NOVEMBER 1, 2017

EXTERNAL / INTERNAL NETWORK PENETRATION TEST

Version 1.4

TechCorp, Inc.
Bill Lumbergh | Chief Information Security Officer

ASSESSMENT INFORMATION

Penetration Tester(s)

Hector Monsegur
hector.monsegur@rhinosecuritylabs.com
(888) 944-8679

Client Contact

Bill Lumbergh
Chief Information Security Officer
TechCorp, Inc.

Engagement Manager

Christopher Lakin
chris.lakin@rhinosecuritylabs.com
(888) 944-8679

Project Number

10-17-ITL-SE

Assessment Scope Summary

Engagement Timeframe

10/12/2017 – 10/31/2017

Engagement Scope

10 External IP Addresses
255 Internal IP Addresses

Revision History

Date Change	Author	Notes
10-30-2017	Hector Monsegur	First Draft
10-31-2017	Christopher Lakin	Edits
10-31-2017	Benjamin Caudill	Edits
11-01-2017	Hector Monsegur	Final Draft

TABLE OF CONTENTS

ENGAGEMENT OVERVIEW

Rhino Security Labs provides network penetration testing to identify, analyze, and safely exploit vulnerabilities, demonstrating the associated security risk.

With backgrounds in technology, banking, defense, and healthcare, our consultants are some of the foremost authorities on cybersecurity. These experts ensure the security of existing applications in the enterprise, as well as assisting the security process in all phases of the development lifecycle.

Service Description

Penetration Testing is the process of simulating real-world attacks by using the same techniques as malicious hackers. For a security assessment that goes beyond a simple vulnerability scanner, you need experts in the industry.

External Network Penetration Test

Your perimeter network is attacked every day and even small external vulnerabilities can be damaging. External network penetration testing identifies vulnerabilities on infrastructure devices and servers accessible from the internet.

External penetration testing assess the security posture of the routers, firewalls, Intrusion Detection Systems (IDS) and other security appliances which filter malicious traffic from the internet.

Internal network Assessment

Internal network testing assesses the organization's security from the perspective of an inside user. While this is typically seen as a disgruntled employee, we compare this as an external attacker which has breached the external perimeter or wireless network.

In addition to testing for vulnerabilities, this assessment tests the organizations detection and response capabilities, confirming the effectiveness of SIEM and log aggregation technologies.

Campaign Objectives

Vulnerability Identification

Rhino Security's consultants use the results of the automated scan, paired with their expert knowledge and experience, to conduct a manual security analysis of the client's network. Our assessors attempt to exploit and gain remote unauthorized access to data and systems by identifying potential vulnerabilities in the network. The detailed results of both the vulnerability scan and the manual testing are shown this report.

KEY PERSONNEL

Passionate and forward-thinking, our consultants bring decades of combined technical experience as top-tier researchers, penetration testers, application security experts, and more. Drawing from security experience in the US military, leading technology firms, defense contractors, and Fortune 100, we pride ourselves on both depth and breadth of information security experience.

Chris Lakin - *Cybersecurity Engagement Manager*

Chris Lakin has accumulated over eight years of project management and customer engagement experience across a multitude of industries. A proponent of constant iteration and improvement, his knowledge from time spent in business and marketing adds a valuable perspective to every cybersecurity engagement. Receiving a Masters of Science in Cybersecurity Engineering from the University of Washington, Mr. Lakin excels at connecting the technical with the goals of the business.

Hector Monsegur - *Director of Assessment Services*

Hector Monsegur brings a unique perspective from decade of offensive experience and a desire to make an impact in client security. In working with the US Government, Mr. Monsegur identified key vulnerabilities - and potential attacks - against major federal infrastructure including the US military and NASA. In his role as a security ressearcher at Rhino Security Labs, he has identified countless zeroday vulnerabilities and contributed to dozens of tools and exploits. In his leadership role, his unmatched technical experience is shared to both educate other operators and guide techincal research. Mr. Monsegur is a leading speaker for security organizations and conferences around the world.

Benjamin Caudill - *CEO and Founder*

Benjamin Caudill is an adept cybersecurity professional, researcher, and entrepreneur. A veteran of the defense and aerospace industry, Mr. Caudill led investigations into advanced cyberattacks, coordinating with federal intelligence communities on complex engagements. As Founder and CEO of Rhino Security Labs, Mr. Caudill has built the boutique security firm and turned it into a major player in the penetration testing market. In addition to his executive role, Mr. Caudill oversees company research and development, ensuring the continued development of key offensive technologies.

NETWORK PENETRATION TESTING METHODOLOGY

At Rhino Security Labs, our application penetration testing targets the entire range of vulnerabilities in your external and internal network. Using the same techniques as sophisticated real-world attackers, we providing unique visibility into security risks automated tools often miss. To ensure high quality, repeatable engagements, our penetration testing methodology follows these steps:

1

Reconnaissance

This process begins with detailed scanning and research into the architecture and environment, with the performance of automated testing for known vulnerabilities. Manual exploitation of vulnerabilities follows, for the purpose of detecting security weaknesses in the application.

As with malicious hackers, each penetration test begins with information gathering. Collecting, parsing, and correlation information on the target is key to identifying vulnerabilities.

2

Vulnerability Detection

Once the target has been fully enumerated, Rhino Security Labs uses both vulnerability scanning tools and manual analysis to identify security flaws. With decades of experience and custom-built tools, our security engineers find weaknesses most automated scanners miss.

3

Attack and Post-Exploitation

At this stage of the assessment, our consultants review all previous data to identify and safely exploit identified application vulnerabilities. Once sensitive access has been obtained, the focus turns to escalation and movement to identify technical risk and total business impact.

During each phase of the compromise, we keep client stakeholders informed of testing progress, ensuring asset safety and stability.

4

Assessment Reporting

Once the engagement is complete, Rhino Security Labs delivers a detailed analysis and threat report, including remediation steps. Our consultants set an industry standard for clear and concise reports, prioritizing the highest risk vulnerabilities first. The assessment includes the following:

- Executive Summary
- Strategic Strengths and Weaknesses
- Identified Vulnerabilities and Risk Ratings
- Detailed Risk Remediation Steps
- Assets and Data Compromised During Assessment

5

Optional Remediation

As an optional addition to the standard assessment, Rhino Security Labs provides remediation retesting for all vulnerabilities listed in the report. At the conclusion of the remediation testing and request of the client, Rhino Security Labs will update the report with a new risk level determination and mark which vulnerabilities in the report were in fact remediated to warrant a new risk level.

EXECUTIVE SUMMARY OF FINDINGS

Rhino Security Labs conducted a External/Internal Network Penetration Test for TechCorp, Inc (TechCorp). This test was performed to assess TechCorp defensive posture and provide security assistance through proactively identifying vulnerabilities, validating their severity, and providing remediation steps.

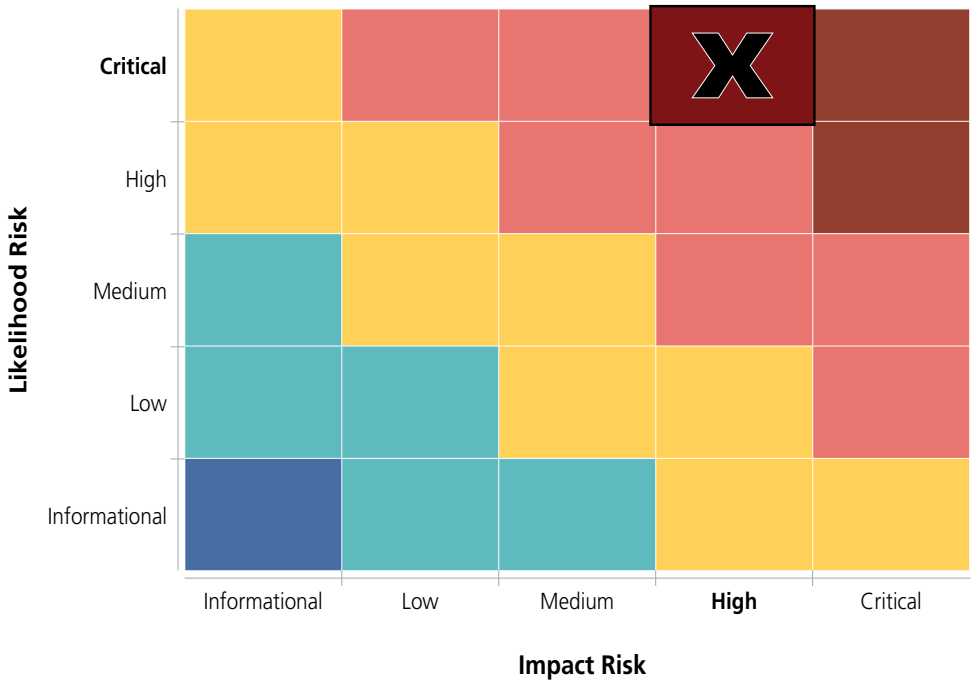
Rhino Security Labs reviewed the security of TechCorp's infrastructure and had determined a Critical risk of compromise from external attackers, as shown by the presence of the vulnerabilities detailed in this report.

The detailed findings and remediation recommendations for these assessments may be found later in the report.

EXTERNAL/INTERNAL NETWORK RISK RATING

Rhino Security Labs calculates network risk based on Exploitation Likelihood (ease of exploitation) and Potential Impact (potential business Impact to the environment).

Overall Risk Rating: CRITICAL



Summary of Strengths

While Rhino Security Labs was tasked with finding issues and vulnerabilities dealing with the current environment, it is useful to know when positive findings appear. Understanding the strengths of the current environment can reinforce security best practices and provide strategy and direction toward a robust defensive posture. The following traits were identified as strengths in TechCorp's environment.

1. Strong log monitoring and incident response processes. Multiple attack vectors were identified and responded to in less than 3 hours.
2. Effective DNS categorization security protections, particularly around blocking uncategorized domains.

Summary of Weaknesses

Rhino Security Labs discovered and investigated many vulnerabilities during the course of its assessments for TechCorp, inc. We have categorized these vulnerabilities into general weaknesses across the current environment, and provide direction toward remediation for a more secure enterprise.

1. Several servers have not applied the MS17-010 patch, leaving dozens of computers vulnerable to WannaCry and other ransomware variants.
2. LLMNR and NBT-NS protocols are enabled, allowing for the passive NTLMv2 hash gathering from users across the network without their knowledge.

Strategic Recommendations

Not all security weaknesses are technical in nature, nor can they all be remediated by security personnel. Companies often have to focus on the root security issues and resolve them at their core. These strategic steps are changes to the operational policy of the organization. Rhino Security Labs recommends the following strategic steps for improving the company's security.

1. Apply MS17-010 to the affected machines in order to prevent a potential ransomware outbreak.
2. Disable LLMNR and NBT-NS on workstations employees use.
3. Review group policy and unfurl unintentional administrative relationships (for example, SVC Accounts being Domain Administrators).
4. Create firewall rules to ensure IPMI devices are only allowed to communicate with authorized devices to prevent unintentional hash disclosures.
5. Strengthen password policy to ten-character minimum. Many of the cracked passwords were 9-characters or less. The passwords also followed generic patterns such as the username and a number after it.

ATTACK NARRATIVE

Rhino Security Labs conducted an External/Internal Network Penetration Test for TechCorp. This test was performed to assess TechCorp's defensive posture and provide security assistance through proactively identifying vulnerabilities, validating their severity, and providing remediation steps.

EXTERNAL NETWORK

First, we identified a misconfigured AWS S3 bucket with sensitive IT Ops data exposed to the internet. This sensitive data included system backups and user directories. The backups were downloaded, and additional hashed passwords were extracted and cracked.

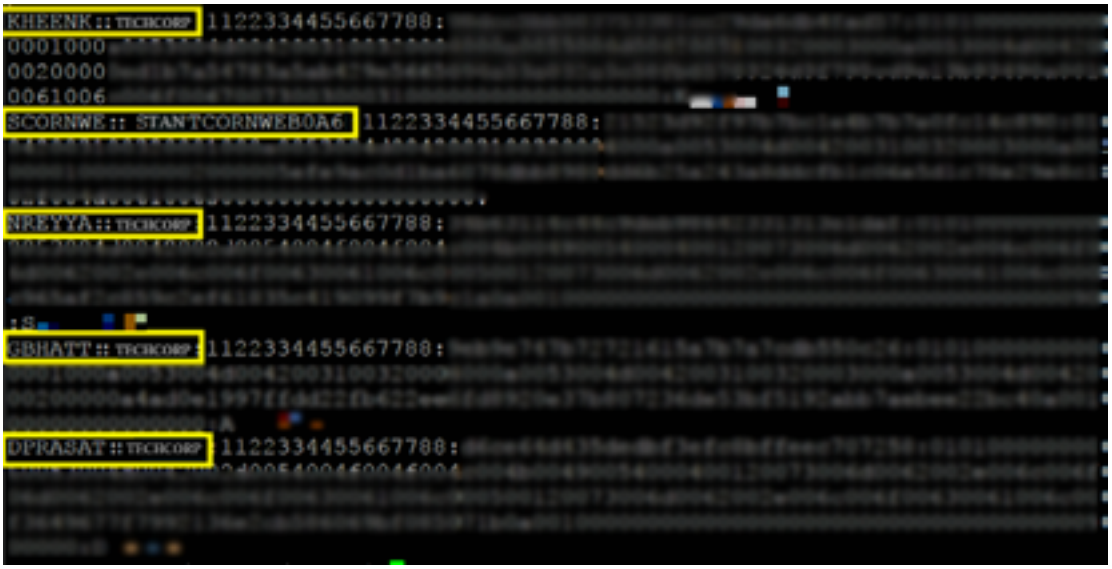
Additionally, an open IPMI 2.0 port was identified, which leaked the MD5 hash of the password as part of the spec. We took that hash and cracked it using our designated password cracking machine.

In enumerating other assets on the perimeter, we also found a VPN. It was soon learned that one of the cracked passwords was valid to the sysadmin's VPN. Through this avenue, we obtained access to the internal network.

INTERNAL NETWORK

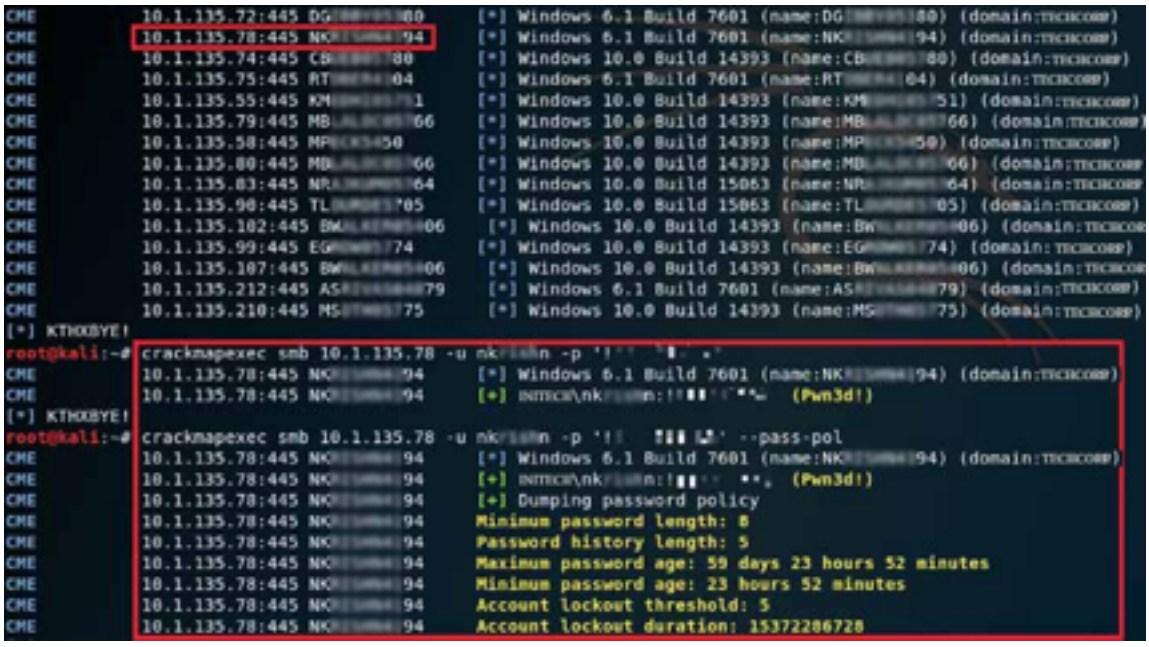
Once on the internal network, the goals of the assessor were two-fold; to perform a network scan of the given address scope and to passively listen for LLMNR traffic on the network to capture user's hashes. In both aspects we were successful, capturing a total of 23 user hashes, 5 of which were cracked offline by our password-cracking machine.

An example of capturing a user's hashed password due to a typo when retrieving an SMB share



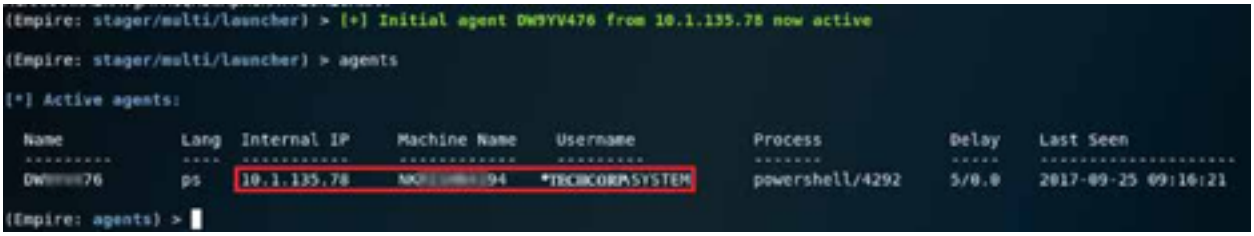
A list of cracked accounts captured using poisoned LLMNR responses.

The following week on Monday, 10/23, our penetration tester reached TechCorp's premises around 9:00 am and joined the network. The first operation performed was a tertiary scan of the Workstation IP address range, looking for key computer names that matched user names harvested from LLMNR hash gathering or phishing. One such computer was the NKRILLN machine to which the user account NKRILLN, whose credentials were phished the week prior, had local Administrative access to.



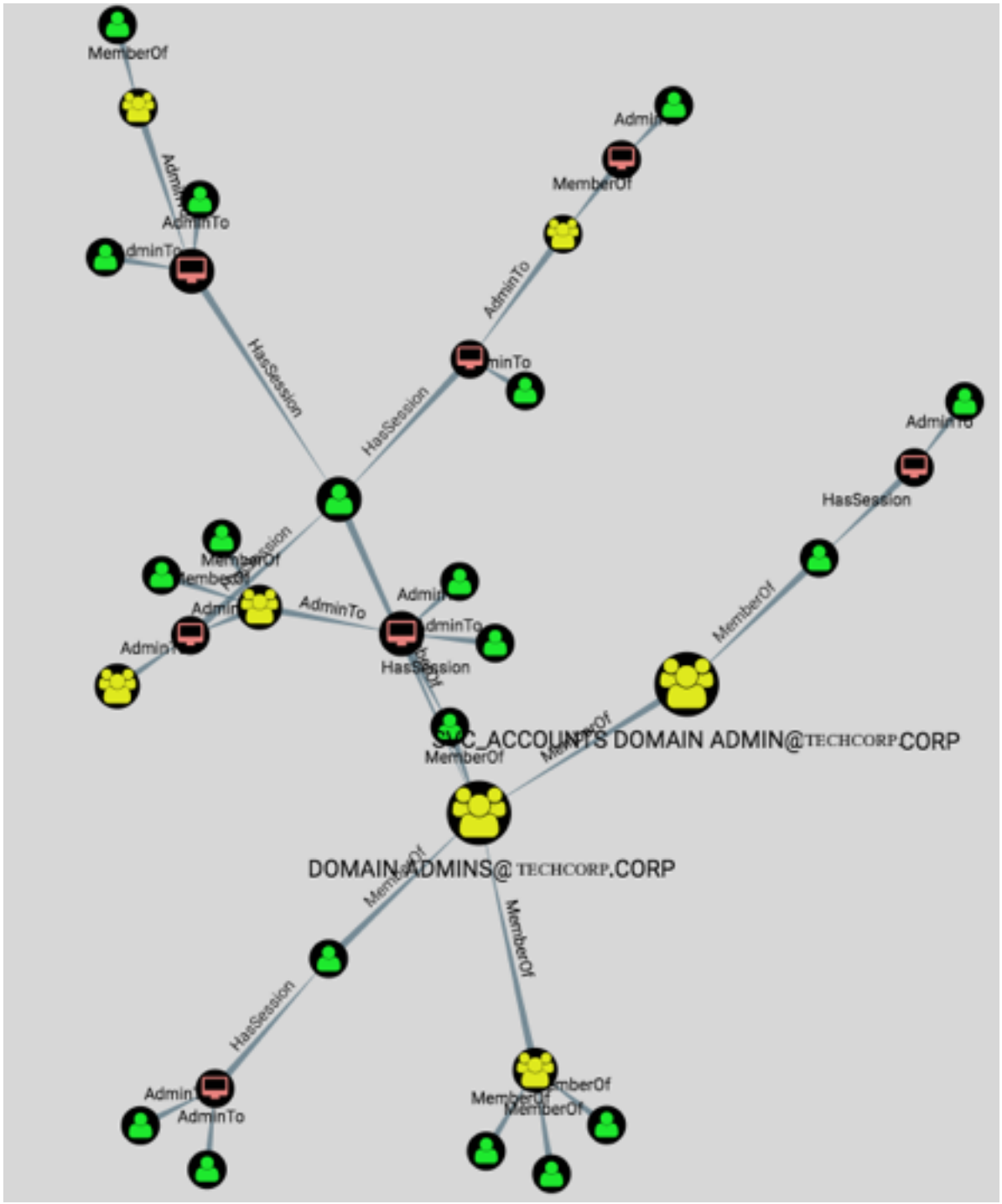
Above shows the assessor enumerating workstations on the 10.1.135.0/24 subnet, then authenticating to NKRILLN's account to their machine and extracting the password policy.

Using these credentials, we executed a PowerShell command over SMB to connect back to our command-and-control (C2) server at 10.1.135.66 and gain a session on the remote machine. This session was then used to enumerate all user sessions, trust relationships, group policies and administrative policies across the domain.

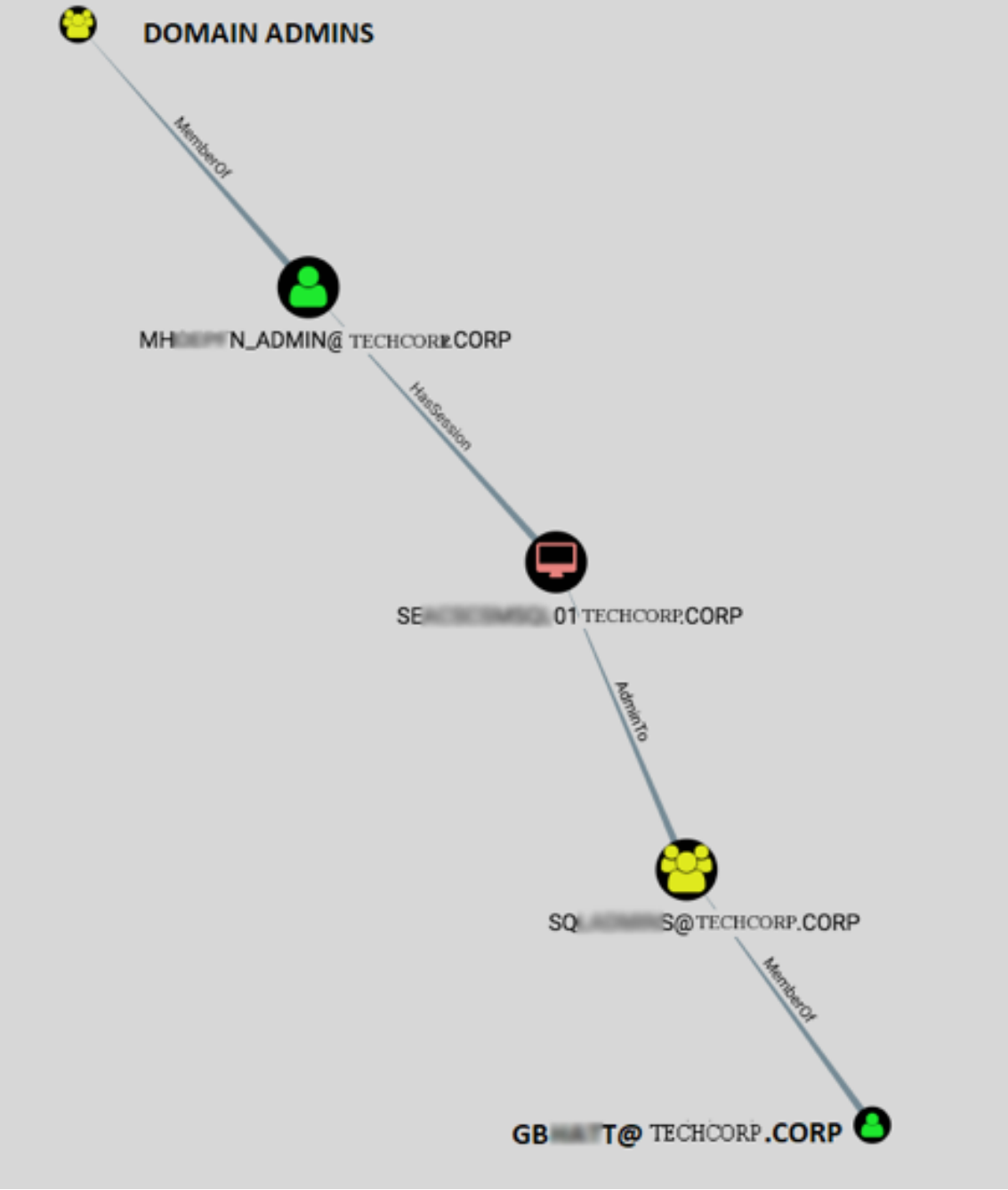


Above shows NKRILLN's machine connecting to our C2 server with elevated privileges.

The purpose of harvesting these policies is to determine how best to conduct what Microsoft calls an "Identity Snowball" attack. The idea of this attack is to roll the privileges of one user to gain control of another user account, and so on and so forth until we reach our target goal; which, in this case is control of a domain admin account and domain controller. The first image below shows all the potential paths to this goal (to gain control of an account in the Domain Admins group), and the second image shows the path we took.

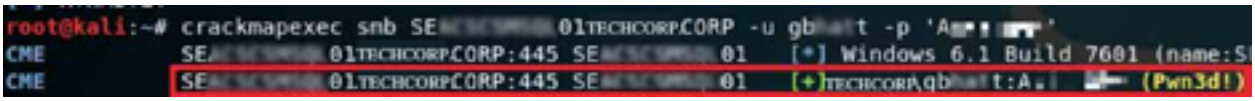


Above shows all the paths possible to gain a Domain Admin account.

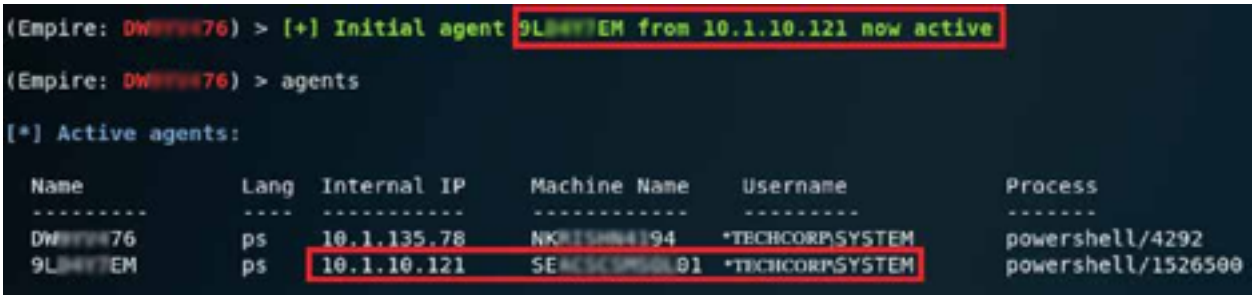


Above shows the path we took to Domain Admin.

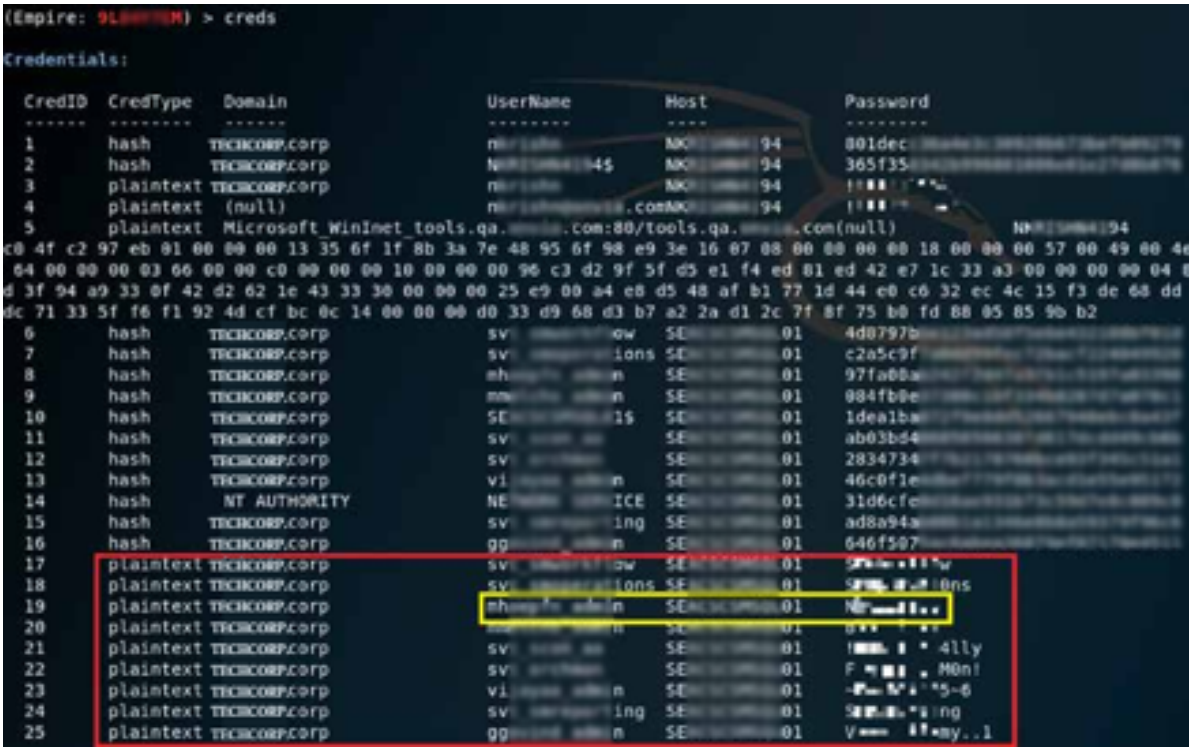
The path we took to the Domain Admins group started with the GBMETT user. This user's password was cracked offline by gathering his hashed password over LLMNR protocol when Chris was on-site. Knowing that he had local admin rights to the machine SEARODSQL01TechCorp.CORP meant that we could hijack the session MHORMEN_ADMINTechCorp.CORP had on the computer. If we could gain execution in this context, we would be able to pivot to the Domain Controller, as MHORMEN_ADMIN is a part of the Domain Admins group.



Above shows that indeed the GBMETT user could authenticate to SEARODSQL01TechCorp.CORP and is a local Admin.

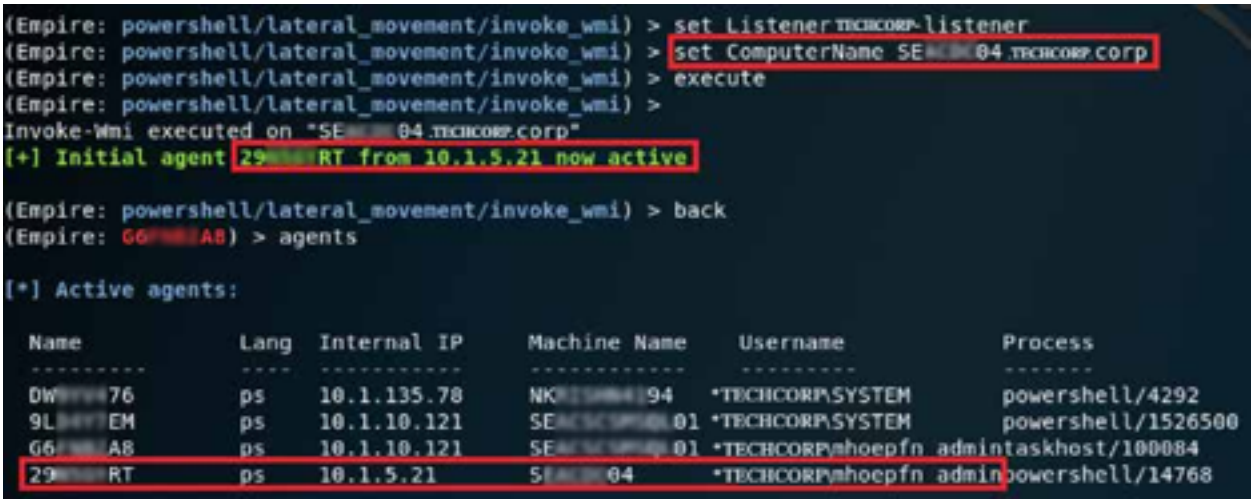


Above shows the SEAPRODSQL01.TechCorp.CORP machine communicating to our C2 server after the initial compromise.



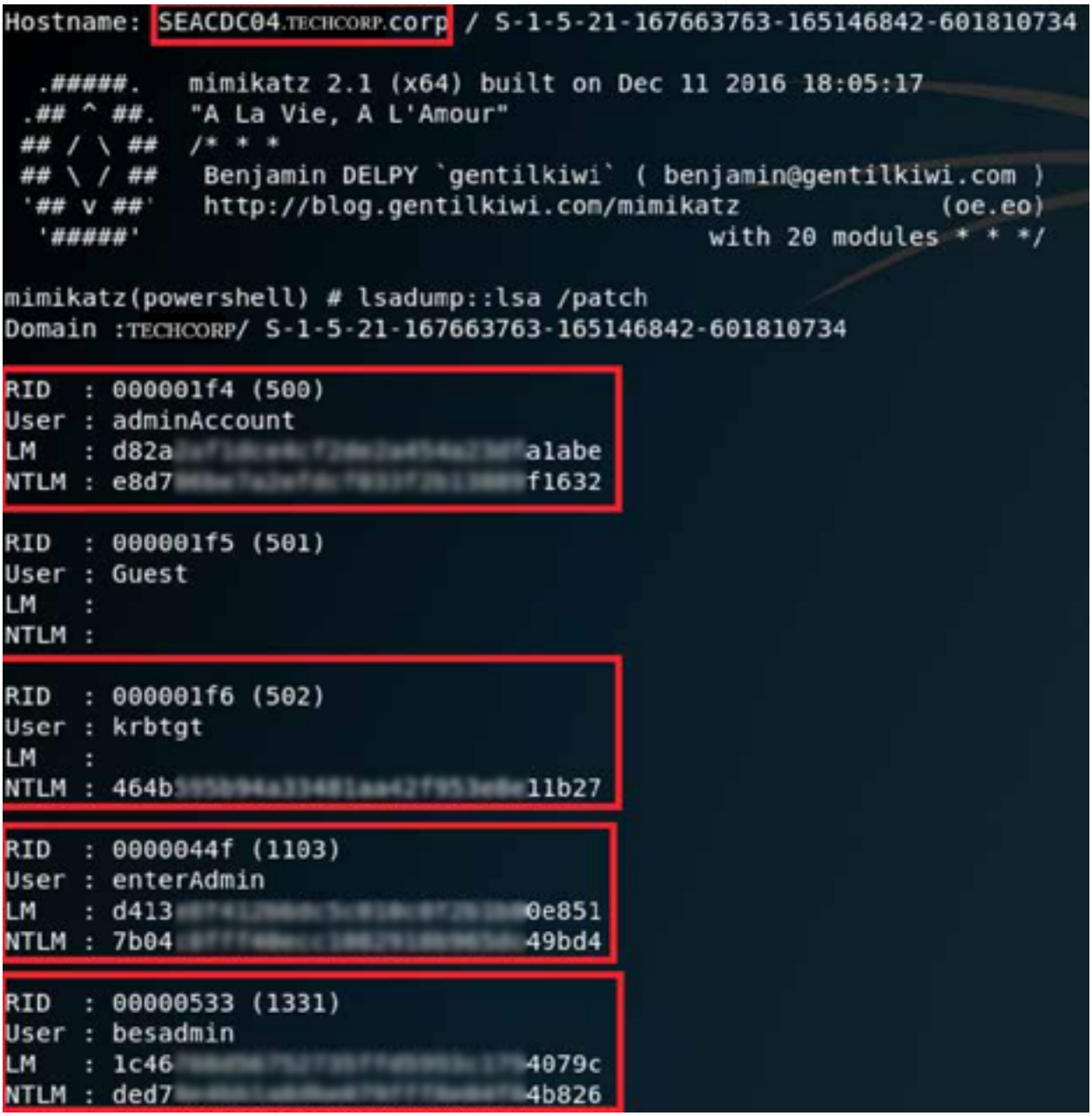
Above shows a list of credentials retrieved from memory (plaintext partially or wholly blurred) on the SEARODSQL01TechCorp.CORP machine. One such account was the MHORMEN_ADMIN account; however, the account password is not relevant due to his established session on the machine

We moved laterally from SEAPRODSQL to the Domain Controller SEAROD04 by invoking Windows Management Interface to launch a session back to our C2 server. Below shows an image of successful connection



Above shows the assessor spreading laterally to the Domain Controller using the context of MHORMEN_ADMIN.

After we established our Administrative session on the Domain Controller, we dumped the NTLM hashes of every user on the controller to demonstrate our control. Since we had local administrative access to every machine on the network, this ended the local privilege escalation of the internal audit at 10:00 am.



Above shows the hash dump of the user accounts in the primary domain, demonstrating a full compromise of the internal network and associated corporate environment. After communicating this objective completion to the client focal, the technical portion of the engagement concluded.

SCOPING AND RULES OF ENGAGEMENT

While real attackers have no limits on network penetration engagements, we do not engage in penetration testing activities that threaten our ethics and personal privacy.

Constraints

In addition, the following limitations were put into place:

- Vulnerabilities which would cause outages or interrupt the client's environment were noted but not validated.
- Penetration testing was limited to the agreed upon engagement period, scope, and other additional boundaries set in the contract and service agreement.

Scope of Service

The predetermined scope for Rhino Security Labs to carry out the Network Penetration Test was:

External Network

Assessment Type

External Blackbox

IP Address Ranges

208.10.10.10 - 208.10.10.20

Description

The external network portion of the assessment is considered blackbox and therefore little to zero information about the external network is given to the Rhino Security Assessment team before the engagement.

Sensitive Assets and Processes

As this engagement is considered blackbox, sensitive assets and processes of the external network were not disclosed to the Rhino Security Assessment team.

Internal Network

Assessment Type

External Graybox

IP Address

192.168.1.0 - 192.168.1.255

Description

The internal network portion of the assessment is considered graybox. This means the Rhino Security Team is given VPN credentials, a specified level of access, and specific flags or areas of concern to properly assess the internal network.

Sensitive Assets and Processes

TechCorp has expressed that the phone configuration is a particular area of concern as an outage would directly impact business. TechCorp is also concerned about a database of TPS Reports which contain sensitive information, so a concerted effort in this area is expected.

SUMMARY VULNERABILITY OVERVIEW

Rhino Security Labs performed an External/Internal Network Penetration Test for TechCorp, Inc. (TechCorp) on 10-12-2017 - 10-31-2017. This assessment utilized both commercial and proprietary tools for the initial mapping and reconnaissance of the site, as well as custom tools and scripts for unique vulnerabilities.

During the manual analysis, assessors attempted to leverage discovered vulnerabilities and test for key security flaws. The following vulnerabilities were determined to be of highest risk, based on several factors including asset criticality, threat likelihood, and vulnerability severity.

Vulnerability Risk Definition and Criteria

The risk ratings assigned to each vulnerability are determined by averaging several aspects of the exploit and the environment, including reputation, difficulty, and criticality.

CRITICAL Critical vulnerabilities pose a very high threat to a company's data, and should be fixed on a top-priority basis. They can allow a hacker to completely compromise the environment or cause other serious impacts to the security of the application

HIGH High severity vulnerabilities should be considered a top priority regarding mitigation. These are the most severe issues and generally, cause an immediate security concern to the enterprise

MEDIUM Medium severity vulnerabilities are a lower priority, but should still be remediated promptly. These are moderate exploits that have less of an impact on the environment.

LOW Low severity vulnerabilities are real but trivially impactful to the environment. These should only be remediated after the HIGH and MEDIUM vulnerabilities are resolved.

INFORMATIONAL Informational vulnerabilities have no impact as such to the environment by themselves. However, they might provide an attacker with information to exploit other vulnerabilities.

VULNERABILITY SUMMARY TABLE

The following vulnerabilities were found within each risk level. It is important to know that total vulnerabilities is not a factor in determining risk level. Risk level is depends upon the severity of the vulnerabilities found.

3	2	6	4	2
Critical	High	Medium	Low	Informational

Total Vulnerabilities: 17

Vulnerability ID - Name **Risk Level**

C1 - AWS S3 Bucket Data Leakage Vulnerability — CRITICAL

Remediation
Configure your S3 bucket to use the bare minimum access required for that group.

C2 - IPMI 2.0 Authentication Password Hash Exposure — CRITICAL

Remediation
Disable IPMI or restrict access to the affected IPMI service(s) using a firewall.

C3 - Windows "ETERNALBLUE" SMB Remote Code Execution Vulnerability — CRITICAL

Remediation
Apply all applicable security patches and updates from Microsoft's official website.

H1 - All Windows Users Running as Local Administrator — HIGH

Remediation
Ensure each user on the Windows system is only provided with the privileges necessary to perform their normal operations.

H2 - LLMNR and NBT-NS Broadcasting Enabled — HIGH

Remediation
Disable LLMNR and NBT-NS broadcasts.

M1 - F5 BIG-IP TLS Remote Memory Disclosure (Ticketbleed) — MEDIUM

Remediation
Update the affected F5 BIG-IP Appliance.

M2 - Splunk Enterprise < 6.0.6 Multiple Vulnerabilities — MEDIUM

Remediation
Upgrade to the latest version of Splunk.

M3 - Windows RDP Server Lacks Identity Validation (MITM Vulnerability) — MEDIUM

Remediation
Force SSL as the transport layer for the service and/or only allow computers with NLA.

M4 - Samba MITM "BadLock" Vulnerability — MEDIUM

Remediation
Update the Operating System and associated services to the latest version.

M5 - Windows SMB NULL Session Permitted — MEDIUM

Remediation
Disable Windows SMB null sessions affected hosts

M6 - NFS Volume is Publicly Mountable — MEDIUM

Remediation
Restrict mounting privileges to only hosts that require them.

L1 - ACME thttpd Webserver < 2.2.6 Multiple Vulnerabilities — LOW

Remediation
Upgrade to the latest version of Acme thttpd.

L2 - DNS Server Allows Cache Snooping — LOW

Remediation
Restrict the processing of DNS queries to only systems that should be allowed to use this nameserver.

L3 - OpenSSL SSL/TLS MITM Vulnerability — LOW

Remediation
Upgrade to the newest OpenSSL version (0.9.8za, 1.0.0m, 1.0.1h).

L4 - SMB Session Signing Disabled — LOW

Remediation
Enable, but don't require, SMB signing.

I1 - Weak TLS Diffie-Hellman Prime — INFORMATIONAL

Remediation
Configure the server to use 2048-bit or stronger Diffie-Hellman groups with safe primes.

I2 - ICMP Timestamp Response — INFORMATIONAL

Remediation
Disable ICMP timestamp responses.

VULNERABILITY FINDINGS

The vulnerabilities below were identified and verified by Rhino Security Labs during the process of this External/ Internal Network Penetration Test for TechCorp. Retesting should be planned following the remediation of these vulnerabilities.

C1 AWS S3 Bucket Data Leakage Vulnerability

Risk Rating: Critical

Exploitation Likelihood: **Critical**
Potential Impact: **Critical**

Description

AWS S3 bucket data leakage occurs when there is a misconfiguration of permissions for that bucket. Some common misconfigurations include public read access for files and public listing access for the buckets themselves. This can allow people to list the files from within your bucket, as well as read the contents of them. An attacker could potentially exploit "write" access to your files to add a key logger to a file that your application includes on its pages, such as a jQuery file. These settings need to be strictly set to prevent unauthorized actions.

Affected IP Address(es)

201.54.25.141
201.54.25.142
201.54.25.143

Remediation

By default, AWS S3 buckets permissions are set up to be very restrictive. It is important to remember that "Everyone" in IAM permissions literally means everyone on the Internet, and would immediately expose the full set of data to anyone who would request it. You need to confirm that only people/groups that you specify are able to "list" or "write" for your buckets. It is best practice to only allow the bare minimum permissions for different users who need access. You also need to confirm that for your individual files, only people/groups that you specify are able to "read" those files.

Testing Process

This vulnerability was discovered by running a custom script against the S3 bucket's domain to enumerate files and directories on the server.

Pictured are logs that were recovered when browsing the contents of the server.

```
djh@DESKTOP-LGBLNCJ:~$ sudo aws s3 ls s3://[redacted]/vi-logs/ --region
 fips-us-gov-west-1
sudo: unable to resolve host DESKTOP-LGBLNCJ
[sudo] password for djh:
2013-08-13 15:14:05        494 EZ1VZL85EGKF8.2013-08-13-20.6NGevHqa.gz
2013-08-13 15:36:04        498 EZ1VZL85EGKF8.2013-08-13-20.Af7A6rVI.gz
2013-08-13 15:16:47        836 EZ1VZL85EGKF8.2013-08-13-20.GZo0Glp0.gz
2013-08-13 15:34:17        426 EZ1VZL85EGKF8.2013-08-13-20.OGYcaTR8.gz
2013-08-13 15:20:10        398 EZ1VZL85EGKF8.2013-08-13-20.tY90D8SU.gz
2013-08-15 16:19:21        481 EZ1VZL85EGKF8.2013-08-15-21.sdxdYRvV.gz
```

Below are entire backups of the vulnerable S3 bucket.

```
djh@DESKTOP-LGBLNCJ:~$ sudo aws s3 ls s3://[redacted]/backups/redis1/ --r
egion fips-us-gov-west-1
sudo: unable to resolve host DESKTOP-LGBLNCJ
2011-07-18 03:30:53        260 2011.07.18.10.30.49.redis1.tar.gz.enc
2011-07-18 03:31:24   25158640 2011.07.18.10.31.13.redis1.tar.gz.enc
```

C2 IPMI 2.0 Authentication Password Hash Exposure

CVE-2013-4786

Risk Rating: Critical

Exploitation Likelihood: **Medium**
Potential Impact: **Critical**

Description

The IPMI 2.0 specification supports HMAC-SHA1 and HMAC-MD5 authentication, both of which send a computed hash to the client that can be used to mount an offline bruteforce attack of the configured password. This is an inherent flaw in the IPMI 2.0 protocol and cannot be fixed through a patch or update.

Affected IP Address(es)

201.54.25.141

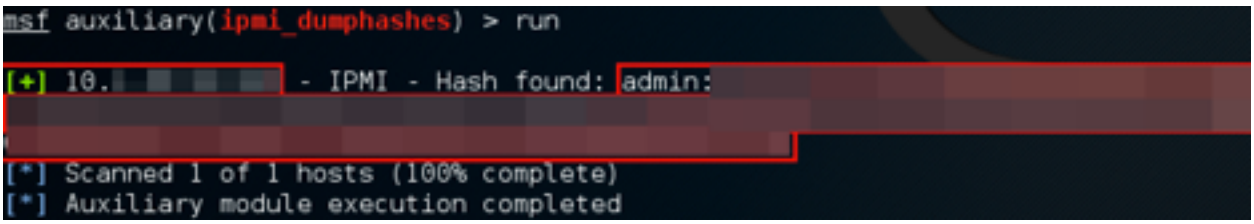
Remediation

Disable IPMI entirely by consulting your vendor's documentation or restrict access to the affected IPMI service(s) using a firewall or other appropriate technology.

Testing Process

This was detected by an automated scanner and confirmed by the assessor by retrieving the user account hashes.

Below shows the assessor gathering the IPMI root hash from the 192.168.4.37 host.



C3 Windows "ETERNALBLUE" SMB Remote Code Execution Vulnerability

MS17-010

Risk Rating: Critical

Exploitation Likelihood: **Medium**
Potential Impact: **Critical**

Description

Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code (See: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148).

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are exploits to the series of vulnerabilities disclosed on 2017/04/14 by a group known as the Shadow Brokers. The infamous WannaCry ransomware used the ETERNALBLUE exploit.

Affected IP Address(es)

192.168.4.125

Remediation

Update all affected Windows systems with the associated Microsoft patches:

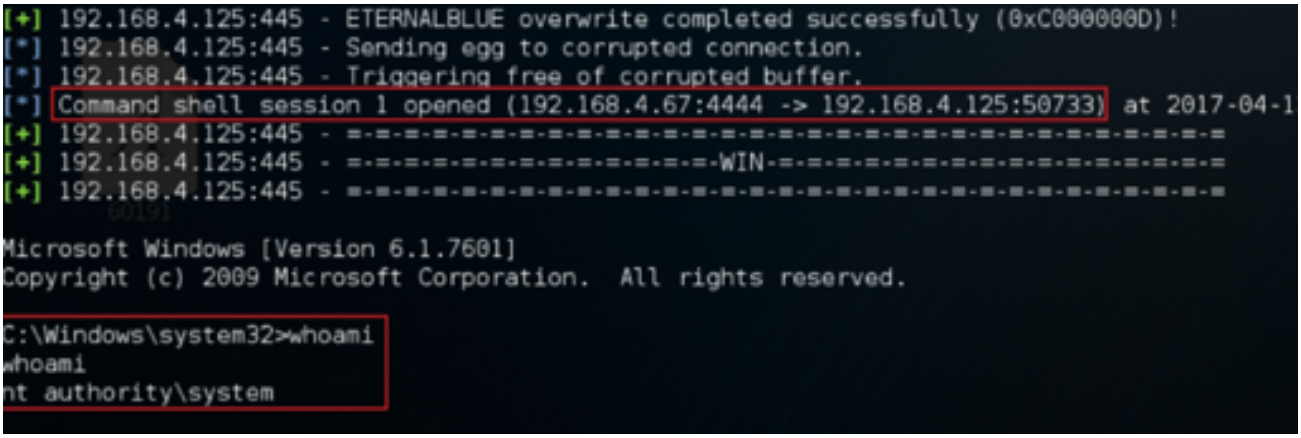
Windows Server 2016: KB4013429
Windows 10: KB4012606 / KB4013198
Windows Server 2012: KB4012214
Windows 8.1: KB4012213 / KB4012216
Windows 7: KB4012212 / KB4012215
Windows Server 2008: KB4012598
Windows Vista: KB4012598

Affected software and associated patching details are available here:
https://technet.microsoft.com/library/security/MS17-010#ID0EHB

Testing Process

This was initially identified by a vulnerability scanning tool, but then confirmed and exploited manually by the penetration tester.

Below shows the assessor opening a command shell with the host under SYSTEM privileges.



Assessor's Note: Due to the nature of this exploit there is a minor chance it can cause machines to crash upon exploitation. As such, we did not risk leverage it as we already had obtained Domain Admin.

H1 All Windows Users Running as Local Administrator

Risk Rating: High

Exploitation Likelihood: **High**
Potential Impact: **High**

Description

On Windows workstations, it is advised that day-to-day operations be performed on a Standard User account to reduce the impact of a successful malware or account compromise attack. Even on single-user systems, it is recommended to have both an Admin and Standard User account to separate permissions. This is significantly more important on systems and networks with a multitude of users, as even a single compromised workstation with local Administrator permissions can compromise the entire network.

Affected IP Address(es)

192.168.1.15
192.168.1.16

Remediation

Create an Administrator account only accessible to users who require additional permissions and provide each individual user with their own Standard User account. Existing accounts can be simply downgraded from admin status through the control panel on any account with administrator privileges.

Testing Process

After compromising either a system (via malware) or user account directly, the penetration tester was able to confirm the escalated privileges that enabled additional movement throughout the network.

H2 LLMNR and NBT-NS Broadcasting Enabled

Risk Rating: High

Exploitation Likelihood: **Medium**
Potential Impact: **Critical**

Description

LLMNR and NBT-NS protocols are used in name resolution on the network. When enabled, if a user or host fails DNS name resolution, the victim will then broadcast an LLMNR or NBT-NS request to see if other computers on the network know where the DNS entry is located.

An attacker on the local network can abuse these protocols by responding to broadcast requests, saying that they are the requested resource. Because of this, the victim will then send their Active Directory username and NTLMv2 password hash to the attacker. The attacker can then perform password cracking offline to recover the credentials.

Affected IP Address(es)

192.168.1.15
192.168.1.16

Remediation

1. Disable LLMNR and NBT-NS. You need to disable both because if LLMNR is disabled, a victim system will automatically attempt to use NBT-NS instead.
2. Prevent inter-VLAN communication - By limiting communication between hosts on the same network, you greatly reduce the success of most local network attacks.
3. Use limited user accounts - Now this won't prevent an attack, but it will limit the damage that a successful attack can do and at least make an attacker work harder. For example, if the victim is using domain administrator credentials, then a successful attack would give up the access to all machines on the network. On the other hand, if the victim is using a limited account, then the attacker will need to work harder to get further access in the environment.

Testing Process

The assessor turned on a responder server which replies to all queries across the network when a certain domain name for a file share cannot be found.

In total, 11 hashes were collected during the engagement but none we cracked using the word lists we had available.

M1 F5 BIG-IP TLS Remote Memory Disclosure (Ticketbleed) CVE-2016-9244

Risk Rating: Medium

Exploitation Likelihood: **Medium**
Potential Impact: **Medium**

Description

Based on its response to a resumed TLS connection, the F5 BIG-IP service appears to be affected by an information disclosure vulnerability, known as Ticketbeed, in the TLS Session Ticket implementation.

The issue is due to the server incorrectly echoing back 32 bytes of memory, even if the Session ID was shorter. A remote attacker can exploit this vulnerability, by providing a 1-byte Session ID, to disclose up to 31 bytes of uninitialized memory which may contain sensitive information such as private keys, passwords, and other sensitive data.

Note that this vulnerability is only exploitable if the non-default Session Tickets option enabled.

The F5 Advisory can be found here: https://support.f5.com/csp/article/K05121675

Affected IP Address(es)

192.168.1.15
192.168.1.16

Remediation

Update the affected F5 BIG-IP Appliance by navigating to https://downloads.f5.com and downloading the latest update ISO.

Testing Process

This was identified by an automated scanner and confirmed by the assessor.

M2 Splunk Enterprise < 6.0.6 Multiple Vulnerabilities

Risk Rating: Medium

Exploitation Likelihood: Medium
Potential Impact: Medium

Description

According to its version number, the Splunk Enterprise hosted on the remote web server is 6.0.x prior to 6.0.6. It is, therefore, affected by the following vulnerabilities:

The included OpenSSL library contains a TLS downgrade weakness. By using fragmented ClientHello messages, a remote, man-in-the-middle attacker can force a downgrade to TLS 1.0. (CVE-2014-3511)

A cross-site scripting vulnerability exists due to improper validation of user-supplied input when parsing events. This allows a remote attacker, using a specially crafted request, to execute arbitrary script code in the user's browser session within the trust relationship. (CVE-2014-8303)

For the Splunk Advisory, see here:
http://www.splunk.com/view/SP-CAAANHS

Affected IP Address(es)

192.168.1.15
192.168.1.16

Remediation

Upgrade to the latest version of Splunk.

Testing Process

This was identified by observing the version number displayed on the Splunk instance.

M3 Windows RDP Server Lacks Identity Validation (MITM Vulnerability) CVE-2005-1794

Risk Rating: Medium

Exploitation Likelihood: **Low**
Potential Impact: **Medium**

Description

The remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MITM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected. A MITM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials.

This flaw exists because the RDP server stores a hard-coded RSAprivate key in the mstlsapi.dll library. Any local user with access to this file (on any Windows system) can retrieve the key and use it for this attack.

See also:

http://www.oxid.it/downloads/rdp-gbu.pdf

http://technet.microsoft.com/en-us/library/cc782610.aspx

Affected IP Address(es)

192.168.1.15

192.168.1.16

Remediation

Force the use of SSL as a transport layer for this service if supported, and/or elect the `Allow connections only from computers running Remote Desktop with Network Level Authentication` setting if it is available.

Testing Process

This was identified using a tool called "Seth" available on GitHub here:

https://github.com/SySS-Research/Seth

M4 Samba MITM "BadLock" Vulnerability

CVE-2016-2118

Risk Rating: Medium

Exploitation Likelihood: Medium
Potential Impact: High

Description

The remote Windows host is affected by an elevation of privilege vulnerability in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels.

A man-in-the-middle attacker able to intercept communications between a client and a server hosting a SAM database can exploit this to force the authentication level to downgrade, allowing the attacker to impersonate an authenticated user and access the SAM database.

Affected IP Address(es)

192.168.1.15
192.168.1.16

Remediation

Update all affected Windows systems with the associated Microsoft patches:

Windows 10: KB3147461
Windows Vista/7/8.1: KB 3149090
Windows Server 2012: KB3149090
Windows Server 2008: KB3149090

Affected software and associated patching details are available here:
https://technet.microsoft.com/library/security/MS16-047

Testing Process

This vulnerability was detected by automated scanning and confirmed manually by the assessor.

M5 Windows SMB NULL Session Permitted

CVE-2015-0240

Risk Rating: Medium

Exploitation Likelihood: **Medium**
Potential Impact: **Medium**

Description

NULL sessions allow anonymous users to establish unauthenticated CIFS sessions with Windows or third-party CIFS implementations such as Samba or the Solaris CIFS Server.

These anonymous users may be able to enumerate local users, groups, servers, shares, domains, domain policies, and may be able to access various MSRPC services through RPC function calls. These services have been historically affected by numerous vulnerabilities. The wealth of information available to attackers through NULL sessions may also allow them to carry out more sophisticated attacks.

Affected IP Address(es)

192.168.1.15
192.168.1.16

Remediation

Disable Windows SMB null sessions affected hosts.

Testing Process

This was discovered by a vulnerability scanning tool and manually confirmed and exploited by the pentester.

M6 NFS Volume is Publicly Mountable

CVE-2015-7358

Risk Rating: Medium

Exploitation Likelihood: **High**
Potential Impact: **Medium**

Description

An NFS volume on the the target host is mountable by everyone. Although this is not necessarily a vulnerability itself, this does not exhibit "best practice" from a security standpoint; mounting privileges should be restricted only to hosts that require them.

Affected IP Address(es)

192.168.1.15
192.168.1.16

Remediation

Restrict mounting privileges to only hosts that require them.

Testing Process

In this case, the host was a Linux machine, which can be easily remotely identified as allowing volumes to be mounted.

L1 ACME thttpd Webserver < 2.2.6 Multiple Vulnerabilities

Risk Rating: Low

Exploitation Likelihood: **Low**
Potential Impact: **Low**

Description

According to its banner, the version of Acme thttpd server running on the remote host is prior to 2.26. It is, therefore, affected by multiple vulnerabilities:

- Multiple buffer overflow conditions exist in the htpasswd utility. A local attacker can exploit these, by calling htpasswd and supplying arbitrary commands along with a username to be added to the password file, to bypass required authentication and execute arbitrary programs with elevated privileges. (CVE-2006-1078)
- A flaw exists in htpasswd that allows a local attacker to gain privileges via shell metacharacters in a command line argument, which can then be used to execute other commands. (CVE-2006-1079)
- An unspecified flaw exists that allows a local attacker to create or touch arbitrary files via a symlink attack on the start_thttpd temporary file. (CVE-2006-4248)

Affected IP Address(es)

192.168.1.15
192.168.1.16

Remediation

Upgrade to the latest version of Acme thttpd.

Testing Process

This vulnerability was identified by the version number returned in the HTTP Response header.

L2 DNS Server Allows Cache Snooping

Risk Rating: Low

Exploitation Likelihood: **Low**
Potential Impact: **Low**

Description

This DNS server is susceptible to DNS cache snooping, whereby an attacker can make non-recursive queries to a DNS server, looking for records potentially already resolved by this DNS server for other clients. Depending on the response, an attacker can use this information to potentially launch other attacks.

Affected IP Address(es)

192.168.1.15
192.168.1.16

Remediation

Restrict the processing of DNS queries to only systems that should be allowed to use this nameserver.

Testing Process

NSE (Nmap Scripting Engine) was used to test for DNS Cache Snooping with a given list of test domains. In reviewing these, the affected host was identified as being vulnerable.

L3 OpenSSL SSL/TLS MITM Vulnerability

Risk Rating: Low

Exploitation Likelihood: **Low**
Potential Impact: **Low**

Description

OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the "CCS Injection" vulnerability.

Affected IP Address(es)

192.168.1.15
192.168.1.16

Remediation

Upgrade to the newest OpenSSL version (0.9.8za, 1.0.0m, 1.0.1h).

Testing Process

The SSL session persisted after an invalid change cipher spec request was sent, indicating the version of SSL is vulnerable to ChangeCipherSpec MitM.

L4 SMB Session Signing Disabled

CVE-2002-1256

Risk Rating: Low

Exploitation Likelihood: **Low**
Potential Impact: **Medium**

Description

This system has SMB signing disabled. SMB signing allows the recipient of SMB packets to confirm their authenticity and helps prevent man in the middle attacks against SMB. SMB signing can be configured in one of three ways: disabled entirely (least secure), enabled, and required (most secure).

Affected IP Address(es)

192.168.1.15
192.168.1.16

Remediation

SMB signing can be configured in one of three ways: disabled entirely (least secure), enabled, and required (most secure). We recommend using enabling, but not requiring, signing due to the complex tradeoff of security and functionality in SMB.

Testing Process

This vulnerability was tested by initiating an SMB session and negotiating the security mode of the traffic. The client returned with a ''security mode 3'', indicating signing is disabled.

I1 Weak TLS Diffie-Hellman Prime

CVE-2015-4000

Risk Rating: Informational

Exploitation Likelihood: **Informational**
Potential Impact: **Informational**

Description

The TLS server uses a Diffie-Hellman group with a prime modulus of less than 1024 bits in length. Current estimates are that that an academic team can break a 768-bit prime and that a state-level actor can break a 1024-bit prime.

Affected IP Address(es)

192.168.1.15
192.168.1.16

Remediation

Configure the server to use 2048-bit or stronger Diffie-Hellman groups with safe primes.

Testing Process

The SSL Implementation on the server was tested and a weak DH-prime was detected.

I2 ICMP Timestamp Response

Risk Rating: Informational

Exploitation Likelihood: **Informational**
Potential Impact: **Informational**

Description

The remote host responded to an ICMP timestamp request. The ICMP timestamp response contains the remote host's date and time. This information could theoretically be used against some systems to exploit weak time-based random number generators in other services.

In addition, the versions of some operating systems can be accurately fingerprinted by analyzing their responses to invalid ICMP timestamp request

Affected IP Address(es)

192.168.1.15
192.168.1.16

Remediation

Disable ICMP timestamp responses. Refer to the software's documentation for specific instructions. Keep in mind some operating systems don't allow you to block ICMP packets, so you'll have to block them at the firewall.

Testing Process

This vulnerability was detected by automated scanning, and confirmed manually by the penetration testers.

APPENDIX A: TOOLS & SCRIPTS

The software and tools used for security analysis are constantly evolving and changing. To stay at the forefront of industry trends, Rhino Security Labs regularly updates and integrates new tools into its social engineering methodology. Below is the toolset our consultants use during a social engineering assessment.

Enterprise and Open Source Tools

Nmap

Nmap is a powerful network security scanning application that uses carefully crafted packets to probe target networks and discover exposed open ports, services, and other host details, such as operating system type.

NeXpose

An enterprise-grade vulnerability assessment tool used to identify many common vulnerabilities in both physical and virtualized systems.

Metasploit Pro

An open-core commercial Metasploit edition for penetration testers. Metasploit Pro includes modules for tracking emails that have been opened, if and when their links have been opened, if their attachments were downloaded and ran, if a user submitted their credentials to a malicious domain and more.

Nessus

Nessus is a proprietary vulnerability scanner that specializes in delivering comprehensive mappings of target system vulnerabilities, including web and network vulnerabilities, misconfigurations, weak passwords and even compliance problems, such as with HIPAA and PCI.

FOCA

FOCA is used for extracting hidden information and metadata from various sources. Examples include pulling names and emails from Word document files, application versions from PDF's, and more. This can be used for specific targeting of users and companies in phishing and other social engineering engagements.

Rhino Security Labs Proprietary Tools and Scripts

Additional Custom Scripts and Application

In addition to the above tools, Rhino Security Labs also makes use of its own proprietary tools and scripts to quickly adapt to new and unique environments.

APPENDIX B: LIST OF CHANGES MADE TO TECHCORP SYSTEMS

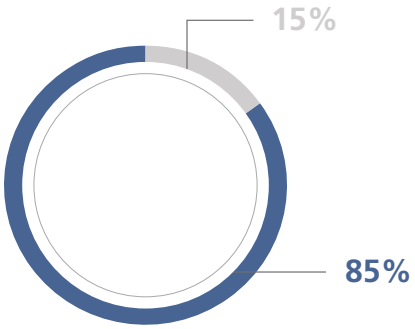
The following changes were made to the environment in scope. These do not necessarily represent a significant impact to the environment, but are included for the full accounting of modifications by the penetration testing team at Rhino Security Labs.

Affected Area	No changes were made to the environment in scope, such as creating new user accounts or uploading files to the target system. This is provided as the full accounting of modifications by the penetration testing team at Rhino Security Labs.

APPENDIX C: PASSWORD COMPLEXITY/RISK

During this penetration test, a number of encrypted (hashed) passwords were obtained, and password cracking attempted. While weak hashing algorithms are listed as separate findings above, below is the breakdown of password risk, based on the results of internal password cracking.

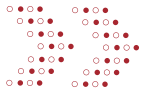
For ease of use, password length by default assumes a uppercase/lowercase/digits in the password. Passwords with special characters (or not containing the assumed character map) have risks raised or lowered as appropriate. Raw results of passwords are not included in this report, but can be requested if required.



Captured Password Hashes:	**1082**	
Hashes Cracked:	**144**	**15%**
Hashes Uncracked:	**938**	**85%**

31	39	65	9	794
Critical	**High**	**Medium**	**Low**	**Very Low**

Risk Level	Defined By:
CRITICAL	Top 1000 most common passwords, or less than 6 character password length
HIGH	Company name in the password, or 6-7 character password length
MEDIUM	8-11 character password length
LOW	12-16+ character password length
VERY LOW	Hash uncracked in allotted time (length/complexity unknown).



PASSWORD CRACKING SPEED (BY HASH ALGORITHM)

While successful password cracking often relies on weak or short passwords, the hashing algorithms themselves make a difference as well. To demonstrate each algorithms risk of password cracking (relative to one another)

Hashes on this network:

NetNTLMv2 (Extracted from internal network):	~13 billion hashes per second
NTLM (Extracted from Domain Controller):	~334 billion hashes per second
LM (Extracted from Domain Controller):	~148 billion hashes per second

Note: The LM hash algorithm contains a range of cryptographic weaknesses and is a critical risk for password cracking, despite being slower than its replacement, NTLM)

Comparison Hashes:

MD5:	~200 billion hashes per second
SHA1:	~68 billion hashes per second
SHA512:	~8 billion hashes per second
bcrypt:	~105,000 hashes per second

888.944.8679
info@rhinosecuritylabs.com
1200 East Pike Street Suite 510 | Seattle, WA 98122