with more places to hide and harder to detect. Also, the added complexity of using both IPv4 and IPv6 can add significant administrative overhead to those responsible for managing a network: they must be aware of security vulnerabilities of both IPv4 and IPv6 protocols. The two protocols are not compatible and a dual stack configuration is required if both protocols are simultaneously used.

Several IPv6 vulnerabilities involves a race condition in IPv6 to IPv4 functionality (reference CVC 2015-4199), using IPv6 can also allow attackers to use malformed IPv6 in addition to IPv4 malformed packets (reference CVC 2015-4191), and several IPv6 implementations can be exploited to conduct a denial of service attacks (reference CVC 2015-4291).

Note that while disabling IPv6 can simplify a network environment, an organization that has already deployed IPv6 on end-user devices no longer has this option. Also, organizations that are planning transitions to IPv6 will likewise need to keep it enabled. Unless an organization is using IPv6, it can

safely be disabled until it's needed. Moreover, note that many endpoint devices may have IPv6 enabled as the default configuration, which would need to be disabled.

Overall, the risk rating for IPv6 in most environments is moderate.

Reference: IPv6 security myths. Internet Society. January 2015.

Disable local LM Hash storage. Instead of storing passwords in clear-text, Windows® (like most operating systems), stores account passwords as a 'hash' digest, which is the result of processing a password through a one-way mathematical function. If a user uses a password of less than 15 characters, Windows generates a LAN Manager hash digest (LM or LANMAN hash) of the password which is stored in the local Security Accounts Manager (SAM) database or in the Active Directory (AD). The LM hash cannot store passwords longer than 14 characters. This hash is considered weak and vulnerable to a brute-force cryptographic attack if captured by an entity. The LM hash digest is stored using the DES encryption system using a 56-bit key length and the implementation contained several weaknesses, making it highly vulnerable to attack. This weakness is a legacy problem existing before Windows XP. A recommendation from Microsoft is to disable the LM hash and use the latest version of NT LAN Manager (NTLM) and Kerberos authentication protocol.

The LM hash is considered an obsolete solution from prior to and including the XP version of Windows. However, according to Microsoft documentation, in order to accommodate mixed and legacy OS environments, the LM hash is still present in Windows 7, 8 and Windows server 2012, although disabled by default. However, it has been reported that in Windows Server 2008 environments, the LM hash was still enabled by default. Thus, disabling the LM hash on a local device ensures this feature is off in older versions of Windows or not inadvertently turned-on in newer versions of Windows.

Overall, the risk rating of storing a local LM hash in high. It's possible in mixed and legacy Windows environments that it may be needed. With Windows XP and Windows Server 2003 no longer supported by Microsoft anyway however, organizations should have upgraded to more recent products. It's suggested the LM hash be turned off unless absolutely necessary.

Disable SMBv1. The Server Message Block (SMB) protocol is a network file sharing protocol. SMB's primary role is to establish a session to shared server resources in the client-server environment. While file sharing is the main purpose, SMB also negotiates and determines protocol configurations on a network that impact print ques, file access authentication, file locking and file directory change notifications.

SMB is a protocol that enables client-server configuration and control and runs at the layer 7 (application layer) of the OSI model. SMB uses TCP and NetBIOS on the network and can utilize protocols in the SMB protocol family such as the SMB Mailslot protocol. A mailslot is a temporary file that resides in memory allowing for message exchanges in the client server environment. Needless to say, the SMB family of protocols is multifaceted arrangement.

SMBv1 has had serious vulnerabilities. For example, a corruption vulnerability allows an authenticated remote code execution in Windows when SMB incorrectly processes logging activities, resulting in memory corruption. An attacker could take administrative control of a target system, including the right to install, change programs, delete data or create and modify user accounts. SMBv1 has had several

vulnerabilities with most of them prior to 2009. However, problems with this protocol have continued; see Microsoft security bulletin MS15-083.

Newer versions including SMBv2 and SMBv3 have addressed the vulnerabilities in SMBv1. Windows server 2003 was the last to use SMBv1, but third party legacy resources like printers, scanners, and NAS devices may still need SMBv1. Overtime, dependencies on SMBv1 should be removed. Regarding SMBv2 or SMBv3, Microsoft does not recommend turning off these services except as a temporary troubleshooting measure since doing so will significantly reduce important client-server communications to include message authentication and encryption services. Reference Microsoft support message on SMB.

Overall, the risk rating of keeping SMBv1 enabled is moderate. Most environments can reduce this risk by turning off the legacy SMBv1 unless doing so causes client-server communication problems.

Disable LM, NTLMv1. NTLMv2 contains some significant security improvements not in LM or NTLMv1. NTLMv2 significantly increases authentication (initial login) and session (ongoing) security technology. NTLMv2 was released with NT 4.0 Service Pack 4 (SP4). NTLMv2 also provides mutual authentication with servers. Environments can significantly improve security by ensuring only NTLMv2 is enabled and not NTLMv1 or LM/LANMAN. If an organization doesn't have LM or NTLMv1 clients, it should disable these services (Reference Microsoft Windows Security Essentials, Darril Gibson).

For additional information, reference the *Disable local LM hash storage* and *Restrict all incoming NTLM Traffic* entries.

The overall risk rating for LM and NTLMv1 is medium-high. NTLMv2 is stronger; if possible in an environment, LM and NTLMv1 should be disabled.

Disable UPnP. Universal Plug and Play (UPnP) is a widely used protocol that streamlines communication between computers and networked devices. It's typically enabled by default on networked devices ranging from routers, printer media severs, Wi-Fi access points, TVs and storage devices as well as most operating systems including Windows, OS X and Linux. It's also enabled by default on most networked consumer electronics since it conveniently allows interoperability between devices. UPnP is an open protocol that uses the TCP/IP protocol suite including HTTP, XML and SOAP.

The problem is that UPnP suffers from several basic security vulnerabilities. In 2012 alone, NIST listed eight vulnerabilities with a CVSS rating of 10.0, the most serious. Most of these involve a stack-based buffer overflow vulnerability in UPnP devices allowing remote attackers to execute arbitrary code or enabling a denial of service attack (for example, see CVE-2012-5958). Basic vulnerabilities include that authentication is rarely done by UPnP devices, privileged capabilities are exposed to untrusted networks and UPnP-using products contain significant software bugs and flaws. (Reference Rapid 7 whitepaper on the topic.) Moreover, these flaws are easily exploitable using free, open source hacking tools. It's unlikely that manufactures will disable the UPnP protocol in the near future since they allow for quick and easy connections between electronic devices. Some updates to UPnP have addressed some of the security vulnerabilities.

Overall, the risk rating of keeping UPnP enabled is high. Most business environments can reduce this risk by turning off the UPnP protocol on endpoint devices.

Enable Security Event Logging. Turning on the Windows security event logging has several advantages. Considering that most organizations will be attacked and possibly penetrated, it's important to be able to identify and isolate security exploits and incidents. Security event logging can be invaluable in capturing information regarding authentication, system access, configuration changes and even help provide data when a possible attack is occurring. Logging can also provide evidence and aid investigations in the event a crime was committed on a particular device. Specific actions that can be tracked include changes to user account and resource permissions, failed user logon attempts, failed attempts to access resources, and attempts to modify system files. Logs can also help administrators with troubling shooting problems. It is recommended that organizations enable security event logs.