**Text

Description automatically generated**

**Charleston Southern University**

**Security Assessment Findings Report**

Business Confidential

*Date: January 10, 2022*

**Table of Contents**

Table of Contents 2

Confidentiality Statement 3

Assessment Overview 3

Assessment Components 3

Internal Penetration Test 3

Findings by Severity 4

Scope of Attack 5

Summary 6

Security Posture Strengths 7

Security Posture Weaknesses 7

Internal Findings 8

Outdated Hardware and Software 8

SMB Signing Disabled on Multiple Assets 9

Cracking of User Hashed Passwords 10

Lack of MFA and UAC allowed for remote authentication to

the Domain Controller 11

Privilege Escalation Via Token Impersonation 11

Dumping Administrator Password Hashes Via Mimikatz (Kiwi) 12

Gathering Active Directory Information Using IPv6 DNS Takeover 13

Active Directory Enumeration with Bloodhound 14

Remediation Steps 15 - 16

Conclusion and Recap 17

**Statement of Confidentiality**

This document is the sole property of Charleston Southern University (CSU). This report contains confidential and proprietary information about CSU and its assets. Duplication or use of this document requires consent from CSU.

**Assessment Overview**

From January 10th to April 20th, CSU conducted an internal penetration test to find the stance of their security posture, as well as the ability for an attacker to move laterally within their network.

The phases of the penetration test included:

Documentation and Reporting

Exploitation

Exploit Discovery

Planning

**Assessment Components**

Internal Penetration Test

An internal penetration test is a simulation of a real-world attack where a malicious threat actor has compromised the target network and is now looking to move laterally or escalate their privileges. The test included system enumeration, target enumeration, exploitation, privilege escalation, and domain compromise. Discovered vulnerabilities and corresponding remediation steps will be displayed throughout the rest of this document.

**Findings By Severity**

|  |  |  |
| --- | --- | --- |
| Severity Rating | CVSS v3.1 Score Range | Definition |
| Critical | 9.0-10.0 | Exploitation of the vulnerability is easily done, resulting in a system compromise. |
| High | 7.0-8.9 | Exploitation is more difficult; however, the vulnerability allows elevation of privileges to occur. |
| Moderate | 4.0-6.9 | Vulnerabilities are present but are not exploitable. |
| Low | 0.1-3.9 | Exploitation of this vulnerability is not possible, but patching would reduce the organization’s surface of attack. |
| Informational | 0.0 | No vulnerabilities are present. However, disclosure of information is present. |

**Scope**

|  |  |
| --- | --- |
| Assessment | IP Ranges |
| Internal Penetration Test | 192.168.190.0/24 |

**Out of Scope**

CSU asked for no network interference and no-brute force attacks.

**In Scope**

CSU allowed a basic user account with a Kali Linux Virtual Machine installed to simulate a real-world attack.

**Summary**

CSU’s internal security posture was evaluated from the dates of January 10th to April 20th. By enumeration techniques and vulnerability scanning, the penetration tester was able to leverage critical vulnerabilities that allowed for complete domain compromise. The addressment of these vulnerabilities is of upmost importance to ensure the confidentiality, integrity, and availability of the CSUs proprietary data and assets.

The table below demonstrates how the penetration tester was able to move laterally and compromise administrator accounts.

|  |  |  |
| --- | --- | --- |
| Step | Action | Remediation |
| 1 | **Information Gathering**   * Used Nmap to scan every IP in the network and find easily exploitable machines. * Vulnerability scanned with Nessus. * Gathered Active Directory using IPv6 DNS Takeover. * Found password hashes using LLMNR Poisoning. * Found a software on a windows machine that is vulnerable to a buffer overflow exploit | 1. Block unnecessary ports. 2. Upgrade older versions of Windows. 3. Disable IPv6 if not being used. 4. Disable LLMNR if not needed or implement Network Access Control. 5. Application Container or remove software. |
| 2 | **Exploitation**   * Developed a custom buffer overflow exploit using python to gain initial access to Bucky’s PC. | 1. Upgrade older versions of Windows, implement defender, and remove vulnerable apps. |
| 3 | **Enumeration**   * Enumerated the system with Bloodhound to find detailed Active Directory Information and route of attack. | 1. Implement signature based AV on all endpoints. |
| 4 | **Privilege Escalation**   * Used Token Impersonation and Password Dumping Techniques to find administrator credentials. | 1. Enforce strong encryption standards. 2. Reconfigure Kerberos. |

**Security Posture Strengths**

Windows Defender

During the assessment, the tester was unable to execute some malicious software on devices protected with an up-to-date version of Windows Defender. Defender made the IT department aware of the attackers IP address and allowed the blue-team a chance in containing the user.

**Security Posture Weaknesses**

Vulnerable Software

Bucky’s PC was vulnerable to a buffer-overflow exploit do to the Vulnserver application being run on the machine. This software, if labeled critical, must be containerized or, if not labeled critical, must be removed from the device.

Weak Password Change Policy

Because there was no enforced password change policy, the attacker was able to discover Bucky’s password.

Missing Third-Party Antivirus

The penetration tester was able to navigate the internal network with relative ease, due to the absence of antivirus software or a SIEM implementation.

SMB Signing Disabled on Multiple Devices

SMB Signing was found to be disabled on multiple devices, allowing an attacker to see the SMB shares of these assets. The penetration tester was successful in doing so via an SMB relay attack, which allowed compromise of multiple user and administrator SMB shares.

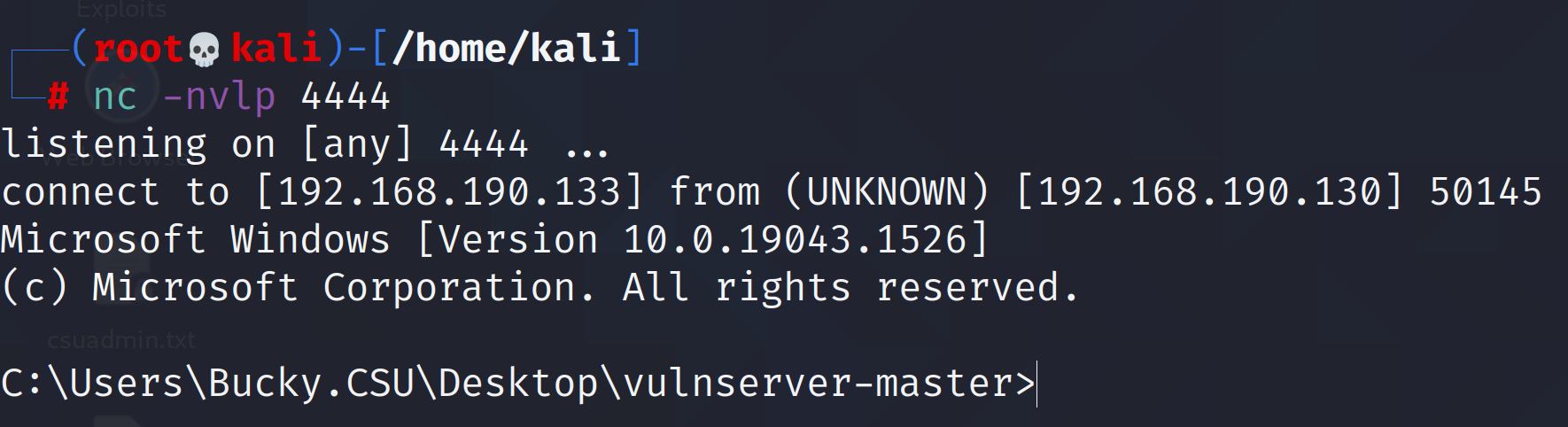
**Internal Findings**

**1. Outdated Hardware and Software**

|  |  |
| --- | --- |
| Description | The tester found cases of outdated and vulnerable applications on systems and hardware. |
| Impact | Critical |
| Systems | 192.168.190.0/24 |
| References | [Security and Privacy Controls for Federal Information Systems and Organizations (nist.gov)](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf) – Appendix F > FAMILY: Configuration Management > CM 2 Baseline Configuration > Control Enhancement 2. |

**Proof of Concept:** Text

Description automatically generated

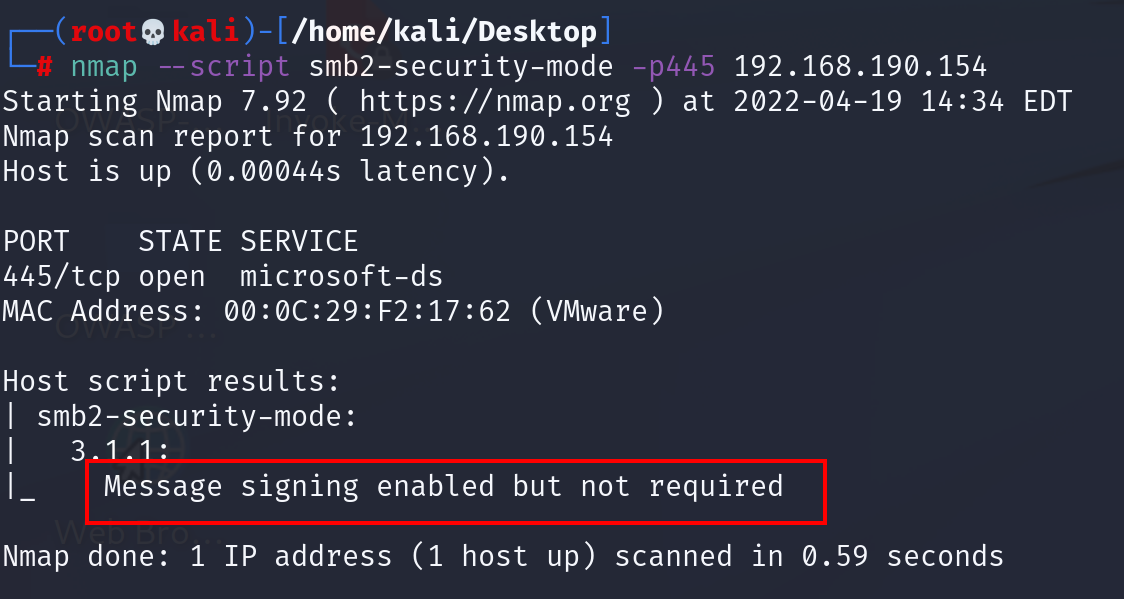
****

****

**2.** **SMB Signing Disabled on Multiple Assets**

|  |  |
| --- | --- |
| Description | The tester found multiple instances of SMB Message Signing being disabled by default. Allowing use of SMB Relay Attacks to find open shares on machines. |
| Impact | High |
| Systems | 192.168.190.154, 192.168.190.152 |
| References | [Security and Privacy Controls for Federal Information Systems and Organizations (nist.gov)](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf) – Appendix F > FAMILY: Access Control > AC -1 Access Control Policy and Procedures > Control Enhancements 1-9. |

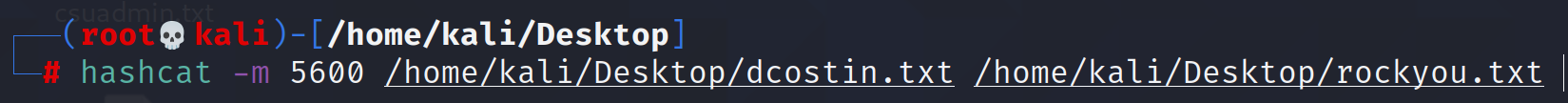
**Proof of Concept**



**3. Cracking of User Hashed Passwords**

|  |  |
| --- | --- |
| Description | A vulnerability exists that allowed the tester to exploit and crack account hashed passwords. |
| Impact | Critical |
| Systems | 192.168.190.154 |
| References |  |

**Proof of Concept**

****

**Text

Description automatically generated**

**4.** **Lack of MFA and UAC allowed for remote authentication to the Domain Controller.**

|  |  |
| --- | --- |
| Description | Remote connection to the domain controller was feasible due to a lack of MFA on the network and user account control. |
| Impact | Critical |
| Systems | 192.168.190.148 |
| References |  |

**Proof of Concept**

**Text

Description automatically generated**

**5.** **Privilege Escalation Via Token Impersonation**

|  |  |
| --- | --- |
| Description | The tester was able to successfully impersonate an administrative token on the Domain Controller. The token does not expire until the server is rebooted. |
| Impact | High |
| Systems | 192.168.190.151 |
| References | [Token Impersonation with Incognito (sevenlayers.com)](https://www.sevenlayers.com/index.php/345-token-impersonation-with-incognito) |

**Proof of Concept**

**Text

Description automatically generated**

**6.** **Dumping Administrator Passwords Hashes Via Mimikatz (Kiwi)**

|  |  |
| --- | --- |
| Description | The tester was able to find cached log-in passwords hashes on the domain controller to escalate their privileges. |
| Impact | Critical |
| Systems | 192.168.190.151 |
| References | [Dumping User Passwords from Windows Memory with Mimikatz | Windows OS Hub (woshub.com)](http://woshub.com/how-to-get-plain-text-passwords-of-windows-users/)  [Security and Privacy Controls for Federal Information Systems and Organizations (nist.gov)](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf) – Appendix F > FAMILY: Identification and Authentication > IA 2 – Identification and Authentication (Organizational Users) > Control Enhancements 8, 9, and 11. |

**Proof of Concept**

Text

Description automatically generated

Text

Description automatically generated

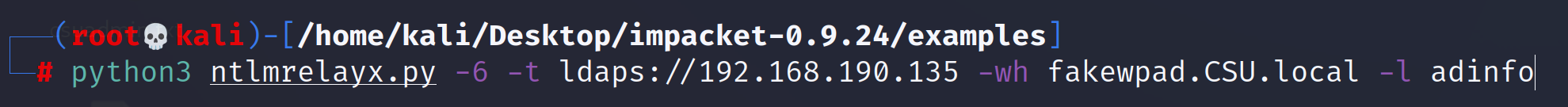
**7.** **Gathering Active Directory Information Using IPv6 DNS Takeover**

|  |  |
| --- | --- |
| Description | The tester was able to gather all Active Directory information using a DNS takeover attack that exploited IPv6. The tester acted as a domain controller sending spoofed replies to machines in order to receive information that was then put into a directory. |
| Impact | Informational |
| Systems | All systems |
| References | [mitm6 – compromising IPv4 networks via IPv6 – Fox-IT International blog](https://blog.fox-it.com/2018/01/11/mitm6-compromising-ipv4-networks-via-ipv6/) |

**Proof of Concept**

**Graphical user interface, text

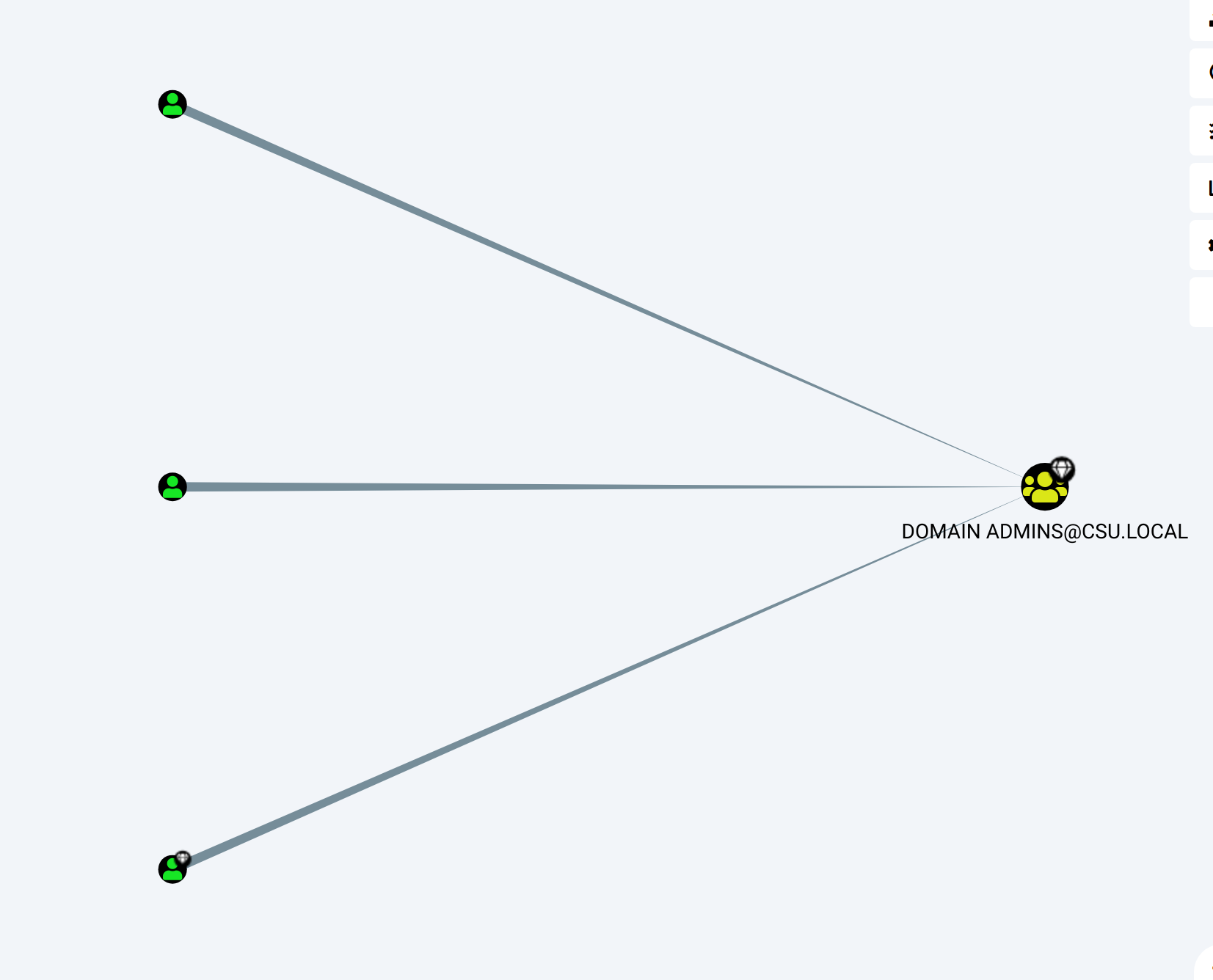
Description automatically generated**

****

**8. Active Directory Enumeration with Bloodhound**

|  |  |
| --- | --- |
| Description | The tester was able to successfully upload and execute the bloodhound PowerShell script on those machines not using antivirus. Bloodhound allowed for complete enumeration of the csu.local domain. |
| Impact | Information |
| Systems | All Systems |
| References | [BloodHound/SharpHound.ps1 at 804503962b6dc554ad7d324cfa7f2b4a566a14e2 · BloodHoundAD/BloodHound (github.com)](https://github.com/BloodHoundAD/BloodHound/blob/804503962b6dc554ad7d324cfa7f2b4a566a14e2/Ingestors/SharpHound.ps1)  [Active Directory Enumeration: BloodHound (hackingarticles.in)](https://www.hackingarticles.in/active-directory-enumeration-bloodhound/) |

**Proof of Concept**



**Remediation Steps**

|  |  |
| --- | --- |
| Who | IT Dept |
| Steps | **1. Outdated Hardware and Software**  - Take steps towards automating operating system version upgrades.  - Budget for new hardware and supported operating system versions. |

|  |  |
| --- | --- |
| Who | IT Dept |
| Steps | **2. SMB Signing Disabled**  - Enable SMB Signing on all devices.  - SMB Signing is disabled by default on desktops. |

|  |  |
| --- | --- |
| Who | IT Dept |
| Steps | **3. User Negligence**  - Never store passwords in plaintext on desktop.  - Use password safe that encrypts data at rest. |

|  |  |
| --- | --- |
| Who | IT Dept |
| Steps | **4. Hashed Passwords Found Using LLMNR Poisoning**  - Disable LLMNR if not being used.  - Disable NBT-NS.  - Require network access control through NAC devices.  - Require strong user passwords to deter hash cracking.  - Educate employees on the need for strong passwords. |

|  |  |
| --- | --- |
| Who | IT Dept |
| Steps | **5. Privilege Escalation Via Token Impersonation**  - Limit user / group token creation permissions.  - Account Tiering. Only allowing domain admins to access domain controllers and creating a separate workstation admin to control workstations.  - Local Admin Restrictions. Install Local Administrator Password Solution (LAPS) to mitigate against password re-use. https://securitytutorials.co.uk/illustrated-tutorial-for-installing-microsoft-laps/ |

|  |  |
| --- | --- |
| Who | IT Dept |
| Steps | **6. Dumping Administrator Passwords Via Mimikatz (Kiwi)**  - Install Antivirus on all endpoints.  - Disable Wdigest.  - Disable Credman.  - Enforce strong encryption standards. AES256.  - Enforce strong hashing standards. SHA512 or RIPEMD.  - Enforce strong password complexity requirements among all users to diminish hash cracking. |

|  |  |
| --- | --- |
| Who | IT Dept |
| Steps | **7. Gathering Active Directory Information Using IPv6 DNS Takeover**  - Disable IPv6 if not being used within the network.  - Disable WPAD if not being used.  - Enable LDAP signing and channel binding to stop LDAP and LDAPS relaying. |

|  |  |
| --- | --- |
| Who | IT Dept |
| Steps | **8. Active Directory Enumeration with Bloodhound**  - Install Antivirus on all endpoints.  - Use Bloodhound proactively to look of Active Directory vulnerabilities.  - Audit privileged user behaviors.  - Audit local groups and permission with computers that contain sensitive data. |

**Conclusion and Recap**

The overall security posture of Charleston Southern University is solid when fully implemented. There are several loopholes that were found in the assessment that led to system compromise. Many other avenues of attack were found, but only one was fully tested and exploited. For now, it is important for CSU to implement antivirus on all devices. An antivirus solution is proven to be effective in mitigating all areas of remote code execution, malicious file upload, and local privilege escalation. Not only this, but CSU should look to audit their open ports internally to harden them accordingly. CSU should also seek to utilize red-teaming tools (i.e., Bloodhound, Nmap, Nessus, Metasploit) as a method of continuously testing their network infrastructure. The continuous hardening of the CSU network is a positive step towards creating a secure infrastructure and should continue in order to increase their overall security posture.