Text, logo

Description automatically generated with medium confidence



Network Penetration Test

**Report of Findings**

**HTB Certified Penetration Testing Specialist (CPTS) Exam Report**

**Candidate Name: <FULL NAME HERE>**

**Trilocor Robotics**

Month Day, Year

Version 1.0

Table of Contents

[Statement of Confidentiality 3](#_Toc113515291)

[Engagement Contacts 4](#_Toc113515292)

[Executive Summary 5](#_Toc113515293)

[Approach 5](#_Toc113515294)

[Scope 6](#_Toc113515295)

[Assessment Overview and Recommendations 6](#_Toc113515296)

[Network Penetration Test Assessment Summary 7](#_Toc113515297)

[Summary of Findings 7](#_Toc113515298)

[Internal Network Compromise Walkthrough 8](#_Toc113515299)

[Detailed Walkthrough 8](#_Toc113515300)

[Remediation Summary 12](#_Toc113515301)

[Short Term 12](#_Toc113515302)

[Medium Term 12](#_Toc113515303)

[Long Term 12](#_Toc113515304)

[Technical Findings Details 13](#_Toc113515305)

[Appendices 18](#_Toc113515306)

[Appendix A – Finding Severities 18](#_Toc113515307)

[Appendix B – Host & Service Discovery 19](#_Toc113515308)

[Appendix C – Subdomain Discovery 20](#_Toc113515309)

[Appendix D – Exploited Hosts 21](#_Toc113515310)

[Appendix E – Compromised Users 22](#_Toc113515311)

[Appendix F – Changes/Host Cleanup 23](#_Toc113515312)

[Appendix G – Flags Discovered 24](#_Toc113515313)

# Statement of Confidentiality

The contents of this document have been developed by Hack The Box. Hack The Box considers the contents of this document to be proprietary and business confidential information. This information is to be used only in the performance of its intended use. This document may not be released to another vendor, business partner or contractor without prior written consent from Hack The Box. Additionally, no portion of this document may be communicated, reproduced, copied or distributed without the prior consent of Hack The Box.

The contents of this document do not constitute legal advice. Hack The Box’s offer of services that relate to compliance, litigation or other legal interests are not intended as legal counsel and should not be taken as such. The assessment detailed herein is against a fictional company for training and examination purposes, and the vulnerabilities in no way affect Hack The Box external or internal infrastructure.

# Engagement Contacts

|  |  |  |
| --- | --- | --- |
| Trilocor Contacts | | |
| **Primary Contact** | **Title** | **Primary Contact Email** |
| Yelon Husk | Chief Executive Officer | [yelon@trilocor.local](mailto:yelon@trilocor.local) |
| **Secondary Contact** | **Title** | **Secondary Contact Email** |
| Ben Rollin | Chief Technical Officer | [ben@trilocor.local](mailto:ben@trilocor.local) |

|  |  |  |
| --- | --- | --- |
| Assessor Contact | | |
| **Assessor Name** | **Title** | **Assessor Contact Email** |
| <Candidate Name> | Security Consultant | <Candidate Email> |

# Executive Summary

Trilocor Robotics Ltd. (“Trilocor” herein) contracted <ASSESSOR NAME> to perform a Network Penetration Test of Trilocor’s externally facing network to identify security weaknesses, determine the impact to Trilocor, document all findings in a clear and repeatable manner, and provide remediation recommendations.

Approach

<ASSESSOR NAME> performed testing under a “black box” approach from <START DATE> to <END DATE> without credentials or any advance knowledge of Trilocor’s externally facing environment with the goal of identifying unknown weaknesses. Testing was performed from a non-evasive standpoint with the goal of uncovering as many misconfigurations and vulnerabilities as possible. Testing was performed remotely from <ASSESSOR NAME>‘s assessment labs. Each weakness identified was documented and manually investigated to determine exploitation possibilities and escalation potential. <ASSESSOR NAME> sought to demonstrate the full impact of every vulnerability, up to and including internal domain compromise. If <ASSESSOR NAME> were able to gain a foothold in the internal network as a result of external network testing, Trilocor allowed for further testing including lateral movement and horizontal/vertical privilege escalation to demonstrate the impact of an internal network compromise.

Scope

The scope of this assessment was one external IP address, two internal network ranges, the TRILOCOR.LOCAL Active Directory domain, and any other Active Directory domains owned by Trilocor discovered if internal network access were achieved.

In-Scope Assets

|  |  |
| --- | --- |
| Host/URL/IP Address/Domain | Description |
| 10.129.x.x | <FILL IN DESCRIPTION> |
| 172.16.139.0/24 | Trilocor internal network |
| 172.16.210.0/24 | Trilocor internal network |
| trilocor.local | Trilocor internal AD domain |
| <OTHER DISCOVERED INTERNAL DOMAIN(s)> | <FILL IN DESCRIPTION> |

Table : Scope Details

Assessment Overview and Recommendations

During the penetration test against Trilocor, <ASSESSOR NAME> identified <NUMBER (#)> findings that threaten the confidentiality, integrity, and availability of Trilocor’s information systems. The findings were categorized by severity level, with five (5) of the findings being assigned a high-risk rating, one (1) medium-risk, and one (1) low risk. There was also one (1) informational finding related to enhancing security monitoring capabilities within the internal network.

<INSERT EXECUTIVE SUMMARY HERE>

Trilocor should create a remediation plan based on the [Remediation Summary](#_Remediation_Summary) section of this report, addressing all high findings as soon as possible according to the needs of the business. Trilocor should also consider performing periodic vulnerability assessments if they are not already being performed. Once the issues identified in this report have been addressed, a more collaborative, in-depth Active Directory security assessment may help identify additional opportunities to harden the Active Directory environment, making it more difficult for attackers to move around the network and increasing the likelihood that Trilocor will be able to detect and respond to suspicious activity.

# Network Penetration Test Assessment Summary

<ASSESSOR NAME> began all testing activities from the perspective of an unauthenticated user on the internet. Trilocor provided the tester with network ranges but did not provide additional information such as operating system or configuration information.

Summary of Findings

During the course of testing, <ASSESSOR NAME> uncovered a total of <NUMBER (#)> findings that pose a material risk to Trilocor’s information systems. <ASSESSOR NAME> also identified <one informational finding> that, if addressed, could further strengthen Trilocor’s overall security posture. Informational findings are observations for areas of improvement by the organization and do not represent security vulnerabilities on their own. The below table provides a summary of the findings by severity level.

|  |  |  |  |
| --- | --- | --- | --- |
| Finding Severity | | | |
| **High** | **Medium** | **Low** | **Total** |
| **5** | **1** | **1** | **7** |

Table : Severity Summary

Below is a high-level overview of each finding identified during testing. These findings are covered in depth in the [Technical Findings Details](#_Technical_Findings_Details) section of this report.

|  |  |  |
| --- | --- | --- |
| Finding # | Severity Level | Finding Name |
| 1. | **High** | LLMNR/NBT-NS Response Spoofing |
| 2. | **High** | Weak Kerberos Authentication (“Kerberoasting”) |
| 3. | **High** | Local Administrator Password Re-Use |
| 4. | **High** | Weak Active Directory Passwords |
| 5. | **High** | Tomcat Manager Weak/Default Credentials High |
| 6. | **Medium** | Insecure File Shares |
| 7. | **Low** | Directory Listing Enabled |
| 8. | **Info** | Enhance Security Monitoring Capabilities |

Table : Finding List

# Internal Network Compromise Walkthrough

During the course of the assessment <ASSESSOR NAME> was able gain a foothold via the external network, move laterally, and compromise the internal network, leading to full administrative control over the TRILOCOR.LOCAL Active Directory domain and <INSERT DOMAIN NAME> Active Directory domain. The steps below demonstrate the steps taken from initial access to compromise and does not include all vulnerabilities and misconfigurations discovered during the course of testing. Any issues not used as part of the path to compromise are listed as separate, standalone issues in the [Technical Findings Details](#_Technical_Findings_Details_1) section, ranked by severity level. The intent of this attack chain is to demonstrate to Trilocor the impact of each vulnerability shown in this report and how they fit together to demonstrate the overall risk to the client environment and help to prioritize remediation efforts (i.e., patching two flaws quickly could break up the attack chain while the company works to remediate all issues reported). While other findings shown in this report could be leveraged to gain a similar level of access, this attack chain shows the initial path of least resistance taken by the tester to achieve domain compromise.

Detailed Walkthrough

<ASSESSOR NAME> performed the following to fully compromise the TRILOCOR.LOCAL domain.

1. <LIST HIGH LEVEL STEPS>

**Detailed reproduction steps for this attack chain are as follows:**

<FILL IN DETAILED ATTACK CHAIN STEPS>

<ASSESSOR NAME> then performed the following to fully compromise the <INSERT OTHER INTERNAL DOMAIN NAME(S)> domain.

1. <LIST HIGH LEVEL STEPS>

**Detailed reproduction steps for this attack chain are as follows:**

<FILL IN DETAILED ATTACK CHAIN STEPS>

# Remediation Summary

As a result of this assessment there are several opportunities for Trilocor to strengthen its external and internal network security. Remediation efforts are prioritized below starting with those that will likely take the least amount of time and effort to complete. Trilocor should ensure that all remediation steps and mitigating controls are carefully planned and tested to prevent any service disruptions or loss of data.

Short Term

* [**Finding 2**] – Set strong (24+ character) passwords on all SPN accounts
* <FILL IN AS APPROPRIATE>
* Enforce a password change for all users because of the domain compromise

Medium Term

* [**Finding 1**] – Disable LLMNR and NBT-NS wherever possible
* <FILL IN AS APPROPRIATE>

Long Term

* Perform ongoing internal network vulnerability assessments and domain password audits
* Perform periodic Active Directory security assessments
* Educate systems and network administrators and developers on security hardening best practices compromise
* Enhance network segmentation to isolate critical hosts and limit the effects of an internal compromise
* <FILL IN AS APPROPRIATE>

<FILL IN BASED ON FINDINGS, EXAMPLES LEFT FOR REFERENCE>

# Technical Findings Details

**<EXAMPLE HIGH, MEDIUM, LOW, INFO FINDINGS>**

1. LLMNR/NBT-NS Response Spoofing - High

|  |  |
| --- | --- |
| CWE | [CWE-522](https://cwe.mitre.org/data/definitions/522.html) |
| CVSS 3.1 Score | 9.5 |
| Description (Incl. Root Cause) | By responding to LLMNR/NBT-NS network traffic, adversaries may spoof an authoritative source for name resolution to force communication with an adversary-controlled system. This activity may be used to collect or relay authentication materials.  Link-Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS) are Microsoft Windows components that serve as alternate methods of host identification. LLMNR is based upon the Domain Name System (DNS) format and allows hosts on the same local link to perform name resolution for other hosts. NBT-NS identifies systems on a local network by their NetBIOS name. |
| Security Impact | Adversaries can spoof an authoritative source for name resolution on a victim network by responding to LLMNR (UDP 5355)/NBT-NS (UDP 137) traffic as if they know the identity of the requested host, effectively poisoning the service so that the victims will communicate with the adversary-controlled system. If the requested host belongs to a resource that requires identification/authentication, the username and NTLMv2 hash will then be sent to the adversary-controlled system. The adversary can then collect the hash information sent over the wire through tools that monitor the ports for traffic or through Network Sniffing and crack the hashes offline through Brute Force to obtain the plaintext passwords. In some cases where an adversary has access to a system that is in the authentication path between systems or when automated scans that use credentials attempt to authenticate to an adversary-controlled system, the NTLMv2 hashes can be intercepted and relayed to access and execute code against a target system relay step can happen in conjunction with poisoning but may also be independent of it.  Several tools exist that can be used to poison name services within local networks such as NBNSpoof, Metasploit, and Responder. |
| Affected Domain | * TRILOCOR.LOCAL |
| Remediation | * Disable LLMNR and NetBIOS in local computer security settings or by group policy if they are not needed within an environment * Use host-based security software to block LLMNR/NetBIOS traffic. Enabling SMB Signing can stop NTLMv2 relay attacks. * Network intrusion detection and prevention systems that can identify traffic patterns indicative of MiTM activity can be used to mitigate activity at the network level. * Network segmentation can be used to isolate infrastructure components that do not require broad network access. This may mitigate, or at least alleviate, the scope of MiTM activity. |
| External References | <https://attack.mitre.org/techniques/T1557/001/> |

Detailed Reproduction Steps: <SHOW ALL STEPS, NOT JUST A SINGLE SCREENSHOT>

Running the [Responder](https://github.com/lgandx/Responder) tool to attempt to obtain user account password hashes.

|  |
| --- |
| $ sudo responder -I eth0 -wrfv  \_\_  .----.-----.-----.-----.-----.-----.--| |.-----.----.  | \_| -\_\_|\_\_ --| \_ | \_ | | \_ || -\_\_| \_|  |\_\_| |\_\_\_\_\_|\_\_\_\_\_| \_\_|\_\_\_\_\_|\_\_|\_\_|\_\_\_\_\_||\_\_\_\_\_|\_\_|  |\_\_|  NBT-NS, LLMNR & MDNS Responder 3.0.6.0  <SNIP>  [+] Generic Options:  Responder NIC [eth0]  Responder IP [192.168.195.168]  Challenge set [random]  Don't Respond To Names ['ISATAP']  [+] Current Session Variables:  Responder Machine Name [WIN-TWWXTGD94CV]  Responder Domain Name [3BKZ.LOCAL]  Responder DCE-RPC Port [47032]  [+] Listening for events...  <SNIP>  [SMB] NTLMv2-SSP Client : 192.168.195.205  [SMB] NTLMv2-SSP Username : TRILOCOR\bsmith  [SMB] NTLMv2-SSP Hash : bsmith::TRILOCOR:7ecXXXXXX98ebc|

Figure : Running Responder

Successfully cracking a password hash with [Hashcat](https://github.com/hashcat/hashcat) to reveal the clear text password value.

|  |
| --- |
| $ hashcat -m 5600 bsmith\_hash /usr/share/wordlists/rockyou.txt  hashcat (v6.1.1) starting...  <SNIP>  Dictionary cache hit:  \* Filename..: /usr/share/wordlists/rockyou.txt  \* Passwords.: 14344385  \* Bytes.....: 139921507  \* Keyspace..: 14344385  BSMITH::TRILOCOR:7eccd965c4b98ebc:73d1b2c8c5f9861eefd31bb45085a651::<REDACTED> |

Figure : Cracking a Password with Hashcat

1. Insecure File Shares - Medium

|  |  |
| --- | --- |
| CWE | [CWE-284](https://cwe.mitre.org/data/definitions/284.html) |
| CVSS 3.1 Score | 6.2 |
| Description (Incl. Root Cause) | The tester uncovered multiple file shares where all Domain Users have read/write access. |
| Security Impact | An attacker who gains a foothold in this domain can use this access to search for files containing sensitive data such as credentials and potentially write malicious files to the file shares. |
| Affected Domain | * TRILOCOR.LOCAL |
| Remediation | Review file share privileges to ensure that users are granted access in accordance with the principal of least privilege. |
| External References | <https://attack.mitre.org/techniques/T1135/> |

Detailed Reproduction Steps:

Viewing file shares accessible to a standard Domain user with the [CrackMapExec](https://github.com/byt3bl33d3r/CrackMapExec/) tool.

|  |
| --- |
| $ sudo crackmapexec smb 192.168.195.205 -u asmith -p <REDACTED> --shares  SMB 192.168.195.205 445 MS01 [\*] Windows 10.0 Build 17763 x64 (name:MS01) (domain:TRILOCOR.LOCAL) (signing:False) (SMBv1:False)  SMB 192.168.195.205 445 MS01 [+] TRILOCOR.LOCAL\asmith:<REDACTED>  SMB 192.168.195.205 445 MS01 [+] Enumerated shares  SMB 192.168.195.205 445 MS01 Share Permissions Remark  SMB 192.168.195.205 445 MS01 ----- ----------- ------  SMB 192.168.195.205 445 MS01 ADMIN$ Remote Admin  SMB 192.168.195.205 445 MS01 Backups READ  SMB 192.168.195.205 445 MS01 C$ Default share  SMB 192.168.195.205 445 MS01 IPC$ READ Remote IPC  SMB 192.168.195.205 445 MS01 Migration Data READ  SMB 192.168.195.205 445 MS01 Software READ,WRITE |

Figure : Listing Accessible Shares

1. Directory Listing Enabled - Low

|  |  |
| --- | --- |
| CWE | [CWE-548](https://cwe.mitre.org/data/definitions/548.html) |
| CVSS 3.1 Score | 4.3 |
| Description (Incl. Root Cause) | The web application exposes a directory listing of some files in the web root and subfolders. |
| Security Impact | The severity of this finding depends on the sensitivity of the files exposed on the web server. If the directory exposes only files intended for public consumption, then the risk is lower but if an attacker can gain access to sensitive information such as configuration files, they may be able to use these to gain further access to the application or web server. |
| Affected Host(s) | * 192.168.195.215 (80/TCP) |
| Remediation | Restrict access to files and directories based on the concept of least privilege. Enforce authentication wherever possible and disable directory listing in the web server configuration. |
| External References | <https://attack.mitre.org/techniques/T1083/>  <https://www.acunetix.com/blog/articles/directory-listing-information-disclosure/> |

Detailed Reproduction Steps:

Using a web browser, browsing to the affected host lists the directory contents.

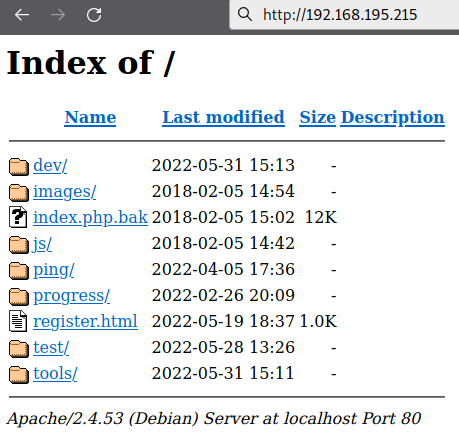


Figure : Directory Listing

1. Enhance Security Monitoring Capabilities - Info

|  |  |
| --- | --- |
| CWE | [CWE-693](https://cwe.mitre.org/data/definitions/693.html) |
| Description (Incl. Root Cause) | It appeared that Trilocor did not notice “noisy” activities during the course of testing. The tester was also not blocked when using standard open-source penetration testing tools. |
| Security Impact | If network and endpoint detection and response are inadequate, an attacker who can gain a foothold in the internal network may be able to move laterally, perform post-exploitation, and achieve persistence easily. |
| Remediation | Consider investing in a more advanced network monitoring solution, configuring logging on all hosts, and processing them for anomalies using a SIEM tool, and implementing endpoint detection on each server and workstation that is more difficult to bypass and tamper with. The organization should not rely on endpoint protection alone. When combined with a defense-in-depth security strategy, they can be an excellent tool for detecting an attacker who gains internal network access and is forced to perform “noisier” and riskier activities to the nature of the hardened environment. |
| External References | <https://attack.mitre.org/tactics/TA0005/> |

# Appendices

Appendix A – Finding Severities

Each finding has been assigned a severity rating of high, medium, or low. The rating is based off of an assessment of the priority with which each finding should be viewed and the potential impact each has on the confidentiality, integrity, and availability of Trilocor’s data.

|  |  |
| --- | --- |
| Rating | Severity Rating Definition |
| **High** | Exploitation of the technical or procedural vulnerability will cause substantial harm. Significant political, financial, and/or legal damage is likely to result. The threat exposure is high, thereby increasing the likelihood of occurrence. Security controls are not effectively implemented to reduce the severity of impact if the vulnerability were exploited. |
| **Medium** | Exploitation of the technical or procedural vulnerability will significantly impact the confidentiality, integrity, and/or availability of the system, application, or data. Exploitation of the vulnerability may cause moderate financial loss or public embarrassment. The threat exposure is moderate-to-high, thereby increasing the likelihood of occurrence. Security controls are in place to contain the severity of impact if the vulnerability were exploited, such that further political, financial, or legal damage will not occur.  - OR -  The vulnerability is such that it would otherwise be considered High Risk, but the threat exposure is so limited that the likelihood of occurrence is minimal. |
| Low | Exploitation of the technical or procedural vulnerability will cause minimal impact to operations. The Confidentiality, Integrity and Availability (CIA) of sensitive information are not at risk of compromise. Exploitation of the vulnerability may cause slight financial loss or public embarrassment. The threat exposure is moderate-to-low. Security controls are in place to contain the severity of impact if the vulnerability were exploited, such that further political, financial, or legal damage will not occur.  - OR -  The vulnerability is such that it would otherwise be considered Medium Risk, but the threat exposure is so limited that the likelihood of occurrence is minimal. |

Table : Severity Definitions

Appendix B – Host & Service Discovery

|  |  |  |  |
| --- | --- | --- | --- |
| IP Address | Port | Service | Notes |
| **<FILL IN AS APPROPRIATE>** |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table : Discovered Hosts and Services

Appendix C – Subdomain Discovery

|  |  |  |
| --- | --- | --- |
| URL | Description | Discovery Method |
| **<FILL IN DISCOVERED VHOSTS/SUBDOMAINS>** |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Table : Discovered Subdomains

Appendix D – Exploited Hosts

|  |  |  |  |
| --- | --- | --- | --- |
| Host | Scope | Method | Notes |
| **<FILL IN AS APPROPRIATE>** |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table : Exploitation Attempt Details

Appendix E – Compromised Users

|  |  |  |  |
| --- | --- | --- | --- |
| Username | Type | Method | Notes |
| **<FILL IN AS APPROPRIATE>** |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table : User Accounts Compromised

Appendix F – Changes/Host Cleanup

|  |  |  |
| --- | --- | --- |
| Host | Scope | Change/Cleanup Needed |
| **<FILL IN AS APPROPRIATE>** |  |  |
|  |  |  |

Table : Assessment Artifacts

Appendix G – Flags Discovered

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Flag # | Host | Flag Value | Flag Location | Method Used |
| 1. | ***NIX01*** | *<MD5 HASH>* | *Web root* | *Unrestricted file upload (example)* |
| 2. |  |  |  |  |
| 3. |  |  |  |  |
| 4. |  |  |  |  |
| 5. |  |  |  |  |
| 6. |  |  |  |  |
| 7. |  |  |  |  |
| 8. |  |  |  |  |
| 9. |  |  |  |  |
| 10. |  |  |  |  |
| 11. |  |  |  |  |
| 12. |  |  |  |  |
| 13. |  |  |  |  |

Table : Flags Discovered