HACKTHEBOX

Security Incident Report

Campfire HTB Report

HTB Certified Defensive Security Analyst (HTB CDSA) Exam Report

Candidate Name: Samuel Tanner

December 2, 2025

Version: TODO 1.0

Table of Contents

1 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.

2 Engagement Contacts

Contacts		
Primary Contact	**Title**	**Contact Email**
Samuel Tanner	Systems Engineer	stannersec@proton.me

3 Exam Objectives (Read Carefully)

To be awarded the HTB Certified Defensive Security Analyst (CDSA) certification, you must:

- Obtain a minimum of 80 points while investigating **Incident 1** by submitting 16 out of the 20 flags listed below **AND**
- Compose and submit a commercial-grade security incident report **for both incidents** that encompasses an **Executive Summary** and **Technical Analysis** sections **for each incident**, adhering strictly to the format and content outlined in the **Security Incident Reporting** module.
  - While the Impact Analysis and the Response and Recovery Analysis, including diagrams, can be excluded, the Technical Analysis for both incidents must be exceptionally thorough.
  - Each stage of the cyber kill chain needs to be addressed, and any activities related to process injection should be scrutinized thoroughly, considering aspects like the origin, destination, and whether a process was sacrificial.
  - Each detection should be elucidated step by step, inclusive of the associated data sources, SIEM queries, and tool commands.

4 Executive Summary

On May 21, 2024, at 03:18:09 UTC, a Kerberoasting attack was detected on the enterprise network. The investigation identified unauthorized credential harvesting activities targeting service accounts, specifically the MSSQLService account. The threat actor utilized sophisticated attack tools including Rubeus.exe and PowerView to enumerate and extract Kerberos service tickets for offline password cracking.

Kerberoasting Attack

Incident ID: HTB-CAMPFIRE-2024-001

Incident Severity: High

Incident Status: **In Progress**

Incident Overview:

On May 21, 2024, at 03:18:09 UTC, a Kerberoasting attack was detected on the enterprise network. The investigation identified unauthorized credential harvesting activities targeting service accounts, specifically the MSSQLService account. The threat actor utilized sophisticated attack tools including Rubeus.exe and PowerView to enumerate and extract Kerberos service tickets for offline password cracking.

Key Findings:

Key Findings:

- **Attack Type:** Kerberoasting (Credential Access - MITRE ATT&CK T1558.003)
- **Compromised User:** Alonzo.spire
- **Attack Origin IP:** 172.17.79.129
- **Targeted Service:** MSSQLService
- **Tools Identified:** Rubeus.exe, PowerView.ps1
- **Attack Success:** Confirmed - Service ticket extraction successful

Immediate Actions:

Priority 1: Containment**

1. **Disable Compromised Accounts:**
    - Immediately disable `Alonzo.spire` user account
    - Reset password for `MSSQLService` account
    - Force password reset for all service accounts with SPNs
2. **Isolate Affected Systems:**
    - Quarantine workstation at IP 172.17.79.129
    - Block network access for compromised user account
    - Enable enhanced monitoring on database servers
3. **Artifact Collection:**
    - Preserve Rubeus.exe file for malware analysis

- Export full PowerShell event logs (Event ID 4104, 4103)
- Collect full Event ID 4769 logs for the past 30 days
- Create forensic image of affected workstation

4. **Threat Hunting:**
   - Search for additional Rubeus.exe instances across environment
   - Identify other users executing PowerView or similar tools
   - Review all Event 4769 logs for RC4 encryption usage
   - Check for lateral movement from MSSQLService account

Priority 2: Validation

1. Review database access logs for MSSQLService account
2. Audit all systems accessible with MSSQLService credentials
3. Check for unauthorized data exfiltration
4. Verify integrity of critical databases

7.2 SHORT-TERM ACTIONS (1-7 Days)

Detection Enhancement:

1. **Enable Advanced Logging:**
   - Ensure PowerShell Script Block Logging (Event 4104) enabled domain-wide
   - Enable PowerShell Module Logging (Event 4103)
   - Configure Kerberos logging on all domain controllers
   - Implement Sysmon for enhanced endpoint visibility
2. **Deploy Detection Rules:**
   - Alert on Event ID 4769 with encryption type 0x17 (RC4)
   - Monitor for PowerView/PowerSploit cmdlet execution
   - Detect Rubeus.exe, Mimikatz, and other credential theft tools
   - Flag unusual SPN enumeration queries
3. **SIEM Integration:**
   - Create correlation rule: PowerShell execution + Event 4769 within 5 minutes
   - Alert on service ticket requests for non-computer accounts
   - Monitor for repeated ticket requests (spray attacks)

Configuration Hardening:

1. **Kerberos Hardening:**

```
- Disable RC4 encryption via Group Policy
- Enforce AES256 encryption for all Kerberos operations
- Set "Network security: Configure encryption types allowed for Kerberos"
- Remove RC4_HMAC_MD5 from allowed encryption types
```

2. **Service Account Security:**
   - Implement Managed Service Accounts (MSA) or Group Managed Service Accounts (gMSA)
   - Set 25+ character complex passwords for all service accounts
   - Enable 90-day password rotation for service accounts
   - Remove unnecessary SPN registrations

3. **PowerShell Restrictions:**
    - Implement Constrained Language Mode for standard users
    - Deploy AppLocker/WDAC to block unauthorized script execution
    - Require code signing for all PowerShell scripts
    - Restrict PowerShell remoting to administrative users

7.3 LONG-TERM ACTIONS (1-3 Months)

Strategic Security Improvements:

1. **Active Directory Security:**
    - Audit all service accounts with SPNs
    - Migrate to gMSA for all service accounts
    - Implement Privileged Access Workstations (PAWs)
    - Deploy tiered administrative model (Red Forest)
    - Enable Microsoft Defender for Identity (formerly Azure ATP)
2. **Credential Protection:**
    - Deploy Windows Defender Credential Guard
    - Implement LAPS (Local Administrator Password Solution)
    - Enable Protected Users security group for privileged accounts
    - Implement MFA for all administrative access
3. **Network Segmentation:**
    - Isolate database servers in separate VLAN
    - Implement micro-segmentation for critical assets
    - Require firewall authentication for database access
    - Deploy Zero Trust Network Access (ZTNA) architecture
4. **User Training:**
    - Security awareness training for all users
    - Phishing simulation exercises (likely initial compromise vector)
    - Incident reporting procedures
    - Password hygiene best practices
5. **Monitoring & Response:**
    - Establish 24/7 Security Operations Center (SOC)
    - Implement User and Entity Behavior Analytics (UEBA)
    - Deploy Endpoint Detection and Response (EDR) solution
    - Conduct quarterly purple team exercises
    - Perform annual penetration testing including Kerberoasting scenarios

7.4 COMPLIANCE & REPORTING

1. **Regulatory Notifications:**
    - Determine if breach notification required under applicable regulations
    - Consult with legal counsel regarding disclosure obligations
    - Prepare incident summary for regulatory authorities if required

2. **Internal Reporting:**
    - Notify executive leadership and board of directors
    - Brief IT and security teams on lessons learned
    - Update incident response playbooks
    - Conduct post-incident review (PIR)
3. **Documentation:**
    - Maintain chain of custody for all evidence
    - Document all remediation actions taken
    - Preserve evidence for potential legal proceedings
    - Update risk register with identified vulnerabilities

Stakeholder Impact:

Immediate Risks:

- **Data Breach Potential:** MSSQLService likely has access to sensitive databases
- **Lateral Movement:** Attacker can authenticate as service account across environment
- **Privilege Escalation:** Service accounts often have elevated permissions
- **Persistence:** Compromised credentials enable long-term access
- **Compliance Violations:** Unauthorized access to regulated data (GDPR, HIPAA, PCI-DSS)

Long-term Consequences:

- Reputational damage if breach becomes public
- Regulatory fines and legal liability
- Loss of customer trust
- Incident response and remediation costs

5 Technical Analysis

Kerberoasting Attack

Affected Systems & Data

System/Account	Impact	Status
Alonzo.spire User Account	Compromised	**CRITICAL**
MSSQLService Account	Credentials Exposed	**CRITICAL**
Domain Controllers	Ticket Issuance Exploited	**MEDIUM**
Database Servers	Potential Unauthorized Access	**HIGH**
IP 172.17.79.129 Workstation	Attack Origin Point	**HIGH**

Evidence Sources & Analysis

5.1 Windows Prefetch Analysis

Analysis Performed:

```
Tool: PECmd.exe (Eric Zimmerman's Prefetch Parser)
Location: C:\HTB\Triage\Workstation\2024-05-21T033012_triage_asset\C\Windows\Prefetch
```

Key Findings:

- Rubeus.exe execution confirmed via prefetch artifact
- Execution count and last run time correlates with Event ID 4769 timestamp
- Prefetch metadata indicates execution from `C:\Users\Alonzo.spire\Downloads\`
- No prior execution history detected (first-time execution)

Forensic Significance:

- Establishes program execution on the endpoint
- Provides execution timeline correlation
- Identifies file location and execution context

5.2 PowerShell Script Block Logging Analysis

Event ID 4104 Analysis:

Script Block Content Indicators:

- PowerView cmdlets detected (e.g., `Get-DomainUser`, `Get-DomainSPNTicket`, `Get-NetUser`)
- Active Directory enumeration queries
- SPN discovery and filtering logic
- Output redirection to attacker-controlled location

Significance:

- PowerView is part of PowerSploit offensive security framework
- Used for Active Directory reconnaissance and exploitation
- Script Block Logging (enabled) captured exact commands executed
- Confirms reconnaissance phase preceding Kerberoasting attack

Attacker Operational Security (OPSEC) Failure:

- PowerShell logging not disabled
- Script execution not obfuscated
- Default PowerView syntax used (easily detected)

5.3 Event Log Analysis

Event ID 4769 (Kerberos Service Ticket Request)

Filter Criteria Applied:

```
ServiceName != krbtgt
AND ServiceName NOT LIKE '%$'
```

Results:

- **Service Name:** MSSQLService
- **User:** Alonzo.spire@DOMAIN.LOCAL
- **Source IP:** 172.17.79.129
- **Encryption Type:** 0x17 (RC4-HMAC)
- **Ticket Options:** 0x40810000 (Renewable, Forwardable)
- **Failure Code:** 0x0 (Success)

Analysis:

- Successful service ticket issuance confirmed
- RC4 encryption indicates downgrade attack or legacy configuration
- Non-computer account service (MSSQLService) is high-value target
- Source IP 172.17.79.129 should be investigated for additional compromise indicators

5.4 Timestamp Correlation

Critical Timeline Correlation:

Evidence Source	Timestamp (Local)	Timestamp (UTC)	Correlation
Initial Log Entry	5/20/2024 8:18:09 PM	2024-05-21 03:18:09	Converted from local time (EST/CST-7 hours)
PowerShell Event 4104	-	2024-05-21 03:18:09	Matches prefetch timestamp
Rubeus.exe Prefetch	-	2024-05-21 03:18:09	Matches Event 4769 timestamp

Evidence Source	Timestamp (Local)	Timestamp (UTC)	Correlation
Event ID 4769	-	2024-05-21 03:18:09+	Within same timeframe

Forensic Conclusion: All artifacts align to a single attack event window, confirming coordinated Kerberoasting attack execution.

Indicators of Compromise (IoCs)

3.1 File Artifacts

Artifact	Location	Hash (if available)	Description
Rubeus.exe	C:\Users\Alonzo.spire\Downloads\	Pending Analysis	Kerberoasting attack tool
PowerView.ps1	Memory/Script Block Logs	N/A	AD enumeration framework component

Prefetch Evidence:

- Rubeus.exe prefetch files detected in `C:\Windows\Prefetch\`
- Execution timestamp correlation with Event ID 4769 logs confirmed

3.2 Process Artifacts

Event ID	Event Type	Significance
4769	Kerberos Service Ticket Request	Indicates service ticket requests; filtered for non-krbtgt and non-computer accounts (non-$ entries)
4104	PowerShell Script Block Logging	Reveals PowerView script execution and reconnaissance activities

Event ID 4769 Analysis:

- **Encryption Type:** 0x17 (RC4-HMAC)
- **Significance:** RC4 is weaker and preferred by attackers for faster offline cracking
- **Service Name:** MSSQLService
- **Filtering Rationale:** Non-$ entries indicate user-associated service accounts, not computer accounts; non-krbtgt entries exclude normal TGT requests

3.3 Network Indicators

Indicator Type	Value	Context
IP Address	172.17.79.129	Source IP associated with Kerberos ticket requests and attack activities
Protocol	Kerberos (TCP/UDP 88)	TGS-REQ/TGS-REP traffic observed

3.4 Targeted Accounts

Account	Type	Risk Level	Notes
MSSQLService	Service Account	CRITICAL	High-privilege service account; ticket successfully extracted
Alonzo.spire	User Account	HIGH	Compromised user account used as attack pivot point

Root Cause Analysis

This investigation confirmed a successful Kerberoasting attack against the MSSQLService account on May 21, 2024. The attacker leveraged the compromised user account "Alonzo.spire" to execute reconnaissance using PowerView and credential theft using Rubeus.exe. The attack exploited weak RC4 encryption to extract service tickets for offline password cracking.

Key Takeaways:

1. Service accounts with SPNs remain a critical security vulnerability
2. RC4 encryption support enables faster credential cracking
3. PowerShell logging proved essential for attack detection and analysis
4. Prefetch analysis corroborated malicious tool execution
5. Event ID 4769 filtering effectively identifies Kerberoasting attempts

Incident Status: ACTIVE - Remediation in progress

Next Review Date: December 9, 2025 (7 days)

Technical Timeline

Timestamp (UTC)	Event	Evidence Source	Details
2024-05-21 03:18:09	Initial Attack Activity	Windows Prefetch, Event Logs	Suspicious activity initiated from user Alonzo.spire's workstation
2024-05-21 03:18:09	PowerView Execution	Event ID 4104 (PowerShell Script Block Logging)	PowerView reconnaissance script executed to enumerate domain service accounts
2024-05-21 03:18:09+	Active Directory Enumeration	PowerShell Logs	Service Principal Names (SPNs) enumerated across domain

Timestamp (UTC)	Event	Evidence Source	Details
2024-05-21 03:18:09+	Rubeus.exe Execution	Prefetch Analysis (C:\Windows\Prefetch)	Kerberoasting tool executed from C:\Users\Alonzo.spire\Downloads\
2024-05-21 03:18:09+	Kerberos TGS Request	Event ID 4769	Service ticket requested for MSSQLService using RC4 encryption (Type 0x17)
2024-05-21 03:18:09+	Ticket Extraction	Network Analysis	Kerberos TGS-REP captured from IP 172.17.79.129

Nature of the Attack

Tactic	Technique ID	Technique Name	Observed
Reconnaissance	T1087.002	Account Discovery: Domain Account	✓ (PowerView)
Credential Access	T1558.003	Steal or Forge Kerberos Tickets: Kerberoasting	✓ (Rubeus)
Discovery	T1069.002	Permission Groups Discovery: Domain Groups	✓ (PowerView)
Discovery	T1018	Remote System Discovery	✓ (PowerView)
Execution	T1059.001	Command and Scripting Interpreter: PowerShell	✓ (PowerView)

A Appendix

A.1 Technical Timeline

Timestamp (UTC)	Event	Evidence Source	Details
2024-05-21 03:18:09	Initial Attack Activity	Windows Prefetch, Event Logs	Suspicious activity initiated from user Alonzo.spire's workstation
2024-05-21 03:18:09	PowerView Execution	Event ID 4104 (PowerShell Script Block Logging)	PowerView reconnaissance script executed to enumerate domain service accounts
2024-05-21 03:18:09+	Active Directory Enumeration	PowerShell Logs	Service Principal Names (SPNs) enumerated across domain
2024-05-21 03:18:09+	Rubeus.exe Execution	Prefetch Analysis (C:\Windows\Prefetch)	Kerberoasting tool executed from C:\Users\Alonzo.spire\Downloads\
2024-05-21 03:18:09+	Kerberos TGS Request	Event ID 4769	Service ticket requested for MSSQLService using RC4 encryption (Type 0x17)
2024-05-21 03:18:09+	Ticket Extraction	Network Analysis	Kerberos TGS-REP captured from IP 172.17.79.129

End of Report

This report was rendered
by SysReptor with
♥