ADScan

Internal Penetration Test
Report of Findings

Hackén III

May 30, 2025

Technical Findings Details

north.sevenkingdoms.local

1. noPac/sAMAccountName spoofing (CVE-2021-42287 and CVE-2021-42278)

CWE	**CWE-290**
CVSS	9.0
Description	This privilege escalation is based in the exploitation of two popular CVEs: • CVE-2021-42278 - Name impersonation: it allows to create computer accounts without a trailing ($) in their sAMAccountName attribute. • CVE-2021-42287 - KDC bamboozling: when requesting a Service Ticket for a user (dc01) and that user is not found, the KDC automatically searches agaian with a trailing ($) and if it is found (dc01$), then the user (dc01) just obtained a service ticket of the trailing account (dc01$). This lead to the creation of a computer account with the same the sAMAccountName of the DC, but without the trailing (CVE-2021-42278) and gain a Service Ticket for the original DC by impersonating it with the recently created computer account (CVE-2021-42287).
Security Impact	This vulnerability allows attackers to compromise a domain and acquire domain administrators privileges from a domain user.
Affected Assets	• north.sevenkingdoms.local
Remediation	Apply the lates security patches to Windows domain controllers.
External References	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-42287 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-42278

2. AS-REP Roasting

CWE	**CWE-522**
CVSS	6.9
Description	Preauthentication offers protection against offline Password Cracking. When enabled, a user requesting access to a resource initiates communication with the Domain Controller (DC) by sending an Authentication Server Request (AS-REQ) message with a timestamp that is encrypted with the hash of their password. If and only if the DC is able to successfully decrypt the timestamp with the hash of the user's password, it will then send an Authentication Server Response (AS-REP) message that contains the Ticket Granting Ticket (TGT) to the user. Part of the AS-REP message is signed with the user's password. For each account found without preauthentication, an adversary may send an AS-REQ message without the encrypted timestamp and receive an AS-REP message with TGT data which may be encrypted with an insecure algorithm such as RC4. The recovered encrypted data may be vulnerable to offline Password Cracking attacks similarly to Kerberoasting and expose plaintext credentials.
Security Impact	A successful AS-REP Roasting attack along with cracked passwords could lead to lateral movement and privilege escalation in an AD environment. If a password is cracked for a Domain Administrator account or equivalent, an attacker could gain control over most, if not all, resources in the domain.
Affected Assets	There are no Administrator users. General Users: • brandon.stark
Remediation	Kerberos preauthentication is enabled by default. Older protocols might not support preauthentication therefore it is possible to have this setting disabled. Make sure that all accounts have preauthentication whenever possible and if it is not possible the following steps will help mitigate the risk of this attack: • Enable AES Kerberos encryption instead of RC4 • Use strong 25+ character passwords for these accounts and rotate them periodically
External References	https://attack.mitre.org/techniques/T1558/004/

3. SMB Null Session Authentication on DC

CWE	**CWE-284**
CVSS	6.9
Description	Null session, also known as anonymous authentication, is a special kind of authentication during which the user doesn’t submit any credentials. In an Active Directory environment, when a user connects via a null session on a Domain Controller, he connects as a member of the “Anonymous Logon” group and inherits all ACL’s assigned to this group. By default in modern Active Directory environments, the “Anonymous Logon” group doesn't have any permissions, but in some legacy environments, it is part of the “Pre-Windows 2000 Compatible Access” group, which has permissions to authenticate through a null session on the DCs.
Security Impact	Once connected to a Domain Controller through a null session, attackers are available to enumerate information about your domain, such as users and password policies. With this information, an attacker can learn about any potential vulnerabilities or ways to best attack your systems.
Affected Assets	• north.sevenkingdoms.local
Remediation	• Remove the membership of the “Anonymous Logon” group from the “Pre-Windows 2000 Compatible Access” group • Alternatevely, remove all the ACLs thath allow the members of the “Anonymous Logon” to connect through a null session on the DCs
External References	https://blog.whiteflag.io/blog/guest-vs-null-session-on-windows/

4. Kerberoasting

CWE	**CWE-522**
CVSS	5.3
Description	In an Active Directory (AD) environment, Service Principal Names (SPNs) are used to uniquely identify instances of a Windows service. Kerberos authentication requires that each SPN be associated with one service account (Active Directory user account). Any authenticated AD user can request one or more Kerberos Ticket-Granting Service (TGS) tickets from the domain controller for any SPN accounts. These tickets are encrypted with the associated AD account's NTLM password hash. They can be brute forced offline using a password cracking tool such as Hashcat if a weak password is used along with the RC4 encryption algorithm. If AES encryption is in use, it will take more resources to crack a ticket to reveal the account's clear-text password, but it is possible if weak passwords are in use.
Security Impact	A successful Kerberoasting attack along with cracked passwords could lead to lateral movement and privilege escalation in an AD environment. If a password is cracked for a Domain Administrator account or equivalent, an attacker could gain control over most, if not all, resources in the domain.
Affected Assets	There are no Administrator users. General Users: • sansa.stark • jon.snow • sql_svc
Remediation	Where possible eliminate SPNs in the environment in favor of Group Managed Service Accounts (gMSA) which are not subject to this type of attack. If migration to gMSAs is not possible the following steps will help mitigate the risk of this attack: • Enable AES Kerberos encryption instead of RC4 • Use strong 25+ character passwords for service accounts and rotate them periodically • Limit the privileges of service accounts and avoid creating SPNs tied to highly privileged accounts such as Domain Administrators
External References	https://attack.mitre.org/techniques/T1558/003/

essos.local

5. ZeroLogon (CVE-2020-1472)

CWE	**CWE-290**
CVSS	10.0
Description	The Netlogon service on the remote host is vulnerable to the zerologon vulnerability. An unauthenticated, remote attacker can exploit this, by spoofing a client credential to establish a secure channel to a domain controller using the Netlogon remote protocol (MS-NRPC). The attacker can then use this to change the computer's Active Directory (AD) password, and escalate privileges to domain admin.
Security Impact	This vulnerability allows attackers to compromise a domain and acquire domain administrators privileges from an unauthenticated user.
Affected Assets	• essos.local
Remediation	Apply the lates security patches to Windows domain controllers.
External References	https://attack.mitre.org/techniques/T1210/

6. AS-REP Roasting

CWE	**CWE-522**
CVSS	6.9
Description	Preauthentication offers protection against offline Password Cracking. When enabled, a user requesting access to a resource initiates communication with the Domain Controller (DC) by sending an Authentication Server Request (AS-REQ) message with a timestamp that is encrypted with the hash of their password. If and only if the DC is able to successfully decrypt the timestamp with the hash of the user's password, it will then send an Authentication Server Response (AS-REP) message that contains the Ticket Granting Ticket (TGT) to the user. Part of the AS-REP message is signed with the user's password. For each account found without preauthentication, an adversary may send an AS-REQ message without the encrypted timestamp and receive an AS-REP message with TGT data which may be encrypted with an insecure algorithm such as RC4. The recovered encrypted data may be vulnerable to offline Password Cracking attacks similarly to Kerberoasting and expose plaintext credentials.
Security Impact	A successful AS-REP Roasting attack along with cracked passwords could lead to lateral movement and privilege escalation in an AD environment. If a password is cracked for a Domain Administrator account or equivalent, an attacker could gain control over most, if not all, resources in the domain.
Affected Assets	There are no Administrator users. General Users: • missandei
Remediation	Kerberos preauthentication is enabled by default. Older protocols might not support preauthentication therefore it is possible to have this setting disabled. Make sure that all accounts have preauthentication whenever possible and if it is not possible the following steps will help mitigate the risk of this attack: • Enable AES Kerberos encryption instead of RC4 • Use strong 25+ character passwords for these accounts and rotate them periodically
External References	https://attack.mitre.org/techniques/T1558/004/