

# 2021 ATTACK VECTORS REPORT

Daria Ryabogin  
Jonathan Slusar



RSM



WAR ROOM

## TABLE OF CONTENTS

Foreword.....	1
Penetration Testing: A Step-By-Step Overview.....	2
Executive Summary.....	3
Data Collection Process.....	4
Definitions.....	5
Important Questions.....	6
Internal Attack Vectors: An Overview.....	8
Operating System Patches.....	10
Kerberoasting.....	16
Man-In-The-Middle Attacks.....	22
Password Spraying.....	28
SMB Relay.....	34
Recommendations.....	40
Conclusions.....	42
Acknowledgements.....	43



## Foreword

Recently, the United States has observed a sharp increase in the number of significant compromises for both large and small business alike. As such, while organizations seek to expand in size and revenue, and while mass data breaches become an increasingly disastrous reality, the impact of successful attacks becomes even more substantial.

Unfortunately, the consequences of cyber-attacks typically range from unpleasant to severe—security incidents place considerable strain on organizational resources, invite lawsuits, incite reputational damage and interrupt business operations. Furthermore, mass data breaches can strip an organization of its property without enough evidence to guarantee a successful investigation. When information about an organization is obtained through publicly available sites, using publicly available resources (such as online scanning tools or exploitation tutorials), it can be difficult to trace the attacker. From food delivery services to hospitals and education centers, any unprepared organization that handles social security numbers, card data, health information or even personal addresses is at risk of experiencing a significant loss.

In an effort help prevent such incidents, safeguard reputations and protect sensitive material, many organizations have implemented a multitude of restorative efforts. Because attackers specifically target sensitive data, it is critical for affected parties to be aware of any arrangements for “damage control.” Immediate identification of suspicious behavior, as well as prompt resolution of security-related vulnerabilities ensures that an organization can remain resilient and protected. However, even the most adaptable organization may struggle to master all aspects of information security, while still aligning with internal requirements and regulations.

For many years, RSM has made a continuous effort to assist organizations in addressing these challenges and achieving their desired state of security, while also providing guidance for attack prevention. Through security penetration testing, we simulate attacks on internal networks and closely mimic security breaches without removing an organization’s control over their systems. In essence, the goal of these tests is to determine the level of compromise that an attacker may be able to achieve, while investigating the kind of data accessible to intruders.

With the cybersecurity industry becoming increasingly specialized, it is crucial that we highlight specific subsets of the attack surface. Smaller scopes require as much detail as possible. Inevitably, after performing hundreds of penetration tests every year, we’ve made note of trends in the vulnerability linkages. These exposures show up time and time again.

For this report, we have focused exclusively on internal penetration testing. “Assumed breach” is a common security model, in which controls are tuned with an emphasis on the internal environment. Here, the assumption is that a determined attacker will always find a way into the organization’s network. Because the vectors covered in our testing require some level of access to the target’s environment, organizations must take special care to harden their internal networks to mitigate the damage of an internal threat actor as much as possible.

We hope that the readers of this report are able to leverage our analysis to further secure their networks. For additional information about our penetration testing services or reporting processes, please do not hesitate to contact RSM US LLP.

## Penetration Testing: A Step-By-Step Overview

When performing internal penetration testing, our objective is to simulate an attacker on an organization's internal network. By assessing current security controls, we seek to validate the organization's security posture and configuration standards while investigating the network's resiliency to attack. In order to simulate a real-life attack scenario, we utilize techniques and tools available to threat actors.

1. Prior to testing, we sign a contract with the client that details a specific timeframe for testing. Timeframes are required to ensure that the client can prepare for our attacks—if attacks are performed outside the permitted timeframe, significant damage can be done to the client's systems.
2. We begin penetration testing by evaluating the scope, as agreed upon by the client in previous discussions. In-scope systems typically include network and security infrastructure, servers, user workstations and internal applications.
3. In order to determine the amount of information available about our client, we conduct footprinting. Afterwards, we explore the network for open ports and services, which can be leveraged in simple attacks.
4. Through hacking tools and online resources, we then identify vulnerabilities and public exploits. If public exploits are discovered, we begin attempting execution. We attempt to pass credential information, utilize authentication protocol weaknesses, abuse functionalities and escalate our privileges.
5. While conducting our exploits, any high- or critical-rated vulnerabilities identified on our client's network are reported to the client. If in-scope systems were exploited with Payment Card Industry (PCI) data, Health Insurance Portability and Accountability Act (HIPAA) data, personal information or any other information the client has flagged as "critical," this is also relayed to the client.
6. We conclude our testing by running automated scans, which provide a detailed list of additional vulnerabilities present on the client's network. While we may not have exploited these vulnerabilities during the test itself, they represent potential alternative paths of attack, and should therefore be considered while the client is hardening their environment.
7. All information obtained during a penetration test is reported in a document, which is also sent to the client. This document includes a detailed breakdown of each vulnerability, as well as a narrative of attack and steps for remediation.

## Executive Summary

Internal penetration testing allows clients to obtain valuable information about the security of their networks. This process requires an increased level of trust afforded to the resources outside the client organization. Our resources mimic any scenario, from an external threat actor with a foothold on the network to a malicious insider, such as a disgruntled employee or contractor.

We have studied our most successful attack vectors in detail with respect to internal penetration tests. Below are the trends that have arisen, as well as our key takeaways from this analysis. 60 successfully compromised clients were included in this study, which amounted to almost 250 compromise steps taken by our consultants.

Overall, we have observed that password spraying attacks are the most common in our successful pathways, with man-in-the-middle attacks following closely behind. When correctly exploited, weak authentication protocols and user credentials allow attackers to generate multiple pathways to compromise. Our results indicate that many companies are still not educating users on the benefits of strong passphrases, as well as the dangers of not protecting information in an adequate manner. Once again, improving user awareness and encouraging your employees to exercise strong security practices can help mitigate some of the most common and successful attack vectors.

This report includes detailed information about each of the attack vectors we surveyed in our analysis. In addition, we have provided examples of attack diagrams submitted to our clients over the past year. These diagrams illustrate each step in our compromise pathway, and deliver a visual representation of our approach to manual testing.

**226**

Total steps to  
compromise  
analyzed for this report

**60**

Reports assessed  
for successfully  
compromised  
clients

Percentage of Clients with Compromise Pathways that include the Attack Vector	
1. Operating System Patch Exploitation	21.7% (13 out of 60 clients)
2. Kerberoasting	21.7% (13 out of 60 clients)
3. Man-in-the-Middle Attacks	48.3% (29 out of 60 clients)
4. Password Spraying	66.7% (40 out of 60 clients)
5. SMB Relaying	16.7% (10 out of 60 clients)

# Data Collection Process

Due to the volume of internal penetration tests performed by RSM in a given calendar year, we performed our analysis by targeting a randomly selected subset of successfully compromised client reports. Many of the following attack vectors overlap, or are utilized simultaneously by attackers when one attack pathway seems implausible. It is our hope that the information provided in this section can be used by cybersecurity professionals, IT staff and other relevant parties to better secure their networks from the most common attacks that are performed. To have a penetration test performed for your organization (or for further cybersecurity analysis), please contact RSM US LLP.

The following actions were performed to provide the statistics incorporated into this report:

1

We reviewed 60 internal penetration tests from 2020, chosen at random. All of the internal penetration tests used in our analysis were successful. "Successful" refers to an effective compromise of the organization's Domain Administrator (DA) or Domain Controller (DC), or the procurement of sensitive information.

2

When analyzing each of the 60 penetration tests, we generated a spreadsheet that mapped out each step taken towards compromise. An example is provided below:

Client Name	Step 1	Step 2	Step 3
REDACTED	LLMNR/NBT-NS Spoofing	Cracked Credentials Offline	DA/DC Obtained

3

All of the attack vectors utilized were color coded, with similar attack vectors sharing the same color. As an example, the Link Local Multicast/NetBIOS Name Services (LLMNR/NBT-NS) Spoofing and Internet Protocol Version 6 (IPv6) Poisoning attack share the same color, as both attacks utilize insecure communication protocols and often produce the same end result. In addition, if an action was part of an ongoing attack, it was labeled with the same color as the attack.

4

Afterwards, columns within the spreadsheet were filtered as necessary to determine the most frequent attack vectors used in a given step. This allowed us to map the number of steps required per compromise, and provided us with information about which attack vector corresponded to which step in a given pathway.

5

The final step in a compromise is illustrated by a dark box labeled "DA/DC," indicating that the attack pathway had concluded.

# Definitions

For the purposes of this report, we assume the following definitions:

## Vulnerability

Any factor which exposes the confidentiality, integrity, or availability of data or systems to a threat. Though vulnerabilities represent security weaknesses, not all vulnerabilities can be exploited in meaningful ways.

## Configuration

An arrangement of software or hardware on a computer. Common misconfigurations, for example, refer to common issues within hardware that can be repaired with relative ease.

## Hash

Strings of numbers and letters that act as encryption for user passwords. When a password is created for an account, computers will store that password in a masked form to prevent malicious individuals from freely obtaining user information. However, these hashes can be “cracked” or “uncovered” through various guessing attacks, as described later in this report.

## Attack Vector

A vulnerability whose successful exploitation is instrumental in a compromise. Attack vectors more closely depict the route a threat actor would take in a real-life attack. The distinction between vulnerability and attack vector is of great importance, because analyzing attack vectors helps organizations understand the potential impact—as well as prioritize the remediation—of exposures in their environments.

## Compromise

Obtaining access to critical systems or highly sensitive trophy data.

## Attacker

This is the individual or entity responsible for conducting the attack. The data presented in this report has been collected from penetration tests in which RSM testers posed as attackers—in a real scenario, this can be any individual seeking to obtain sensitive information on an internal system. Attackers can also be called “threat actors.”

## Sensitive Data

Though this is subjective, “sensitive” typically refers to confidential data that can be leveraged by an attacker to perform unwanted actions, such as theft. This data should be protected by passwords and special permissions, and should only be accessible by individuals with assigned privileges. Such data includes social security numbers (SSNs), bank account numbers, driver’s licenses, salary information, health records and passwords.

## Spoofing

This refers to the creation of a “fake” request, account, or message for the purposes of an attack. For example, when attackers try to coerce targets into sending them personal information, they may generate persuasive email messages with “spoofed” login pages.

## Protocol

An established procedure utilized by devices on the same network when transmitting data. Whenever computers need to relay information, a network protocol is in use to ensure that the information is authorized, authentic and protected.

## Remediation

Any preventative or responsive measures that can be taken to avoid future compromises. This can include programs to review vulnerabilities or simple fixes for common security problems.

## Important Questions

### Why create Vulnerability Linkage Diagrams?

We provide our clients with compromise diagrams to present complex information in a visual manner. The diagrams included within this report have all been created for clients over the past year. Though not all of the attack pathways in our diagrams lead to compromise, these visuals demonstrate how an attacker might double back on their steps, or how multiple attack vectors may be necessary to obtain sensitive information.

The following questions are often asked prior to penetration testing, and should be addressed by organizations once the results of a penetration test have been released.

#### 1. What makes an attack successful?

An attack is successful when a malicious individual obtains access to the internal network. This can be achieved by seizing user credentials or escalating domain privileges. In addition, we consider an attack to be complete if sensitive information, such as Social Security Numbers (SSNs), driver's license numbers or bank information is discovered during the attack.

#### 2. How serious are cyberattacks?

Over the past few years, the United States has observed a sharp increase in the number of significant security compromises for both large and small organizations alike. While businesses expand in size and revenue, and while mass data breaches become an increasingly disastrous reality, the consequences of successful attacks are even more substantial. Because sensitive information is targeted within these attacks, organizations can lose significant financial resources, and face data destruction, threats to reputation and integrity, and lawsuits from clients.

#### 3. How do attackers identify vulnerabilities?

Attackers can utilize a variety of resources to target and compromise systems, including vulnerability scanning engines and discovery tools. It is important to note that many initial attack vectors are available to individuals without in-depth technical knowledge of cybersecurity and computer systems. For example, attackers can leverage open-source intelligence (OSINT) techniques to explore publicly available websites for employee information. Once an attacker has compiled a list of possible employees from LinkedIn or Google, they can guess email schemas and attempt common passwords to achieve access.

#### 4. How do attackers know which path to take?

Surprisingly, attackers are typically unaware of outstanding security issues within an organization's network. In order to carve out a viable compromise pathway, attackers may rely on insider information, such as network login details. However, these threat actors typically begin any attack with an enumeration phase, which involves exploring publicly available data for information about previous breaches or employee names. As part of this phase, the attacker may run automated scans, which will provide them with a list of vulnerabilities present on the internal network. Some of the attack vectors in this report, such as missing critical patches, are easier to exploit than others. When an attacker identifies an easily exploitable vulnerability, they are more likely to complete the compromise with that attack, as resources and time are often limited.

## 5. Which vulnerabilities should we be most aware of?

After scans are completed, attackers can identify which critical Microsoft patches are missing on the internal network. These patches must be applied immediately. Exploitation of these vulnerabilities requires little time and no user credentials, and often results in a complete compromise of the victim's machine. In addition, organizations should make an effort to address weak user credentials, as one easy-to-guess password is enough to allow entry to the internal network.

## 6. What makes a vulnerability “exploitable”?

A vulnerability is exploitable if it allows an attacker to craft a definitive path to compromise. Weaknesses in the network can provide attackers with footholds, or “steps,” and can assist attackers in obtaining network details through careful trial and error.

## 7. What steps do we need to take to prevent attacks?

Simple misconfigurations, weak passwords, insecure protocols, missing patches and outdated software must all be examined and remediated to ensure the security of the internal network. In addition, organizations can consider implementing minimum security baselines. Minimum security baselines (MSBs) are available from organizations such as NIST and companies like Microsoft. They provide a standard to which machines should adhere, and disable unneeded features or settings, enable security features that harden the system and allow a consistent approach to system configuration.

## 8. What resources can we use?

If you have any questions about the attacks described in this report, please reach out to RSM for additional information. We also recommend reviewing the vulnerability writeups released by the Open Web Application Security Project (OWASP), the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and Microsoft. To provide additional references, we have included links to the War Room's writeups about the individual attack vectors described in this report.

## 9. What is a “culture of security”?

A culture of security refers to the approach that organizations have to cybersecurity, as well as their intentions, awareness, and support of security training. It is not enough for a company to address vulnerabilities and return to their earlier protocol—an organization needs to build a culture of security if they wish to protect information and employee data.

## How does each attack vector differ in terms of effort, remediation and time?

To answer this question, we have provided a guide at the bottom of each attack vector page. Attacks and steps for their prevention are rated on a scale from Low to High, with Low representing minimal effort and time, Medium requiring additional resources or guidance, and High relying on extensive effort and specialized knowledge.

## Internal Attack Vectors: An Overview

**45%**

of successful compromises (27 out of 60) occurred in three or fewer actions

Through our review, we discovered that just under half of all assessed compromises were completed in three or fewer significant actions during testing. These actions were primarily related to users not having adequate, complex passwords to protect their accounts, or resulted from missing patches on sensitive systems. These incidents highlight the importance of strict password requirements and regular patch monitoring. Because we were able to successfully compromise a domain administrator account in each of these steps, this metric also demonstrates that high-ranking IT staff members are not immune to account compromise, even through relatively simple pathways.

Insecure communication protocols were leveraged as an initial action in

**47%**

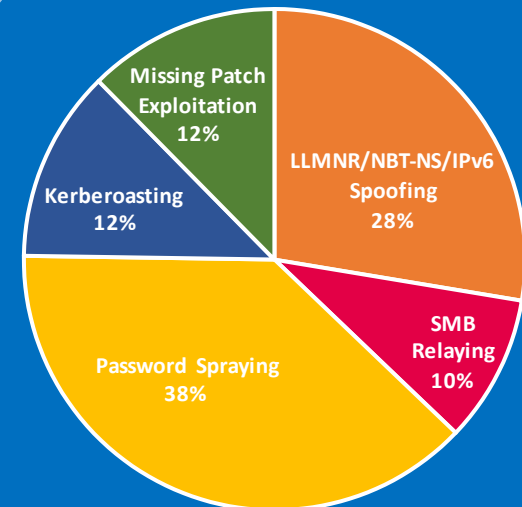
of attacks

In instances where we successfully compromised the Domain Controller (DC) in three steps, we often began by performing initial spoofing attacks that utilized weak communication protocols. Afterwards, we conducted offline dictionary-based password attacks to identify user accounts. However, we did note that Kerberoasting in particular was leveraged within the first two steps in several of the three-step compromises.

Overall, password spraying was conducted as a step to compromise in 40 of the 60 clients we assessed, accounting for 38% of all analyzed attacks. Because this attack is easy to complete, and requires minimal resources on behalf of the threat actor, organizations should ensure that all login pages are equipped with adequate password length requirements. In addition, misconfigured protocols should be reviewed in configuration management programs, and enabled immediately to prevent spoofing and poisoning attacks.

The chart on the following page maps the attack vectors that were leveraged to compromise each of the 60 clients in this analysis. A key has been provided, with colors corresponding to each attack. We have also included full summaries for each attack vector, as well as information about how these attacks are completed and remediation steps for organizations to follow. A general mapping of attack complexity, time and remediation effort is provided at the bottom of each section.

Attack Vectors Utilized in Steps to Compromise



To calculate these percentages, we totaled the number of clients that were compromised with the following attack vectors in at least one step (Kerberoasting, Missing Patches, Missing Protocols, Password Spraying, and SMB Relaying).

Step 1

Step 2

Step 3

Step 4

Step 5

Step 6

Step 7

1	IPv6	SMB	LSA Secrets Dump	DA/DC				
2	LLMNR/IPv6	Offline Crack	Reverse BruteForce AD	Change DA Password	DA/DC			
3	Null Sessions Identified	Password Sprag	LSA Secrets Dump	DA/DC				
4	Null Sessions Identified	Kerberoasting	DA/DC					
5	LLMNR/NBT-NS	Password Sprag	Token Impersonation	DA/DC				
6	Eternal Blue/MS17-010	DA/DC						
7	Password Sprag	DA/DC						
8	LLMNR/NBT-NS	Offline Crack	DA/DC					
9	Zerologon	DA/DC						
10	Password Sprag	DA/DC						
11	Password Sprag	Eternal Blue/MS17-010	DA/DC					
12	Kerberoasting	Offline Crack	DA/DC					
13	LLMNR/NBT-NS	Offline Crack	Password Sprag	DA/DC				
14	LLMNR/NBT-NS	Password Sprag	DA/DC					
15	IPv6	Offline Crack	SMB Relay	DA/DC				
16	Eternal Blue/MS17-010	DA/DC						
17	Absent Patch for RCE	Obtained LSASS	DA/DC					
18	Absent Patch for RCE	Retrieved Credentials from mem	DA/DC					
19	IPv6	Offline Crack	DA/DC					
20	Zerologon	DA/DC						
21	IPv6	Offline Crack	DA/DC					
22	Default Credentials on Identified	DA/DC						
23	Null Sessions Identified	Password Sprag	Kerberoasting	DA/DC				
24	LLMNR/NBT-NS	Offline Crack	DA/DC					
25	LLMNR/NBT-NS	Offline Crack	Dump LSASS	Kerberoasting	Extracted NTLM Hashes	DA/DC		
26	SMB	Dump LSASS	Offline Crack	DA/DC				
27	PrivExchange	DA/DC						
28	LLMNR/NBT-S	Offline Crack	DA/DC					
29	Password Sprag	Dump SAM	Dump LSA Secrets	DA/DC				
30	Kerberoasting	Password Spraging	DA/DC					
31	Zerologon	DA/DC						
32	Eternal Blue/MS17-010	Dump SAM	DA/DC					
33	Null Sessions identified	Password Sprag	Kerberoasting	Dump LSA Secrets	DA/DC			
34	IPv6	SMB	Dump LSASS	DA/DC				
35	LLMNR/NBT-NS	Offline Crack	Kerberoasting	DA/DC				
36	LLMNR/NBT-NS	Offline Crack	Kerberoasting	Dump LSA Secrets	DA/DC			
37	LLMNR/NBT-NS / IPv6	Offline Crack	Kerberoasting	DA/DC				
38	IPv6	NTLM Relay	Dump LSA Secrets	DA/DC				
39	Kerberoasting	Password Sprag	Dump LSASS	DA/DC				
40	IPv6	SMB	Offline Crack	DA/DC				
41	LLMNR/NBT-NS	Retrieved From LDAP	Offline Crack	DA/DC				
42	LLMNR/NBT-NS	Retrieved Credentials from mem	DA/DC					
43	Null Sessions identified	Password Sprag	Eternal Blue/MS17-010	DA/DC				
44	LLMNR/NBT-NS	SMB	Dump SAM	Dump LSASS	SolarVinds	DA/DC		
45	LLMNR/NBT-NS / IPv6	SMB	DNS Poisoning	Offline Crack	Password Sprag	DA/DC		
46	IPv6	Offline Crack	Plaintext Creds	DA/DC				
47	Zerologon	DA/DC						
48	LLMNR/NBT-NS	Offline Crack	Password Sprag	Retrieved Creds from memory		DA/DC		
49	LLMNR/NBT-NS	SMB	Dump SAM	Pass Hashes	Retrieved Creds from memory	DA/DC		
50	MS17-010	Retrieved Creds From memory	DA/DC					
51	Null Sessions Identified	Password Sprag	Kerberoasting	Offline Crack	DA/DC			
52	ASREP Roasting	Offline Crack	DA/DC					
53	Eternal Blue/MS17-010	Retrieved Creds From memory	Password Sprag	Dump LSASS	Offline Crack	DA/DC		
54	LLMNR/NBT-NS	SMB	Retrieved Creds from memory	Password Sprag	Dump LSASS	Offline Crack	DA/DC	
55	Password Sprag	Dump LSASS	Offline Crack	DA/DC				
56	LLMNR/NBT-NS	SMB	Dump LSASS	Password Sprag	DA/DC			
57	NFS Plaintext Creds identified	Dump LSASS	Plaintext Creds	DA/DC				
58	Kerberoasting	Offline Crack	Dump LSASS	Password Sprag	DA/DC			
59	LLMNR/NBT-NS / IPv6	Offline Crack	DA/DC					
60	Null Sessions Identified	Password Sprag	Watering Hole Attack	IPv6	SMB Relay	DA/DC		

This is a copy of the spreadsheet we used when mapping out the attack vectors for this report. The following Key details which colors correspond to which attacks:

Key				
Operating System Patches	Kerberoasting	Man-in-the-Middle Attacks (LLMNR/NBT-NS/IPv6 Spoofing)	Password Spraying	SMB Relaying

# Operating System Patches

Missing operating system patches, particularly those for Windows systems, are often the first thing attackers seek when presented with a potential target. These vulnerabilities can be detected through simple automated scans, and their exploits are readily available online with detailed instructions. When exploited successfully, missing patches, such as the missing MS17-010 “EternalBlue” patch, will result in remote code execution as a system user, which is the highest level of privilege available locally in Windows. As a result, these attacks are relatively easy to execute, and exceptionally damaging to an organization’s security environment and reputation.

Patch exploitation has been the most significant starting point for compromises over the past three years. The recently discovered ZeroLogon vulnerability accounted for several of our observed patch compromises in 2021. Unauthenticated remote code execution vulnerabilities can allow attackers to elevate their privileges, bypass authentication and obtain password hashes (strings of encryption) that can later be cracked. Most notably, these vulnerabilities can be avoided through regular scanning and patching. Organizations without adequate asset, change and vulnerability management programs place themselves at significant risk, as these flaws can appear without warning.



## PROCESS

Missing patch vulnerabilities can be exploited within minutes, and can inflict a significant amount of damage for an organization. To begin this attack, the threat actor will run automated scanning software and investigate which patches are absent on the organization’s systems. Once these vulnerabilities are identified, the attacker will utilize an installed version of Metasploit and follow step-by-step instructions to send payloads to their target IP addresses. Afterwards, the attacker can add users, join administrator groups and elevate their privileges. In the case of the ZeroLogon vulnerability, an unauthenticated user can bypass the authentication process entirely and connect to systems remotely, then obtain administrator passwords. Similarly, the MS17-010 patch leverages flaws in system protocols to execute unauthenticated attacks.

## REMEDATION OPTIONS

Organizations seeking to protect themselves from potential patch exploitation attacks should regularly review their patch management program. This program can assist in proactively managing vulnerabilities on the devices within their network, and will involve considerably less time and effort than responding after exploitation has already occurred. Patch management is one of the most basic forms of protecting systems—without a formalized patch management process, even the most rudimentary hackers can gain full access to devices within a network. As part of this program, patch management processes should include identifying newly released patches, testing patches, deploying patches based on criticality, rolling back patches and installing emergency patching.

### Level of Difficulty for Attacker

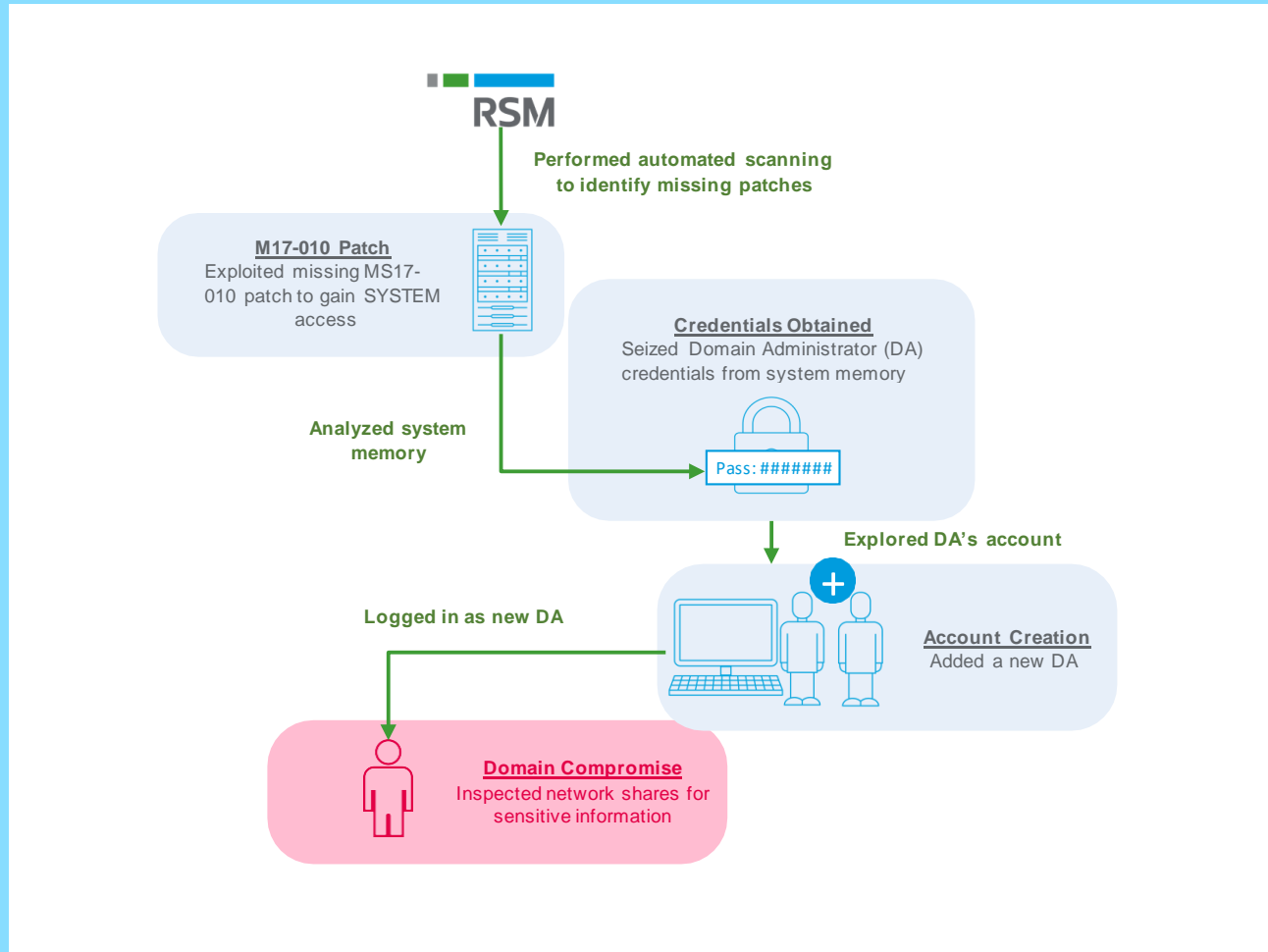
**LOW**

### Level of Remediation Difficulty for Client

**LOW**

### Length of Time for Compromise

**LOW**



## Diagram Walkthrough

Typically, exploiting operating system patches requires initial scanning to identify which patches are actually missing. In the vulnerability linkage diagram above, we have detailed the steps taken to conduct a simple patch exploitation attack. These attacks can allow a user unauthenticated access to the internal network, and are exceptionally easy to complete. On the following pages, we have included diagrams for compromises that required additional steps, such as token stealing and payload uploads.

RSM

**Missing Patch Exploitation**  
Successful exploitation of MS17-010 patch allowed SYSTEM level access



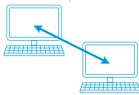
**Memory Dump**  
Collected NTLM hash for administrator account after dumping SAM table



**Spraying Attacks and Token Stealing**  
Sprayed subnets for additional privileges and performed token stealing to obtain Domain Administrator access



**Mapping**  
Performed port scanning and mapped computer relationships to identify systems with CDE access

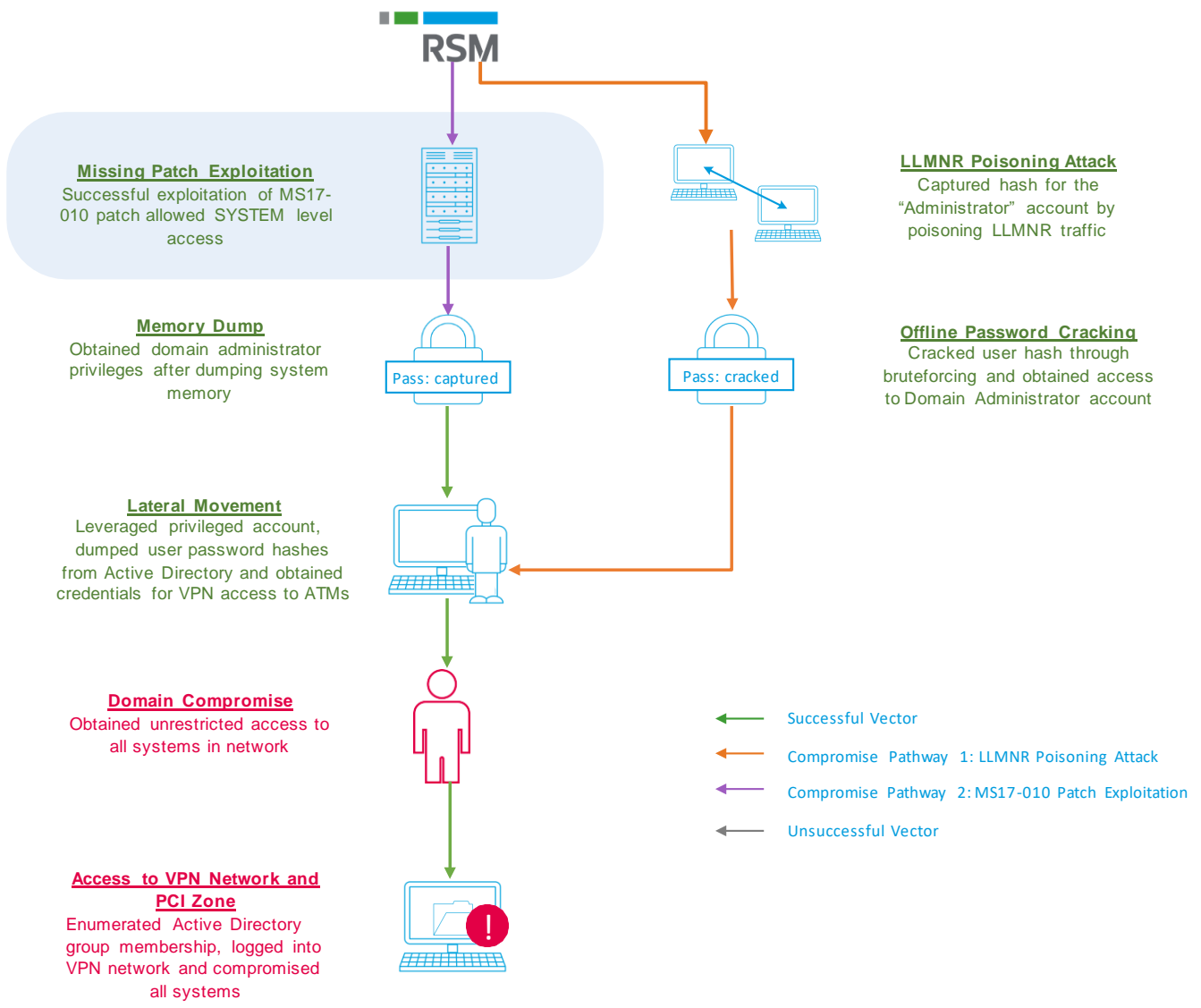


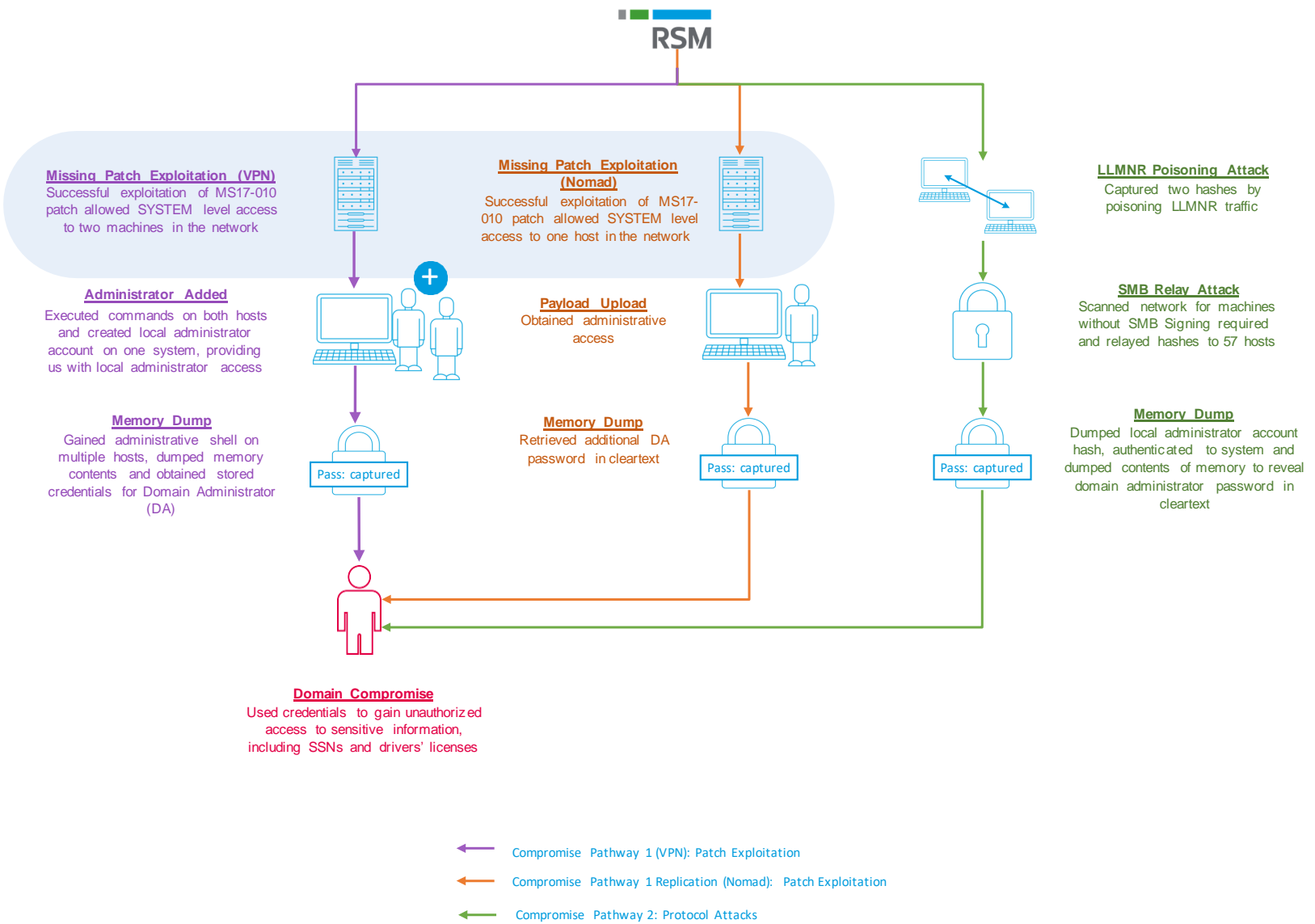
**Domain Compromise**  
Performed code execution on server, abused permissions and created local administrator account



**Access to PCI Zone**  
Relaying allowed access to Payment Card Industry (PCI) zone, which provided SSNs, passwords and employee information and health records







# RSM

**Zerologon Patch Exploitation**  
Successful exploitation of Zerologon vulnerability allowed us to access database containing every Active Directory user's password hash



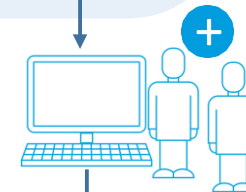
**MS17-010 Patch Exploitation**  
Successful exploitation of MS17-010 patch allowed SYSTEM level access to four hosts in the network



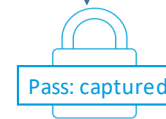
**Hash Cracking**  
Cracked password hashes through offline bruteforcing attacks and impersonated users



**Administrator Added**  
Executed commands on hosts and created local administrator account for local administrator access



**Memory Dump**  
Gained administrative shells, dumped memory contents and obtained stored credentials for Domain Administrator (DA)



**Domain Compromise**  
Used credentials to gain access to sensitive information



# Kerberoasting

Kerberoasting attacks are used to capture hashed passwords using the Kerberos network authentication protocol. Password hashes refer specifically to encryption strings that protect user credentials—essentially, a computer will mask a user’s password with a variety of numbers and letters, which can be retrieved from a system’s memory through cracking attacks. The Kerberos protocol protects network services by allowing users and servers to verify each other’s identity. However, if exploited successfully, an attacker connected to the network can leverage Kerberos authentication to crack hashed credentials with relative ease. This is because Kerberos requests are common, and insecure user passwords and encryption protocols contribute both to the success of these attacks and the overall weakness of an organization’s network security.

This attack also targets Active Directory services, and typically only takes several hours to complete. Because this attack only utilizes local commands, it can be virtually undetectable. When coupled with offline cracking attacks, a Kerberoasting attack frequently leads to compromise and expanded access.



## PROCESS

An attacker connected to the network can exploit this protocol by requesting Kerberos tickets for accounts configured with service principal names (SPNs). A portion of these tickets contain data encrypted with the New Technology LAN Manager (NTLM) hash of the targeted account, meaning an attacker can attempt to crack them into plaintext in order to obtain the user’s password. If the service account passwords are weak, then an attacker will likely crack them through offline dictionary attacks. In these attacks, the threat actor (or tester) will compute hashes for various passwords and compare them to each other. After being performed repeatedly, a match will indicate that the attacker has cracked the hash, and the system’s credentials have been identified.

## REMEDATION OPTIONS

In order to prevent successful Kerberoasting attacks, we recommend reviewing Kerberos delegation settings and ensuring they are configured as “constrained.” When delegations are unconstrained, they allow an account or system to act on behalf of other users that connect to it, and can be leveraged by services that require user impersonation between multiple systems. As such, a compromise of an account or system configured with unconstrained delegation could result in a compromise of the entire domain. Most importantly, organizations should consider utilizing a honeypot account, which is a more advanced technique used to detect potential Kerberos authentication exploits. Honeypots are effectively “bait” for attackers, and are often accounts that appear older, posing as administrators with Active Directory privileges. These accounts are used specifically to entice attackers, and will relay information to the organization if successfully targeted.

Level of Difficulty for Attacker

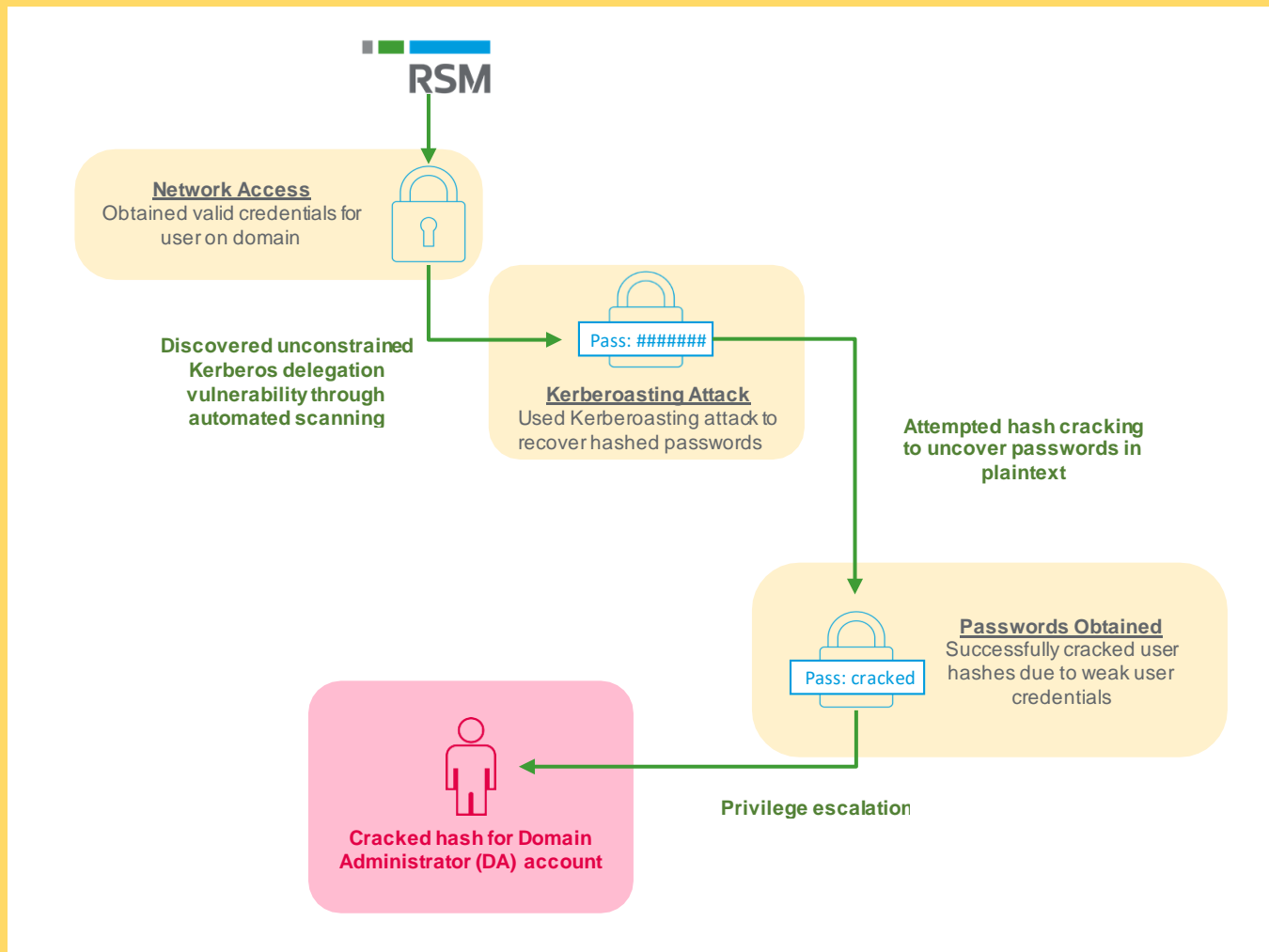
**MEDIUM**

Level of Remediation Difficulty  
for Client

**MEDIUM**

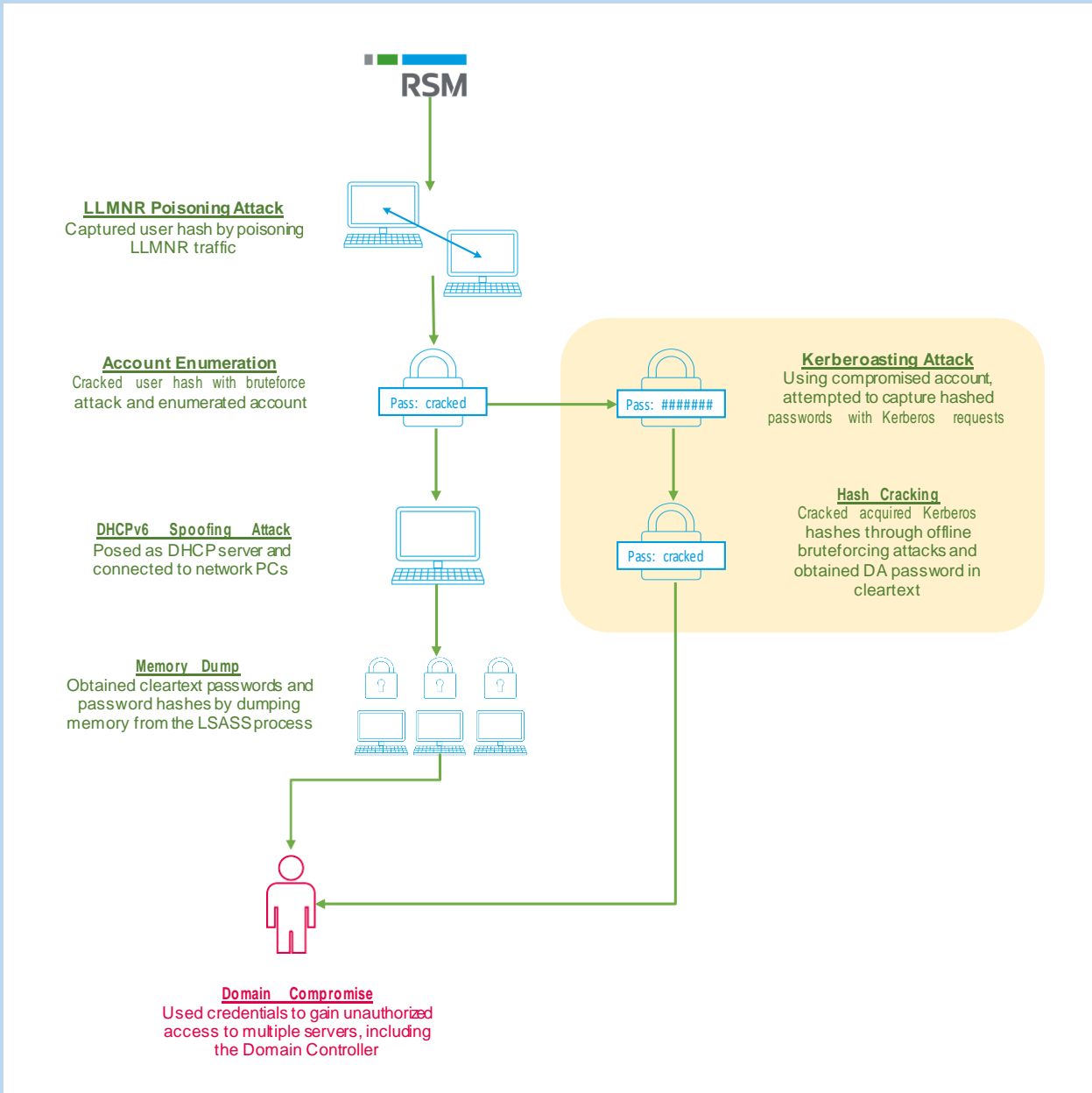
Length of Time for Compromise

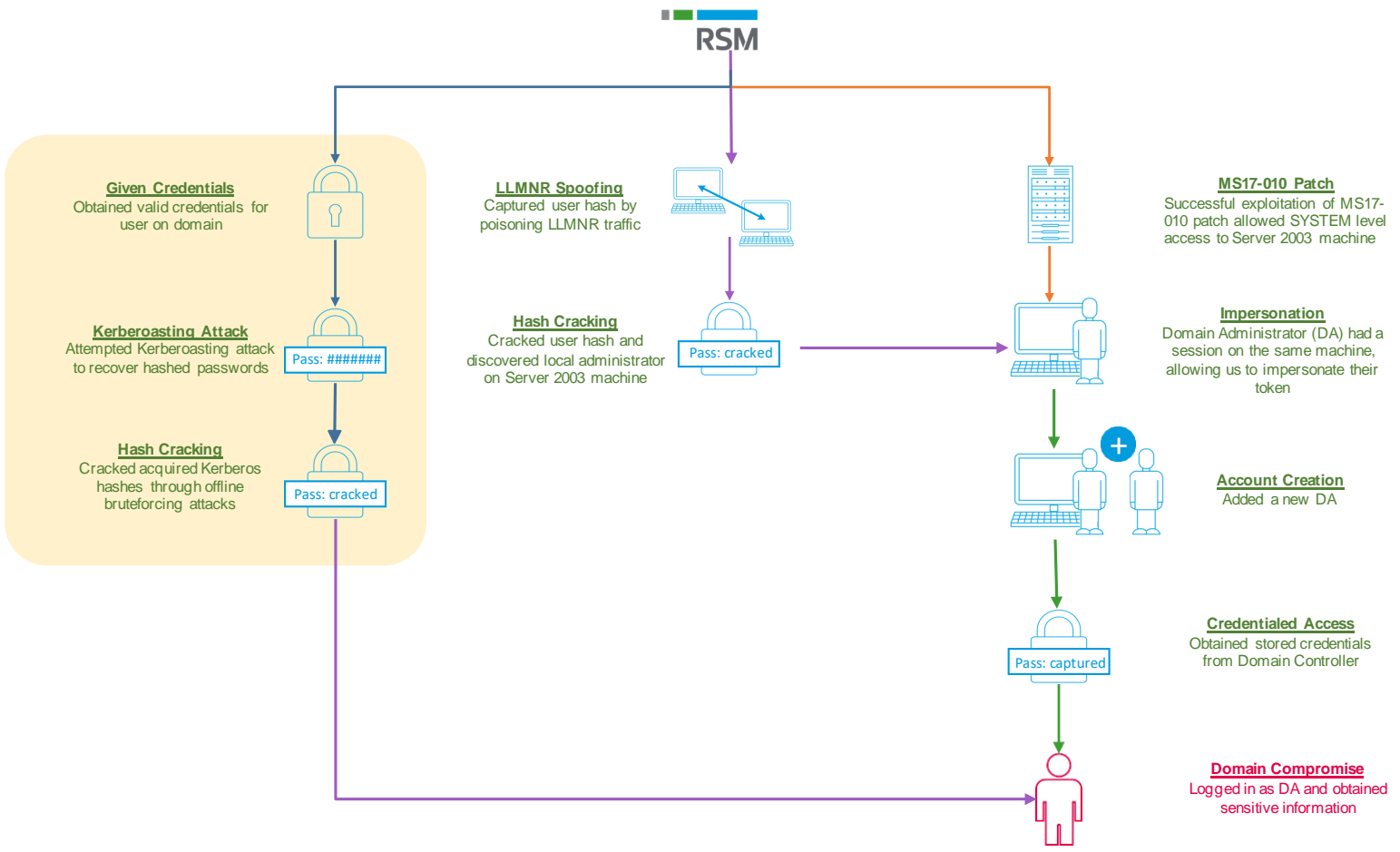
**MEDIUM**



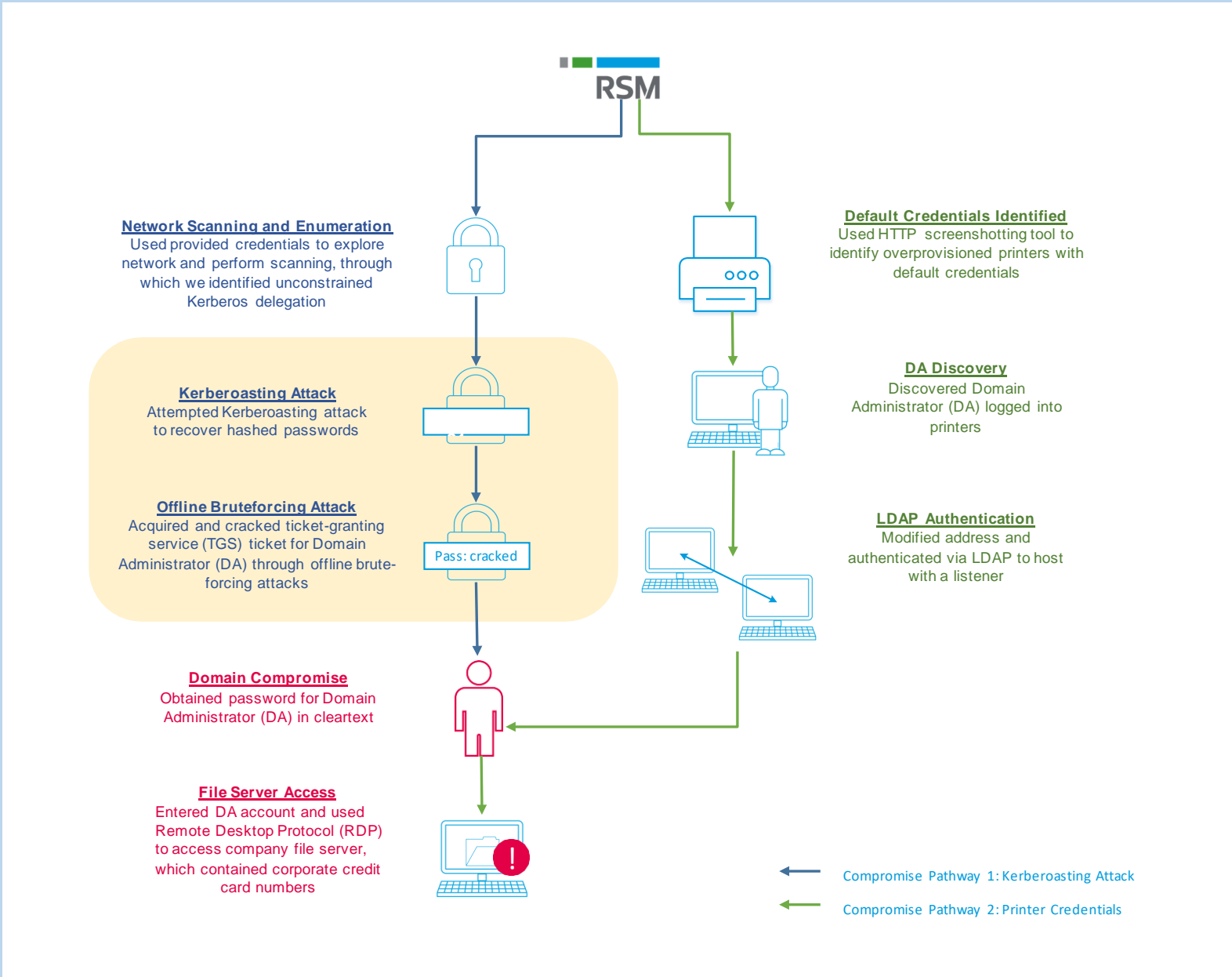
## Diagram Walkthrough

Kerberoasting is often attempted when other attacks are insufficient. As such, this attack vector is depicted alongside other vectors, which are detailed later in this report. The following diagrams illustrate some of our attempts to perform Kerberoasting—as evidenced on the next two pages, Kerberoasting is a difficult attack to complete, and though hashed passwords can be obtained with relative ease, cracking these hashes requires significant time and effort on behalf of the attacker.





- ← Compromise Pathway 1: Kerberoasting
- ← Compromise Pathway 2: MS17-010 Patch Exploitation
- ← Compromise Pathway 3: Man-in-the-Middle Attack





**Information Querying**  
Discovered null sessions on in-scope domain controller, performed anonymous queries for Active Directory information and created list of valid usernames



**Password Spraying Attack**  
Performed password spraying and gained access to user account



**Kerberoasting Attack**  
Because user account possessed local administrator privileges on two machines, requested Kerberos tickets and cracked ticket for Domain Administrator account (DA)



**Domain Compromise**  
Used DA account to extract NTLM user hashes from domain controller and viewed W-2 forms and Social Security Numbers (SSNs)



## Man-in-the-Middle Attacks

By analyzing the data collected from the previous year, we noted that our most common initial attack vectors leveraged insecure communication protocols. These protocols, which include LLMNT/NBT-NS and IPv6, are enabled on Windows-based operating systems by default, and force systems to generate broadcast requests when host names cannot be resolved. An attacker can then intercept this request, respond by claiming to be the resource in question, and encourage victim machines to authenticate to the spoofed system. Hashed credentials are transmitted during this process, which can be cracked through additional compromise steps. These attacks are referred to as “man-in-the-middle,” because the attacker acts as a malicious third party, and actively relays spoofed information between unsuspecting systems.

Overall, man-in-the-middle attacks provide malicious actors with a valid set of credentials, which they can utilize to access the target organization’s domain. However, though such vulnerabilities can be difficult to exploit, organizations should be aware that insecure protocols are an enterprise-wide issue. As such, recovering from such attacks can require a significant amount of time, energy and resources, and preventative measures should be taken prior to any potential attacks.



### PROCESS

While conducting our penetration tests, we primarily focused on IPv6 spoofing and LLMNR/NBT-NS poisoning attacks. First, the attacker will perform automated scanning to discover default protocols enabled on the target network. In IPv6 spoofing, an attacker will then take advantage of modern Windows-based operating systems with traditional IPv4 configurations seeking IPv6 configurations. By posing as an IPv6 DHCP server, the attacker can cause systems on the network to connect to them, collect web traffic and retrieve password hashes. In LLMNR/NBT-NS poisoning attacks, the attacker intercepts traffic, sends poisoned responses to LLMNR/NBT-NS broadcast messages and obtains hashed credentials in the process.

### REMEDIATION OPTIONS

To prevent these attacks and remediate vulnerabilities efficiently, we recommend that organizations implement minimum security baselines (MSBs). These baselines are a configuration standard to which machines should adhere, and disable unneeded features or settings, enable system-hardening features, and provide a consistent approach to device configurations. Implementing MSBs will ensure that the organization’s protocols are consistently reviewed, and that any default settings are replaced with updated encryption algorithms and protections. LLMNR/NBT-NS and IPv6 protocols should be disabled with Group Policy Object (GPO).

Level of Difficulty for Attacker

**MEDIUM**

Level of Remediation Difficulty for Client

**HIGH**

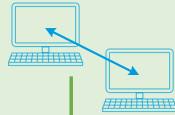
Level of Time for Compromise

**HIGH**



Discovered default LLMNR protocols through initial scanning

**LLMNR Poisoning Attack**  
Obtained domain information by poisoning LLMNR traffic



Relayed connections to LDAP

**Password Guessing**

Leveraged domain information to guess valid username and password combination for domain administrator



Used administrator credentials to continue exploring network

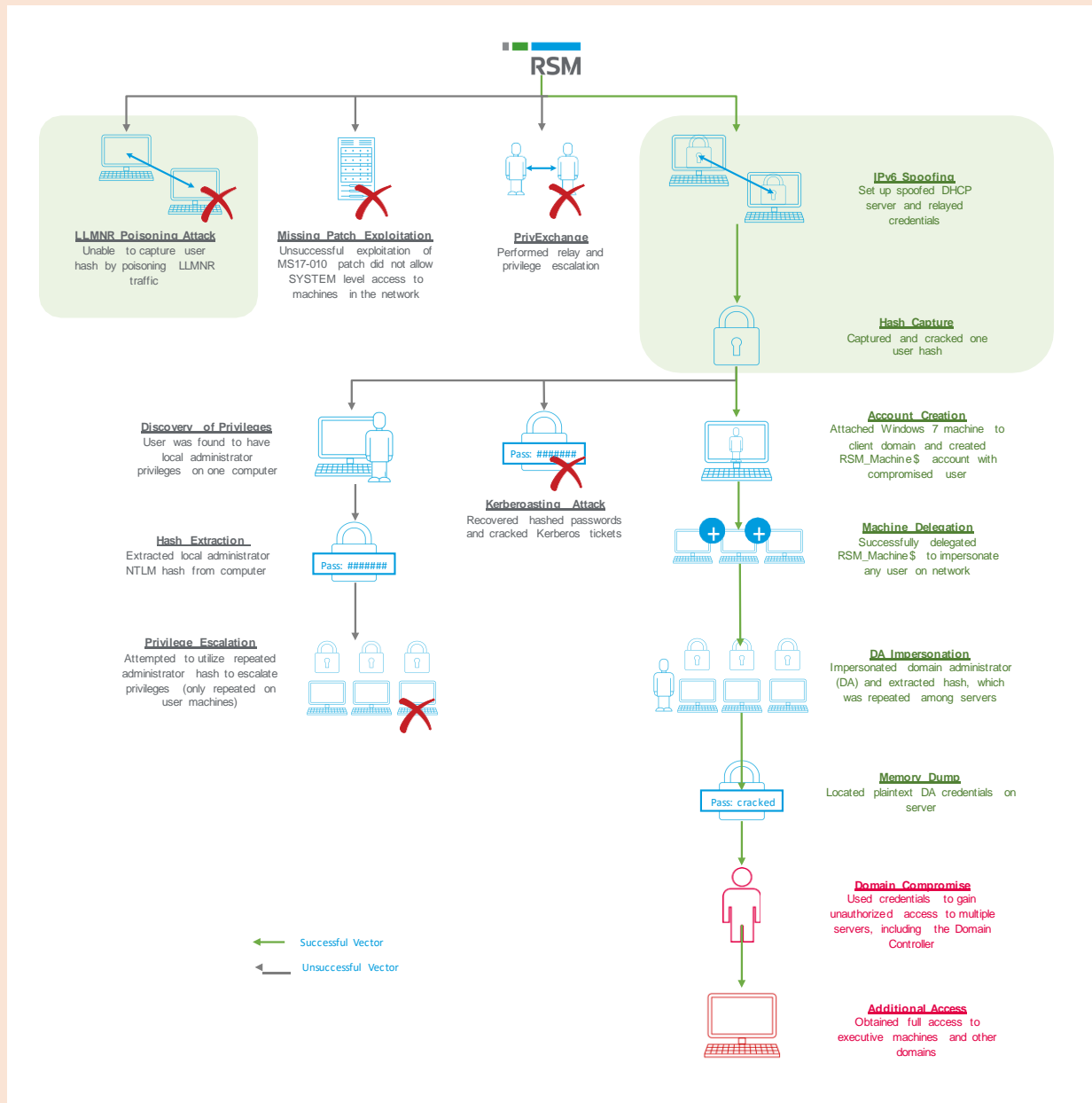
**Domain Compromise**

Obtained unauthorized access to SQL passwords, domain account passwords and anti-virus passwords

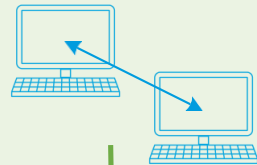


## Diagram Walkthrough

As one of our most common and most successful attacks, man-in-the-middle vectors appear frequently in our client diagrams. The following pages include several examples of spoofing and poisoning attacks.



  
**RSM**



**LLMNR Poisoning Attack**  
Obtained domain information  
by poisoning LLMNR traffic  
and relaying connections to  
LDAP

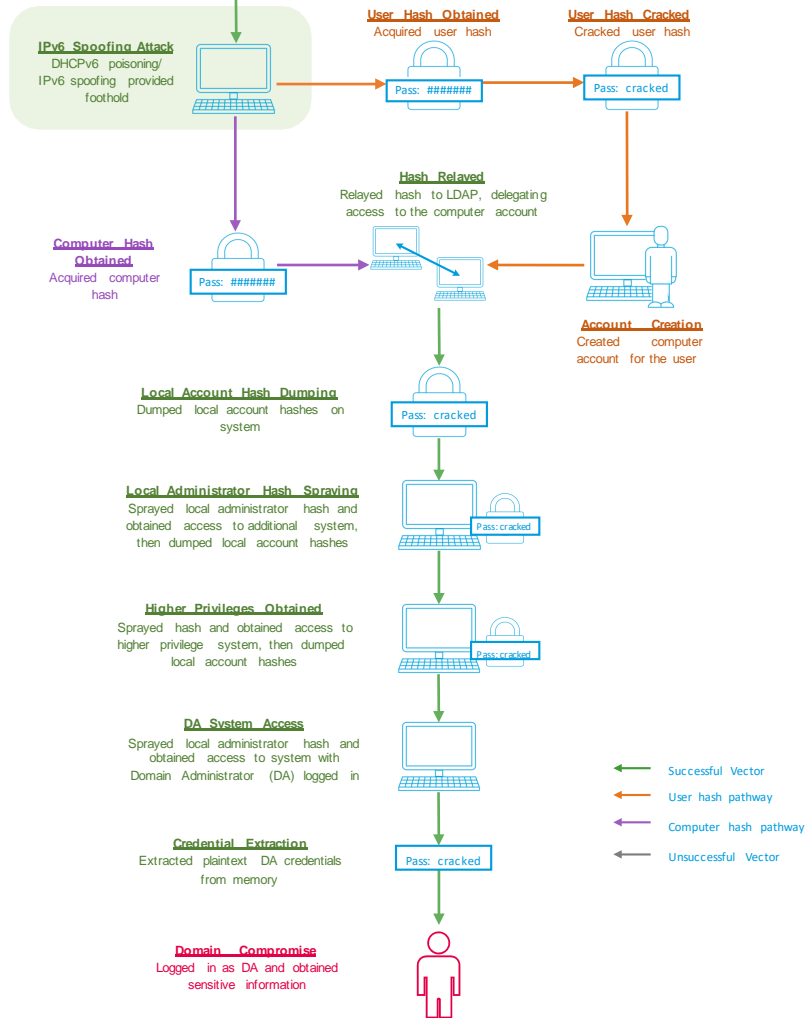


**Password Guessing**  
Leveraged domain information to  
guess valid username and  
password combination for  
Domain Administrator (DA)

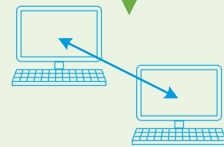


**Domain Compromise**  
Used administrator credentials to  
gain unauthorized access to SQL  
passwords, domain account  
passwords and anti-virus password

RSM



  
**RSM**



**LLMNR Poisoning Attack and NTLM Relay**

Captured eight hashed passwords, relayed to server and dumped local SAM hashes from system



**User Compromise**

Compromised local administrator hash and moved laterally through network, then logged into workstations with local administrator access, compromised server and seized credentials for user account



**Administrative Privileges Obtained**

Queried Active Directory to determine user permissions and gained administrative privileges to most systems in network



**Domain Compromise**

Used pass the hash technique to log into active session for Domain Administrator (DA)

# Password Spraying

This vector is a catch-all category pertaining to weak credentials within web applications and email accounts. As demonstrated by our data from 2020, weak passwords can be leveraged by malicious actors to complete a variety of successful attacks, and can allow an attacker direct entry to the internal network. In order to encourage as many users as possible to quickly create accounts for a service, some applications do not enforce a minimum number of characters. As a result, users generate memorable passwords with few restrictions—passwords that can be identified by hackers within seconds through bruteforcing attacks. A weak password on an internal login page can allow an attacker to easily view personal information, emails and client details. As such, this attack vector is arguably the simplest and most trivial pathway to compromise, while simultaneously permitting an intruder to obtain a significant amount of sensitive data.

Occasionally, we perform password guessing attacks against Active Directory accounts, which are also targeted when capturing password hashes in NetBIOS spoofing attacks. Consequently, weak passwords can generate problems twice over—combined, these two vectors account for nearly half of our successful internal compromises.



## PROCESS

These passwords can be identified in two main attack categories, known as brute-force attacks and password-spraying. In brute-force attacks, the threat actor utilizes a list of common passwords to attempt multiple passwords against one specific user. However, in password-spraying attacks (referred to as “reverse brute-force” attacks), the attacker guesses a small number of weak passwords against an entire list of users. In this way, the attacker can make a high number of guesses while minimizing the likelihood of triggering lockout thresholds. Common passwords include variations of the word “password,” season and year (such as “Summer21”) and company names.

## REMEDATION OPTIONS

In order to ensure that a password is strong, it is crucial that predictable or sequential patterns are avoided. In addition, users should be cautioned against utilizing the same password between different accounts or applications. If a password is shared between a standard user and an administrator, attacks can progress even further on the internal network. In general, we recommend that an organization enforce a strong password policy that prevents users from creating easily guessable passwords. This policy would ideally require 12 characters at a minimum, along with a combination of varying letter capitalization, numbers and special characters. For increased security, company information should be avoided, and the user should consider implementing a long passphrase. These passphrases are considerably more difficult to compromise, but may be easier to remember.

Level of Difficulty for Attacker

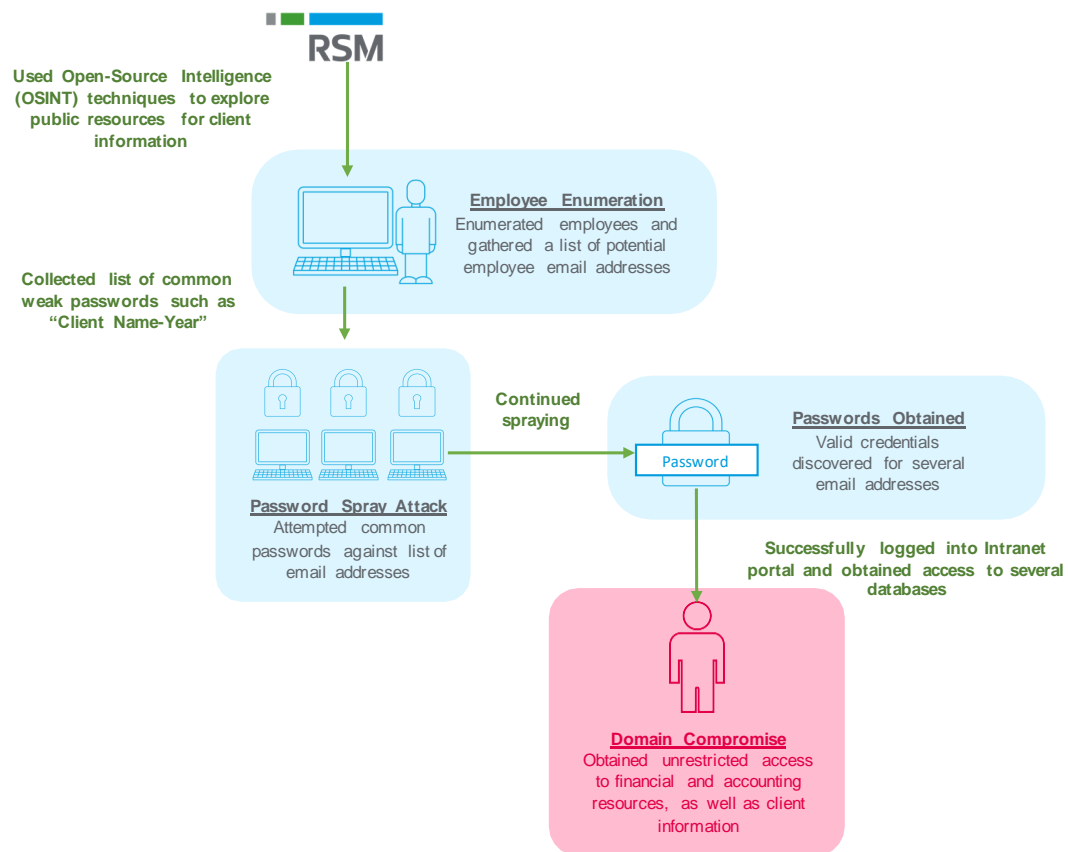
**LOW**

Level of Remediation Difficulty

**LOW**

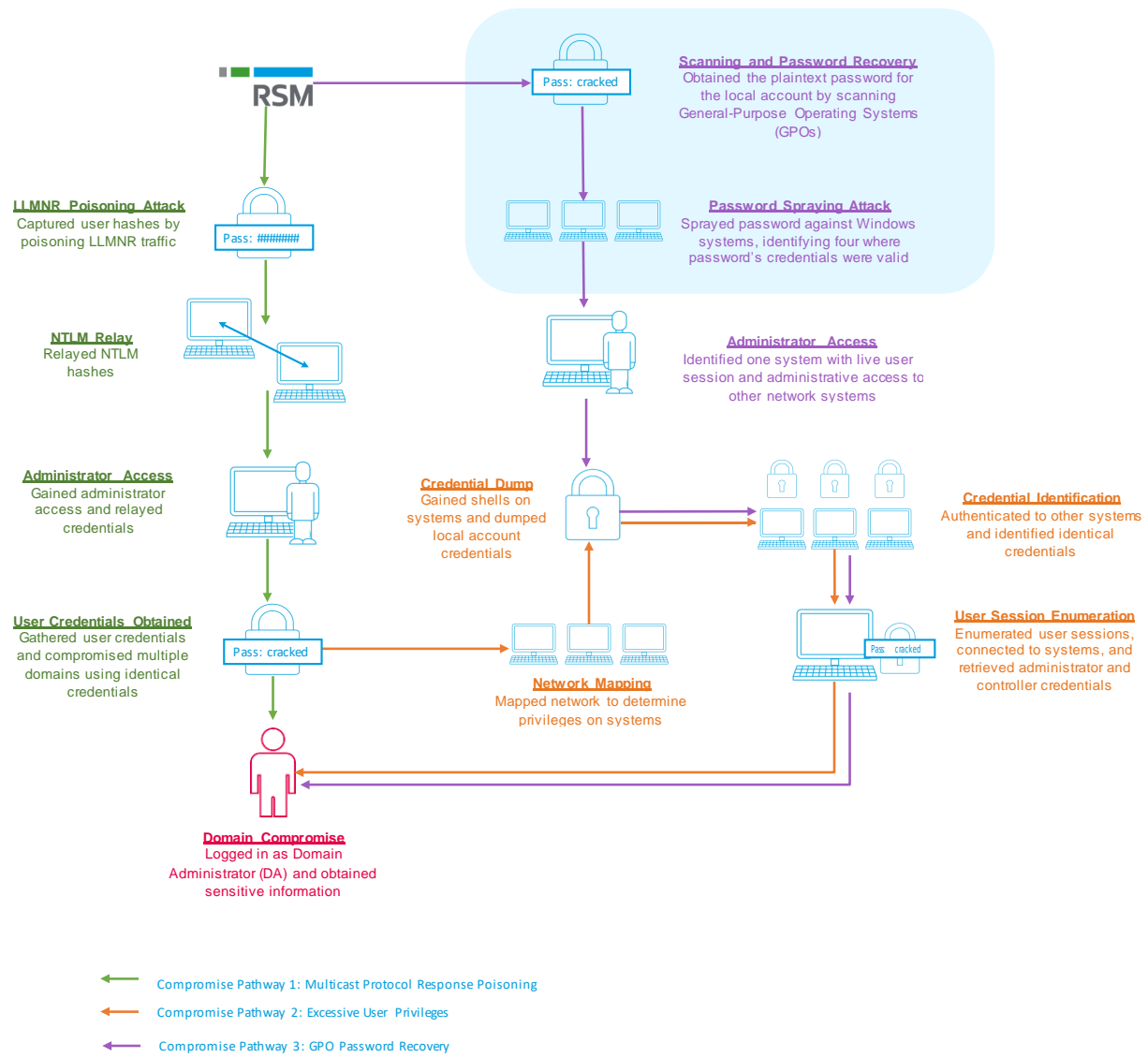
Length of Time for Compromise

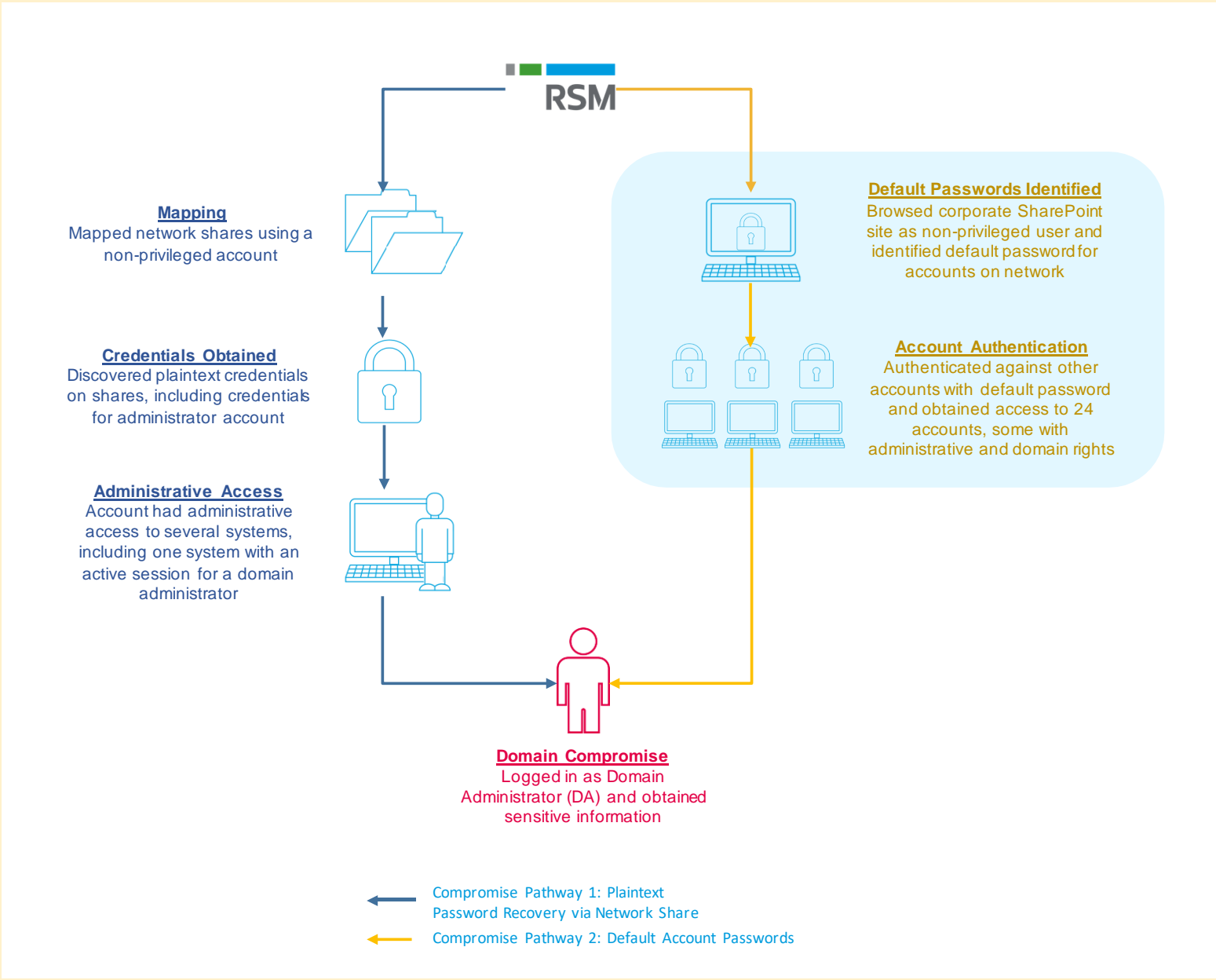
**MEDIUM**



## Diagram Walkthrough

The following collected diagrams detail password spraying attacks when coupled with other attack vectors. Due to the number of successful password-related attacks we've performed, a majority of our compromise diagrams involve at least some form of password guessing or bruteforcing. As this is our most common attack vector, it is crucial that password best practices be noted in corporate policy and emphasized during security awareness training. To encourage strong passwords from a technical perspective, an organization may consider the use of an Active Directory plugin, which can act as a password blacklist to prevent users from choosing certain passwords. For more information about long passphrases, password policies and remediation options, please see <https://warroom.s.com/stanford-password-policy/>.







**Management Frame Protection (MFP) Reconfiguration**

Discovered MFP with scan-to-share credentials, reconfigured MFP and intercepted authorization attempt



**Interception of Credentials**  
Cracked intercepted credentials to plaintext and identified systems on which intercepted credentials had administrator rights



**Insecure Administrative Rights Configuration Discovered**  
Insecure configuration revealed domain users group with local administrator rights to 30 systems



**User Access and AD Enumeration**  
Used intercepted credentials to perform AD enumeration and identify systems with repeated local administrator password



**Sessions Established on Additional Systems**

Extracted hashes for user session and performed memory dumping



**Domain Compromise**  
Gained access to account identified as domain administrator



RSM



**Employee Enumeration**  
Using OSINT, enumerated employees and gathered a list of 400 potential employees



**Password Spray**  
Sprayed list of weak and guessable passwords against OWA and O365 portals



**Password Compromised**  
Gained credentials from webmail portal



**Mailbox Access**  
Successfully logged into Outlook Web Access (OWA) mailbox with credentials



**Citrix Gateway Access**  
Successfully logged into Mobility Citrix Gateway with credentials



**Domain Compromise**  
Obtained unrestricted access to Internal Network from Citrix applications

## SMB Relay

Server Message Block (SMB) protocols allow Windows machines to communicate with one another by transferring files or executing remote command operations. When required, systems enabled with SMB signing are obligated to verify the authenticity of incoming SMB requests. However, if this protocol and its authentication services are targeted in an SMB Relay attack, systems without SMB signing will send requests to network resources, which are recognized and intercepted by attackers. Throughout this interception, the request, which contains a user's hashed credentials, is relayed to a target of the attacker's choice by masquerading as a legitimate user. If the original user's credentials are valid on the target system, the attacker can then gain access.

These attacks typically target administrator or privileged accounts, as intercepting these credentials will provide an attacker with access to internal systems and information. In addition, SMB Relay attacks rely primarily on initial scanning services, as these automated methods indicate which of the network's systems lack signing protections. Coupled with other simple misconfigurations, such as information disclosure vulnerabilities or insecure encryption algorithms, SMB Relay can escalate to full domain compromise, and can allow malicious actors to obtain a range of sensitive data.

16.7%

of clients (10 out of 60)  
had a compromise  
pathway involving a  
SMB Relay attack

### PROCESS

The SMB protocol utilizes New Technology LAN Manager (NTLM) authentication to validate remote users, and the SMB Relay attack seeks to relay NTLMv2 hashes to remotely execute code with administrative privileges. The attack leverages the challenge-response authentication mechanism used by NTLM, but the attack also takes advantage of application-layer protocols that inherently "trust" authentication requests they receive. The attacker begins by sending poisoned responses to broadcast requests that cause other systems on the network to attempt to authenticate against the attacker's system. Many protocols can be abused in this step, such as ARP, IPv6/DHCP, LLMNR, or NBT-NS. After enticing a victim system to attempt a remote authentication request, the attacker forwards the authentication request to a secondary system on the network against which they wish to authenticate.

### REMEDATION OPTIONS

Because this attack relies on authentication utilized by most organizations, it is crucial that SMB signing is enforced through group policy. In order to prevent SMB Relaying in the future, organizations can also consider moving to Kerberos authentication.

To successfully execute this attack, the malicious actor only requires network access, scanning tools and an easily downloadable script. As a result, any individual with an internal WiFi password or login information can perform this attack and obtain information.

Level of Difficulty for Attacker

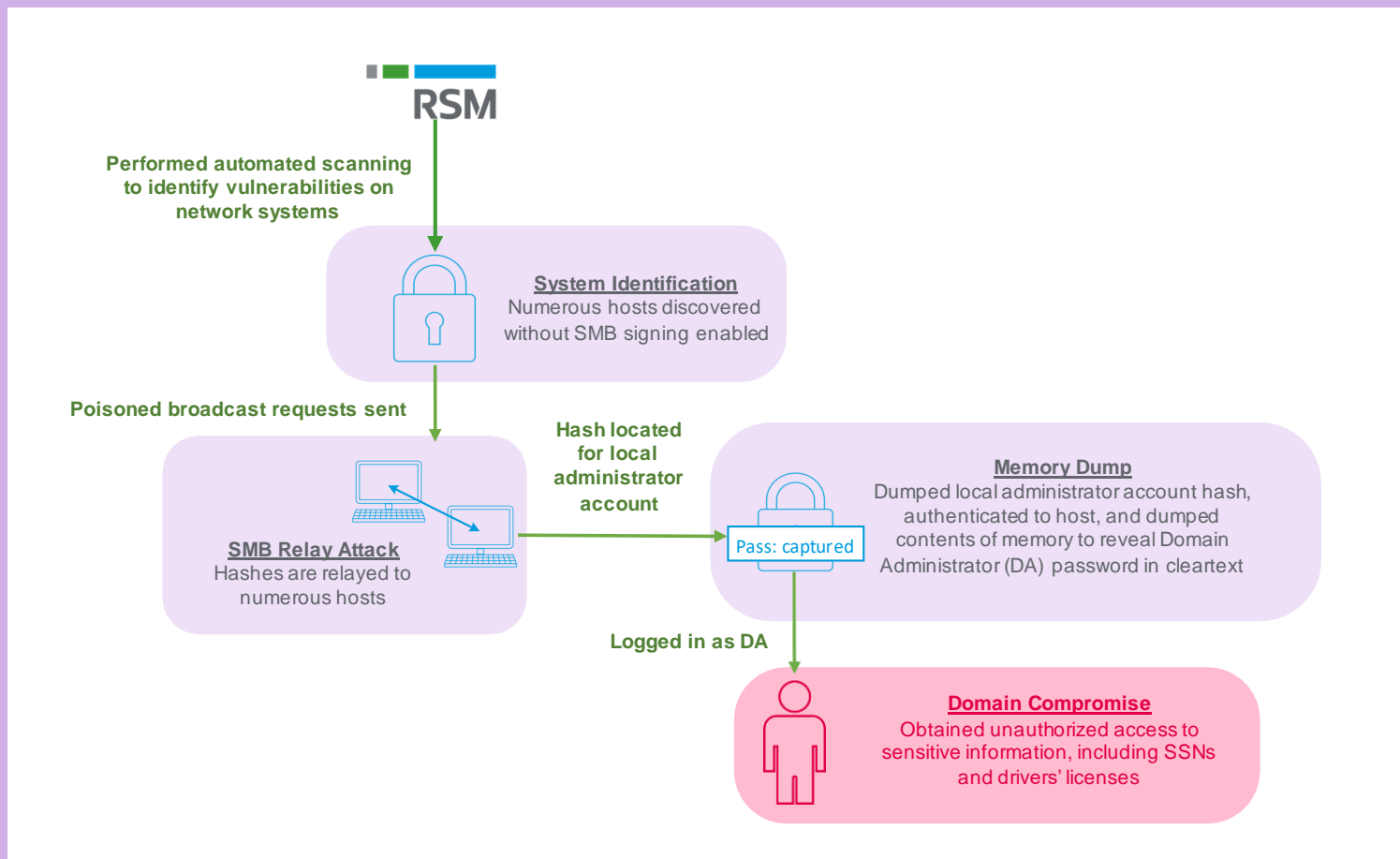
MEDIUM

Level of Remediation Difficulty  
for Client

LOW

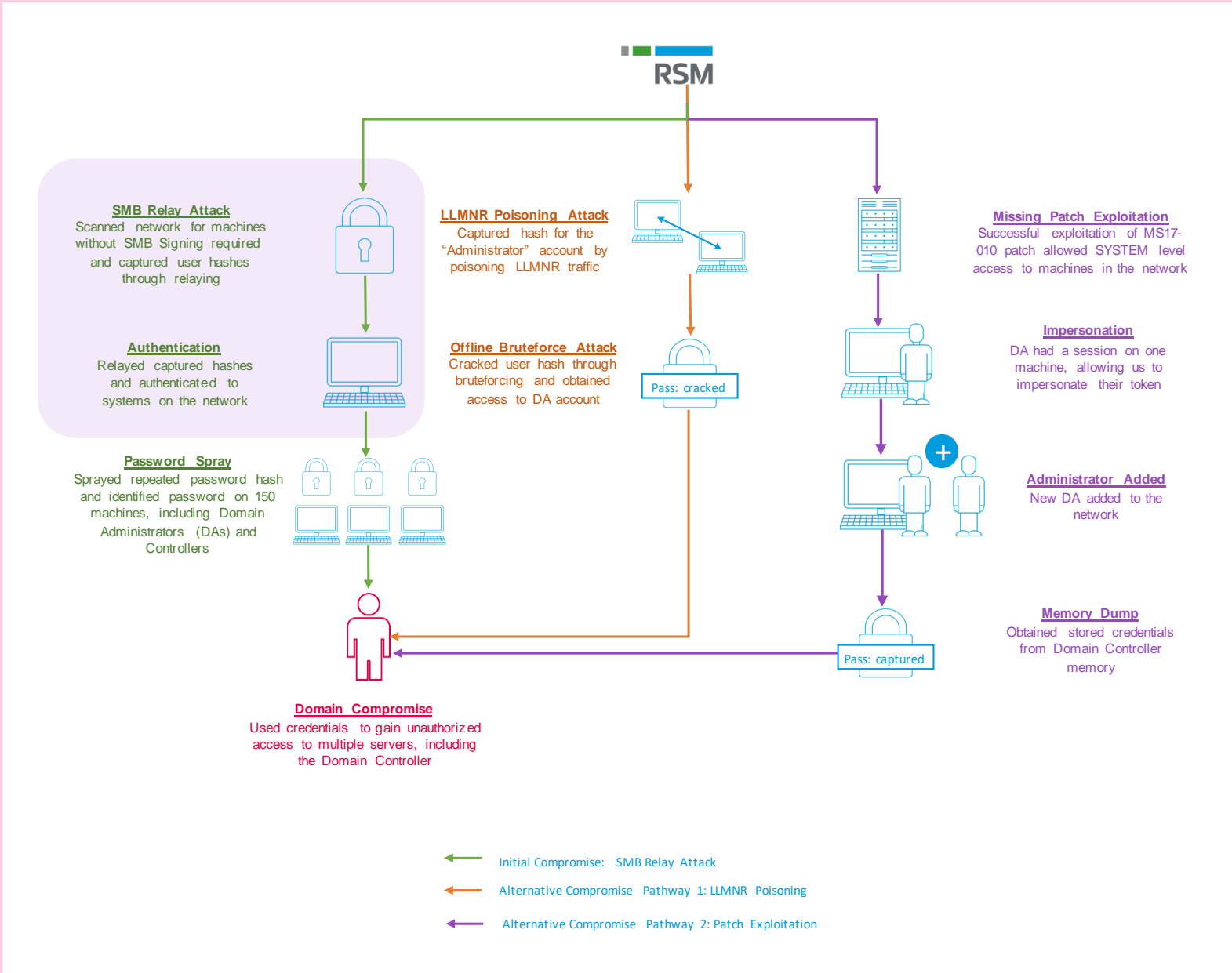
Length of Time for Compromise

LOW



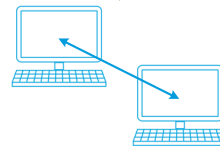
## Diagram Walkthrough

The following diagrams detail our use of SMB Relay attacks in successful compromises. SMB Relaying relies on a lack of signing on multiple systems within a network. Though many organizations have enabled signing to prevent these attacks (making this technique less successful than the others noted in this report), it is still an issue for many organizations. For more information about SMB Relay attacks, please reference <https://warroom.rsm.us.com/smb-relay/>.



**RSM**

**LLMNR/NetBIOS and IPv6 Spoofing**  
Intercepted broadcast requests and set up spoofed DHCP server to relay credentials



**SMB Relay and Hash Dump**  
Performed SMB relay attacks to obtain admin access on multiple machines and dump hashes on machines



**Local Admin Access and Pass-the-Hash**  
Credentials for shared local admin account provided local admin rights on machine; used pass-the-hash technique to harvest Domain Administrator (DA) credentials



**Password Cracking**  
Logged into Domain Controller, extracted hashes and cracked hashes using password cracking attacks



**Domain Compromise**  
Used credentials to gain unauthorized access to SSNs and HIPAA data

# RSM

**Network Scanning**  
Evaluated vulnerabilities through scanning and identified multiple hosts without SMB signing enabled

**SMB Relay Attack**  
Sent poisoned broadcasts and relayed hashes to hosts without signing

**Memory Dump**  
Identified hash for local administrator and dumped host memory to identify Domain Administrator (DA) password in cleartext

**Employee Enumeration**  
Using OSINT, enumerated employees and gathered a list of potential employees

**Phishing Attack**  
Sent spoofed email to 20 employees and received credentials for two users

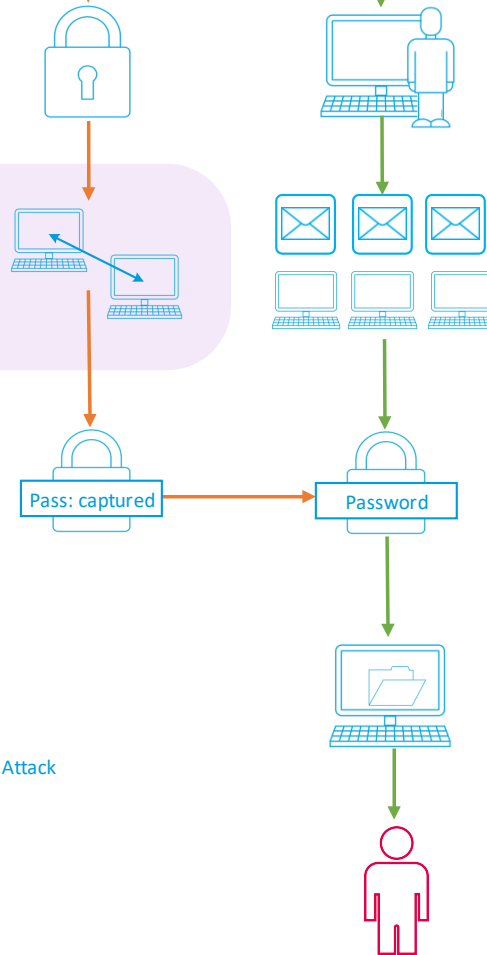
**Account Login**  
Validated credentials and successfully logged into account with administrator privileges

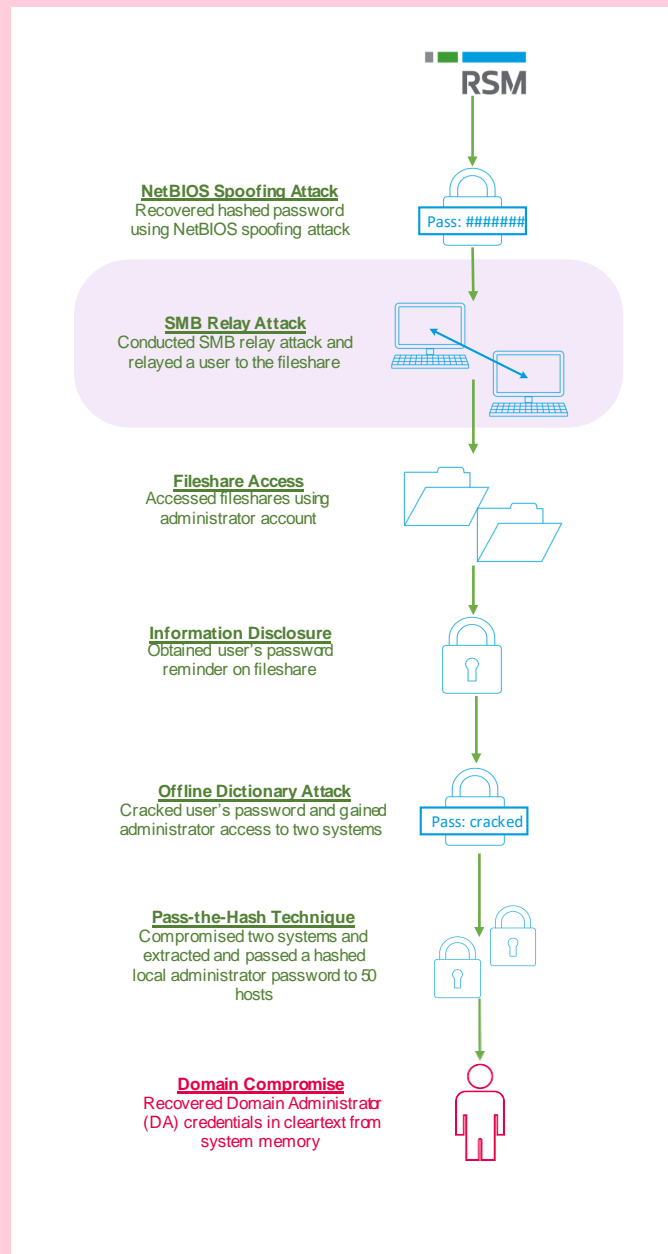
**Database Access**  
Obtained access to IBM development database

**Domain Compromise**  
Obtained unrestricted access to financial and accounting resources, as well as potential client information

← Compromise Pathway 1: SMB Relay Attack

← Compromise Pathway 2: Phishing





## Recommendations

After completing our analysis and examining our results, we noted that network and data security relies on a variety of factors.

### The Human Factor

In order to ensure that an organization is protected against future attacks, it is integral to perform security awareness training and emphasize security architecture best practices. These actions will protect internal networks, as lack of understanding regarding threats and attack vectors can be exploited easily by malicious actors.

To oversee and manage these security problems, organizations should assign qualified, dedicated individuals. Consistent security training should be conducted for employees, designed specifically to discuss data protection policies and password strength. Ongoing awareness campaigns will allow employees to refresh their knowledge and increase their awareness of security incidents.

Overall, the easiest way to improve an organization's security profile is to prevent simple attacks from occurring in the first place. As discussed earlier in this report, certain attack vectors (such as weak passwords or missing patches) can be leveraged in a compromise with minimal resources and effort. In other words, these vulnerabilities are considered "low-hanging fruit" that allows potential attackers to take the path of least resistance. By reviewing and updating password and patch management policies, increasing passwords in length and complexity, remediating missing patches, and implementing new versions of software, organizations can prevent or cushion the potential impact of debilitating attacks. Furthermore, the use of multi-factor authentication wherever possible will significantly reduce (but not excuse) the risks associated with weak passwords.

Misconfigured protocols and other simple misconfigurations typically stem from human-centered shortcomings, including user issues, employee ignorance, and organizational inaction. Strengthening monitoring capabilities and training employees to recognize security problems will mitigate risk. These facets should be included in general security awareness training programs as well.

The attack vectors in this report provide an overview of exposures and techniques for internal compromise. However, an organization may not be aware of the extent to which their environment is at risk. In order to properly assess their networks, organizations should conduct regular security assessments. Such assessments will effectively leverage the organization's current governance model, internal tools and processes to provide an in-depth analysis of network weaknesses.

## Strategic Planning

For long-term protective actions, program-level initiatives should be built out on the same principles we have outlined above. Vulnerability and patch management programs guarantee that vulnerabilities are addressed in a timely manner without impacting production. Minimum security baselines, as previously mentioned in the report, are an organization-wide initiative used to apply device and software security standards to every system on the network. Change management initiatives safeguard network security as devices are added and removed from the network. Organizations of an appropriate security program maturity level should also pursue more targeted planning, which includes Secure Software Development Lifecycles and Security Testing or Audit programs.

Ultimately, organizations should push towards a zero-trust model. Only those individuals with a business case need for data and systems (also known as “least privilege”) should be allowed access to these sensitive areas. Unfortunately, though it may feel natural to afford internal resources more flexibility, particularly when it comes to applying best-practice protections, just one misstep can lead to disaster. A company-wide application of least privilege to people, processes and technology can help safeguard the security of the organization and its employees.

Finally, establishing a strong security governance program is key to ensuring that your organization develops a consistent, repeatable approach to addressing your cybersecurity risks. Sufficiently mitigating the attack vectors detailed in this report requires more than tactical fixes. It requires a strategic approach to ensure the appropriate allocation of resources, delineation of roles and responsibilities, ongoing monitoring of these issues, alignment of people/processes/technology, and integration into your organization’s enterprise risk management strategy. Clear ownership of the security program—coupled with the support of a trusted security advisor—provides the kind of direction and oversight needed to ensure that you can continue your business operations knowing your systems and data are secure.

## Conclusions

By analyzing several dozen internal penetration testing reports from 2020, we have noted that many of the problems identified in our previous Attack Vectors reports continue to impact businesses today. As noted in previous years, insecure protocols and poorly constructed passwords comprised the majority of RSM's successful compromises on internal systems.

Clients often assume that internal networks are a trusted space, and assume that any individual operating within the confines of the corporate network are safe from potential exploits. Unfortunately, these networks require just as many controls and monitoring precautions as perimeter networks.

The results of this report highlight the continued importance of strong program-level initiatives, including security awareness training, asset and change management and minimum security baseline implementation.

We encourage the readers of this report to examine the attack vectors presented to effectively and efficiently safeguard your internal network environment.

## Acknowledgements

Primary Authors:

- Daria Ryabogin (Daria.Ryabogin@rsmus.com)
- Jonathan Slusar (Jonathan.Slusar@rsmus.com)

This report would not have been possible without the efforts of the following individuals:

- Ken Smith (Ken.Smith@rsmus.com)
- Erica Cummings (Erica.Cummings@rsmus.com)

**Disclaimer**

This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute audit, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person. Internal Revenue Service rules require us to inform you that this communication may be deemed a solicitation to provide tax services. This communication is being sent to individuals who have subscribed to receive it or who we believe would have an interest in the topics discussed.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit [rsmus.com/aboutus](http://rsmus.com/aboutus) for more information regarding RSM US LLP and RSM International.

RSM, the RSM logo and the power of being understood are registered trademarks of RSM International Association.

© 2021 RSM US LLP. All Rights Reserved.