Endida Internal Pen Test Service

ENDIDA
NEXT GENERATION CYBER DEFENCE

Sample Executive Summary Report

Prepared for Endida Ltd

Friday, 18 August 2023

2. Impact Summary

The pentest identified critical impacts that require immediate attention. These impacts represent critical vulnerabilities that can be leveraged by an attacker to compromise your network.

Domain Compromise (1)

Compromised 1 domain via 4 separate attack vectors

Once a domain is fully compromised, all hosts, domain user accounts, data, infrastructure and applications tied to that domain should be considered fully compromised. Additionally, applications running on a domain-joined machine or any application that uses Active Directory integration to authenticate users should be considered fully compromised.

- Domain SMOKE.NET

Critical Infrastructure Compromise (5)

Compromised 5 critical applications or devices via 6 separate attack vectors

Critical infrastructure consists of key devices and applications that provide attackers a privileged position in the network from which they can access a wealth of sensitive data and launch further attacks.

- Smart Install service at 10.0.220.254:4786
- LDAP service at 10.0.40.99:389
- Web service at 10.0.40.99:443
- Smart Install service at 10.0.229.254:4786
- Jenkins application at 10.0.225.100:8080

Host Compromise (14)

Compromised 14 hosts via 40 separate attack vectors

Host compromise can lead to attackers gaining access to sensitive information, maintaining persistence within your network, and obtaining lateral movement within your networks.

The top 5 are listed below.

- Host 10.0.100.100
- Host 10.0.100.101
- Host 10.0.40.103
- Host 10.0.220.55 (win2k3)
- Host 10.0.229.11 (fs.smoke.net)

Domain User Compromise (7)

Compromised 7 domain users

Once a domain user is compromised, anything that user account has access to should be considered compromised.

The top 5 are listed below.

- Domain Admin a-jsmith in domain SMOKE.NET
- Domain User ns$ in domain SMOKE.NET
- Domain User fs$ in domain SMOKE.NET
- Domain User jsmith in domain SMOKE.NET
- Domain User svc_TESTGMSA2$ in domain SMOKE.NET

Brand Compromise (1)

Compromised 1 subdomain

Brand compromise covers ways in which an attacker can harm your company's reputation by, for instance, defacing the company's website, hosting malware off the company's domain, or carrying out phishing attacks that appear to originate from the company.

- Subdomain doodle.h3ai.io

Sensitive Data Exposure (13)

Compromised sensitive data on 13 stores via 21 separate attack vectors

Sensitive data exposures can be used by attackers to obtain user credentials, PII (Personally Identifiable Information), financial account data, and other business-critical information to further exploit or gain profit.

The top 5 are listed below.

- Bitbucket repo fakegit2 in account kbuch07
- GitLab repo fakegit2 in account kbuch
- GitLab repo secret_test in account kbuch
- Host 10.0.220.55 (win2k3)
- Host 10.0.229.11 (fs.smoke.net)

Ransomware Exposure (8)

Ransomware exposure on 8 stores via 24 separate attack vectors

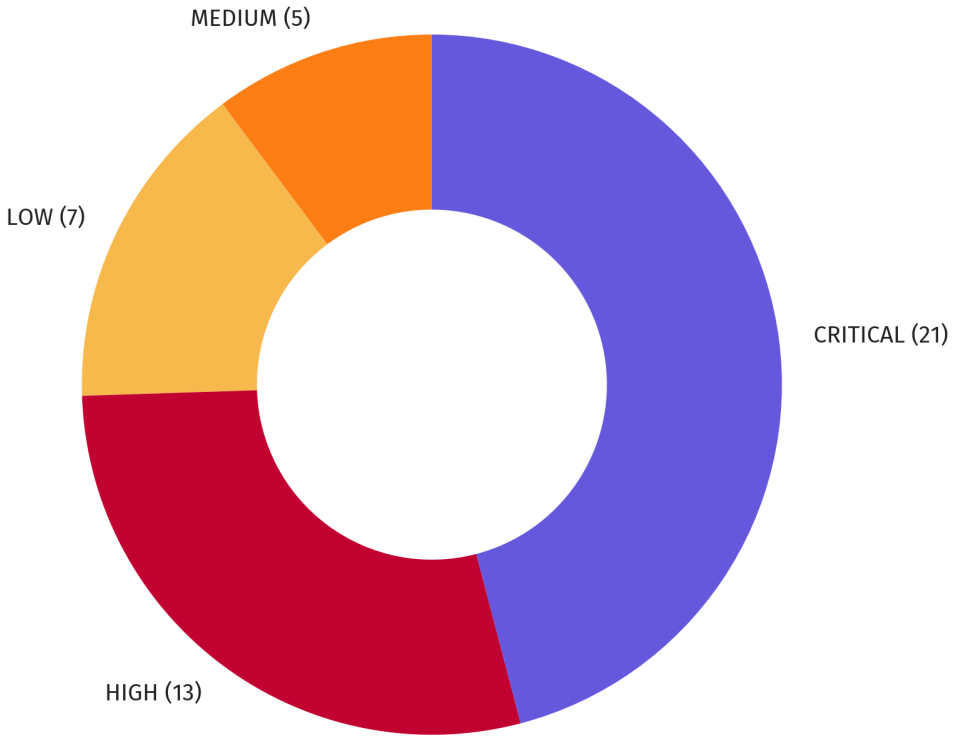
Ransomware exposures can be used by attackers to obtain access to business-critical data stores, encrypt them with a secret key, and demand a ransom payment from your company before releasing the decryption key. Ransomware attacks can cause severe disruption to your business operations, even after the ransom is paid, as data stores must be decrypted and affected services restored.

The top 5 are listed below.

- Host 10.0.220.55 (win2k3)
- Host 10.0.229.11 (fs.smoke.net)
- Host 10.0.225.100
- Host 10.0.220.51 (win7.smoke.net)
- Domain controller 10.0.229.1 (dc.smoke.net)

3. Weaknesses & Mitigations

The pentest identified CRITICAL degrees of risk within the target network, including **40 confirmed weaknesses** and **6 potential weaknesses.** These risks allow an attacker to steal data, disrupt operations, and cause financial or reputational loss.



Weaknesses by Severity

The following weaknesses were identified as having the highest degree of risk. Each weakness includes recommended mitigations and remediations.

The top 5 are listed below.

1. CRITICAL Windows SMB Remote Code Execution Vulnerability **(CVE-2017-0144, affecting 5 hosts)**

   Mitigations:

   Apply the updates referenced in Microsoft Security Bulletin MS17-010.

   Block access to SMB services (139/tcp, 445/tcp) from untrusted networks such as the Internet. If at all possible disable SMBv1

2. CRITICAL Weak or Default Credentials - Cracked Credentials **(H3-2021-0020, affecting 14 hosts)**

   Mitigations:

   Ensure a strong password policy is in place and users are properly trained on best practices. Consider the use of a password manager to store complex passwords where possible.

Identify a configuration management process that ensures default credentials are changed before systems are deployed in a production environment.

Implement multi-factor authentication where possible.

3. CRITICAL SMB Signing Not Required **(H3-2021-0030, affecting 7 hosts)**

   Mitigations:

   Enable and require SMB signing via Group Policy or Local Security Policy.

4. CRITICAL NBT-NS Poisoning Possible **(H3-2021-0035, affecting 1 host)**

   Mitigations:

   Disable NBT-NS in the network adapter settings by selecting 'Disable NetBIOS over TCP/IP. Alternatively, disable by using a registry key.

5. CRITICAL Netlogon Elevation of Privilege Vulnerability **(CVE-2020-1472, affecting 1 host)**

   Mitigations:

   Apply the updates referenced in Microsoft Security Bulletin CVE-2020-1472 and configure the registry key that will enable Enforcement Mode.

   On February 9, 2021 a Windows Update will automatically enable Enforcement Mode on all Domain Controllers regardless of the registry key value.