Offensive Security

Vulnerability Assessment & Penetration Testing Report

Month Year

# Restriction on Disclosure and Use of Information Sharing

This report contains sensitive and confidential information about the security and controls framework designed and implemented at XYZ Company. The report also highlights certain security and controls weaknesses identified during the vulnerability assessment and penetration test carried out by Offensive Security Red Team (herein after referred to as the penetration testing team, Offensive Security Red Team or OSRT).

The information contained in this report can be maliciously used to exploit the vulnerabilities reported in the present installation and configuration. We/I, therefore, strongly recommend that management treat this report as classified information and restrict circulation of this report; and control the process of making additional copies thereof. The distribution of this report should be limited to concerned and appropriate officials only. This report is issued to inform management of potential weaknesses and risks in the application assessed by the Offensive Security Red Team and should not be used for any other purpose.

The readers of this report should also note that an attempt has been made to generalize the contents of this report as far as possible, to avoid giving unnecessary details, which may facilitate any undesired hacking attack.

This report is for internal use only and cannot be shared with any third party without prior written consent of Information Security and Compliance leadership Team and the Offensive Security Red Team.

Version Control

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Author** | **Date** | **Rationale** |
| 1.0 | OSRT | MM/DD/YYYY | 1st Draft |
| 1.1 | OSRT | MM/DD/YYYY | Review of 1st Draft |
| 1.2 | OSRT | MM/DD/YYYY | Final Draft |

# Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period in scope.

Time-limited engagements do not allow for a full evaluation of all security controls. OSRT prioritized assessment to identify the weakest security controls an attacker would exploit. To ensure continued success of these security controls in place, OSRT will conduct similar assessments on a quarterly basis.

# 

Table of Contents

[Restriction on Disclosure and Use of Information Sharing 2](#_Toc82816758)

[Disclaimer 3](#_Toc82816759)

[1. Executive Summary 4](#_Toc82816760)

[1.1 Engagement Description 5](#_Toc82816761)

[1.2 Engagement Overall Severity Rating 5](#_Toc82816762)

[1.3 Engagement Overview 5](#_Toc82816763)

[1.4 Summary of Strengths 5](#_Toc82816764)

[1.5 Summary of Top Findings 5](#_Toc82816765)

[1.6 Summary of All Findings 6](#_Toc82816766)

[2. Scope of Engagement 7](#_Toc82816767)

[3. Penetration Testers & Qualifications 8](#_Toc82816768)

[4. Methodologies and Policies 8](#_Toc82816769)

[5. Tools Used 9](#_Toc82816770)

[6. Vulnerabilities and Findings 9](#_Toc82816771)

[6.1 Vulnerabilities and Findings – Bastion Hosts 10](#_Toc82816772)

[6.2 Vulnerabilities and Findings – Active Directory 21](#_Toc82816773)

[6.3 Vulnerabilities and Findings – Citrix Hosts 33](#_Toc82816774)

[6.4 Vulnerabilities and Findings – Splunk Hosts 46](#_Toc82816775)

[7. Additional Scans and Reports 52](#_Toc82816776)

# **Executive Summary**

Offensive Security Red Team (OSRT) performed penetration testing of XYZ’s internal network and infrastructure in order to determine the overall threat of potential compromise to XYZ Inc. This security engagement occurred during the period from Month Dateth, Year to Month Dateth, Year and was assigned a severity rating based upon the volume of exposures and the overall impact toward XYZ Inc.

* 1. Engagement Description

This engagement was designated as an internal penetration test that simulates an attacker or malicious insider that has already gained access to the internal network. For this access, the corporate XYZ Inc. VPN was utilized by each member of the OSRT with their issued accounts. These accounts have been validated to not include any additional permissions outside of VPN access.

* 1. Engagement Overall Severity Rating

|  |  |
| --- | --- |
| Engagement | Overall Risk Rating |
| Internal Penetration Test | Medium |

* 1. Engagement Overview

OSRT attempted to gain unauthorized access to systems from the perspective of an attacker originating from inside the network as a malicious insider threat. Efforts were placed on identification of vulnerabilities that could provide exploitation then allowing an attacker to gain access to the XYZ Inc. network, infrastructure, and data. The methodologies for each component phase of the engagement may be found below in the [Methodologies and Policies](#_Methodologies_and_Policies) section. Additionally, the tools and host used as part of these methodologies can be found within the [Tools Used](#_Tools_Used) and [Scope of Engagement](#_Scope_of_Engagement) sections.

During this security engagement, OSRT was able to evade detection throughout the effort, however was unable to fully compromise any of the systems within the given scope and compressed time frame. Several vulnerabilities were identified and from those, OSRT was able to obtain an “SA” level account by exploiting open RDP access with easily guessable default credentials. This account was submitted to the approriate team for immediate reset.

Based on the severity of the deficiencies discovered, the overall security posture of XYZ Inc. can be shown to exhibit a moderate level of maturity. It is also worth noting that for most of the identified issues, remediation efforts require a low level of effort and complexity. Throughout testing, care was taken to ensure that the OSRT did not interrupt XYZ’s services or impact business operations.

* 1. Summary of Strengths

From the results of this engagement, OSRT found the following strengths within the XYZ Inc. network environment:

* Active Directory domain segmentation encountered (XYZINC.XYZ.com vs. AMERICAS.XYZ.com)
* Based on the scope provided, XYZ Inc. utilizes XYZ SIEM for logging and monitoring
* Some type of network level throttling was observed in both scanning activities and exploitation attempts. This may indicate network level protections including:
  + Allow/Block Lists (Temporary)
  + IDS or IPS
  + Access Controls (Port Filtering, Network Level Resets to Connections)
* Of the systems in scope, none were found to show an outdated operating system or application platform
* Patching appeared to be up to date or mitigation efforts were put in place as none of the systems were vulnerable to several recent 0day exploits (Print Nightmare/OMIGOD)
  + SMBv1 was identified as well, but unable to be leveraged for exploit
  1. Summary of Top Findings
* **Undetected Malicious Activity - Host Scanning & SSH/RDP Brute Force Attacks:** OSRT identified potential areas for improvement in alerting and/or response to efforts of the testing. These areas would allow an attacker to persist unchecked all while given the ability to identify vulnerable hosts, ports, and potential services as well as attack/exploit them.
  + **Best Practice:** Establish proper alerting and response practices focused on identification of these activities. These can then be tested by utilizing our in place Purple Team engagements to validate and confirm identification.
  + **Why It Matters:** Attackers often utilize very well documented and easy to use tooling. If these reconnaissance activities could be identified and halted it would leave an attacker at a disadvantage and potentially even stop their efforts.
* **Information Disclosure:** Information disclosure, also known as information leakage, was identified during testing. This was found in the form of open/unused ports, service enumeration, domain level information (domain name, NetBIOS, ability to query active directory), and responses found during SSH/RDP brute force attacks (validating username:password enumeration).
  + **Best Practice:** Close or disallow access to unused or unneeded ports and services. Consider network level access controls which only allow access if the granted user is authorized.
  + **Why It Matters:** Attackers will leverage any information they are able to obtain in order to exploit an environment. If ports and service information were not available the attacker would be unable to discern any potential attacks outside of best guesses. For example, if a given host is only known by IP, but able to be scanned exposing ports that are native to only active directory – this would be an easy indication that this machine could be a domain controller or hold sensitive information (even from the NetBIOS name – E.g. INF**DC**00#).
  1. Summary of All Findings

OSRT identified zero (0) critical severity findings, zero (0) high severity findings, five (5) medium severity findings, and two (2) low severity findings during the course of the engagement. Below you will find a breakdown of the engagement’s vulnerabilities bu finding.

1.6.1 Total Findings

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Components** | **Critical** | **High** | **Medium** | **Low** | **Total** |
| Internal Penetration Test | 0 | 0 | 5 | 8 | 13 |

1.6.2 Summary of All Findings

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Vulnerability Name | Risk Rating | Status |
| C1.S1 | XXXX | Critical | Open |
| H1.S2 | XXXX | High | Open |
| M1.S3 | XXXX | Medium | Open |
| L1.S4 | XXXX | Low | Open |

# **Scope of Engagement**

The scope of the assessment was limited to the following devices:

| **No.** | **IP Address** | **Hostname** | **PCI** | **Product** |
| --- | --- | --- | --- | --- |
| 1 |  |  |  |  |
| 2 |  |  |  |  |

# **Penetration Testers & Qualifications**

The XYZ Inc. OSRT is organizationally independent from any group that manages the environment being tested. An organizational chart can be provided for validation. The OSRT have over a decade of individual security experience, from start-ups, finance, retail, data centers, healthcare, e-commerce and bug bounty programs.  The Team includes the following members:

|  |  |  |
| --- | --- | --- |
| **Name** | **Email** | **Title** |
| Sanil Almeida | sanilalmeida@gmail.com | Penetration Tester – Red Team |
|  |  |  |
|  |  |  |

Certifications include:

* Computer Hacking Forensics Investigator (CHFI)
* Offensive Security Certified Professional (OSCP)
* Certified Penetration Testing Engineer (CPTE)
* Certified Ethical Hacker (CEH)

# **Methodologies and Policies**

The phases of penetration testing activities include the following:

* Pre-engagement Interactions – discussing engagement with stakeholders
* Reconnaissance – Using both passive and active scanning to map network
* Threat Modelling – Creation of an attack plan to penetrate the network
* Vulnerability Analysis – The use of vulnerability scanners to find vulnerable endpoints
* Exploitation – Exploitation of these vulnerabilities to gain access to the host
* Post Exploitation – Privilege escalation and data exfiltration
* Reporting – Creating a summary of our findings

Manual penetration testing will be used to attempt to find vulnerabilities in the PCI segmentation (Cloud and On-Premise) hosts, based on the following methodologies:

* **NIST 800-115**
* <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf>
* **OWASP Security Standards**
* <https://owasp.org/www-project-top-ten/>
* **Penetration Testing Execution Standards Technical Guidelines (PTES)**

* [http://www.pentest-standard.org/index.php/PTES\_Technical\_Guidelines](http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines" \t "_blank)

OSRT policies governing penetration testing:

* **Penetration Testing and Vulnerability Assessment Policies:**
  + [https://folio.XYZ.com/:w:/s/eDiscovery\_Forensic/EaZL2We\_I29KtNJzPkbfCdsBpd2vpMW\_PZ9YB6YXs2PSsg?e=zxQewE](https://folio.gap.com/:w:/s/eDiscovery_Forensic/EaZL2We_I29KtNJzPkbfCdsBpd2vpMW_PZ9YB6YXs2PSsg?e=zxQewE)
* **PCI-DSS Penetration Testing and Vulnerability Assessment Policies:**
  + [https://folio.XYZ.com/:w:/s/eDiscovery\_Forensic/ET8eDAUepWpGvYJHxsGmAFgBxNY4fh0d4qKAj3GJHdVuvg?e=a6Awh3](https://folio.gap.com/:w:/s/eDiscovery_Forensic/ET8eDAUepWpGvYJHxsGmAFgBxNY4fh0d4qKAj3GJHdVuvg?e=a6Awh3)
* **Web Application Penetration Testing Policies:**
  + [https://folio.XYZ.com/:w:/s/eDiscovery\_Forensic/EXuck-2Mz3tJtrTaUv6cbHcBr\_hFxFOdQBzQHVNR9edXjQ?e=qM0aTa](https://folio.gap.com/:w:/s/eDiscovery_Forensic/EXuck-2Mz3tJtrTaUv6cbHcBr_hFxFOdQBzQHVNR9edXjQ?e=qM0aTa)
* **Network Penetration Testing Policies:**
  + [https://folio.XYZ.com/:w:/s/eDiscovery\_Forensic/EZqezuSTgZ9GgIGFS7Gi34ABQsF9JZ\_BoosguQGehPQ5Xg?e=1usove](https://folio.gap.com/:w:/s/eDiscovery_Forensic/EZqezuSTgZ9GgIGFS7Gi34ABQsF9JZ_BoosguQGehPQ5Xg?e=1usove)
* **Attack Surface Policies:**
  + [https://folio.XYZ.com/:w:/s/eDiscovery\_Forensic/EZ\_EJlJcm\_9DjJm1YgV1aL0BwyN-FgS4qDnOw7CXiX0UEQ?e=mUZf4g](https://folio.gap.com/:w:/s/eDiscovery_Forensic/EZ_EJlJcm_9DjJm1YgV1aL0BwyN-FgS4qDnOw7CXiX0UEQ?e=mUZf4g)
* **Scoping Questionnaire:**
  + [https://folio.XYZ.com/:w:/s/eDiscovery\_Forensic/Ec1IVta-r25BpwQ-91vdRq0BrijMYY6yvwmu1iAWoPAlDQ?e=mp7Egc](https://folio.gap.com/:w:/s/eDiscovery_Forensic/Ec1IVta-r25BpwQ-91vdRq0BrijMYY6yvwmu1iAWoPAlDQ?e=mp7Egc)

# **Tools Used**

The following tools will be used for the penetration test:

|  |  |
| --- | --- |
| **Category** | **Tool Name** |
| **Reconnaissance** | * Nmap Security Scanner   + Network discovery and security auditing * OpenVAS [Open Vulnerability Assessment Scanner]   + Vulnerability scanner * Nikto/Nikto2   + Opensource web server and vulnerability scanner * Nessus Essentials   + Network discovery, security auditing, and vulnerability scanning * OWASP Zed Attack Proxy [ZAP]   + Web application security and vulnerability scanner * Netsparker   + Web application security and vulnerability scanner * Metasploit   + Penetration testing framework with prebuilt security and vulnerability scanners |
| **Exploitation** | * Metasploit   + Penetration testing framework with prebuilt exploits * Nmap Security Scanner [Exploit Scripts]   + Preconfigured scripts for exploitation * Python Scripting   + CVE-2021-38647 PoC Script (OMIGOD)     - <https://github.com/horizon3ai/CVE-2021-38647>   + crowbar.py (via Impacket – Built into Kali)     - Brute force RDP script   + eternal\_checker.py     - <https://github.com/3ndG4me/AutoBlue-MS17-010/blob/master/eternal_checker.py>     - SMBv1 Eternal Blue exploit script |

# **Vulnerabilities and Findings**

Findings will have a severity rating of Low, Medium, High, Critical and if permitted, an industry standard scoring (E.g. NDS, CVE, or others depending on relevance) if it is a disclosed vulnerability. If the finding either directly or indirectly leads to a PCI/CDE zone or PII data, it will be listed as CRITICAL or HIGH based on accessibility. Each finding disclosed will have the following items attached:

1. Name of exploit/vulnerability
2. Vulnerability Impact
3. CVSS Score
4. Risk Rating
5. Impacted Assets
6. Description of the issue
7. Recommended Remediation Steps
8. Proof of Concept

CVSS v3.0 Score Details (<https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator>):

|  |  |
| --- | --- |
| **Category** | *Scope Range* |
| **Low** | *0.0 - 3.9* |
| **Medium** | *4.0 - 6.9* |
| **High** | *7.0 - 8.9* |
| **Critical** | *9.0 - 10.0* |

***Figure 6.0:***XYZ Inc. Remediation Prioritization Methodology for Security Findings:

|  |  |  |  |
| --- | --- | --- | --- |
| **Severity** | **Risk** | **Description** | **Resolution SLA/Priority** |
| **S1** | Critical | Immediate risk to XYZ Inc assets, data, systems or privacy risk | Immediate – **24 Hours** |
| **S2** | High | Risk of access, failed control, or privacy issue but has mitigation in place to monitor while fix is completed | < = **30 days** |
| **S3** | Medium | Risk of Access or security breach feasible but mitigation controls in place | < = **90 days** with Remediation Plan |
| **S4** | Low | Security recommendation/best-practice | < = **180 days** with Remediation Plan |

# 6.1 Vulnerabilities and Findings

Scope:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No.** | **IP Address** | **Hostname** | **PCI** | **Product** |
| 1 |  |  |  |  |
| 2 |  |  |  |  |

Tools:

|  |  |
| --- | --- |
| **Category** | **Tool Name** |
| **Reconnaissance** | * Nmap Security Scanner   + Network discovery and security auditing * OpenVAS [Open Vulnerability Assessment Scanner]   + Vulnerability scanner * Nikto/Nikto2   + Opensource web server and vulnerability scanner * Nessus Essentials   + Network discovery, security auditing, and vulnerability scanning * OWASP Zed Attack Proxy [ZAP]   + Web application security and vulnerability scanner * Netsparker   + Web application security and vulnerability scanner * Metasploit   + Penetration testing framework with prebuilt security and vulnerability scanners |
| **Exploitation** | * Metasploit   + Penetration testing framework with prebuilt exploits * Nmap Security Scanner [Exploit Scripts]   + Preconfigured scripts for exploitation * Python Scripting   + CVE-2021-38647 PoC Script (OMIGOD)     - <https://github.com/horizon3ai/CVE-2021-38647>   + crowbar.py (via Impacket – Built into Kali)     - Brute force RDP script   + eternal\_checker.py     - <https://github.com/3ndG4me/AutoBlue-MS17-010/blob/master/eternal_checker.py>     - SMBv1 Eternal Blue exploit script |

Vulnerability Overview:

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Vulnerability Name | Risk Rating | Status |
| C1..S1 | Undetected Malicious Activity – Host Scanning | Critical | Open |
| H1.S2 | TLS Version 1.0 and 1.1 Protocol Detection | High | Open |
| M1.S3 | Information Disclosure Vulnerability | Medium | Open |
| L1.S4 | SSL Self-Signed Certificate Vulnerability | Critical | Open |

* 1. C1.S1 – [Title of the finding]

|  |  |
| --- | --- |
| [C1.S1] Title | |
| Description of the finding. | |
| **Impacted Assets** | In-scope devices |
| **Risk** | **Severity:** C1.[S1] |
| **Likelihood:** These activities occur after primary controls fail. [Sample likelihood] |
| **Impact:** Undetected internal network attacks allow adversaries to expand control. [Sample impact] |
| **CVSS Score** | **9.3** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N [Sample CVSS score] |
| **Injection Parameter** | N/A |
| **Attack** | N/A |
| **Recommendation** | Review SIEM strategy and WAF settings for the hosts that are accessible through HTTP. Some attacks may be difficult to detect but have been noted for information and review.  Attacks Undetected:   * Web vulnerability scans with Nessus, Netsparker, Nikto and OWASP ZAP * Active vulnerability scans with Burp Suite Pro * Network vulnerability scans with Nmap * Host vulnerability scans with Nessus |
| Proof of Concept | |
| As this vulnerability stems from all of the reconnaissance that was performed by the OSRT for the segmentation evaluation - the tools below will serve as the proof of concept.   * Nmap Security Scanner   + Network discovery and security auditing * OpenVAS [Open Vulnerability Assessment Scanner]   + Vulnerability scanner * Nikto/Nikto2   + Opensource web server and vulnerability scanner * Nessus Essentials   + Network discovery, security auditing, and vulnerability scanning * OWASP Zed Attack Proxy [ZAP]   + Web application security and vulnerability scanner * Netsparker   + Web application security and vulnerability scanner * Metasploit   + Penetration testing framework with prebuilt security and vulnerability scanners   The concept of scanning should be evaluated for possible detection and blocking as this information ultimately leads to enumeration of vulnerabilities that can be exploited. It is understandable that maintaining security posture in the internal environments may require legitimate scanning to determine vulnerabilities and patching compliance, in this case, a system based on whitelisting will reduce this threat vector. | |

* 1. H1.S2 – [Title of the Finding]

|  |  |
| --- | --- |
| [M3.S3] Title of the Finding | |
| The remote service accepts connections encrypted using TLS 1.0 and 1.1 which has a number of cryptographic design flaws. The most notable and well documented exploits being POODLE1 or BEAST2. These exploits leverage this vulnerability in order to perform Man-in-the-Middle (MiTM) attacks which lead to data exfiltration. Newer versions of TLS such as 1.2 and 1.3 are designed against these flaws and should be used whenever possible.  As of March 31, 2020, endpoints that aren’t enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits. | |
| **Impacted Assets** | All in-scope hosts. |
| **Risk** | **Severity:** MEDIUM[S3] |
| **Likelihood:** This vulnerability can be exploited if primary controls fail such as authentication on the remote desktop protocol. |
| **Impact:** Information transmitted over the remote server can be tampered with, forged or read by a man-in-the-middle over TLS version that is no longer supported by many web browsers and web servers. |
| **CVSS Score** | **3.6** CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:C/C:L/I:L/A:N |
| **Injection Parameter** | N/A |
| **Attack** | N/A |
| **Recommendation** | Update the configuration of the affected application and use a minimum of TLS 1.2 or higher with AES-GCM suites subject to browser and web server support. |
| Proof of Concept | |
| Step 1. Execute Nessus Plug-in scan to enumerate the vulnerable TLSv1 version:    ***Figure M3.S3.1:*** *Nessus Plug-In Script for TLSv1 Cipher*  Exploits & References:  <https://nvd.nist.gov/vuln/detail/CVE-2014-3566>1  <https://nvd.nist.gov/vuln/detail/CVE-2011-3389>2  <https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/insecure-transportation-security-protocol-supported-tls-10/> | |

* 1. M1.S3 – [Title of the Finding]

|  |  |
| --- | --- |
| [M1.S3] [Title of the Finding] | |
| Information disclosure, also known as information leakage, was identified during testing. This was found in the form of open/unused ports, service enumeration, domain level information (E.g. domain name, netbios name, ability to query active directory), and responses found during SSH/RDP brute force attacks (validating username:password enumeration). | |
| **Impacted Assets** | All in-scope hosts. |
| **Risk** | **Severity:** MEDIUM[S3] |
| **Likelihood:** This vulnerability can be executed by running simple network scans with tools like Nmap or host scanning with Nessus. This is classified as a basic or novice skill and one that every attacker would use for reconnaissance. |
| **Impact:** Attackers will leverage any information they are able to obtain in order to exploit an environment. If ports and service information were not available the attacker would be unable to discern any potential attacks outside of best guesses. For example, if a given host is only known by IP, but able to be scanned exposing ports that are native to only active directory – this would be an easy indication that this machine could be a domain controller or hold sensitive information (even from the NetBIOS name – E.g., INF**DC**00#). |
| **CVSS Score** | **3.1** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:N |
| **Injection Parameter** | N/A |
| **Attack** | N/A |
| **Recommendation** | * Close or disallow access to unused or unneeded ports and services. Consider network level access controls which only allow access if the granted user is authorized.   + At a minimum, defaulting to “filtered” port status for all unused or exploitable ports should be enabled * Disable NetBIOS Name Service (NBT-NS) on all machines (this is enabled by default on all machines). Resolution of hosts will then rely on corporate controlled servers (DNS and WINS).   + To disable NetBIOS over TCP/IP, a script must be deployed to every system on the network or managed via group policy.   + The setting can be found on every windows machinein advanced TCP/IP Settings:   The Disable NetBIOS over TCP/IP option windows 10 how to disable netbios  ***Figure M4.S3.1:*** *Setting NetBIOS Name Resolution by Using Windows Interface* |
| Proof of Concept | |
| Curl command with verbose output querying port 22 (SSH):    ***Figure M4.S3.2:*** *Information Disclosure Using “curl” Command*  nmap Scan with -A (run all – includes default scripts):    ***Figure M4.S3.3:*** *Information Disclosure Using “nmap” Scan Command (Port 3389 – RDP)*    ***Figure M4.S3.4:*** *Information Disclosure Using “nmap” Scan Command to Identify AD DC*  **Exploit Proof of Concept and Supporting Documentation:**  <https://docs.microsoft.com/en-us/previous-versions/tn-archive/ee692589(v=technet.10)?redirectedfrom=MSDN> | |

* 1. L1.S4 – [Title of the finding]

|  |  |
| --- | --- |
| [L1.S4] Title of the Finding | |
| The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote hosts is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host. | |
| **Impacted Assets** | All in-scope hosts. |
| **Risk** | **Severity:** LOW [S4] |
| **Likelihood:** This vulnerability can be exploited through MITM attacks and once inside the network or server, an attacker can leverage other means to escalate privileges. |
| **Impact:** If compromised, self-signed certificates can pose a number of challenges to XYZinc. If an attacked already gained access to the system, he can spoof the identity of the URL and lure users in order to steal credentials or access sensitive data. Certificate Authorities can revoke a certification when they discover it has been compromised, but organizations cannot revoke a self-certificate. |
| **CVSS Score** | **3.9** CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:C/C:L/I:L/A:N |
| **Injection Parameter** | N/A |
| **Attack** | N/A |
| **Recommendation** | Generate or purchase a proper SSL certificate for this service. |
| Proof of Concept | |
| Step 1. Perform Nmap scan:  Graphical user interface, text, application  Description automatically generated  ***Figure L1.S4:*** *Self Signed Certificate* | |

* 1. L2.S4 - SSL Certificate Cannot Be Trusted

|  |  |
| --- | --- |
| [L2.S4] SSL Certificate Cannot Be Trusted | |
| The certificate cannot be validated as the certificate trust chain is broken. | |
| **Impacted Assets** | All in-scope hosts. |
| **Risk** | **Severity:** LOW [S4] |
| **Likelihood:** This vulnerability could be exploited if an attacker carries out a MiTM attack against the remote host. |
| **Impact:** This situation can occur in three different ways, in which the chain of trust can be broken, as stated below:   * The top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority. * The certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates. * The certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize. * If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host. |
| **CVSS Score** | **3.1** CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L |
| **Injection Parameter** | N/A |
| **Attack** | N/A |
| **Recommendation** | Replace the affected certificates with one that is valid and that follows proper SSL security. |
| Proof of Concept | |
| Nessus Essentials and nmap was used to scan the above targets yielding the sample outputs below:    ***Figure L5.S4.1:*** *Nessus Output*    ***Figure L5.S4.2:*** *nmap Host Scan Output*  **Exploit Proof of Concept and Supporting Documentation:**  <https://remme.io/blog/nist-report-best-practice-for-tls-certificate-management> | |

* 1. L5.S4 - SSL Medium Strength Cipher Suites Supported (SWEET32)

|  |  |
| --- | --- |
| [L5.S4] SSL Medium Strength Cipher Suites Supported (SWEET32) | |
| The remote hosts supports the use of SSL ciphers that offer medium strength encryption. The attack focuses on certain ciphers' design flaws. An attacker can recover small portions of plaintext using the SWEET32 attack. SWEET32 attack is used to break/intercept communication that works with DES/3DES cipher suite. A man-in-the-middle attack can be leveraged to steal large amount of encrypted traffic between TLS/SSL server and client. | |
| **Impacted Assets** | All in-scope hosts. |
| **Risk** | **Severity:** LOW [S4] |
| **Likelihood:** This vulnerability can be exploited if plaintext is repeatedly encrypted (e.g. HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts. |
| **Impact:** If n number of ciphertexts is obtained by the attacker, he may be able to derive the plaintext. The attacker would be able to steal user credentials, elevate to administrative privilege accounts and expose other sensitive data. |
| **CVSS Score** | **3.1** CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L |
| **Injection Parameter** | N/A |
| **Attack** | N/A |
| **Recommendation** | Update the configuration of the affected application, to disallow use of RC4 ciphers. Consider using TLS 1.3 or higher with AES-GCM suites subject to browser and web server support.  A note on this vulnerability:  To execute the full attack we need to transfer enough data (~785gb) to recover a two-block secret and we would need to send 4 KB size request/sec. This would affect XYZ Inc’s environment causing noticeable bandwidth utilization and thus has been labeled as unlikely to be executed in this environment. It was also taken into consideration that the original exploit required an uninterrupted block of time that ended up totalling ~19 hours. In a real world scenario, given enough time and resources it would be possible for an attacker to exploit this vulnerability. |
| Proof of Concept | |
| Nessus Essentials was used to scan the above target yielding the output below:  Graphical user interface, text, application  Description automatically generated  ***Figure L5.S4:*** *Nessus Output*  **Exploit Proof of Concept and Supporting Documentation:**  <https://sweet32.info/>  <https://nvd.nist.gov/vuln/detail/CVE-2016-2183> | |

# 6.2 Vulnerabilities and Findings – Active Directory

Scope:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No.** | **IP Address** | **Hostname** | **PCI** | **Product** |
| 3 |  |  |  |  |
| 4 |  |  |  |  |
| 5 |  |  |  |  |
| 6 |  |  |  |  |
| 7 |  |  |  |  |

Tools:

|  |  |
| --- | --- |
| **Category** | **Tool Name** |
| **Reconnaissance** | * Nmap Security Scanner   + Network discovery and security auditing * OpenVAS [Open Vulnerability Assessment Scanner]   + Vulnerability scanner * Nikto/Nikto2   + Opensource web server and vulnerability scanner * Nessus Essentials   + Network discovery, security auditing, and vulnerability scanning * OWASP Zed Attack Proxy [ZAP]   + Web application security and vulnerability scanner * Netsparker   + Web application security and vulnerability scanner * Metasploit   + Penetration testing framework with prebuilt security and vulnerability scanners |
| **Exploitation** | * Metasploit   + Penetration testing framework with prebuilt exploits * Nmap Security Scanner [Exploit Scripts]   + Preconfigured scripts for exploitation * Python Scripting   + CVE-2021-38647 PoC Script (OMIGOD)     - <https://github.com/horizon3ai/CVE-2021-38647>   + crowbar.py (via Impacket – Built into Kali)     - Brute force RDP script   + eternal\_checker.py     - <https://github.com/3ndG4me/AutoBlue-MS17-010/blob/master/eternal_checker.py>     - SMBv1 Eternal Blue exploit script |

Vulnerability Overview:

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Vulnerability Name | Risk Rating | Status |
| C1.S1 | XXXXX | Critical | Open |
| H1.S2 | XXXXX | High | Open |
| M1.S3 | XXXXX | Medium | Open |
| L1.S4 | XXXXX | Low | Open |

1. M1.S1 - Undetected Malicious Activity – Host Scanning

|  |  |
| --- | --- |
| [M1.S3] Undetected Malicious Activity - Host Scanning | |
| Failure to detect all malicious activity on the host assessment and vulnerability scans. | |
| **Impacted Assets** | All in-scope hosts. |
| **Risk** | **Severity:** MEDIUM[S3] |
| **Likelihood:** These activities occur after primary controls fail. |
| **Impact:** Undetected internal network attacks allow adversaries to expand control. |
| **CVSS Score** | **5.3** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N |
| **Injection Parameter** | N/A |
| **Attack** | N/A |
| **Recommendation** | Review SIEM strategy and WAF settings for the hosts that are accessible through HTTP. Some attacks may be difficult to detect but have been noted for information and review.  Attacks Undetected:   * Web vulnerability scans with Nessus, Netsparker, Nikto and OWASP ZAP * Active vulnerability scans with Burp Suite Pro * Network vulnerability scans with Nmap |
| Proof of Concept | |
| As this vulnerability stems from all of the reconnaissance that was performed by the OSRT for the segmentation evaluation - the tools below will serve as the proof of concept.   * Nmap Security Scanner   + Network discovery and security auditing * OpenVAS [Open Vulnerability Assessment Scanner]   + Vulnerability scanner * Nikto/Nikto2   + Opensource web server and vulnerability scanner * Nessus Essentials   + Network discovery, security auditing, and vulnerability scanning * OWASP Zed Attack Proxy [ZAP]   + Web application security and vulnerability scanner * Netsparker   + Web application security and vulnerability scanner * Metasploit   + Penetration testing framework with prebuilt security and vulnerability scanners   The concept of scanning should be evaluated for possible detection and blocking as this information ultimately leads to enumeration of vulnerabilities that can be exploited. It is understandable that maintaining security posture in the internal environments may require legitimate scanning to determine vulnerabilities and patching compliance, in this case, a system based on whitelisting will reduce this threat vector. | |

1. H1.S2 - TLS Version 1.0 and 1.1 Protocol Detection

|  |  |
| --- | --- |
| [M3.S3] TLS Version 1.0 and 1.1 Protocol Detection | |
| The remote service accepts connections encrypted using TLS 1.0 and 1.1 which has a number of cryptographic design flaws. The most notable and well documented exploits being POODLE1 or BEAST2. These exploits leverage this vulnerability in order to perform Man-in-the-Middle (MiTM) attacks which lead to data exfiltration. Newer versions of TLS such as 1.2 and 1.3 are designed against these flaws and should be used whenever possible.  As of March 31, 2020, endpoints that aren’t enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits. | |
| **Impacted Assets** | All in-scope hosts. |
| **Risk** | **Severity:** MEDIUM[S3] |
| **Likelihood:** This vulnerability can be exploited if primary controls fail such as authentication on the remote desktop protocol. |
| **Impact:** Information transmitted over the remote server can be tampered with, forged or read by a man-in-the-middle over TLS version that is no longer supported by many web browsers and web servers. |
| **CVSS Score** | **3.6** CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:C/C:L/I:L/A:N |
| **Injection Parameter** | N/A |
| **Attack** | N/A |
| **Recommendation** | Update the configuration of the affected application and use a minimum of TLS 1.2 or higher with AES-GCM suites subject to browser and web server support. |
| Proof of Concept | |
| Step 1. Execute Nessus Plug-in scan to enumerate the vulnerable TLSv1 version:    ***Figure M3.S3.1:*** *Nessus Plug-In Script for TLSv1 Cipher*  Exploits & References:  <https://nvd.nist.gov/vuln/detail/CVE-2014-3566>1  <https://nvd.nist.gov/vuln/detail/CVE-2011-3389>2  <https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/insecure-transportation-security-protocol-supported-tls-10/> | |

1. M1.S3 – [Title of the Finding]

|  |  |
| --- | --- |
| [M4.S3] [Title of the Finding] | |
| Description of the finding here. | |
| **Impacted Assets** | In-scope hosts |
| **Risk** | **Severity:** MEDIUM[S3] |
| **Likelihood:** This vulnerability can be executed by running simple network scans with tools like nmap or host scanning with Nessus. This is classified as a basic or novice skill and one that every attacker would use for reconnaissance. |
| **Impact:** Attackers will leverage any information they are able to obtain in order to exploit an environment. If ports and service information were not available the attacker would be unable to disern any potential attacks outside of best guesses. For example, if a given host is only known by IP, but able to be scanned exposing ports that are native to only active directory – this would be an easy indication that this machine could be a domain controller or hold sensitive information (even from the netbios name – E.g. INF**DC**00#). |
| **CVSS Score** | **3.1** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:N |
| **Injection Parameter** | N/A |
| **Attack** | N/A |
| **Recommendation** | * Close or disallow access to unused or unneeded ports and services. Consider network level access controls which only allow access if the granted user is authorized.   + At a minimum, defaulting to “filtered” port status for all unused or exploitable ports should be enabled * Disable NetBIOS Name Service (NBT-NS) on all machines (this is enabled by default on all machines). Resolution of hosts will then rely on corporate controlled servers (DNS and WINS).   + To disable NetBIOS over TCP/IP, a script must be deployed to every system on the network or managed via group policy.   + The setting can be found on every windows machinein advanced TCP/IP Settings:   The Disable NetBIOS over TCP/IP option windows 10 how to disable netbios  ***Figure M4.S3.1:*** *Setting NetBIOS Name Resolution by Using Windows Interface* |
| Proof of Concept | |
| nmap Scan with -A (run all – includes default scripts):  ***Figure M4.S3.1:*** *Information Disclosure Using “nmap” Scan Command to Identify AD DC*  **Exploit Proof of Concept and Supporting Documentation:**  <https://docs.microsoft.com/en-us/previous-versions/tn-archive/ee692589(v=technet.10)?redirectedfrom=MSDN> | |

1. L1.S4 – [Title of the Finding]

|  |  |
| --- | --- |
| [L2.S4] Title of the Finding | |
| The certificate cannot be validated as the certificate trust chain is broken. | |
| **Impacted Assets** | 10.3.65.198 [PGRCCINFDC005] |
| **Risk** | **Severity:** LOW [S4] |
| **Likelihood:** This vulnerability could be exploited if an attacker carries out a MiTM attack against the remote host. |
| **Impact:** This situation can occur in three different ways, in which the chain of trust can be broken, as stated below:   * The top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority. * The certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates. * The certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize. * If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host. |
| **CVSS Score** | **3.1** CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L |
| **Injection Parameter** | N/A |
| **Attack** | N/A |
| **Recommendation** | Replace the affected certificates with one that is valid and that follows proper SSL security. |
| Proof of Concept | |
| Nessus Essentials was used to scan the above targets yielding the sample outputs below:    ***Figure L5.S4.1:*** *Nessus Output*  **Exploit Proof of Concept and Supporting Documentation:**  <https://remme.io/blog/nist-report-best-practice-fo-tls-certificate-management> | |

# Vulnerabilities and Findings –

Scope:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No.** | **IP Address** | **Hostname** | **PCI** | **Product** |
| 8 |  |  |  |  |
| 9 |  |  |  |  |

Tools:

| **Category** | **Tool Name** |
| --- | --- |
| **Reconnaissance** | * Nmap Security Scanner   + Network discovery and security auditing * OpenVAS [Open Vulnerability Assessment Scanner]   + Vulnerability scanner * Nikto/Nikto2   + Opensource web server and vulnerability scanner * Nessus Essentials   + Network discovery, security auditing, and vulnerability scanning * OWASP Zed Attack Proxy [ZAP]   + Web application security and vulnerability scanner * Netsparker   + Web application security and vulnerability scanner * Metasploit   + Penetration testing framework with prebuilt security and vulnerability scanners |
| **Exploitation** | * Metasploit   + Penetration testing framework with prebuilt exploits * Nmap Security Scanner [Exploit Scripts]   + Preconfigured scripts for exploitation * Python Scripting   + CVE-2021-38647 PoC Script (OMIGOD)     - <https://github.com/horizon3ai/CVE-2021-38647>   + crowbar.py (via Impacket – Built into Kali)     - Brute force RDP script   + eternal\_checker.py     - <https://github.com/3ndG4me/AutoBlue-MS17-010/blob/master/eternal_checker.py>     - SMBv1 Eternal Blue exploit script |

Vulnerability Overview:

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Vulnerability Name | Risk Rating | Status |
| C1.S1 | XXXXX | Critical | Open |
| H1.S2 | XXXXX | High | Open |
| M1.S3 | XXXXX | Medium | Open |
| L1.S4 | XXXXX | Low | Open |

1. C1.S1 – [Title of the Finding]

|  |  |
| --- | --- |
| [M1.S3] Title of the Finding | |
| Description of the finding. | |
| **Impacted Assets** | All in-scope hosts. |
| **Risk** | **Severity:** MEDIUM[S3] |
| **Likelihood:** These activities occur after primary controls fail. |
| **Impact:** Undetected internal network attacks allow adversaries to expand control. |
| **CVSS Score** | **5.3** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N |
| **Injection Parameter** | N/A |
| **Attack** | N/A |
| **Recommendation** | Review SIEM strategy and WAF settings for the hosts that are accessible through HTTP. Some attacks may be difficult to detect but have been noted for information and review.  Attacks Undetected:   * Web vulnerability scans with Nessus, Netsparker, Nikto and OWASP ZAP * Active vulnerability scans with Burp Suite Pro * Network vulnerability scans with Nmap |
| Proof of Concept | |
| As this vulnerability stems from all of the reconnaissance that was performed by the OSRT for the segmentation evaluation - the tools below will serve as the proof of concept.   * Nmap Security Scanner   + Network discovery and security auditing * OpenVAS [Open Vulnerability Assessment Scanner]   + Vulnerability scanner * Nikto/Nikto2   + Opensource web server and vulnerability scanner * Nessus Essentials   + Network discovery, security auditing, and vulnerability scanning * OWASP Zed Attack Proxy [ZAP]   + Web application security and vulnerability scanner * Netsparker   + Web application security and vulnerability scanner * Metasploit   + Penetration testing framework with prebuilt security and vulnerability scanners   The concept of scanning should be evaluated for possible detection and blocking as this information ultimately leads to enumeration of vulnerabilities that can be exploited. It is understandable that maintaining security posture in the internal environments may require legitimate scanning to determine vulnerabilities and patching compliance, in this case, a system based on whitelisting will reduce this threat vector. | |

1. H1.S2 – Title of the Finding

|  |  |
| --- | --- |
| [M3.S3] Title of the Finding | |
| The remote service accepts connections encrypted using TLS 1.0 and 1.1 which has a number of cryptographic design flaws. The most notable and well documented exploits being POODLE1 or BEAST2. These exploits leverage this vulnerability in order to perform Man-in-the-Middle (MiTM) attacks which lead to data exfiltration. Newer versions of TLS such as 1.2 and 1.3 are designed against these flaws and should be used whenever possible.  As of March 31, 2020, endpoints that aren’t enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits. | |
| **Impacted Assets** | 10.119.58.204 [gvmw2cctxjpn007.XYZinc.XYZ.com]  10.119.60.113 [gvmw2cctxcnx111.XYZinc.XYZ.com]  10.119.60.121 [gvmw2cctxcnx129.XYZinc.XYZ.com]  10.119.60.132 [gvmw2cctxcnx137.XYZinc.XYZ.com]  10.119.60.140 [gvmw2cctxcnx155.XYZinc.XYZ.com]  10.119.60.16 [gvmw2cctxcnx071.XYZinc.XYZ.com] |
| **Risk** | **Severity:** MEDIUM[S3] |
| **Likelihood:** This vulnerability can be exploited if primary controls fail such as authentication on the remote desktop protocol. |
| **Impact:** Information transmitted over the remote server can be tampered with, forged or read by a man-in-the-middle over TLS version that is no longer supported by many web browsers and web servers. |
| **CVSS Score** | **3.6** CVSS:3.0/AV:L/AC:H/PR:L/UI:R/S:C/C:L/I:L/A:N |
| **Injection Parameter** | N/A |
| **Attack** | N/A |
| **Recommendation** | Update the configuration of the affected application and use a minimum of TLS 1.2 or higher with AES-GCM suites subject to browser and web server support. |
| Proof of Concept | |
| Step 1. Execute Nessus Plug-in scan to enumerate the vulnerable TLSv1 version:    ***Figure M3.S3.1:*** *Nessus Plug-In Script for TLSv1 Cipher*  Exploits & References:  <https://nvd.nist.gov/vuln/detail/CVE-2014-3566>1  <https://nvd.nist.gov/vuln/detail/CVE-2011-3389>2  <https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/insecure-transportation-security-protocol-supported-tls-10/> | |

1. M1.S3 – Title of the Finding

|  |  |
| --- | --- |
| [M1.S3] Title of the Finding | |
| Information disclosure, also known as information leakage, was identified during testing. This was found in the form of open/unused ports, service enumeration, domain level information (E.g. domain name, NetBIOS name, ability to query active directory), and responses found during SSH/RDP brute force attacks (validating username:password enumeration). | |
| **Impacted Assets** | All in-scope hosts. |
| **Risk** | **Severity:** MEDIUM[S3] |
| **Likelihood:** This vulnerability can be executed by running simple network scans with tools like Nmap or host scanning with Nessus. This is classified as a basic or novice skill and one that every attacker would use for reconnaissance. |
| **Impact:** Attackers will leverage any information they are able to obtain in order to exploit an environment. If ports and service information were not available the attacker would be unable to discern any potential attacks outside of best guesses. For example, if a given host is only known by IP, but able to be scanned exposing ports that are native to only active directory – this would be an easy indication that this machine could be a domain controller or hold sensitive information (even from the NetBIOS name – E.g. INF**DC**00#). |
| **CVSS Score** | **3.1** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:N |
| **Injection Parameter** | N/A |
| **Attack** | N/A |
| **Recommendation** | * Close or disallow access to unused or unneeded ports and services. Consider network level access controls which only allow access if the granted user is authorized.   + At a minimum, defaulting to “filtered” port status for all unused or exploitable ports should be enabled * Disable NetBIOS Name Service (NBT-NS) on all machines (this is enabled by default on all machines). Resolution of hosts will then rely on corporate controlled servers (DNS and WINS).   + To disable NetBIOS over TCP/IP, a script must be deployed to every system on the network or managed via group policy.   + The setting can be found on every windows machinein advanced TCP/IP Settings:   The Disable NetBIOS over TCP/IP option windows 10 how to disable netbios  ***Figure M4.S3.1:*** *Setting NetBIOS Name Resolution by Using Windows Interface* |
| Proof of Concept | |
| Curl command with verbose output querying port 22 (SSH):  Text  Description automatically generated  ***Figure M4.S3.2:*** *Information Disclosure Using “curl” Command*  nmap Scan with -A (run all – includes default scripts):  Text  Description automatically generated  ***Figure M4.S3.3:*** *Information Disclosure Using “nmap” Scan Command (Port 3389 – RDP)*  *Text  Description automatically generated*  ***Figure M4.S3.4:*** *Information Disclosure Using “nmap” Scan Command to Identify AD DC*  **Exploit Proof of Concept and Supporting Documentation:**  <https://docs.microsoft.com/en-us/previous-versions/tn-archive/ee692589(v=technet.10)?redirectedfrom=MSDN> | |

1. L1.S4 – Title of the Finding

|  |  |
| --- | --- |
| [L1.S4] Title of the Finding | |
| Failure to detect all malicious activity on the port enumeration exploit and RDP brute force attacks. | |
| **Impacted Assets** | All in-scope hosts. |
| **Risk** | **Severity:** MEDIUM[S3] |
| **Likelihood:** These activities occur after primary controls fail. |
| **Impact:** Undetected internal network attacks allow adversaries to expand control. An attacker with stolen valid credentials list would be able to escalate the attack in order to compromise data, extract sensitive data or cause denial of service. An attacker without valid credentials could use simple methods to obtain usernames through OSINT or AD DC enumeration and combine with a password list (E.g. rockyou.txt – built into Kali linux).  NOTE: This attack resulted in enumeration of a valid “SA\_” account, this account was found to be not usable due to some network or authentication controls as RDP access was not obtained nor could this username and password be used to query the AD DC for information a credential ADuser can obtain. This account was remediated (password reset) by the CDC-MIR team post discovery. |
| **CVSS Score** | **5.3** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N |
| **Injection Parameter** | N/A |
| **Attack** | Metasploit module, crowbar python script  Attacks Undetected:   * RDP Enumeration Attack using Metasploit * RDP Brute Force Attack Using Metasploit * RDP Brute Force Attack using Crowbar |
| **Recommendation** | * Review SIEM strategy and alerts specific to RDP logon attempts. * Implement rate limiting, strong passwords, and enforce a password lockout policy. * Ensure that the amount of incoming and outgoing traffic to or from the network is monitored. * Close or disallow access to unused or unneeded ports and services. Consider network level access controls which only allow access if the granted user is authorized.   + At a minimum, defaulting to “filtered” port status for all unused or exploitable ports should be enabled * Enable 2FA/MFA to all hosts that allow RDP access. |
| Proof of Concept | |
| Using crowbar, all in scope host list, list of XYZ AZ/SA accounts, and a guessable password list – it allowed OSRT to perform RDP brute force attacks that resulted in the identification of a valid username and password with RDP access to 10.119.54.13. As this technique uses hundreds if thousands of attempts, given the timeframe of this engagement this would have potentially exposed more credentials or like access to other devices with RDP access.      ***Figure M5.S3.1:*** *Crowbar RDP Brute Force Attack – NOTE: SA\_Sa7b0h4 Identified With Weak Guessable Credentials* | |

# Vulnerabilities and Findings – Splunk Hosts

Scope:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No.** | **IP Address** | **Hostname** | **PCI** | **Product** |
| 27 |  |  |  |  |
| 28 |  |  |  |  |
| 29 |  |  |  |  |
| 30 |  |  |  |  |

Tools:

|  |  |
| --- | --- |
| **Category** | **Tool Name** |
| **Reconnaissance** | * Nmap Security Scanner   + Network discovery and security auditing * OpenVAS [Open Vulnerability Assessment Scanner]   + Vulnerability scanner * Nikto/Nikto2   + Opensource web server and vulnerability scanner * Nessus Essentials   + Network discovery, security auditing, and vulnerability scanning * OWASP Zed Attack Proxy [ZAP]   + Web application security and vulnerability scanner * Netsparker   + Web application security and vulnerability scanner * Metasploit   + Penetration testing framework with prebuilt security and vulnerability scanners |
| **Exploitation** | * Metasploit   + Penetration testing framework with prebuilt exploits * Nmap Security Scanner [Exploit Scripts]   + Preconfigured scripts for exploitation * Python Scripting   + CVE-2021-38647 PoC Script (OMIGOD)     - <https://github.com/horizon3ai/CVE-2021-38647>   + crowbar.py (via Impacket – Built into Kali)     - Brute force RDP script   + eternal\_checker.py     - <https://github.com/3ndG4me/AutoBlue-MS17-010/blob/master/eternal_checker.py>     - SMBv1 Eternal Blue exploit script |

Vulnerability Overview:

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Vulnerability Name | Risk Rating | Status |
| C1.S1 | XXXX | Critical | Open |
| H1.S2 | XXXX | High | Open |
| M1.S3 | XXXX | Medium | Open |
| L1.S4 | XXXX | Low | Open |

1. C1.S1 – Title of the Finding

|  |  |
| --- | --- |
| [C1.S1] Title of the Finding | |
| Failure to detect all malicious activity on the host assessment and vulnerability scans. | |
| **Impacted Assets** | All in-scope hosts. |
| **Risk** | **Severity:** MEDIUM[S3] |
| **Likelihood:** These activities occur after primary controls fail. |
| **Impact:** Undetected internal network attacks allow adversaries to expand control. |
| **CVSS Score** | **5.3** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N |
| **Injection Parameter** | N/A |
| **Attack** | N/A |
| **Recommendation** | Review SIEM strategy and WAF settings for the hosts that are accessible through HTTP. Some attacks may be difficult to detect but have been noted for information and review.  Attacks Undetected:   * Web vulnerability scans with Nessus, Netsparker, Nikto and OWASP ZAP * Active vulnerability scans with Burp Suite Pro * Network vulnerability scans with Nmap |
| Proof of Concept | |
| As this vulnerability stems from all of the reconnaissance that was performed by the OSRT for the segmentation evaluation - the tools below will serve as the proof of concept.   * Nmap Security Scanner   + Network discovery and security auditing * OpenVAS [Open Vulnerability Assessment Scanner]   + Vulnerability scanner * Nikto/Nikto2   + Opensource web server and vulnerability scanner * Nessus Essentials   + Network discovery, security auditing, and vulnerability scanning * OWASP Zed Attack Proxy [ZAP]   + Web application security and vulnerability scanner * Netsparker   + Web application security and vulnerability scanner * Metasploit   + Penetration testing framework with prebuilt security and vulnerability scanners   The concept of scanning should be evaluated for possible detection and blocking as this information ultimately leads to enumeration of vulnerabilities that can be exploited. It is understandable that maintaining security posture in the internal environments may require legitimate scanning to determine vulnerabilities and patching compliance, in this case, a system based on whitelisting will reduce this threat vector. | |

1. H1.S2 – Title of the Finding

|  |  |
| --- | --- |
| [H1.S2] Title of the Finding | |
| Failure to detect all malicious activity on the port enumeration exploit and ssh brute force attacks. | |
| **Impacted Assets** | 10.107.66.211 [syslog05.phx.XYZinc.com]  10.117.54.86 [gvmx1csplfwdrapp311.prod.azwus2.XYZtech.com] |
| **Risk** | **Severity:** MEDIUM[S3] |
| **Likelihood:** These activities occur after primary controls fail. |
| **Impact:** Undetected internal network attacks allow adversaries to expand control. An attacker with stolen valid credentials list would be able to escalate the attack in order to compromise data, extract sensitive data or cause denial of service. |
| **CVSS Score** | **5.3** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N |
| **Injection Parameter** | N/A |
| **Attack** | Metasploit module, nmap brute force script |
| **Recommendation** | Review SIEM strategy and WAF settings for the hosts that are publicly accessible through HTTP. Some attacks may be difficult to detect but have been noted for information and review.  Attacks Undetected:   * SSH Enumeration Attack using Metasploit * SSH Brute Force Attack using Metasploit   Implement rate limiting and enforce password lockout policy. Ensure that the amount of incoming and outgoing traffic to or from the network is monitored. |
| Proof of Concept | |
| Using a Metasploit ssh\_version module, enumerated ssh versions that are existing on the hosts:    ***Figure M2.S3.1:*** *Enumerating ssh versions on hosts*  Using Metasploit ssh\_enumusers module, ran a brute force attack to enumerate users:    ***Figure M2.S3.2:*** *SSH Brute Force Attack Using Metasploit* | |

1. M1.S3 – Title of the Finding

|  |  |
| --- | --- |
| [M1.S3] Title of the Finding | |
| Information disclosure, also known as information leakage, was identified during testing. This was found in the form of open/unused ports, service enumeration, domain level information (E.g. domain name, NetBIOS name, ability to query active directory), and responses found during SSH/RDP brute force attacks (validating username:password enumeration). | |
| **Impacted Assets** | All in-scope hosts. |
| **Risk** | **Severity:** MEDIUM[S3] |
| **Likelihood:** This vulnerability can be executed by running simple network scans with tools like Nmap or host scanning with Nessus. This is classified as a basic or novice skill and one that every attacker would use for reconnaissance. |
| **Impact:** Attackers will leverage any information they are able to obtain in order to exploit an environment. If ports and service information were not available the attacker would be unable to discern any potential attacks outside of best guesses. For example, if a given host is only known by IP, but able to be scanned exposing ports that are native to only active directory – this would be an easy indication that this machine could be a domain controller or hold sensitive information (even from the netbios name – E.g. INF**DC**00#). |
| **CVSS Score** | **3.1** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:N |
| **Injection Parameter** | N/A |
| **Attack** | N/A |
| **Recommendation** | * Close or disallow access to unused or unneeded ports and services. Consider network level access controls which only allow access if the granted user is authorized.   + At a minimum, defaulting to “filtered” port status for all unused or exploitable ports should be enabled * Disable NetBIOS Name Service (NBT-NS) on all machines (this is enabled by default on all machines). Resolution of hosts will then rely on corporate controlled servers (DNS and WINS).   + To disable NetBIOS over TCP/IP, a script must be deployed to every system on the network or managed via group policy.   + The setting can be found on every windows machinein advanced TCP/IP Settings:   The Disable NetBIOS over TCP/IP option windows 10 how to disable netbios  ***Figure M4.S3.1:*** *Setting NetBIOS Name Resolution by Using Windows Interface* |
| Proof of Concept | |
| nmap Scan with -A (run all – includes default scripts):    ***Figure M4.S3.1:*** *Information Disclosure Using “nmap” Scan*  **Exploit Proof of Concept and Supporting Documentation:**  <https://docs.microsoft.com/en-us/previous-versions/tn-archive/ee692589(v=technet.10)?redirectedfrom=MSDN> | |

1. L1.S4 – Title of the Finding

|  |  |
| --- | --- |
| [L1.S4] Title of the Finding | |
| Failure to detect all malicious activity on the port enumeration exploit and RDP brute force attacks. | |
| **Impacted Assets** | 10.107.66.211 [syslog05.phx.XYZinc.com] |
| **Risk** | **Severity:** MEDIUM[S3] |
| **Likelihood:** These activities occur after primary controls fail. |
| **Impact:** Undetected internal network attacks allow adversaries to expand control. An attacker with stolen valid credentials list would be able to escalate the attack in order to compromise data, extract sensitive data or cause denial of service. An attacker without valid credentials could use simple methods to obtain usernames through OSINT or AD DC enumeration and combine with a password list (E.g. rockyou.txt – built into Kali linux).  NOTE: This attack resulted in enumeration of a valid “SA\_” account, this account was found to be not usable due to some network or authentication controls as RDP access was not obtained nor could this username and password be used to query the AD DC for information a credential ADuser can obtain. This account was remediated (password reset) by the CDC-MIR team post discovery. |
| **CVSS Score** | **5.3** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N |
| **Injection Parameter** | N/A |
| **Attack** | Metasploit module, crowbar python script  Attacks Undetected:   * RDP Enumeration Attack using Metasploit * RDP Brute Force Attack Using Metasploit * RDP Brute Force Attack using Crowbar |
| **Recommendation** | * Review SIEM strategy and alerts specific to RDP logon attempts. * Implement rate limiting, strong passwords, and enforce a password lockout policy. * Ensure that the amount of incoming and outgoing traffic to or from the network is monitored. * Close or disallow access to unused or unneeded ports and services. Consider network level access controls which only allow access if the granted user is authorized.   + At a minimum, defaulting to “filtered” port status for all unused or exploitable ports should be enabled * Enable 2FA/MFA to all hosts that allow RDP access. |
| Proof of Concept | |
| Using crowbar, all in scope host list, list of XYZ AZ/SA accounts, and a guessable password list – it allowed OSRT to perform RDP brute force attacks that resulted in the identification of a valid username and password with RDP access to 10.119.54.13. As this technique uses hundreds if thousands of attempts, given the timeframe of this engagement this would have potentially exposed more credentials or like access to other devices with RDP access.      ***Figure M5.S3.1:*** *Crowbar RDP Brute Force Attack – NOTE: SA\_Sa7b0h4 Identified With Weak Guessable Credentials* | |

# Additional Scans and Reports

The OSRT will provide all reported information gathered during testing. This includes vulnerability scans in executive and detailed formats and a detailed findings Excel spreadsheet. These reports contain raw vulnerability scans and additional vulnerabilities not exploited.