



Research Article

Threats Hidden in Office Network: Mechanism of Credential Harvesting for Lateral Movement

Tung-Lin Lee¹, I-Hsien Liu¹, Chu-Fen Li², Jung-Shian Li^{1,*}

¹Department of Electrical Engineering / Institute of Computer and Communication Engineering, National Cheng Kung University, No.1, University Rd., East Dist., Tainan City 70101, Taiwan

²Department of Finance, National Formosa University, Yunlin County 632, Taiwan

ARTICLE INFO

Article History

Received 09 November 2020

Accepted 09 July 2021

Keywords

IWA

active directory

phishing

credential harvesting

cybersecurity

ABSTRACT

With the advent of the Internet of Things (IoT) era, the concept of smart office has gradually come true. To facilitate the management, IoT devices often follow authentication mechanisms as windows domain used, which would cause severe problems once hackers steal those credentials. This study analyzes the restriction of previous research and proposes a new technique that could cause credential leaks and organizes an attack mechanism to evaluate the most suitable strategy in various scenarios.

© 2021 *The Authors*. Published by Atlantis Press International B.V.

This is an open access article distributed under the CC BY-NC 4.0 license (<http://creativecommons.org/licenses/by-nc/4.0/>).

1. INTRODUCTION

In an environment with Active Directory (AD), all resource access authorization authentication would be handled by Active Directory, so that every Server [EX: Exchange server, Network Attached Storage (NAS)] does not need to verify the user's authentication credential itself. Moreover, to allow users to log in once and access services without re-entering authentication factors, Integrated Windows Authentication (IWA) was introduced with Microsoft Windows 2000 [New Technology (NT) 5.0] and included with later Windows NT-based operating systems.

Due to the IWA, users could access several related servers without having to log in repeatedly. However, this single sign-on configuration could be leveraged by hackers to launch attacks such as the NT LAN Manager (NTLM) relay attack [1] or cracking authentication hashes [2], and then the hackers can log in to the victim's computer with a password that has been recovered maliciously, which becomes an effective way to gain footholds into the Enterprise's intranet and moving through the whole environment.

The second section introduced background knowledge of IWA, as well as several well-known related security research. In the third section, we will introduce our research which could expand the coverage of the previous attack surface and technique to bypass existing security mechanisms, then we combine previous research with our findings to construct a decision-making mechanism to decide the most applicable attack strategy that could be implemented in various scenarios. Finally, the fourth section will be our conclusion.

2. BACKGROUND

In this section, we will introduce the most widely used authentication in IWA which is NTLM. Besides, we will discuss the protocol that supports NTLM as well as typical attacks that focus on it.

2.1. NTLM Overview

Although Kerberos is the most secure authentication protocol in IWA, integrating IoT products with Kerberos implies that devices must join the windows domain first, which is nearly impossible for most IoT devices. On the other hand, NTLM is widely used not only for protocols such as SMB, LDAP, MSSQL, HTTP but also used for applications such as wi-fi or remote desktop connection and NTLM is easier to implement for most software.

NTLM is a challenge-response authentication protocol as shown in Figure 1. First, the client sends a negotiate message advertising its capabilities to the server. Then the server responds with a challenge message. Third, the client encrypts the challenge message with its username and password as a authenticate message, and then the server will verify whether the password is correct or not.

Although NTLM has been widely used for decades and has been updated (the most important update is from NTLMv1 to NTLMv2) many times, its security mechanism has often been challenged. Nevertheless, Kerberos is much more complicated to configure and there is downward compatibility for the third-party software requirement which does not support Kerberos as an authentication option, using NTLM for authentication is usually a necessary option even if Kerberos is being implemented [3].

*Corresponding author. Email: jshi@mail.ncku.edu.tw

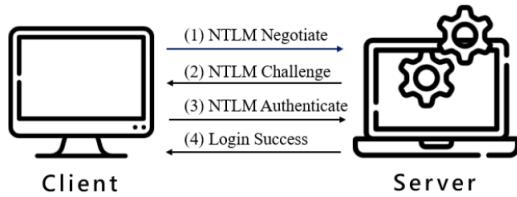


Figure 1 | The NTLM challenge–response mechanism.

2.2. Typical Attack and Previous Research

The security concerns of the NTLM authentication protocol are reflected in two aspects, Cryptography security and the authentication process. On the cryptographic aspect, the NTLMv1 used Data Encryption Standard (DES) for the encryption. However, DES has been proved to be broken since the hash could be cracked in 20 min. Although NTLMv2 does stand as secure, it would still be cracked through the dictionary attack. In other words, if the computer user chose a password that has been leaked then cracking the hash could be easy. Even though most devices support NTLMv2 and have priority adopting it, NTLMv2 by default falling back to NTLMv1 on the windows operating system. Namely, if one side (client or server) insists on using NTLMv1, the other side would simply agree to use it.

On the authentication process aspect, there is another attack method called NTLM relay or so-called pass the hash. The attack method is another variant of the man-in-the-middle attack as shown in Figure 2. Although there are some mitigations such as enhanced protection for authentication, still there are ways to bypass those mechanisms such as “drop the mic” [4]. Through the NTLM relay attack, an attacker could connect the server through the remote procedure call, thereby affecting the entire operation of the enterprise.

2.3. NTLM Leak

The key point to trigger all the attacks that have been mentioned is to make victims initiatively send a login request to the malicious server. Generally, there are two ways to make this happen, through malicious file or Link-Local Multicast Name Resolution (LLMNR)/NetBIOS spoofing.

The article [5] introduced the file types that could cause the NTLM leak such as HTML files, PDF, Windows media player, Microsoft Office files. These files initiatively request resources embedded in the Universal Naming Convention (UNC) path through the SMB protocol once the user opens the file. After that, the server responds with the challenge message, then the client would respond with the authenticate message due to the Single sign-on implementation of IWA. However, if the UNC path points to IP Address where the hacker responds query as a malicious server, users would leak their NTLM hash without awareness of what is happening.

These malicious files are often sent as attachments in phishing emails. Fortunately, only PDF and Microsoft Office files are common email attachment file types. To protect users vulnerable to this type of attack, Adobe Acrobat reader would pop out a warning message box and ask the user whether the UNC path is

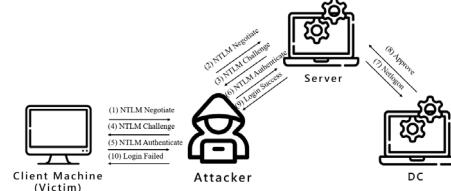


Figure 2 | The NTLM relay attack with active dictionary.

trustworthy if the PDF file contains the UNC path. In contrast, open in protected view is the only mitigation Microsoft provides to protect user’s device from malware and other threats download from the Internet. If users were not informed of what is contained in the file and the threat hiding in it, they may rashly press the button “Enable Editing” after that user would still leak their NTLM hash.

Before we come to LLMNR/NetBIOS spoofing [6], we talk about Windows Name Resolution first. Windows Name Resolution resolves Uniform Resource Locator (URL), as following order: Hosts, DNS (cache/server), Local LMHOST File, LLMNR, NetBIOS. LLMNR/NetBIOS perform name resolution for hosts in the same intranet. Since both LLMNR/NetBIOS listen on User Datagram Protocol (UDP) they can be spoofed. If the user’s computers set the Local Area Network setting as “automatically detect setting” which is a configuration by default. Once users’ browsers such as chrome were opened, their device would send a broadcast message to see if there would be Web Proxy Auto-Discovery Protocol (WPAD) server to provide a Proxy Auto-Config (PAC) file. The intention of WPAD is to make Network Manager’s work easier for Proxy configuration to put a PAC file in the WPAD server instead of setting all the devices in intranet one-by-one. However, By spoofing LLMNR/NetBIOS hacker could hijack WPAD and thus become a Proxy Server or respond a challenge message over WPAD protocol to the client. Both manners would cause the NTLM leak.

3. MECHANISM OF CREDENTIAL HARVESTING

3.1. Bypassing Microsoft Office Mitigation

The NTFS file format supports using the named Zone: Identifier in the alternate data stream to mark files from the Internet. If the file happens to be an Office document, it would be opened in Protected View. However, compressed files remain a special case. When compressed files are being decompressed, the unzipped file should inherit the characteristics of Zone: identifier.

Although most compression software aware of these security concerns, different compression modes in the same decompress software might cause different results. Taking the most popular extractor 7zip as an example, it will propagate Zone: Identifier only when the compressed file is being open in the archive. Namely, modes such as “Extract All” were not secure which could cause the NTLM leak once the office file is opened. The article “Downloads and the Mark-of-the-Web” [7] discusses it before, yet we re-experimented the latest version of several popular extractor and found slightly different results, e.g., “Table 1.”

Table 1 | Popular extractor list

Extractor	Double-click in Archive	Extract All/Here
Windows Explorer	Not vulnerable	Not vulnerable
WinRAR	Not vulnerable	Not vulnerable
7zip	Vulnerable	Not vulnerable
WinZip	Not vulnerable	Vulnerable
IZArc	Could not open	Vulnerable



Figure 3 | The attack simulation scenario of bypassing firewall.

3.2. Bypassing Firewall

In the previous research of Microsoft Offices, NTLM leak could only transport through the SMB protocol. However, Most Network Manager would prohibit outbound or inbound SMB connections. Because notorious exploit or hacker tools such as “EternalBlue” and “PsExec” are transported over SMB protocol. Our research attempts to change the UNC path into other URLs for the purpose of causing the NTLM leak through other protocols. Finally, we found out that manipulating the UNC path into a URL with HTTP/HTTPS or LDAP protocol would also cause the NTLM leak. Nevertheless, URL with HTTP(S) would only cause the leak when the setting on the users’ computer is “automatic logon only on Intranet zone” or “automatic logon with current username and password”. In contrast, URL with LDAP will trigger NTLM leak just as SMB, but to avoid being block by firewall as shown in Figure 3.

3.3. Credential Harvesting in Intranet

Our research could not only attack computers connect to the internet, but also could attack others that are not connecting to the internet by changing the URL hidden in the Microsoft Offices files pointing to computers that have been infected instead of the C&C server on the internet. It is worth notice that NTLM leak over SMB protocol is also not an available option inside the intranet. Although SMB protocol is often used inside the intranet for file sharing and printing which does not cause any suspicion, deploying a rogue SMB server in the intranet is nearly impossible. Because the Transmission Control Protocol (TCP) port SMB used has been bound by the Network Neighborhood or samba binding the same port with an existed service is unrealistic. However, NTLM leak over HTTP(S) or LDAP would do the job stealthy.

Because the NTLM leak over HTTP has its’ restriction, it is less practical than NTLM leak over LDAP. However, in MDsec’s research [8] reveals an approach leaking NTLM over WebDAV with internet shortcut or URL files. Although leaking through WebDAV shares the same restriction as HTTP, since WebDAV is an extension of HTTP, it only required the victim to open a shared folder instead of a malicious file which would have a higher chance of harvesting more credentials if the condition fulfilled.

Table 2 | Comparison between methods of credential leaks

Protocol	Restriction	Victim interaction
SMB [5]	Firewall often prohibit inbound SMB connection	Open folder/file
WebDAV [8]	Internet option	Open folder or office file
WPAD [6]	LLMNR/NetBIOS and WPAD is not disable	Open application support WPAD
LDAP	None	Open office file

To once more reduce the user interaction that our strategy relies on, adopting LLMNR/NetBIOS spoofing is the best choice under the premise of the target intranet has no WPAD server and LLMNR/NetBIOS were not prohibited. Table 2 demonstrates the comparison between methods of credential leaks.

4. CONCLUSION

Intelligent office technologies improve the working environment through many aspects, yet these technologies share the same security concerns with the Windows domain. This paper analyzes the restriction of previous research causing NTLM leak and proposes a new technique without those restrictions in the victim’s intranet and a decision-making mechanism to determine the most proper strategy that could be implemented in real situations. The comparison between those strategies is shown in Table 2.

We provide few points of advice as shown below to defend against NTLM leak and related attacks:

1. Deploy Anti-virus Scanning Email Attachments
2. Disable NTLMv1 Protocol
3. Disable WPAD Protocol

Finally, we provide mitigation to prevent similar attacks of our own research.

CONFLICTS OF INTEREST

The authors declare they have no conflicts of interest.

ACKNOWLEDGMENT

This work was supported by the Ministry of Science and Technology (MOST) in Taiwan under contract number MOST 110-2218-E-006-013-MBK.

REFERENCES

- [1] S. Maddala, S. Patil, Agentless Automation Model for Post Exploitation Penetration Testing, in: A. Pandian, K. Ntalianis, R. Palanisamy (Eds.), International Conference on Intelligent Computing, Information and Control Systems, ICICCS 2019, Springer, Cham, 2020, pp. 529–539.
- [2] E. Tirado, B. Turpin, C. Beltz, P. Roshon, R. Judge, K. Gagneja, A New Distributed Brute-Force Password Cracking Technique, in: R. Doss, S. Piramuthu, W. Zhou (Eds.), International Conference

- on Future Network Systems and Security, FNSS 2018, Springer, Cham, 2018, pp. 117–127.
- [3] W. Mattin, One-Click to OWA, DEF CON 26, Las Vegas, America, 2018.
- [4] S. Marina, Z. Yaron, Relaying Credentials has Never Been Easier: How to Easily Bypass the Latest NTLM Mitigation, DEF CON 27, Las Vegas, America, 2019.
- [5] Y. Koster, Living off the Land: Stealing NetNTLM Hashes, 2018.
- [6] J. Wang, J. Zhou, NTLM Relay is Dead, Long Live NTLM Relay, HITBSecConf, Amsterdam, Netherland, 2018.
- [7] Downloads and the Mark-of-the-Web, 2016.
- [8] MdSec Research, Farming for Red Teams: Harvesting NetNTLM, 2021.

AUTHORS INTRODUCTION

Mr. Tung-Lin Lee



He was born in Keelung, Taiwan in 1995. He received his B.S. degree from the Department of Electrical and Computer Engineering, National Taiwan Ocean University, Taiwan in 2019. He is acquiring the master's degree in Department of Electrical Engineering/ Institute of Computer and Communication Engineering, National Cheng Kung University in Taiwan.

Dr. I-Hsien Liu



He is a research fellow in the Taiwan Information Security Center @ National Cheng Kung University (TWISC@NCKU) and Department of Electrical Engineering, National Cheng Kung University, Taiwan. He obtained his PhD in 2015 in Computer and Communication Engineering from the National Cheng Kung University. His research interests are Cyber-Security, Wireless Network, Group Communication and Reliable Transmission.

Prof. Chu-Fen Li



She is an Associate Professor in the Department of Finance at the National Formosa University, Taiwan. She received her PhD in Information Management, Finance and Banking from the Europa-Universität Viadrina Frankfurt, Germany. Her current research interests include intelligence finance, e-commerce security, financial technology, IoT security management, as well as financial institutions and markets. Her papers have been published in several international refereed journals such as European Journal of Operational Research, Journal of System and Software, International Journal of Information and Management Sciences, Asia Journal of Management and Humanity Sciences, and others.

Prof. Jung-Shian Li



He is a full Professor in the Department of Electrical Engineering, National Cheng Kung University, Taiwan. He graduated from the National Taiwan University, Taiwan, with B.S. in 1990 and M.S. degrees in 1992 in Electrical Engineering. He obtained his PhD in 1999 in Computer Science from the Technical University of Berlin, Germany. He teaches communication courses and his research interests include wired and wireless network protocol design, network security, and network management. He is currently involved in funded research projects dealing with optical network, VANET, Cloud security and resource allocation, and IP QoS architectures. He is the director of Taiwan Information Security Center @ National Cheng Kung University. He serves on the editorial boards of the International Journal of Communication Systems.