Pentera™
Penetration Test
Summary Report

The Pentera™ automated penetration test report summarizes the vulnerabilities, exploit achievements, and remediation action items recommended in your network based on the latest ethical hacking pentesting techniques.

Disclaimer:
For security reasons, this report is anonymized and excludes sensitive data

PENTERA

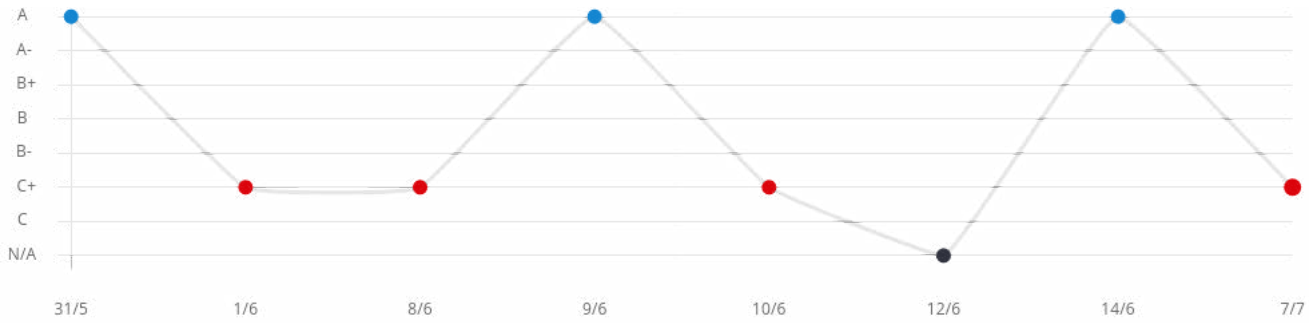
TABLE OF CONTENTS

Executive Summary

Cyber Resilience Score & Settings

Name:	**BB-Stealthy**
Description:	Black Box Test - Stealthy Attacker - Weekly
Type:	**Penetration Testing (Black Box)**
Time & Duration:	Jul 07 2023 12:02 - Jul 07 2023 14:30, 02:28
Included IP Range(s):	**192.168.90.0 - 192.168.90.9, 192....** 2 Ranges
Action Approval Score:	20% – 30/152
User Input:	**2 - IP Range(s)**

Resilience Score Over Last 8 Tasks



Resilience Score Card

Critical Assets — Low
Congratulations! Pentera wasn't able to compromise any critical assets in your network

Credentials and Account Takeover — Critical
Gained access to 16 accounts (14 of them privileged): 14 Local administrator user(s), 1 Unix/Linux user(s) and 1 network service user(s)

Sniffing — Medium
Sniffed 1 credentials and performed 11 relay attacks

Password Strength — High
Cracked 5 out of 16 passwords: 4 Strong, 1 Easy

Lateral Movement — Medium
Performed lateral movement to 1 Windows Workstation(s), 1 Windows Server(s) and 1 Unix/Linux host(s)

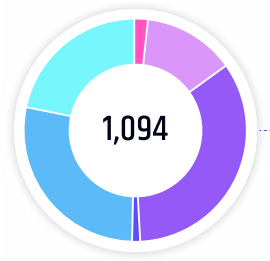
Accessible Data — Critical
Gained access to 358660 File(s), 11 Hosts (with complete access) and 1 Network service(s)

Host Takeover — Critical
Pentera was able to 'take over'[1] 11 out of 28 hosts (39%): 5 Windows Workstation(s), 4 Windows Server(s) and 2 Unix/Linux host(s)

AV/EDR Bypass — Low
Congratulations! Pentera wasn't able to bypass your Antivirus/EDR solutions

External Attack Surface – Key Findings

Asset Inventory



- 10 Domains
- 163 Subdomains
- 361 IP Addresses
- 5 Networks
- 324 Services
- 231 Websites

231 Websites	56 Critical	175 High	85 Medium	57 Low
324 Services	37 Critical	55 High	34 Medium	568 Low
361 IP Addresses	25 Critical	3 High	12 Medium	81 Low

Achievements

9.8	**Executed copy command**	3 occurrences
9.8	**Exploited CVE-2020-1938 on Apache Tomcat**	2 occurrences
9.4	**Gathered valuable information from host**	1 occurrences

Vulnerabilities

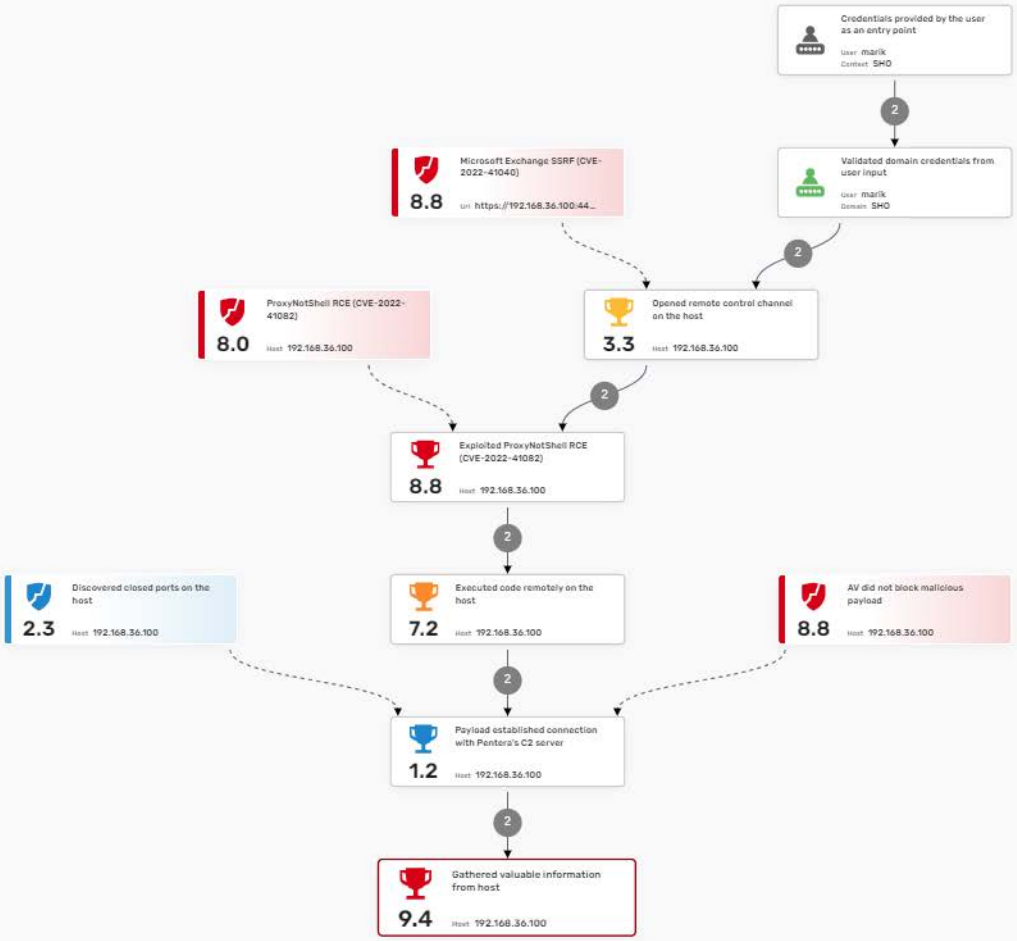
9.9	**ASP.NET Insecure Deserialization**	5 occurrences
9.8	**Oracle WebLogic RCE (CVE-2020-14882)**	2 occurrences
6.5	**Citrix ADC unauthenticated access (CVE-2020-8193)**	2 occurrences

Attractions

Extreme	**Potential Log4Shell (CVE-2021-44228)**	6 occurrences
Serious	**Website using self-signed certificate**	20 occurrences
Serious	**Website using expired certificate**	7 occurrences

Internal Attack Surface – Key Findings

Attack Vectors



Achievements

Pentera accomplished 158 achievements in total. Every achievement represents a discrete successful action performed by Pentera.

10
Severity

(1) Created Domain Admin user

An attacker may create a user with domain admin privileges in order to persist his existence in the network. It is recommended to monitor activity in privileged user groups and keep track of any changes in privileged users especially when adding a new domain admin.

9.8
Severity

(1) Exploited CVE-2019-19781 on Citrix ADC server

By exploiting this vulnerability, an unauthenticated attacker could execute arbitrary code remotely as high privileged user via a directory traversal vulnerability.

9.4
Severity

(10) Gathered valuable information from host

An attacker might find sensitive information and credentials on the host that might help in further attacks

Vulnerabilities

21 Critical	8 High	8 Medium	22 Low

Pentera identified a total of 59 vulnerability occurrences across 4 severity levels

#1 Remediation Priority [1]

4.7 Severity

Host can be forced to authenticate by a rogue server

1 occurrences

In cases where the DNS server fails in name resolution queries, the LLMNR, NetBIOS-NS and mDNS services attempt to resolve them. Since those are a broadcast protocols, anyone can respond to the query. An attacker may refer the request to a machine in his control using a man-in-the-middle attack, And obtain sensitive data such as username and password hash.

#2 Remediation

5.8 Severity

SMB server on endpoint does not validate clients

1 occurrences

#3 Remediation Priority [1]

9.8 Severity

CVE-2019-19781

1 occurrences

Accessible Shared Files

Pentera was able to gain access to 351802 files, 101290 folders, over 1 shares

Shares with **Anonymous** User access

0 Folders	0 Files

Shares with **Domain** User access

101290 Folders	351802 Files

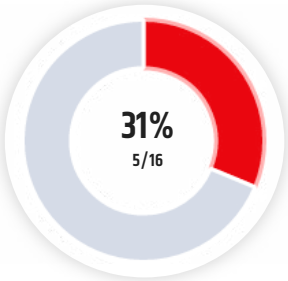
Open Shares with Domain User Access

Host	Share	Details
WIN10B	C$	Contains 101290 folders and 351802 files.

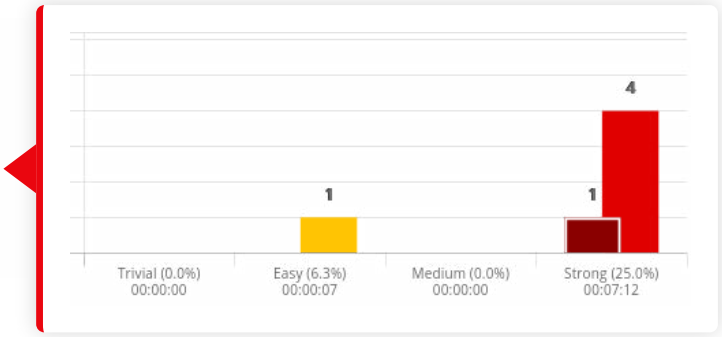
Identity Strength

Cracked Passwords

Cracking Success Rate



Cracking Difficulty



Non-privileged Users: trivial easy medium strong privileged users

Leaked Credentials

48

Users Compromised by the Leaked Data

Active Directory users that Pentera was able to compromise using the leaked data.

1,186

Total Leaked Data

Leaked data entries associated with your organization gathered from third parties, the darknet, and other sources.

6.2
Severity

Password can be cracked leveraging leaked username and medium GPU effort

21 occurrences

Attackers can leverage leaked usernames found or sold on the darknet to gain initial access into the organization. Leaked usernames pose a risk because they can be leveraged in dictionary attacks and enhance password cracking techniques.

leaked email: william.***@******.com	leaked email: matt.***@******.com	leaked email: chris.***@******.com
leaked email: javier.***@******.com	leaked email: jennie.***@******.com	leaked email: jacob.***@******.com

4.7
Severity

Password can be cracked using a custom dictionary and high GPU effort

3 occurrences

Many password cracking tools rely on dictionary rulesets, so it is important to avoid common passwords (such as Aa123456 or P@ssw0rd) and regular, unmodified dictionary terms. Inserting intentional, idiosyncratic misspellings or using acronyms is the recommended best practice. You can enhance Pentera's cracking abilities by uploading a custom wordlist to Pentera's Custom Dictionary and retest to uncover passwords that could be predicted or guessed by attackers who invest in social engineering techniques and are familiar with their targets.

leaked email: elizabeth.***@******.com	mon***	anna.***

Ransomware Readiness

Percentage of hosts that proved resilient to ransomware. Excludes hosts with no files to test

Type	**Maze Ransomware Emulation**
Time	Apr 20, 2023, 13:04 - Apr 21, 2023, 13:15
Test Name	**Automated_Maze_(2022,04,20)_v5.2.2**
Description	20042023 Advanced Targeted Testing
IP Ranges	172.20.3.0 - 172.20.3.255, 172.21.5.0.... 2 Ranges
Data Exfiltration to	Designated C2
Targeted Hosts of Testing Candidates*	80% (80 / 100)

Action Success Rate

55% (6 of 11)

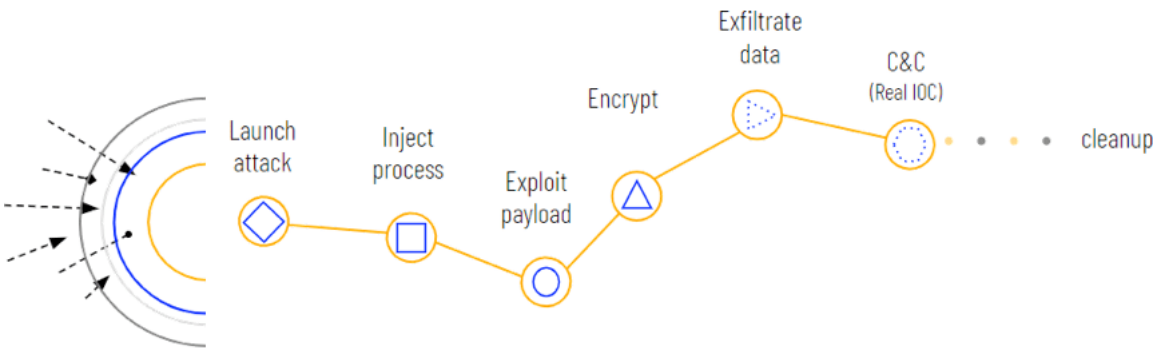
Payload Launch	**55%**
File Enumeration	**100%**
Process Manipulation	**0%**
Encryption	**100%**
Data Exfiltration	**100%**
Host Modification	**100%**

AV / EDR Bypass
65 Hosts
Encrypted files while bypassing endpoint security controls

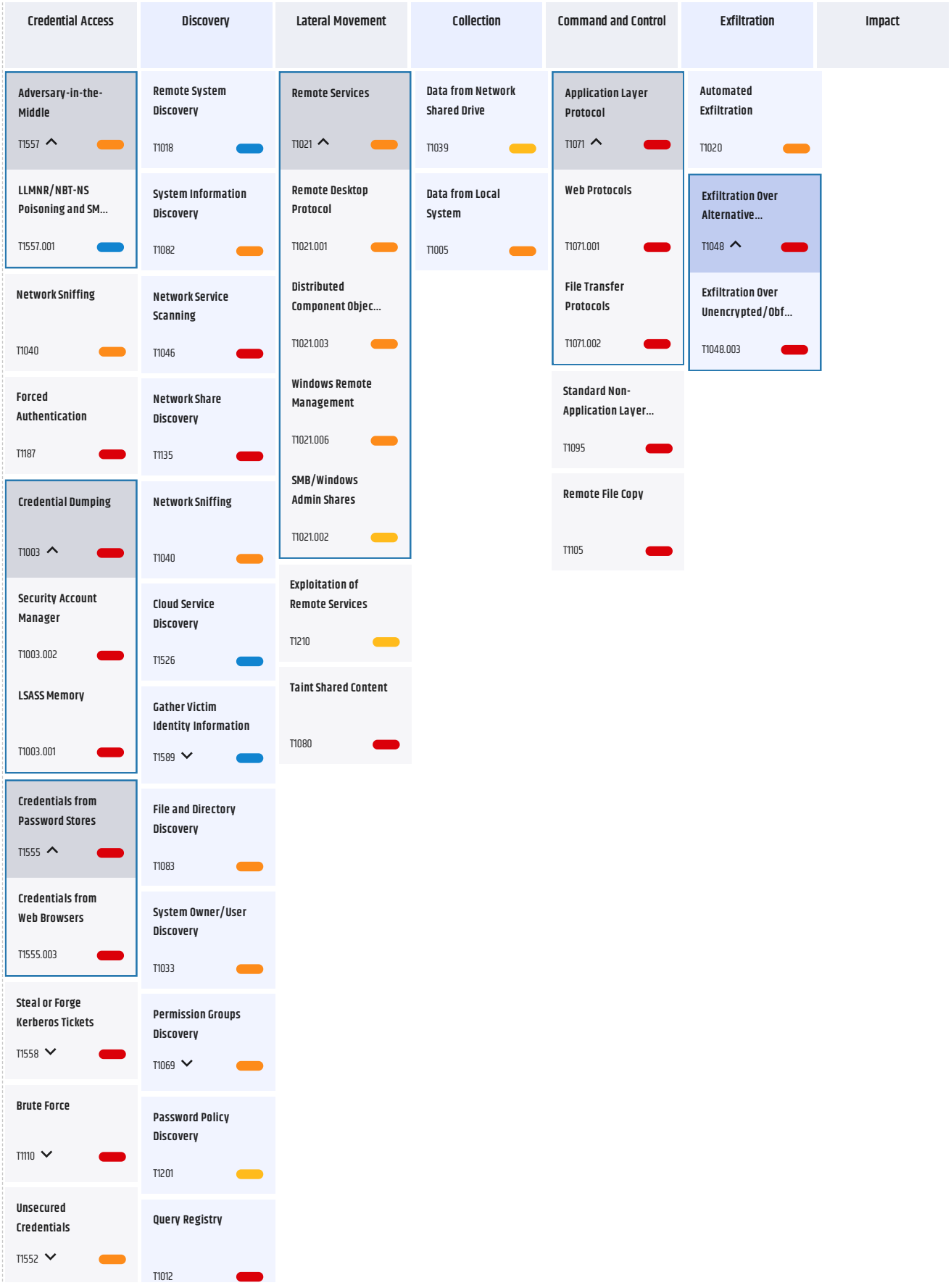
Ransomware Completed
60 Hosts
Performed all campaign-related actions

Ransomware Interrupted
15 Hosts
Interrupted by security controls or network connectivity issues

Found No Files To Encrypt
5 Hosts
Targeted standard user-related files



MITRE ATT&CK Heat Map



Remediation Wiki

Name Resolution Protocols (LLMNR/NBNS/mDNS)

MITRE

LLMNR/NBT-NS Poisoning and Relay (T1171)

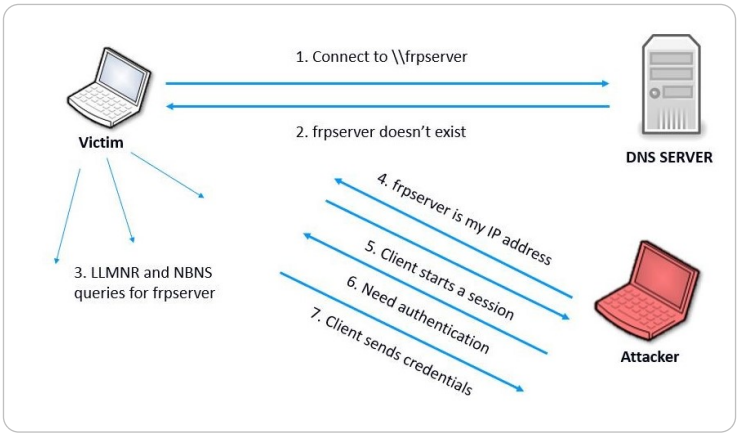
Insight

LLMNR (Link-Local Multicast Name Resolution), NBNS (Netbios Name Service) and mDNS (Multicast Domain Name Service) are Microsoft Windows protocols which serve as alternate methods of Name Resolution. If a machine tries to resolve a particular host, but DNS resolution fails, the machine will then attempt to ask all other machines on the local network for the correct address via LLMNR, NBNS or mDNS. Since this operation is performed using broadcast or multicast queries with no means of validation, it is susceptible to malicious answers distributed by an attacker, effectively poisoning the network.

Impact

An attacker can listen on a network for these LLMNR (UDP/5355) or NBNS (UDP/137) broadcasts and respond to them, pretending that the location of the requested host is at the attacker's machine.

Let's look at an example in the diagram below:



1. The victim machine wants to go the print server at \\ftpserver, but mistakenly types in \\frpserver
2. The DNS server responds to the victim that no dns record was found
3. The victim turn to the network and asks by using LLMNR or NBNS if there is anyone knows the location of \\pntserver
4. The attacker responds to the victim that \\pntserver is his own IP address
5. The victim believes the attacker and starts a session with him
6. The attacker asks the victim to authenticate
7. The client sends its credentials (NTLMv1 / NTLMv2)
8. The attacker can now crack the hash to discover the password

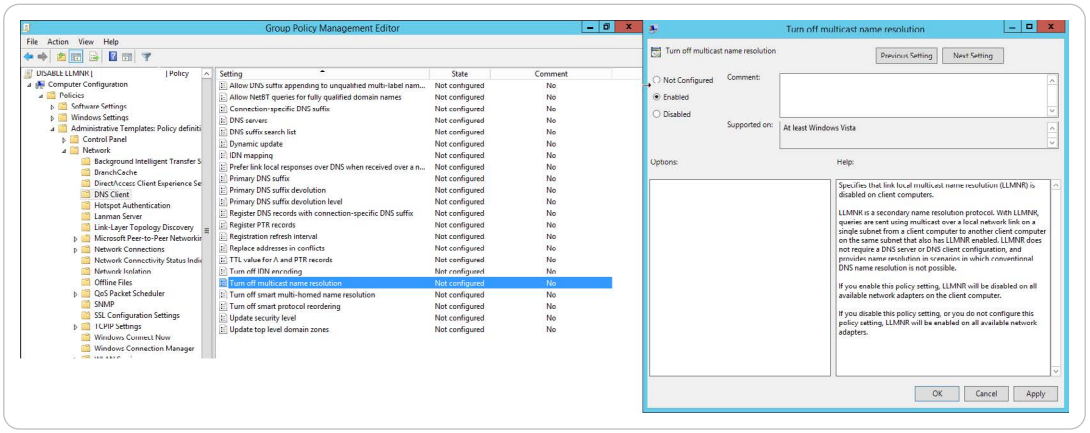
Recommendations

Disable the protocols: mDNS, LLMNR, and NBNS.

Disable mDNS

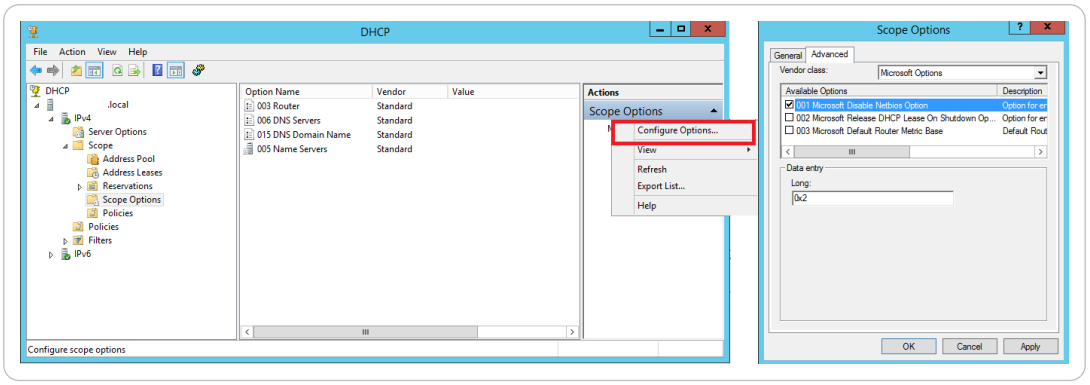
There is a `mDNSResponder.exe` process that belongs to the `Bonjour Service` in Windows, which is Apple's "Zero Configuration Networking" application, typically installed automatically by iTunes, Skype and others. It can be disabled by using GPO.

Disable LLMNR via GPO



1. Create a new GPO record for all computers in the environment.
2. Navigate to **Local Computer Policy / Computer Configuration / Administrative Templates / Network / DNS Client**.
3. Set **Turn Off Multicast Name Resolution** to **Enabled**.

Disable NBNS in a DHCP enviroment



1. Go to DHCP Management
2. Go to "scope options" for the network you are changing
3. Right click and Configure Options
4. Select Advanced tab and change "Vendor class" to "Microsoft Options"
5. In the "Available Options" frame, select and check the box "001 Microsoft Disable Netbios Option"
6. In the "Data Entry" frame, change the data entry to 0x2
7. Click "OK". The new settings will take affect when the clients renew their addresses.

Disable NBNS on a single host

1. Open the **Control Panel** > **Network and Sharing Center**.
2. Select **Change adapter settings**.