Jay's Bank Application Penetration Testing

Security Assessment Findings Report

Date: June 1st, 2024

Table of Contents

Table of Contents 2
Confidentiality Statement 4
Disclaimer 4
Contact Information 4
Assessment Overview 5
Assessment Components 5
Internal Penetration Test 5
Finding Severity Ratings 6
Risk Factors 6
Likelihood 6
Impact 6
Scope 7
Scope Exclusions 7
Client Allowances 7
Executive Summary 8
Scoping and Time Limitations 8
Testing Summary 8
Tester Notes and Recommendations 9
Key Strengths and Weaknesses 10
Vulnerability Summary & Report Card 11
Internal Penetration Test Findings 11
Technical Findings 13
Internal Penetration Test Findings 13
Finding IPT-001: Insufficient LLMNR Configuration (Critical) 13
Finding IPT-002: Security Misconfiguration – Local Admin Password Reuse (Critical) 14
Finding IPT-003: Security Misconfiguration – WDigest (Critical) 15
Finding IPT-004: Insufficient Hardening – Token Impersonation (Critical) 16
Finding IPT-005: Insufficient Password Complexity (Critical) 17
Finding IPT-006: Security Misconfiguration – IPv6 (Critical) 18
Finding IPT-007: Insufficient Hardening – SMB Signing Disabled (Critical) 19
Finding IPT-008: Insufficient Patch Management – Software (Critical) 20
Finding IPT-009: Insufficient Patch Management – Operating Systems (Critical) 21
Finding IPT-010: Insufficient Patching – MS08-067 - ECLIPSEDWING/NETAPI (Critical) 22
Finding IPT-011: Insufficient Patching – MS12-020 – Remote Desktop RCE (Critical) 23
Finding IPT-012: Insufficient Patching – MS17-010 - EternalBlue (Critical) 24
Finding IPT-013: Insufficient Patching – CVE-2019-0708 - BlueKeep (Critical) 25
Finding IPT-014: Insufficient Privileged Account Management – Kerberoasting (High) 26

Finding IPT-015: Security Misconfiguration – GPP Credentials (High) 27
Finding IPT-016: Insufficient Authentication - VNC (High) 28
Finding IPT-017: Default Credentials on Web Services (High) 29
Finding IPT-018: Insufficient Hardening – Listable Directories (High) 30
Finding IPT-019: Unauthenticated SMB Share Access (Moderate) 31
Finding IPT-020: Insufficient Patch Management – SMBv1 (Moderate) 32
Finding IPT-021: IPMI Hash Disclosure (Moderate) 33
Finding IPT-022: Insufficient SNMP Community String Complexity (Moderate) 34
Finding IPT-023: Insufficient Data in Transit Encryption - Telnet (Moderate) 35
Finding IPT-024: Insufficient Terminal Services Configuration (Moderate) 36
Finding IPT-025: Steps to Domain Admin (Informational) 37
Additional Scans and Reports 37

Confidentiality Statement

Dokumen ini merupakan properti eksklusif dari SafeGuard Solutions. Dokumen ini berisi informasi yang bersifat rahasia dan milik perusahaan. Penggandaan, distribusi, atau penggunaan, baik secara keseluruhan maupun sebagian, dalam bentuk apapun, memerlukan persetujuan dari SafeGuard Solutions.

SafeGuard Solutions dapat membagikan dokumen ini kepada pihak auditor yang terikat oleh perjanjian kerahasiaan untuk menunjukkan kepatuhan pada persyaratan pengujian penetrasi.

Disclaimer

Pengujian penetrasi dianggap sebagai representasi pada suatu waktu tertentu. Temuan dan rekomendasi mencerminkan informasi yang dikumpulkan selama penilaian dan bukan perubahan atau modifikasi yang dilakukan di luar periode tersebut.

Engagement dengan batasan waktu tidak memungkinkan untuk melakukan evaluasi penuh terhadap semua kontrol keamanan. SafeGuard Solutions memberikan prioritas pada penilaian untuk mengidentifikasi kontrol keamanan yang paling rentan yang dapat dieksploitasi oleh penyerang. SafeGuard Solutions merekomendasikan untuk melakukan penilaian serupa secara tahunan oleh penilai internal atau pihak ketiga untuk memastikan kelangsungan keberhasilan kontrol tersebut.

Contact Information

Name	Title	Contact Information
Safeguard Solutions		
John Smith	Jays Bank	Email: jsmith@democorp.com
TCM Security		
Khansa Adia Rahma	Lead Penetration Tester	Email: khansaadiar@gmail.com

Assessment Overview

Pada Pada tanggal 1 June 2024, saya melakukan penetration testing terhadap infrastruktur perusahaan startup teknologi, Jay's Bank. Pentest ini bertujuan untuk mengevaluasi keamanan sistem dengan menerapkan prinsip Ethical Hacking. Perusahaan Jay's Bank telah menyewa layanan SafeGuard Solutions untuk mengidentifikasi dan melaporkan kerentanan yang ada dalam infrastruktur mereka.

Berikut adalah gambaran umum dari aktivitas dan langkah-langkah yang akan dilakukan selama penetration testing:

Perencanaan:

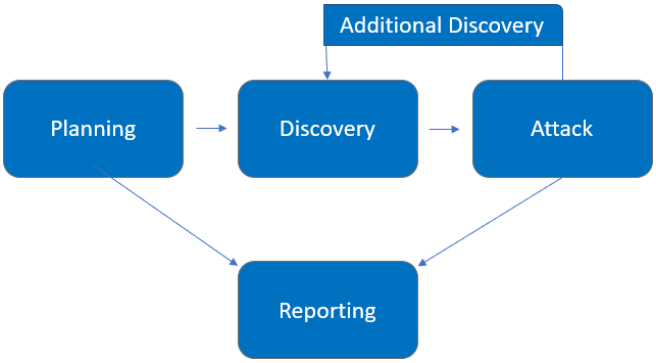
Mendapatkan informasi tentang tujuan dan kebutuhan pelanggan, dalam hal ini Jay's Bank, untuk menentukan fokus dan ruang lingkup penilaian keamanan.
Mendefinisikan peraturan dan batasan dalam rules of engagement untuk menetapkan area yang akan diuji dan batasan-batasan yang harus diikuti selama proses penilaian.
Pendahuluan:

Melakukan pemindaian jaringan dan enumerasi pada alamat IP yang diberikan, yaitu 167.172.75.216, untuk mengidentifikasi sistem, layanan, dan kerentanan potensial yang ada dalam infrastruktur Jay's Bank.
Mengumpulkan informasi yang relevan untuk memahami arsitektur dan konfigurasi sistem yang dievaluasi.
Eksploitasi:

Menguji kerentanan yang ditemukan melalui eksploitasi yang sesuai dengan prinsip ethical hacking.
Melakukan upaya untuk memperoleh akses yang lebih lanjut atau eskalasi hak akses terhadap sistem yang terdampak.
Mengidentifikasi dan memvalidasi kerentanan dengan memanfaatkan celah keamanan yang mungkin ada dalam infrastruktur Jay's Bank.
Pelaporan:

Mendokumentasikan semua kerentanan yang ditemukan selama proses penilaian keamanan.
Membuat laporan yang mencakup deskripsi rinci tentang kerentanan yang ditemukan, langkah-langkah yang diambil untuk mengeksplorasi kerentanan tersebut, dan rekomendasi untuk memperbaikinya.
Laporan juga akan mencakup temuan tentang kekuatan dan kelemahan perusahaan Jay's Bank dalam hal keamanan.

.



Assessment Components

Internal Penetration Test

Dalam komponen ini akan mensimulasikan serangan dari dalam jaringan dengan melakukan pemindaian, serangan jaringan lanjutan, pemanfaatan kredensial, pergerakan lateral, dan eksfiltrasi data. Tujuannya adalah untuk mengidentifikasi kerentanan pada jaringan internal Jay's Bank dan memberikan rekomendasi yang dapat meningkatkan pertahanan keamanannya.

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Temuan dengan tingkat keparahan "Critical" adalah temuan yang memiliki potensi dampak serius terhadap keamanan sistem dan informasi yang dievaluasi. Temuan ini dapat menyebabkan kerugian finansial yang signifikan, kebocoran data sensitif, atau akses tidak sah yang dapat mengakibatkan kerusakan parah pada infrastruktur yang diuji.
High	7.0-8.9	Temuan dengan tingkat keparahan "High" adalah temuan yang memiliki potensi dampak yang signifikan terhadap keamanan sistem dan informasi yang dievaluasi. Temuan ini mungkin dapat menyebabkan pelanggaran kebijakan keamanan, pengungkapan data sensitif yang terbatas, atau memberikan akses yang tidak sah ke sumber daya penting.
Moderate	4.0-6.9	Temuan dengan tingkat keparahan "Medium" adalah temuan yang memiliki potensi dampak moderat terhadap keamanan sistem dan informasi yang dievaluasi. Temuan ini mungkin mencakup kerentanan yang memerlukan tindakan perbaikan untuk mengurangi risiko serangan atau melindungi data sensitif dalam situasi tertentu.
Low	0.1-3.9	Temuan dengan tingkat keparahan "Low" adalah temuan yang memiliki dampak yang rendah terhadap keamanan sistem dan informasi yang dievaluasi. Meskipun temuan ini tidak menyebabkan ancaman yang signifikan, tetapi masih memerlukan perhatian dan tindakan perbaikan untuk meningkatkan keamanan secara keseluruhan.
Informational	N/A	Temuan dengan tingkat keparahan "Informational" adalah temuan yang memberikan informasi tambahan atau saran yang dapat meningkatkan pemahaman tentang sistem dan infrastruktur yang dievaluasi. Temuan ini mungkin tidak langsung terkait dengan keamanan, tetapi dapat memberikan wawasan yang berharga untuk pembenahan atau perbaikan di masa depan.

Risk Factors

Risk is measured by two factors: Likelihood and Impact:

Likelihood

Likelihood mengukur potensi kerentanan dieksploitasi. Penilaian diberikan berdasarkan tingkat kesulitan serangan, ketersediaan alat, tingkat keahlian penyerang, dan lingkungan klien.

Impact

Dampak mengukur efek potensial kerentanan terhadap operasional, termasuk kerahasiaan, integritas, dan ketersediaan sistem dan/atau data klien, kerugian reputasi, dan kerugian finansial.

Scope

Assesment	Details
IP	167.172.75.216
IP	167.172.75.216

Scope Exclusions

Serangan Denial of Service (DoS): Penilaian risiko ini tidak melibatkan serangan Denial of Service (DoS) terhadap sistem perusahaan Jay's Bank.

Serangan Phishing/Social Engineering: Penilaian risiko ini tidak mencakup serangan phishing atau teknik Social Engineering terhadap perusahaan Jay's Bank.

Fisik: Penilaian risiko ini tidak mencakup evaluasi terhadap aspek fisik seperti keamanan fisik gedung, kunci fisik, atau pengamanan fisik lainnya.

Sosial: Penilaian risiko ini tidak mencakup evaluasi terhadap faktor-faktor sosial seperti kebijakan keamanan, pelatihan karyawan, atau kesadaran keamanan pengguna.

Aplikasi Pihak Ketiga: Penilaian risiko ini tidak mencakup evaluasi terhadap aplikasi pihak ketiga yang digunakan oleh perusahaan Jay's Bank, kecuali jika aplikasi tersebut secara langsung terhubung dengan infrastruktur yang sedang dievaluasi.

Client Allowances

Penetration Testing: SafeGuard Solutions diizinkan untuk melakukan penetration testing pada infrastruktur perusahaan Jay's Bank.

Vulnerability Identification: SafeGuard Solutions diizinkan untuk mengidentifikasi kerentanan yang ada dalam sistem perusahaan Jay's Bank.

Reporting: SafeGuard Solutions diizinkan untuk membuat laporan yang mendetail tentang kerentanan yang ditemukan pada sistem perusahaan Jay's Bank.

Timeliness: SafeGuard Solutions diizinkan untuk memproses celah kerentanan yang dilaporkan secara cepat oleh perusahaan Jay's Bank.

Etika: SafeGuard Solutions diminta untuk menghindari melanggar etika dalam melakukan pentest. Tindakan yang melanggar etika dapat mengakibatkan penilaian nol dari Project Manager.

Executive Summary

Memberikan gambaran tentang tingkat kerentanan sistem perusahaan Jay's Bank serta memberikan rekomendasi yang dapat membantu perusahaan untuk meningkatkan keamanan dan melindungi aset mereka dari ancaman keamanan yang ada. Harapannya, pentest ini akan membantu perusahaan Jay's Bank untuk memiliki pemahaman yang lebih baik tentang kelemahan keamanan yang ada dalam infrastruktur mereka, serta memberikan langkah-langkah yang diperlukan untuk memperkuat keamanan sistem mereka.

Scoping and Time Limitations

Pentest pada perusahaan Jay's Bank memiliki lingkup penilaian risiko yang mencakup infrastruktur perusahaan dengan fokus pada jaringan beralamat IP 167.172.75.216. Penilaian risiko tidak melibatkan evaluasi terhadap aspek fisik, sosial, serta aplikasi pihak ketiga, kecuali jika terhubung langsung dengan infrastruktur yang dievaluasi. Pentest ini akan dilaksanakan dalam batas waktu yang telah ditentukan untuk memberikan hasil yang fokus dan tepat waktu kepada perusahaan Jay's Bank.

Testing Summary

Tanggal: [28 May 2024 – 1 June 2024]

Saya telah berhasil menyelesaikan penilaian risiko Ethical Hacking pada infrastruktur perusahaan Jay's Bank. Penilaian risiko ini difokuskan pada jaringan dengan alamat IP 167.172.75.216. Dalam pentest ini, telah dilaksanakan berbagai teknik dan metode Ethical Hacking untuk mengidentifikasi kerentanan yang ada dalam sistem perusahaan Jay's Bank.

Selama pentest, saya telah melakukan penetration testing untuk menguji keamanan infrastruktur perusahaan Jay's Bank. Kami mengidentifikasi beberapa kerentanan yang dapat dieksploitasi, termasuk kerentanan pada sistem operasi dan aplikasi yang berjalan dalam jaringan tersebut. Kami juga melakukan analisis kerentanan yang mendalam dan menguji keefektifan pengamanan yang ada.

Namun, penting untuk dicatat bahwa pentest ini mengikuti pengkecualian lingkup yang telah ditentukan. Kami tidak melakukan serangan Denial of Service (DoS) atau serangan phishing/social engineering. Evaluasi terhadap aspek fisik dan sosial juga dikecualikan dari penilaian risiko ini. Kami juga tidak mengevaluasi aplikasi pihak ketiga kecuali jika mereka terhubung langsung dengan infrastruktur yang sedang dievaluasi.

Hasil ini akan disampaikan kepada perusahaan Jay's Bank dalam bentuk laporan yang mendetail. Laporan akan mencakup daftar kerentanan yang ditemukan beserta rekomendasi mitigasi yang dapat diterapkan untuk memperkuat keamanan sistem mereka. Kami merekomendasikan agar perusahaan Jay's Bank segera mengambil tindakan untuk memperbaiki kerentanan yang teridentifikasi demi menjaga keamanan dan melindungi aset mereka dari ancaman keamanan yang ada.

Kami berterima kasih kepada perusahaan Jay's Bank atas kesempatan ini dan kami berkomitmen untuk menjaga kerahasiaan informasi yang kami peroleh selama pentest. Kami siap untuk memberikan bantuan lebih lanjut dan konsultasi dalam rangka meningkatkan keamanan sistem perusahaan Jay's Bank.

Tester Notes and Recommendations

Setelah melakukan penilaian risiko Ethical Hacking pada infrastruktur perusahaan Jay's Bank, kami ingin memberikan beberapa catatan dan rekomendasi berdasarkan hasil praktikum kami:

Kerentanan Sistem Operasi: Kami menemukan beberapa kerentanan pada sistem operasi yang digunakan oleh perusahaan Jay's Bank. Kami merekomendasikan perusahaan untuk segera menerapkan pembaruan keamanan terbaru dan memastikan bahwa sistem operasi dijaga agar tetap diperbarui secara berkala.

Kerentanan Aplikasi: Selama praktikum, kami mengidentifikasi beberapa kerentanan pada aplikasi yang berjalan dalam jaringan perusahaan. Kami merekomendasikan perusahaan untuk melakukan pemeriksaan keamanan aplikasi secara rutin, termasuk pengujian penetrasi dan penerapan praktik pengembangan aman.

Pengelolaan Akses: Kami menemukan celah dalam pengelolaan akses yang dapat memungkinkan akses yang tidak sah ke sistem perusahaan. Kami merekomendasikan perusahaan untuk menerapkan prinsip least privilege, yaitu memberikan akses yang tepat sesuai dengan kebutuhan pekerjaan, serta mengaktifkan sistem autentikasi yang kuat dan melaksanakan kebijakan pengelolaan kata sandi yang ketat.

Monitoring Keamanan: Kami merekomendasikan perusahaan Jay's Bank untuk meningkatkan pengawasan keamanan dengan mengimplementasikan sistem pemantauan jaringan yang canggih dan mengaktifkan deteksi serangan intrusi. Dengan memantau dan mendeteksi aktivitas yang mencurigakan, perusahaan dapat mengidentifikasi dan menangani ancaman keamanan dengan lebih efektif.

Pelatihan Kesadaran Keamanan Karyawan: Penting untuk memberikan pelatihan kesadaran keamanan kepada seluruh karyawan perusahaan Jay's Bank. Hal ini akan membantu meningkatkan pemahaman mereka tentang praktik keamanan yang tepat, mengurangi risiko serangan fisik dan sosial, serta meningkatkan kepatuhan terhadap kebijakan keamanan yang telah ditetapkan.

Strengths and Weaknesses

Strengths:

Focused Scope: The ethical hacking assessment had a focused scope, concentrating on the infrastructure of Jay's Bank and specifically targeting the IP address 167.172.75.216. This allowed for a targeted evaluation of the network's security, ensuring a thorough assessment of the designated areas.

Methodological Approach: The SafeGuard Solutions team employed various ethical hacking techniques and methodologies to identify vulnerabilities within the targeted network. This systematic approach ensured comprehensive coverage and increased the chances of discovering potential security risks.

Timely Execution: The assessment was conducted within the specified time limitations, ensuring that the results were delivered promptly. This timeliness enables Jay's Bank to address the identified vulnerabilities swiftly and enhance their overall security posture.

Weaknesses:

Exclusion of Physical Security: The assessment did not encompass the evaluation of physical security aspects, such as building security, physical locks, or other physical security measures. This limitation may leave potential vulnerabilities unexplored, as physical security can play a crucial role in overall system protection.

Omission of Social Factors: The assessment did not encompass the evaluation of social factors, such as security policies, employee training, or user awareness. Neglecting these factors may overlook potential human-related risks and vulnerabilities that can be exploited by adversaries.

Limited Evaluation of Third-Party Applications: The assessment excluded the evaluation of third-party applications unless they were directly connected to the assessed infrastructure. This limitation may lead to potential security gaps if vulnerabilities exist within those applications, even if they are indirectly related to the targeted network.

Vulnerability Summary & Report Card

The following tables illustrate the vulnerabilities found by impact and recommended remediations:

Internal Penetration Test Findings

13	5	6	0	1
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Internal Penetration Test		
IPT-001: Insufficient LLMNR Configuration	Critical	Disable multicast name resolution via GPO.
IPT-002: Security Misconfiguration – Local Admin Password Reuse	Critical	Utilize unique local admin passwords and limit local admin users via least privilege.
IPT-003: Security Misconfiguration – Wdigest	Critical	Disable WDigest via GPO.
IPT-004: Insufficient Hardening – Token Impersonation	Critical	Restrict token delegation.
IPT-005: Insufficient Password Complexity	Critical	Implement CIS Benchmark password requirements / PAM solution.
IPT-006: Security Misconfiguration – IPv6	Critical	Restrict DHCPv6 traffic and incoming router advertisements in Windows Firewall via GPO.

IPT-007: Insufficient Hardening – SMB Signing Disabled	Critical	Enable SMB signing on all Demo Corp domain computers.
IPT-008: Insufficient Patch Management – Software	Critical	Update to the latest software version.
IPT-009: Insufficient Patch Management – Operating Systems	Critical	Update Operating Systems to the latest version.
IPT-010: Insufficient Patching – MS08-067 - ECLIPSEDWING/NETAPI	Critical	Apply the appropriate Microsoft patches to remediate the issue.
IPT-011: Insufficient Patching – MS12-020 – Remote Desktop RCE	Critical	Apply the appropriate Microsoft patches to remediate the issue.
IPT-012: Insufficient Patching – MS17-010 - EternalBlue	Critical	Apply the appropriate Microsoft patches to remediate the issue.
IPT-013: Insufficient Patching – CVE-2019-0708 - BlueKeep	Critical	Apply the appropriate Microsoft patches to remediate the issue.

Finding	Severity	Recommendation
IPT-014: Insufficient Privileged Account Management – Kerberoasting	High	Use Group Managed Service Accounts (GMSA) for privileged services.
IPT-015: Security Misconfiguration – GPP Credentials	High	Apply vendor patching. Do not use GPP cpasswords.
IPT-016: Insufficient Authentication - VNC	High	Enable authentication on the VNC Server.
IPT-017: Default Credentials on Web Services	High	Change default credentials or disable unused accounts.
IPT-018: Insufficient Hardening – Listable Directories	High	Restrict access and conduct web app assessment.
IPT-019: Unauthenticated SMB Share Access	Moderate	Disable SMB share or require authentication.
IPT-020: Insufficient Patch Management – SMBv1	Moderate	Upgrade to SMBv3 and apply latest patching.
IPT-021: IPMI Hash Disclosure	Moderate	Disable IPMI over LAN if it is not needed.
IPT-022: Insufficient SNMP Community String Complexity	Moderate	Disabled SNMP if not required.
IPT-023: Insufficient Data in Transit Encryption - Telnet	Moderate	Migrate to TLS protected protocols.
IPT-024: Insufficient Terminal Services Configuration	Moderate	Enable Network Level Authentication (NLA) on the remote RDP server.
IPT-025: Steps to Domain Admin	Informational	Review action and remediation steps.

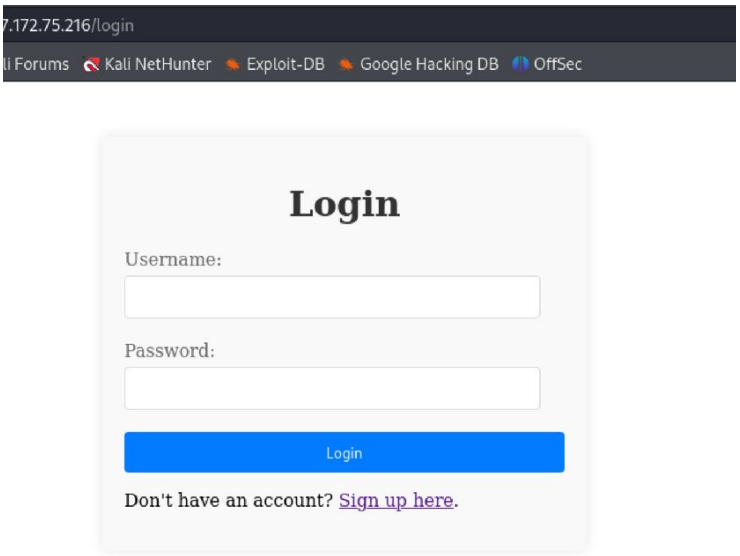
Technical Findings

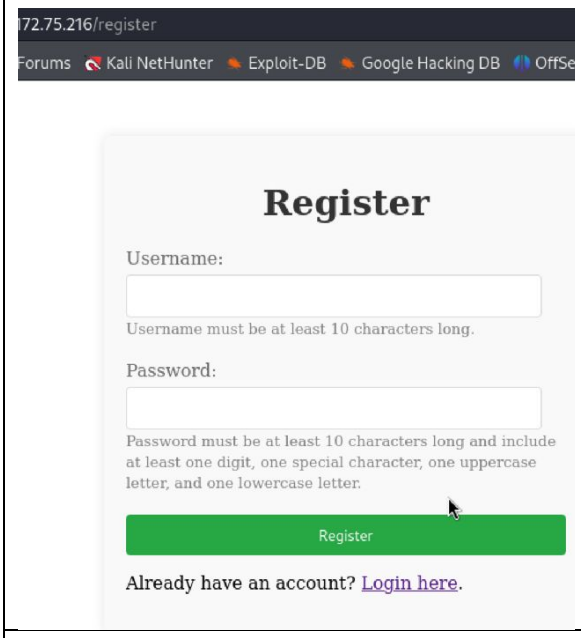
Internal Penetration Test Findings

I. Reconnaissance

- Tahap **ini memeriksa aplikasi web,** membuka browser di Kali Linux dan akses aplikasi Jay's Bank melalui `http://167.172.75.216`.

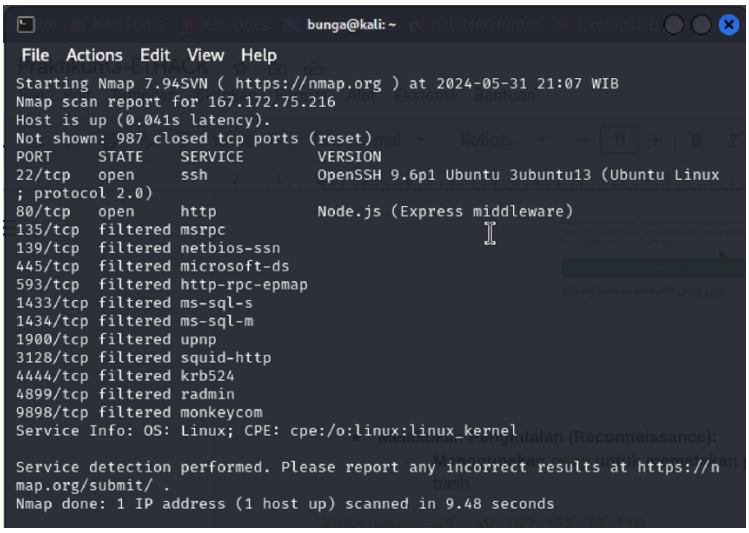
- Amati fungsi-fungsi utama aplikasi, halaman login, pendaftaran, dan semua fitur yang terlihat.
- **Melakukan Pengintaian (Reconnaissance):**
  Menggunakan `nmap` untuk memetakan port terbuka: bash
  `sudo nmap -sS -sV 167.172.75.216`



Selanjutnya,

```
sudo nmap -sS -sV 167.172.75.216
```



Hasil pemindaian menunjukkan bahwa host dengan IP 167.172.75.216 memiliki beberapa port terbuka, antara lain:

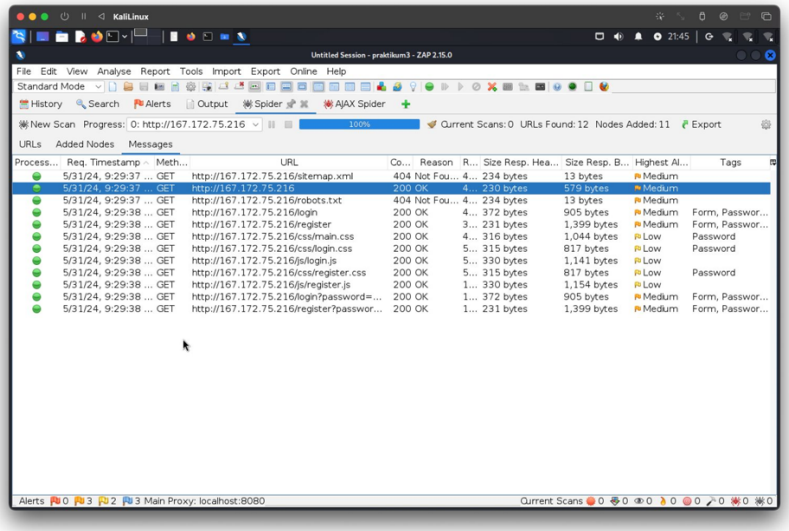
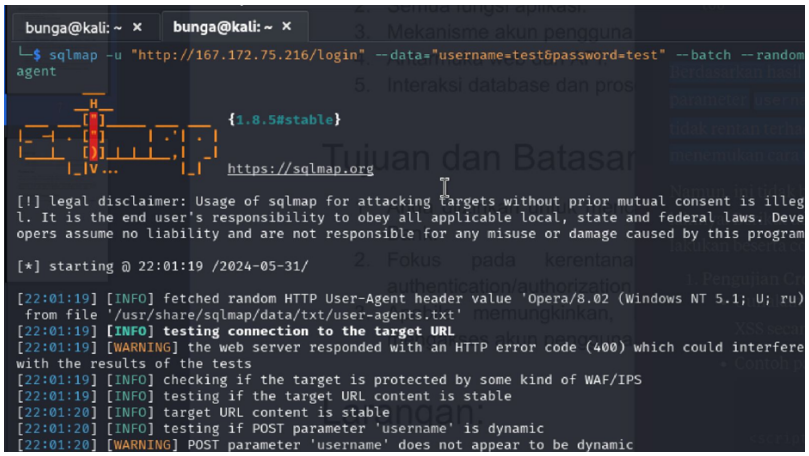
1. Port 22 (SSH) - Menjalankan layanan OpenSSH versi 9.6p1.
2. Port 80 (HTTP) - Menjalankan aplikasi web Node.js dengan middleware Express.

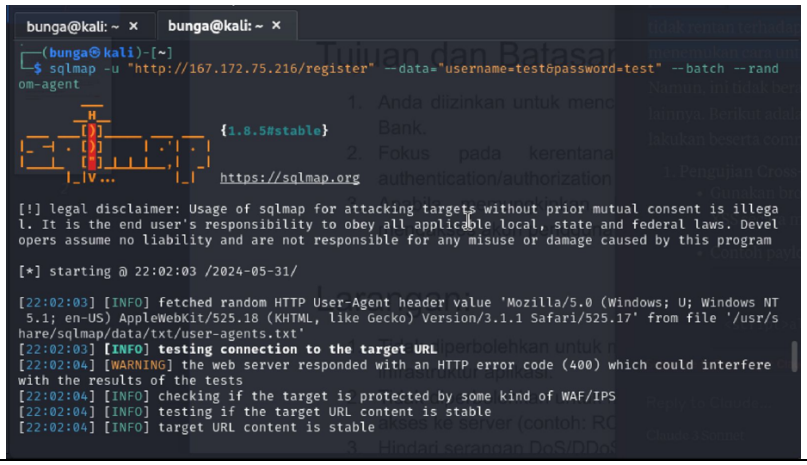
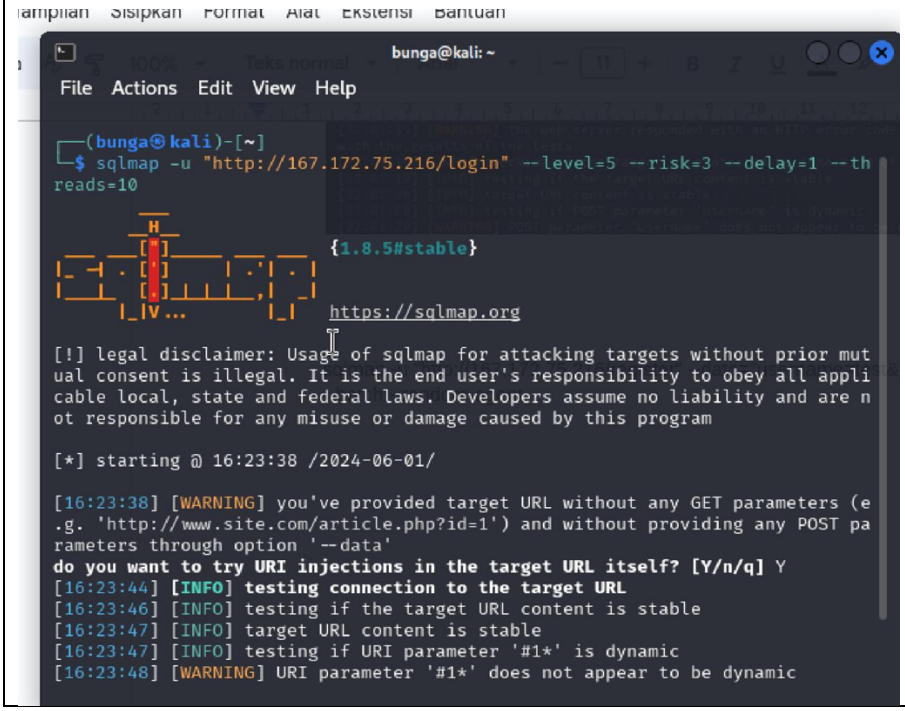
Selain itu, beberapa port lain seperti 135, 139, 445, 593, 1433, 1434, 1900, 3128, 4444, 4899, dan 9898 terfilter atau tertutup.

II. Pengujian Kerentanan Web

Menggunakan alat seperti OWASP ZAP atau Burp Suite untuk melakukan pengujian kerentanan pada aplikasi web yang berjalan di port 80 (HTTP).

Menggunakan OWASP ZAP, dengan men jalankan perintah untuk memulai ZAP: zaproxy

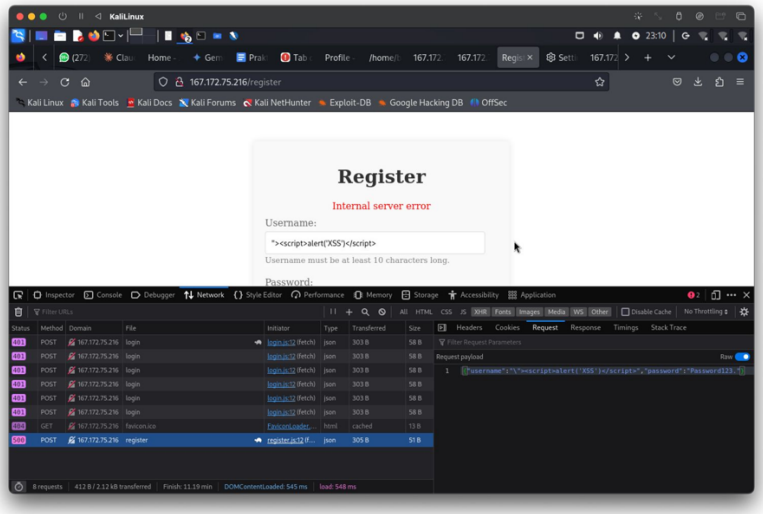
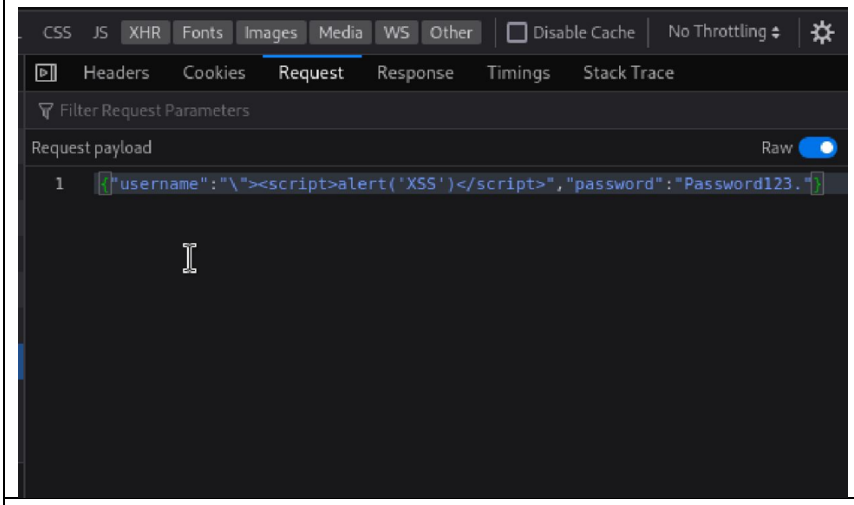
	Permintaan HTTP yang dilakukan mencakup mengambil file CSS, JavaScript, halaman login, halaman registrasi, halaman utama, robots.txt, dan sitemap.xml. Permintaan juga mencakup percobaan login dan registrasi dengan menggunakan kredensial "ZAP" sebagai username dan password.
sqlmap -u "http://167.172.75.216/login" --data="username=test&password=test" --batch --random-agent 	Pengujian SQL Injection pada parameter `username` dan `password` pada halaman login.

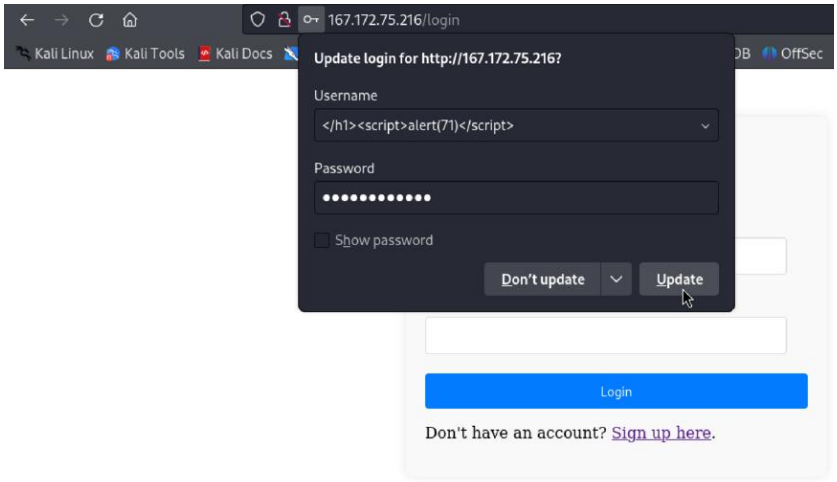
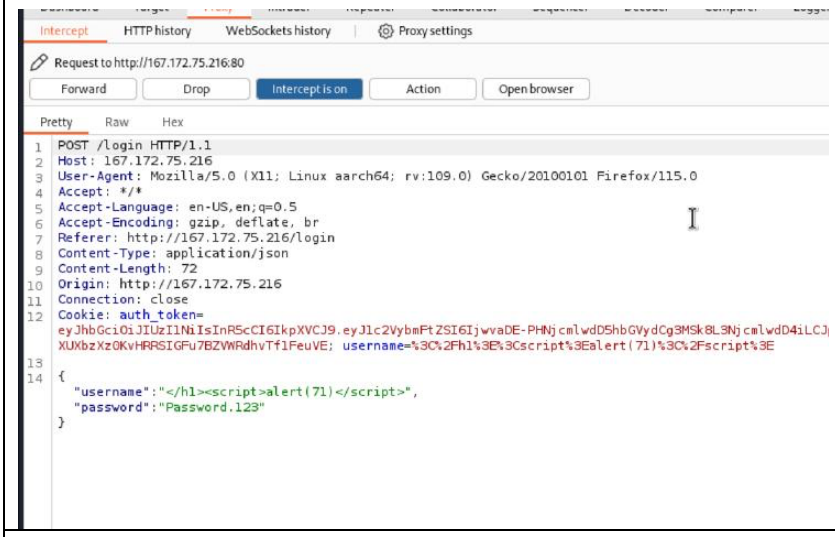
sqlmap -u "http://167.172.75.216/register" --data="username=test&password=test" --batch --random-agent  	Pengujian SQL Injection pada parameter `username` dan `password` pada halaman registrasi. Parameter `username` dan `password` pada halaman login dan registrasi tidak rentan terhadap serangan SQL Injection.
sqlmap -u "http://167.172.75.216/login" --level=5 --risk=3 --delay=1 --threads=10  	untuk melakukan pengujian yang mendalam dan agresif pada endpoint login tersebut, dengan tingkat risiko yang tinggi dan dengan memperhatikan jeda waktu untuk menghindari deteksi atau pemblokiran oleh mekanisme keamanan.

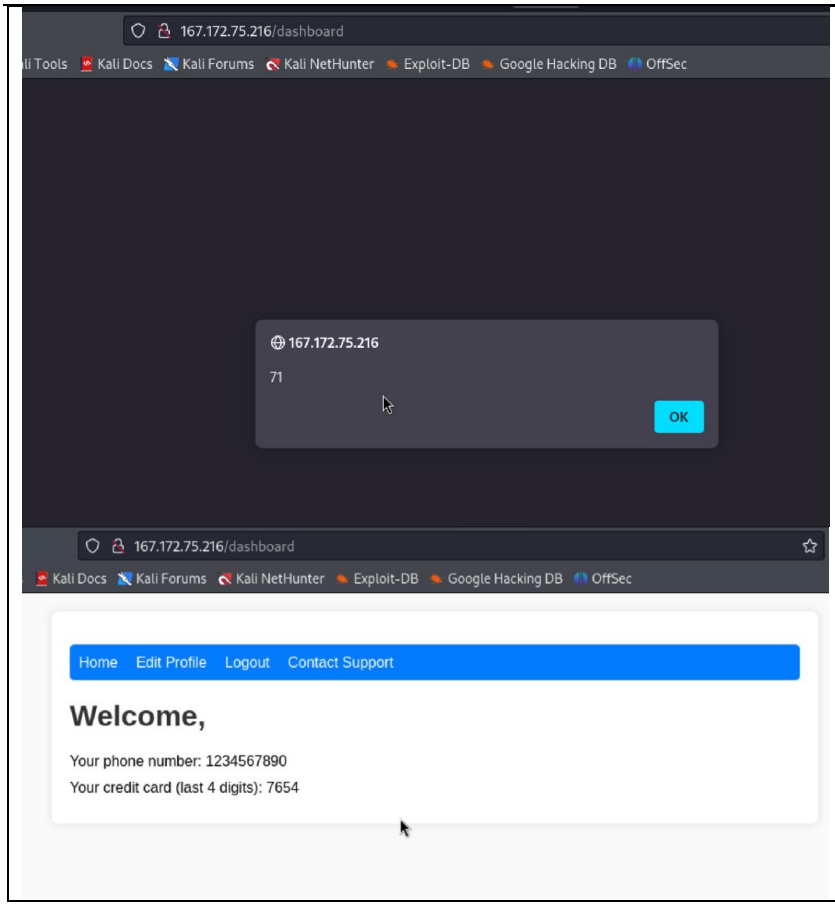
III. Analisis Kerentanan (Vulnerability Assessment)

1. Pengujian Cross-Site Scripting (XSS)

- Menggunakan input halaman login dan registrasi untuk memasukkan script xss

<script>alert('XSS')</script>   	Menyisipkan tag skrip yang akan menampilkan kotak dialog dengan angka 71 saat dieksekusi oleh browser.
Login dan sign up dengan </h1><script>alert(71)</script>	

	
Melakukan spidering dengan Burp Suite 	
Setelah dilakukan kelengkapan profile, buka dan login Kembali menggunakan </h1><script>alert(71)</script> **Sehingga akan muncul pop up xss SEBAGAI BERIKUT:**	ada kotak dialog atau pesan yang muncul dengan alert(71), maka itu menunjukkan kerentanan XSS.



IV. Eksploitasi (Exploitation)

menganalisis hasil dari langkah sebelumnya untuk menemukan kerentanan yang dapat dieksploitasi.

Finding IPT-001: Insufficient LLMNR Configuration (Critical)

Description:	Demo Corp allows multicast name resolution on their end-user networks. TCMS captured 20 user account hashes by poisoning LLMNR traffic and cracked 2 with commodity cracking software. The cracked accounts were used to leverage further access that led to the compromise of the Domain Controller.

Risk:	Likelihood: High – This attack is effective in environments allowing multicast name resolution. Impact: Very High – LLMNR poisoning permits attackers to capture password hashes to either crack offline or relay in real-time and pivot laterally in the environment.
System:	All
Tools Used:	Responder, Hashcat
References:	Stern Security - Local Network Attacks: LLMNR and NBT-NS Poisoning NIST SP800-53 r4 IA-3 - Device Identification and Authentication NIST SP800-53 r4 CM-6(1) - Configuration Settings

Evidence

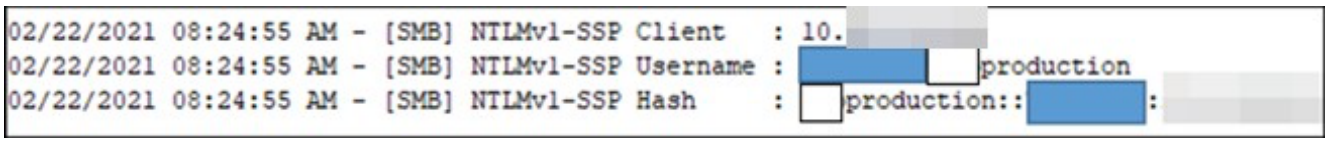


Figure 1: Captured hash of "production"

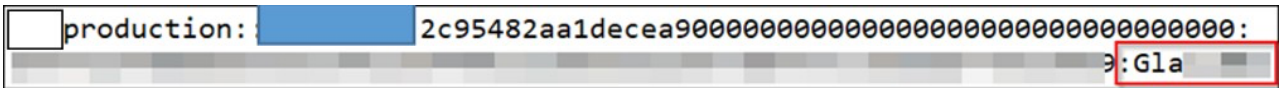


Figure 2: Cracked hash of "production"

Remediation

Disable multicast name resolution via GPO. For full mitigation and detection guidance, please reference the MITRE guidance here.

The cracked hashes demonstrate a deficient password complexity policy. If multicast name resolution is required, Network Access Control (NAC) combined with application whitelisting can limit these attacks.

Finding IPT-002: Security Misconfiguration – Local Admin Password Reuse (Critical)

Description:	TCMS utilized local administrator hashes to gain access to other machines in the network via a 'pass-the-hash' attack. The local administrator hashes were obtained via machine access provided by the cracked account in IPT-001. Pass-the-hash attacks do not require knowing the account password to successfully log into a machine. Thus, reusing the same local admin password (and therefore the same hash) on multiple machines will permit system access to those computers. TCMS leveraged this attack to gain access to ~50 machines within the main office. This led to further account access and the eventual compromise of the domain controller.
Risk:	Likelihood: High – This attack is effective in large networks with local admin password reuse. Impact: Very High – Pass-the-hash permits an attacker to move laterally and vertically throughout the network.
System:	All
Tools Used:	Impacket, Crackmapexec
References:	https://capec.mitre.org/data/definitions/644.html https://tcm-sec.com/pentest-tales-001-you-spent-how-much-on-security/

Evidence

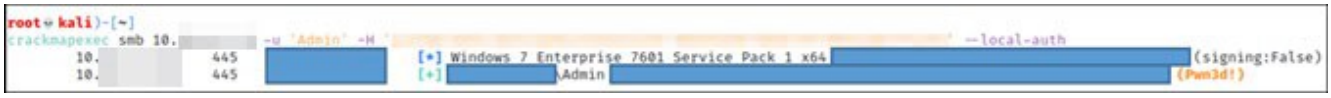


Figure 3: Local admin hash used to gain access to machine

Remediation

Utilize unique local admin passwords. Limit local admin users via least privilege. Consider implementing a PAM solution. For full mitigation and detection guidance, please reference the MITRE guidance here.

Finding IPT-003: Security Misconfiguration – WDigest (Critical)

Description:	Demo Corp permitted out-of-date operating systems within their network, including Windows 7, 8, Server 2008, and Server 2012. These operating systems, by default, permit WDigest, which stores all current logged-in user's passwords in clear-text. TCMS leveraged machine access gained in IPT-001 and IPT-002 to move laterally throughout the network until uncovering a machine with Domain Admin credentials stored in WDigest.
Risk:	Likelihood: Moderate – This attack is effective in networks with older operating systems. Impact: Very High – WDigests credentials are stored in clear text, which can permit the theft of sensitive accounts, such as Domain Administrators.
System:	All systems older than Windows 10 and Server 2016
Tools Used:	Metasploit, Kiwi
References:	https://stealthbits.com/blog/wdigest-clear-text-passwords-stealing-more-than-a-hash/

Evidence

Figure 4: Cleartext passwords of Domain Administrators

Remediation

Disable WDigest via GPO. For full mitigation and detection guidance, please reference the guidance here.

Finding IPT-004: Insufficient Hardening – Token Impersonation (Critical)

Description:	TCMS impersonated the token of “supcb” to obtain Domain Administrator privileges.
Risk:	Likelihood: High – The penetration tester viewed and impersonated tokens with the use of open-source tools. Impact: Very High - If exploited, an attacker gains domain administrator access.
System:	All
Tools Used:	Metasploit, Incognito
References:	NIST SP800-53 r4 CM-7 - Least Functionality NIST SP800-53 r4 AC-6 - Least Privilege https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/how-to-configure- protected-accounts

Evidence

Figure 5: Impersonation of “sup”

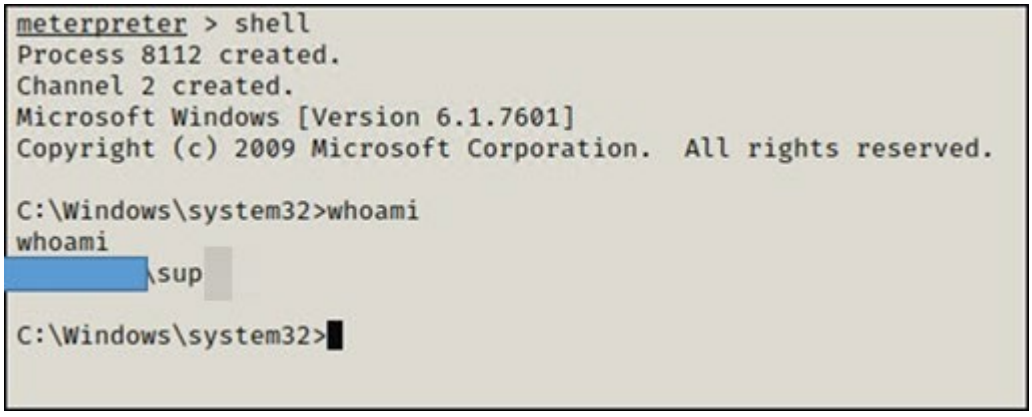


Figure 6: Shell access as Domain Admin “sup”

Remediation

Restrict token delegation. For full mitigation and detection guidance, please reference the MITRE guidance here.

Finding IPT-005: Insufficient Password Complexity (Critical)

Description:	TCMS dumped hashes from the domain controller and proceeded to attempt common password guessing attacks against all users. TCMS cracked 2,226 passwords using basic password list guessing attacks and low effort brute forcing attacks. 17 cracked accounts had domain administrator rights.
Risk:	Likelihood: High - Simple passwords are susceptible to password cracking attacks. Encryption provides some protection, but dictionary attacks base on common word lists often crack weak passwords. Impact: Very High - Domain admin accounts with weak passwords could lead to an adversary critically impacting Demo Corp ability to operate.
System:	All
Tools Used:	Manual Review
References:	NIST SP800-53 IA-5(1) - Authenticator Management https://www.cisecurity.org/white-papers/cis-password-policy-guide/

Evidence

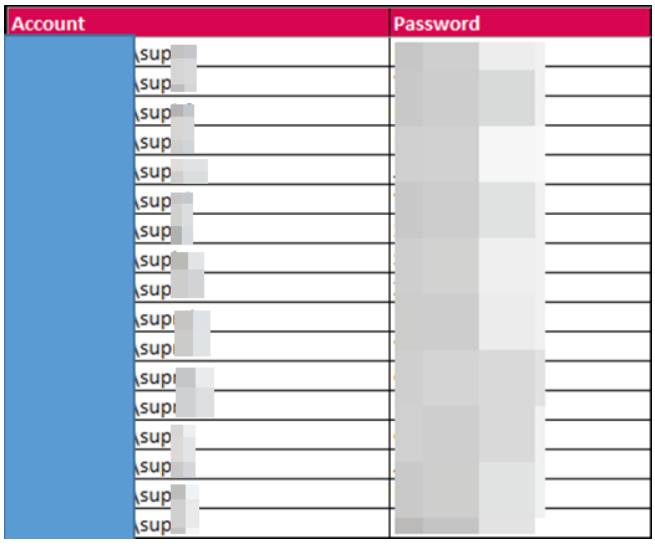


Figure 7: Excerpt of cracked domain hashes

Remediation

Implement CIS Benchmark password requirements / PAM solution. TCMS recommends that Demo Corp enforce industry best practices around password complexity and management. A password filter to prevent users from using common and easily guessable passwords is also recommended. Additionally, TCMS recommends that Demo Corp enforce stricter password requirements for Domain Administrator and other sensitive accounts.

Finding IPT-006: Security Misconfiguration – IPv6 (Critical)

Description:	Through IPv6 DNS poisoning, the TCMS team was able to successfully relay credentials to the Demo Corp domain controller.
Risk:	Likelihood: High – IPv6 is enabled by default on Windows networks. The tools and techniques required to perform this task are trivial. Impact: Very High - If exploited, an attacker can gain domain administrator access.
System:	All
Tools Used:	Mitm6, Impacket
References:	https://blog.fox-it.com/2018/01/11/mitm6-compromising-ipv4-networks-via-ipv6/

Evidence

Figure 8: Successfully relayed LDAP credentials via mitm6

Remediation

1. IPv6 poisoning abuses the fact that Windows queries for an IPv6 address even in IPv4-only environments. If you do not use IPv6 internally, the safest way to prevent mitm6 is to block DHCPv6 traffic and incoming router advertisements in Windows Firewall via Group Policy. Disabling IPv6 entirely may have unwanted side effects. Setting the following predefined rules to Block instead of Allow prevents the attack from working:
    a. (Inbound) Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCPV6-In)
    b. (Inbound) Core Networking - Router Advertisement (ICMPv6-In)
    c. (Outbound) Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCPV6-Out)
2. If WPAD is not in use internally, disable it via Group Policy and by disabling the WinHttpAutoProxySvc service.
3. Relaying to LDAP and LDAPS can only be mitigated by enabling both LDAP signing and LDAP channel binding.

Consider Administrative users to the Protected Users group or marking them as Account is sensitive and cannot be delegated, which will prevent any impersonation of that user via delegation.

Finding IPT-007: Insufficient Hardening – SMB Signing Disabled (Critical)

Description:	Demo Corp failed to implement SMB signing on multiple devices. The absence of SMB signing could lead to SMB relay attacks, yielding system-level shells without requiring a user password.
Risk:	Likelihood: High – Relaying password hashes is a basic technique not requiring offline cracking. Impact: High – If exploited, an adversary gains code execution, leading to lateral movement across the network.
System:	Identified 709 machines, please see the below file for listing. [file removed]
Tools Used:	Nessus, Nmap, MultiRelay, Responder
References:	CIS Microsoft Windows Server 2012 R2 v2.2.0 (Page 180) https://github.com/lgandx/Responder/blob/master/tools/MultiRelay.py

Evidence

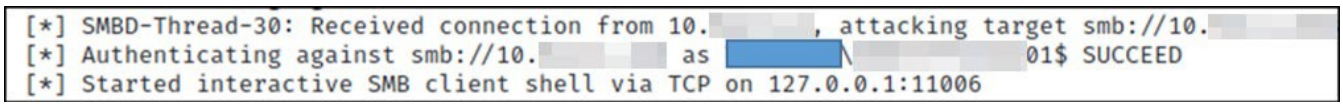


Figure 9: Successful SMB relay

Remediation

Enable SMB signing on all Demo Corp domain computers. Alternatively, as SMB signing can cause performance issues, disabling NTLM authentication, enforcing account tiering, and limiting local admin users can effectively help mitigate attacks. For full mitigation and detection guidance, please reference the MITRE guidance here.

Finding IPT-008: Insufficient Patch Management – Software (Critical)

Description:	Demo Corp permitted various deprecated software in their network. This includes: • Apache version < 2.4.46 • Apache Tomcat version < 7.0.100, 8.5.51, 9.0.31 • Cisoco AireOS version 8.5.151.10 • CodeMeter version 3.05 (5.21.1478.500) • Dropbear SSH Server version 2015.68 • Dell iDRAC7 version 2.63.60.62.01 • Dell iDRAC8 version 2.63.60.61.06 • Dell iDRAC9 version 3.36.36.36.21 • ESXi version 5.5 • ESXi version 6.5 build 15256549 • Flexera FlexNet Publisher version 11.16.0 • IIS version 7.5 • ISC BIND version 9.6.2-P2 • Microsoft DNS Server version 6.1.7601.24261 • Microsoft SQL Server version 11.0.6594.0 • Netatalk OpenSession version < 3.1.12 • PHP version < 7.3.11 • Rockwell Automation RSLinx Classic Above lists all critical and high-rated deprecated software, the majority of which permit serious vulnerabilities, such as remote code execution. For a full patching list, please review the provided Nessus scan documentation.
Risk:	Likelihood: High – An attacker can discover these vulnerabilities with basic tools. Impact: Very High – If exploited, an attacker could possibly gain full remote code execution on or deny service to a system.
Tools Used:	Nessus
References:	NIST SP800-53 r4 MA-6 – Timely Maintenance NIST SP800-53 r4 SI-2 – Flaw Remediation

Remediation

Update to the latest software version. For a full list of vulnerable systems, versions, and patching requirements, please see the below document.

[file removed]

Finding IPT-009: Insufficient Patch Management – Operating Systems (Critical)

Description:	Demo Corp permitted various deprecated software in their network. This includes: • Windows Server 2003 (end of life on July 14, 2015) • Windows Server 2008 R2 (end of life on January 14, 2020) • Windows XP (end of life on April 8, 2014) • Windows 7 (end of life on January 14, 2020) • Ubuntu 11 (end of life on May 9, 2013) • FreeBSD 11.0 (end of life on October, 2016) End of life systems are susceptible to a multitude of vulnerabilities. TCMS did not attempt any attacks against these servers due to the risk of a denial of service, which is out of scope.
Risk:	Likelihood: High – An attacker can discover these vulnerabilities with basic tools. Impact: High – If exploited, an attacker could possibly gain full remote code execution on or deny service to a system.
System:	Identified 139 machines, please see the below file for listing. [file removed]
Tools Used:	Nessus
References:	NIST SP800-53 r4 MA-6 – Timely Maintenance NIST SP800-53 r4 SI-2 – Flaw Remediation

Remediation

Update Operating Systems to the latest version.

Finding IPT-010: Insufficient Patching – MS08-067 - ECLIPSEDWING/NETAPI (Critical)

Description:	Demo Corp permitted an unpatched system on the internal network that is vulnerable to MS08-067. TCM Security confirmed that the vulnerability likely exists but did not attempt the exploit to prevent any denial of service.
Risk:	Likelihood: High – Considered one of the most exploited vulnerabilities in Microsoft Windows as it ships natively with Windows XP. Impact: Very High – If exploited, an attacker gains code execution as the system user. An adversary will require additional techniques to obtain domain administrator access.
System:	10.x.x.x
Tools Used:	Nessus, Nmap
References:	NIST SP800-53 r4 MA-6 – Timely Maintenance NIST SP800-53 r4 SI-2 – Flaw Remediation

Evidence

```
└─# nmap -p445 10.      --script smb-vuln-ms08-067
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-03 20:33 EST
Nmap scan report for      (10.      )
Host is up (0.014s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250

Nmap done: 1 IP address (1 host up) scanned in 10.55 seconds
```

Figure 10: Unpatched MS08-067

Remediation

Apply the appropriate Microsoft patches to remediate the issue. More information on patching MS08-067 can be found here: https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2008/ms08-067

Finding IPT-011: Insufficient Patching – MS12-020 – Remote Desktop RCE (Critical)

Description:	Demo Corp permitted an unpatched system on the internal network that is vulnerable to MS12-020. TCM Security confirmed that the vulnerability likely exists but did not attempt the exploit to prevent any denial of service.
Risk:	Likelihood: High – The vulnerability is easily discoverable and exploitable with open-source tools. Impact: Very High – If exploited, an attacker gains code execution as the system user. An adversary will require additional techniques to obtain domain administrator access.
System:	10.x.x.x
Tools Used:	Nessus, Nmap
References:	NIST SP800-53 r4 MA-6 – Timely Maintenance NIST SP800-53 r4 SI-2 – Flaw Remediation

Evidence

```
┌──(root㉿kali)-[~]
└─# nmap -p3389 10.      --script rdp-vuln-ms12-020
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-03 20:35 EST
Nmap scan report for                                (10.      )
Host is up (0.014s latency).

PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
| rdp-vuln-ms12-020:
|   VULNERABLE:
|   MS12-020 Remote Desktop Protocol Denial Of Service Vulnerability
|     State: VULNERABLE
|     IDs:  CVE:CVE-2012-0152
|     Risk factor: Medium  CVSSv2: 4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:N/A:P)
|           Remote Desktop Protocol vulnerability that could allow remote attackers to cause a denial of service.
|
|     Disclosure date: 2012-03-13
|     References:
|       http://technet.microsoft.com/en-us/security/bulletin/ms12-020
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0152
|
|   MS12-020 Remote Desktop Protocol Remote Code Execution Vulnerability
|     State: VULNERABLE
|     IDs:  CVE:CVE-2012-0002
|     Risk factor: High  CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
|           Remote Desktop Protocol vulnerability that could allow remote attackers to execute arbitrary code on the targeted system.
|
|     Disclosure date: 2012-03-13
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0002
|_      http://technet.microsoft.com/en-us/security/bulletin/ms12-020
```

Figure 11: Unpatched MS12-020

Remediation

Apply the appropriate Microsoft patches to remediate the issue. More information on patching MS12-020 can be found here: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2012/ms12-020

Finding IPT-012: Insufficient Patching – MS17-010 - EternalBlue (Critical)

Description:	Demo Corp permitted several unpatched systems on the internal network that are vulnerable to MS17-010 (EternalBlue). TCM Security confirmed that the vulnerability likely exists but did not attempt the exploit to prevent any denial of service.
Risk:	Likelihood: High – Malicious actors have used SMB exploitations like EternalBlue in recent breaches. Impact: Very High – If exploited, an attacker gains code execution as the system user. An adversary will require additional techniques to obtain domain administrator access.
System:	10.x.x.x
Tools Used:	Nessus, Metasploit, AutoBlue
References:	NIST SP800-53 r4 MA-6 – Timely Maintenance NIST SP800-53 r4 SI-2 – Flaw Remediation

Evidence

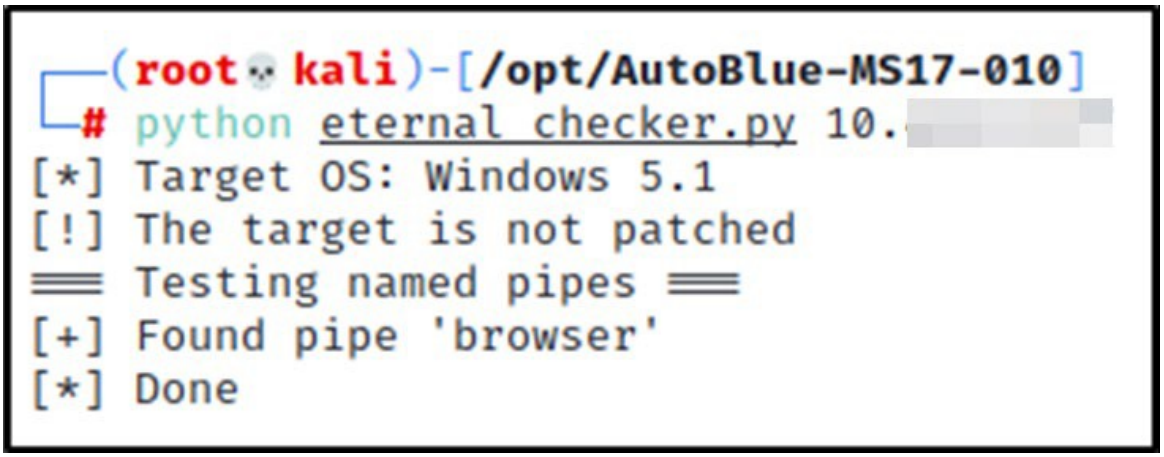


Figure 12: Unpatched MS17-010

Remediation

Apply the appropriate Microsoft patches to remediate the issue. More information on patching MS17-010 can be found here: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

Finding IPT-013: Insufficient Patching – CVE-2019-0708 - BlueKeep (Critical)

Description:	Demo Corp permitted several unpatched systems on the internal network that are vulnerable to CVE-2019-0708 (BlueKeep). TCM Security confirmed that the vulnerability likely exists but did not attempt the exploit to prevent any denial of service.
Risk:	Likelihood: High – The vulnerability is easily discoverable and exploitable with open-source tools. Impact: Very High – If exploited, an attacker gains code execution as the system user. An adversary will require additional techniques to obtain domain administrator access.
System:	10.x.x.x
Tools Used:	Nessus, Nmap
References:	NIST SP800-53 r4 MA-6 – Timely Maintenance NIST SP800-53 r4 SI-2 – Flaw Remediation

Evidence

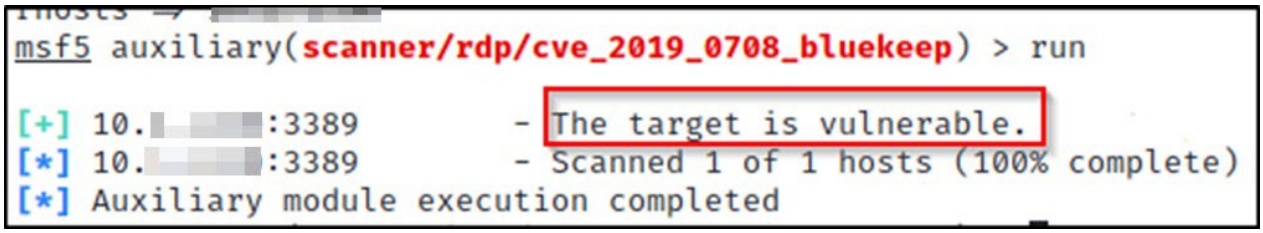


Figure 13: Unpatched CVE-2019-0708

Remediation

Apply the appropriate Microsoft patches to remediate the issue. More information on patching CVE-2019-0708 can be found here: https://support.microsoft.com/en-us/topic/customer-guidance-for-cve-2019-0708-remote-desktop-services-remote-code-execution-vulnerability-may-14-2019-0624e35b-5f5d-6da7-632c-27066a79262e

Finding IPT-014: Insufficient Privileged Account Management – Kerberoasting (High)

Description:	TCMS retrieved all user service principal names (SPNs) from the Demo Corp domain controller using a domain user-level account (IPT-001) in a Kerberoasting attack. Retrieving these user SPNs permitted TCMS to crack 4 account passwords. No service accounts were observed running as domain administrators. User accounts were observed running as a service, which is not best practice.
Risk:	Likelihood: High – Any account joined to the domain can request user SPNs. Impact: High – Using SPNs, it is possible to retrieve sensitive account password hashes and crack them offline.
Tools Used:	Impacket, Hashcat
References:	Kerberoasting details: https://adsecurity.org/?p=2293 Group Managed Service Accounts Overview

Evidence

Account		Location	Password
[redacted]	[redacted]	$MSSQLSvc/ [redacted]	[redacted]
		$MSSQLSvc/	
adfs		$host/adfs	
sqladmin		$MSSQLSvc/UKSQL01	

Figure 14: Cracked service accounts

Remediation

Use Group Managed Service Accounts (GMSA) for privileged services. GMSA accounts can be used to ensure passwords are long, complex, and change frequently. Where GMSA is not applicable, protect accounts by utilizing a password vaulting solution.

TCMS recommends configuring alert logging on domain controllers for Windows event ID 4769 whenever requesting a Kerberos service ticket. These alerts are prone to high false-positive rates but are a supplementary detective control. Tailor a security information and event management tool (SIEM) to alert on excessive user SPN requests.

Finding IPT-015: Security Misconfiguration – GPP Credentials (High)

Description:	Demo Corp utilized “cpasswords” in Group Policy Preference (GPP) which any domain user can query from a domain controller’s SYSVOL folder. Microsoft published the key to decrypt these passwords.
Risk:	Likelihood: High – Any authenticated user can obtain this information and decrypt the password with open source tools. Impact: High – An adversary can use these credentials to move laterally within the network.
Tools Used:	Metasploit
References:	NIST SP800-53 IA-5(1) - Authenticator Management

Evidence

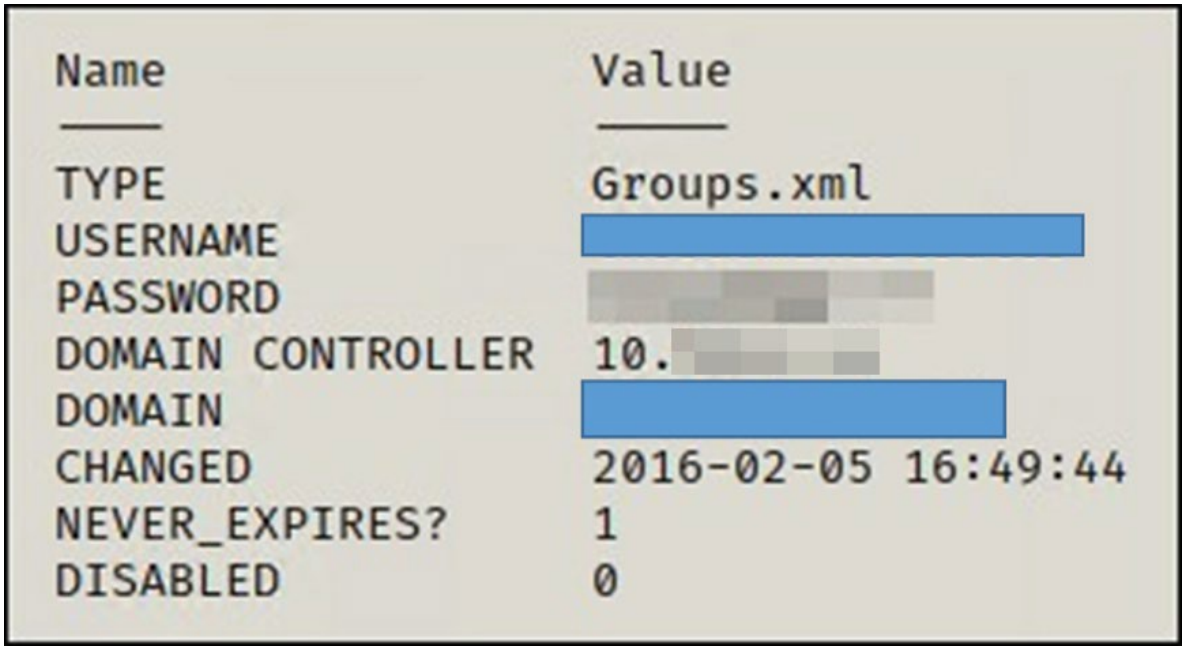


Figure 15: Dumped GPP credentials

Remediation

Apply vendor patching. Do not use GPP cpasswords. Additionally, enabling authentication on the NFS share will protect the confidentiality of the stored information. Exporting authentication logs to a SIEM solution will give incident response teams insights to brute force login attempts.

Finding IPT-016: Insufficient Authentication - VNC (High)

Description:	Demo Corp deployed 3 servers that permitted unauthenticated access via VNC Server.
Risk:	Likelihood: High – Discovering unauthenticated VNC servers is trivial and can be done with open-source tools. Impact: High – Attackers can control industrial devices, destroy data, or shut down systems.
System:	10.x.x.x, 10.x.x.x, 10.x.x.x
Tools Used:	Nessus, VNC Viewer
References:	NIST SP800-53 IA-5(1) - Authenticator Management

Evidence

[image redacted]

Figure 16: Access to system via VNC

Remediation

Enable authentication on the VNC Server.

Finding IPT-017: Default Credentials on Web Services (High)

Description:	TCMS validated default credentials worked on multiple web applications within the Demo Corp environment.
Risk:	Likelihood: High – Credentials are published for these devices and an attackers first authentication attempt. Impact: High – Attackers can control devices, destroy data, or shut down systems.
System:	Default credentials were tested on a sample set of web applications, but suggests checking the following addresses at a minimum: [file removed]
Tools Used:	Manual Review
References:	NIST SP800-53 IA-5(1) - Authenticator Management

Evidence

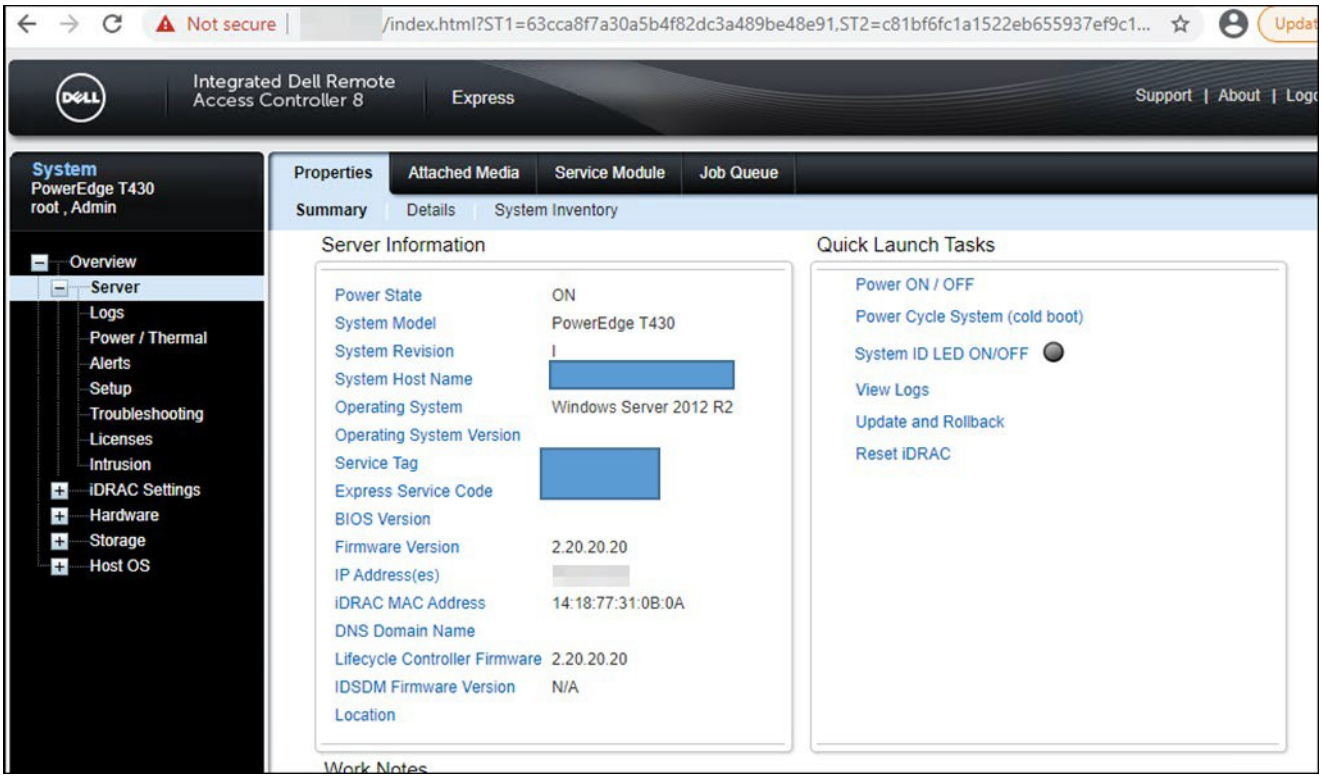


Figure 17: Dell iDRAC access via default credentials

Remediation

Change default credentials or disable unused accounts.

Finding IPT-018: Insufficient Hardening – Listable Directories (High)

Description:	Demo Corp disclosed information by allowing listable directories and storing potentially critical items on web server. It is strongly recommended that Demo Corp perform a thorough web app assessment on this resource.
Risk:	Likelihood: Moderate – Adversaries will discovery content with open source tools. Impact: High – Attackers use this information in conjunction with other attacks for enumeration and cataloging for rapid attacks when vulnerabilities arise.
System:	Full list of discovered listable directories: [file removed]
Tools Used:	Manual Review
References:	NIST SP800-53r4 CM-7 - Least Functionality NIST SP800-53r4 AC-6(3) - Least Privilege

Evidence

Figure 18: Listable directory

Remediation

Restrict access and conduct web app assessment.

Finding IPT-019: Unauthenticated SMB Share Access (Moderate)

Description:	Demo Corp exposed multiple servers with unauthenticated file server access.
Risk:	Likelihood: Moderate – Adversaries will discover these shares with low-noise, basic reconnaissance techniques. Impact: Moderate – Attackers learn about the environment through information leaks.
System:	10.x.x.x
Tools Used:	Nessus, smbclient
References:	NIST SP800-53r4 AC-6(3) - Least Privilege NIST SP800-53 r4 SC-4 - Information in Shared Resources

Evidence

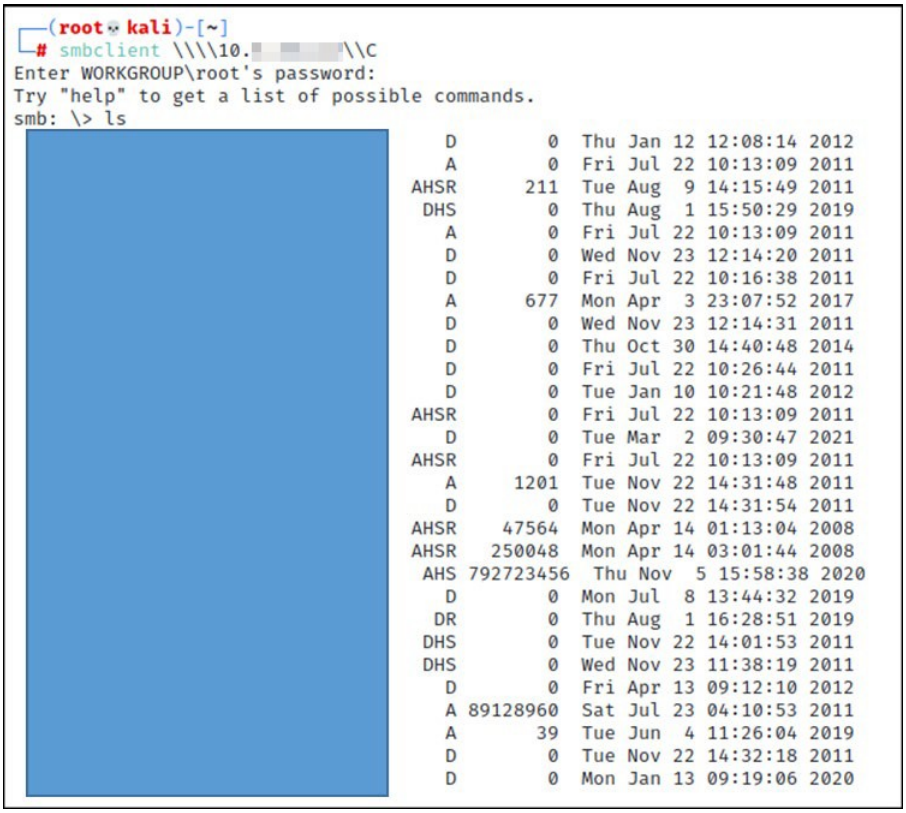


Figure 19: Unauthenticated Share access

Remediation

Disable SMB share or require authentication. Enabling authentication on the share will protect the confidentiality of the stored information. Exporting authentication logs to a SIEM solution will give incident response teams insights to brute force login attempts.

Finding IPT-020: Insufficient Patch Management – SMBv1 (Moderate)

Description:	Demo Corp failed to patch SMBv1. This version is vulnerable to multiple denial of service and remote code execution attacks. TCM Security confirmed that the vulnerability likely exists but did not attempt the exploit to prevent any denial of service.
Risk:	Likelihood: Moderate – Basic scans would identify the SMB version but would require an adversary to be on the internal network and identify an exploit. Impact: Moderate – If exploited, an attacker gains denial of service and code execution capability.
System:	10.x.x.x
Tools Used:	Nessus, Nmap
References:	https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/ NIST SP800-53 r4 SI-2 - Flaw Remediation

Evidence

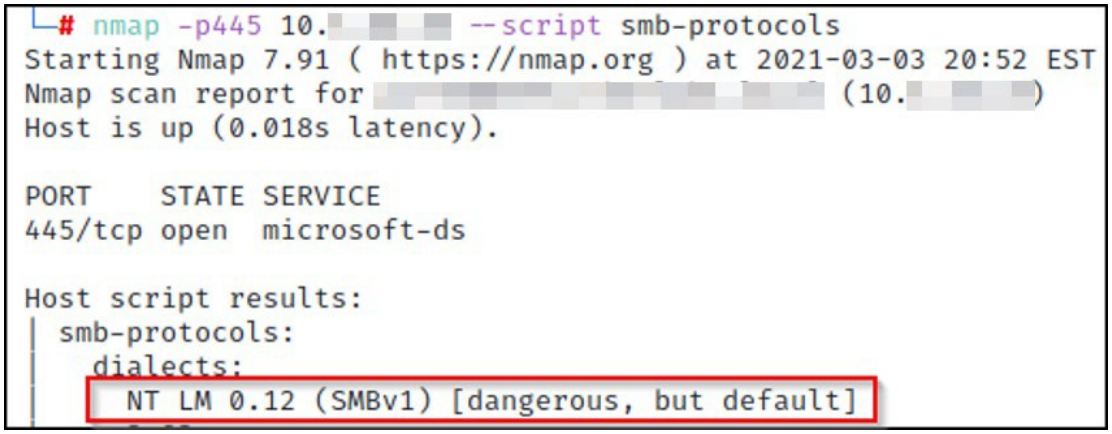


Figure 20: Unauthenticated Share access

Remediation

Upgrade to SMBv3 and apply latest patching.

Finding IPT-021: IPMI Hash Disclosure (Moderate)

Description:	Demo Corp deployed remote host supporting IPMI v2.0. The (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.
Risk:	Likelihood: High – Basic network scans will identify this vulnerability. Impact: Moderate – If exploited, an attacker can gain access to sensitive management devices. TCMS was unable to crack any hashes during the assessment.
System:	Identified 34 machines, please see the below file for listing. [file removed]
Tools Used:	Metasploit
References:	https://blog.rapid7.com/2013/07/02/a-penetration-testers-guide-to-ipmi/

Evidence

```
msf5 auxiliary(scanner/ipmi/ipmi_dumphashes) > run

[+] 10.        :623 - IPMI - Hash found: ADMIN:f8eebcbd001f0002c59416c40661b548d380d3c792a107
[+] 10.        :623 - IPMI - Hash found: admin:0b864a780120000212083f65bff25cb99c739d4da2112c
[+] 10.        :623 - IPMI - Hash found: root:6234bf90022100020649c4cb1b75238fd071fcf0acb2f36
[+] 10.        :623 - IPMI - Hash found: Administrator:b7c1b69c03220002b4b923efc2c8fbc00adab1
```

Figure 21: IPMI Hash Disclosure

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 successfulness of off-line dictionary attacks.
- Using Access Control Lists (ACLs) or isolated networks to limit access to your IPMI management interfaces.

Finding IPT-022: Insufficient SNMP Community String Complexity (Moderate)

Description:	Demo Corp deployed SNMP with default “public” community strings. This configuration exposed read-only access to the system’s management information base (MIB), including the network configurations.
Risk:	Likelihood: High – Basic network scans will identify this vulnerability. Impact: Moderate – If exploited, an attacker can profile the device and focus attacks.
System:	Identified 45 machines, please see the below file for listing. [file removed]
Tools Used:	Nessus, SNMP-Check, Ettercap
References:	NIST SP800-53 r4 AC-17(2) - Remote Access Protection of Confidentiality/Integrity using Encryption

Evidence

```
[+] Try to connect to 10.        :161 using SNMPv1 and community 'public'

[*] System information:

  Host IP address               : 10.
  Hostname                      :
  Description                   : -
  Contact                       : "support@dell.com"
  Location                      : "unknown"
  Uptime snmp                   : -
  Uptime system                 : 382 days, 06:54:09.76
  System date                   : -
```

Figure 22: Information disclosure via public SNMP community strings

Figure 23: Non-public SNMP string captured via Ettercap

Remediation

TCM Security recommends Demo Corp consider the following corrective actions:

- Disabled SNMP if not required
- Filter UDP packets going to port UDP – 161
- Evaluate migration to SNMPv3
- Use password complexity guidelines for community strings

Finding IPT-023: Insufficient Data in Transit Encryption - Telnet (Moderate)

Description:	Demo Corp permitted Telnet which does not encrypt data in transit. Telnet uses plain text authentication and passes all data (including passwords) in clear text and can be intercepted by an attacker.
Risk:	Likelihood: Low – An adversary requires a Man-in-the-Middle position between the client and server. Impact: High – If exploited an adversary may intercept administrative credentials that can be used in other attacks.
System:	Identified 53 machines, please see the below file for listing. [file removed]
Tools Used:	Telnet
References:	NIST SP800-53 r4 AC-17(2) - Remote Access |Protection of Confidentiality / Integrity Using Encryption

Evidence

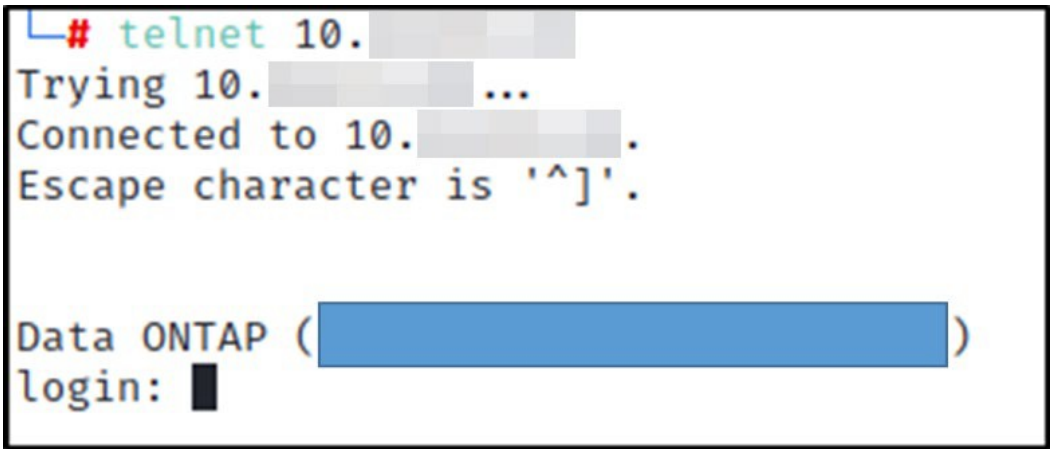


Figure 24: Telnet login prompt

Remediation

Migrate to TLS protected protocols.

Finding IPT-024: Insufficient Terminal Services Configuration (Moderate)

Description:	The remote Terminal Services is not configured to use Network Level Authentication (NLA) only. NLA uses the Credential Security Support Provider (CredSSP) protocol to perform strong server authentication either through TLS/SSL or Kerberos mechanisms, which protect against man-in-the-middle attacks. In addition to improving authentication, NLA also helps protect the remote computer from malicious users and software by completing user authentication before a full RDP connection is established.
Risk:	Likelihood: Low – An attacker can discover these vulnerabilities with basic tools. Impact: High – If exploited, an adversary gains code execution, leading to lateral movement across the network.
System:	Identified 118 machines, please see the below file for listing. [file removed]
Tools Used:	Nessus
References:	https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v=ws.11)

Remediation

Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows.

Finding IPT-025: Steps to Domain Admin (Informational)

The steps below describe how the penetration tester obtained domain administrator access. Each step also provides remediation recommendations to help mitigate risk.

Step	Action	Remediation
1	Poisoned LLMNR responses to obtain NetNTLMv2 hash of regular network user	Disable multicast name resolution via GPO.
2	Cracked NTLM hash offline of domain administrator users 'production' and '[name removed]'	Increase password complexity. Utilize multi-factor. Implement a Privileged Account Management solution. Utilize a password filter.
3	Leveraged password of 'production' account to gain access to several machines within the network	Limit local administrator privileges and enforce least privilege.
4	Dumped hashes on accessed machines to find cleartext password of 'Bartender' account via wdigest	Disable WDigest via GPO.
5	Overly-permissive 'Bartender' account permitted access to a large amount of machines within the network	Limit local administrator privileges and enforce least privilege.
6	Dumped hashes on accessed machines to find cleartext password of Domain Administrator account	Disable WDigest via GPO.
7	Utilized discovered credentials to log into the domain controller.	

Remediation

Review action and remediation steps.

Additional Scans and Reports

TCMS provides all clients with all report information gathered during testing. This includes Nessus files and full vulnerability scans in detailed formats. These reports contain raw vulnerability scans and additional vulnerabilities not exploited by TCM Security.

The reports identify hygiene issues needing attention but are less likely to lead to a breach, i.e. defense-in-depth opportunities. For more information, please see the documents in your shared drive folder labeled "Additional Scans and Reports".

Last Page