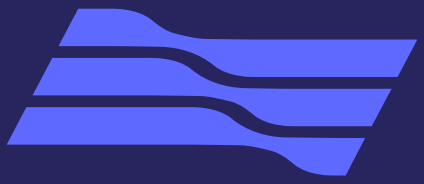


RHODIAN

PENETRATION TEST SAMPLE REPORT

External Network | Internal Network

Prepared For
ACME | John Doe | 555-555-5555 | client@acme.com

Contents

PROJECT DETAILS

Rhodian performed penetration testing for ACME in accordance with information security best practices. Testing was performed from January 10-30, 2022 and was limited to the scope defined below.
The objective of this test was to proactively discover and exploit vulnerabilities which could lead to the compromise of systems or sensitive information in the targeted environment. This report provides the testing methodologies, procedures, findings, and associated remediation recommendations to help ACME strengthen its security posture.

Personnel

ACME	Rhodian
Project Sponsor John Doe 555-555-555 client@acme.com	**Project Lead** Jeff Oden, GPEN,OSWP 303-495-8503 jeff@rhodian.com

Scope

Per direction of ACME, testing was limited to the following:

Project Scope	
Testing Timeframe	
January 10-30, 2024	
Targets	
External Network X.X.X.X/29	**Internal Network** X.X.X.X/24

EXECUTIVE SUMMARY

During January 10-30, 2022, Rhodian performed a targeted penetration test against ACME's external and internal network environments. The goal of the engagement was to simulate a sophisticated attacker attempting to compromise systems and sensitive data or to cause reputational damage to ACME.

External Network – Critical Risk

External network testing was performed remotely from Rhodian owned IP addresses and devices. A vulnerability related to improper sanitization of user input on a web application was discovered during testing. Rhodian was able to exploit this and gain access to sensitive information externally, which eventually led to authenticated access on the web application. While only one significant issue was found externally, it should be remediated as soon as possible to prevent sensitive information and systems from being compromised.

Internal Network – Critical Risk

Internal network testing was performed by mailing a testing appliance to the XXX office. XXX connected our testing appliance to the internal network, emulating the access of a typical employee. The most severe vulnerabilities were related the improper hardening of systems and use of outdated software packages. Rhodian was able to gain full administrator access to the internal ACME domain. With this level of access everything on the domain, including workstations, servers, files, and databases, could be considered compromised. In place controls, such as XXX, were minimally effective in stopping our attacks.

Due to the ever-evolving threat landscape, Rhodian recommends that ACME continue to enhance its security program by performing proactive security assessments on a regular basis.

TECHNICAL DETAILS

Rhodian utilized both automated vulnerability assessment tools and manual testing techniques to perform reconnaissance, gather information and identify vulnerabilities on the in-scope systems. The highest risk vulnerabilities were then chosen for exploitation attempts. Penetration testing is a targeted and time- constrained activity where a certified expert uses various methods to try and safely exploit vulnerabilities to demonstrate actual risk. Since testing is an exploratory process that can consume a potentially unlimited number of hours, not every vulnerability discovered was exploited.

LIMITATIONS

Any outcome of our services is limited to a point-in-time assessment of the environment. Rhodian does not constitute any form of representation, warranty, or guarantee that the systems tested are 100% secure from attack. While our methodology includes both automated and manual testing to identify the most common security vulnerabilities, it is possible that not every vulnerability in the environment was discovered during testing.

The following was not performed during this engagement:

- Testing that could intentionally disrupt the environment such as Denial of Service (DoS) attacks
- Social Engineering attacks
- Client-Side attacks

RISK RATINGS

Based on the assessment performed and the associated findings, Rhodian has assigned a risk rating to each finding. Several quantitative and qualitative processes can be used to analyze risk, but all share the same principle that the risk of a threat is equal to the potential impact multiplied by the likelihood that an event will occur. The risk rating scale below illustrates Rhodian' risk levels from low to critical.

Risk Rating Scale		
Critical		System or data compromise is trivial and of high impact. Exploits are freely available.
High		System or data compromise is possible but more difficult. Exploits are freely available, but attack vectors make exploitation more complex.
Medium		System or data compromise might be possible, but attack vectors require a high level of expertise, were out of scope, or require elevated access.
Low		Minimal risk of system or data compromise. Remediation should be balanced against business needs and compensating controls.

METHODOLOGY

Rhodian' Penetration Testing methodology follows industry standards and best practices.
The following resources provide Penetration Testing guidance:

- Penetration Testing Execution Standard (PTES)
- OWASP Top Ten
- NIST SP 800-115 Technical Guide to Information Security Testing
- Payment Card Industry Information Supplement: Requirement 11.3 Penetration Testing

Penetration testing is conducted in the following phases:

Phase	Description
Discovery	An attack surface is created by discovering systems and service in use on the in-scope environment. A combination of best-practice tools and manual techniques will be used to discover vulnerabilities and misconfigurations.
Analysis	The results from the Discovery phase are analyzed to prioritize high-impact and exploitable vulnerabilities and develop the attack plan.
Exploitation	Manual attempts at safe exploitation are made in an attempt to compromise systems and sensitive information. If necessary, pivoting and privilege escalation will be used to fully demonstrate the risk of the vulnerability. Screenshots or other proof of exploitation are captured as proof of access
Reporting	Rhodian will provide a report which includes an Executive Summary, Methodology and Approach, Attack Narratives, Technical Details, and Remediation Advice for all findings.

VULNERABILITY SCANS

As part of the penetration testing process, Rhodian used one or more automated vulnerability scanning tools. Full details on all vulnerabilities identified can be found in the scan reports provided with separately from this document. These vulnerability scan documents should be used for reference and remediation information only as they may contain false positives not verified during testing. Critical and high-risk vulnerabilities could allow the leakage of sensitive data or lead to full compromise of the vulnerable systems. Rhodian recommends that any critical or high vulnerabilities be remediated immediately.

SUMMARY OF FINDINGS

The following significant vulnerabilities were discovered during testing and are fully described in this report. Rhodian recommends remediating each vulnerability as they represent an unnecessary risk to the environment.

EXTERNAL NETWORK

ID	Risk	Vulnerability	Recommendation
01	Critical	SQL Injection	Steps should be taken to prevent injection attacks against the web application.

INTERNAL NETWORK

ID	Risk	Vulnerability	Recommendation
01	Critical	Intel Common Base Agent CreateProcessA() Function Remote Command Execution	Apply the appropriate update as described in Symantec's advisory, SYM09-007.

EXTERNAL NETWORK DETAILS

This section provides details regarding vulnerabilities which were exploited during the project timeframe, and vulnerabilities which were not exploitable but represent a significant risk to the environment. Where applicable, an attack narrative with step-by-step screenshots will provide evidence of our attacks and help to recreate our findings. Remediation guidance is also provided in line with our findings.

TESTING NARRATIVE

External network testing was performed remotely from Rhodian owned IP addresses and devices. Reconnaissance was performed on the in-scope domains to enumerate hostnames, email addresses, or other sensitive company information. All in-scope IP addresses were scanned multiple times to discover live hosts, open ports, running services, and any known vulnerabilities. The results of this scanning were supplemented with manual exploitation attempts, if possible, and verification if exploitation was not possible. Manual testing, beyond the vulnerability scanning, was performed to discover misconfigurations or additional vulnerabilities.

A vulnerability related to improper sanitization of user input on a web application was discovered during testing. Rhodian was able to exploit this and gain access to sensitive information externally, which eventually led to authenticated access on the web application. While only one significant issue was found externally, it should be remediated as soon as possible to prevent sensitive information and systems from being compromised.

Rhodian prioritized the results of the testing, and the most significant vulnerabilities exploited or discovered are described below.

SIGNIFICANT VULNERABILITIES

Rhodian discovered the following vulnerabilities and strongly recommends that each be remediated, as they represent an unnecessary and potentially significant risk to the overall security posture.

01 – SQL Injection	
CRITICAL RISK	
Description and Impact	A web application was discovered running on the vulnerable IP address. At least 1 parameter in the search function of the application was vulnerable to SQL injection. By injecting SQL statements into the parameters, Rhodian was able to enumerate large amounts of information from the back-end database. Usernames and passwords for the ACME application were discovered and used to successfully login.
Vulnerable Systems	http://x.x.x.x/searchresults.asp?search=1 Search parameter
Recommend-ations	Steps should be taken to prevent SQL injection attacks against the application. While Rhodian only discovered 1 parameter that was vulnerable, a full review of the application should be done. The most effective ways to prevent SQL injection are: • Use of Prepared Statements (Parameterized Queries) • Use of Stored Procedures • Escaping all User Supplied Input

Using the tool SQLmap, Rhodian was able to discover a parameter vulnerable to SQL injection.
<SENSITIVE IMAGE REMOVED>

Once the injection point was discovered, Rhodian enumerated information from the back-end database. The images below show the discovered databases.
<SENSITIVE IMAGE REMOVED>

Rhodian then downloaded information from select databases. Shown below is access to usernames and passwords for a different web application.
<SENSITIVE IMAGE REMOVED>

The credentials were discovered to be valid. Access to the ACME application is achieved.
<SENSITIVE IMAGE REMOVED>

INTERNAL NETWORK DETAILS

This section provides details regarding vulnerabilities which were exploited during the project timeframe, and vulnerabilities which were not exploitable but represent a significant risk to the environment. Where applicable, an attack narrative with step-by-step screenshots will provide evidence of our attacks and help to recreate our findings. Remediation guidance is also provided in line with our findings.

TESTING NARRATIVE

Internal network testing was performed by mailing a testing appliance to the XXX office. XXX connected our testing appliance to the internal network, emulating the access of a typical employee. All in-scope IP addresses were scanned multiple times to discover live hosts, open ports, running services, and any known vulnerabilities. The results of this scanning were supplemented with manual exploitation attempts, if possible, and verification if exploitation was not possible. Manual testing, beyond the vulnerability scanning, was performed to discover misconfigurations or additional vulnerabilities.

The most severe vulnerabilities were related the improper hardening of systems and use of outdated software packages. Rhodian was able to gain full administrator access to the internal ACME domain. With this level of access everything on the domain, including workstations, servers, files, and databases, could be considered compromised. In place controls, such as XXX, were minimally effective in stopping our attacks.

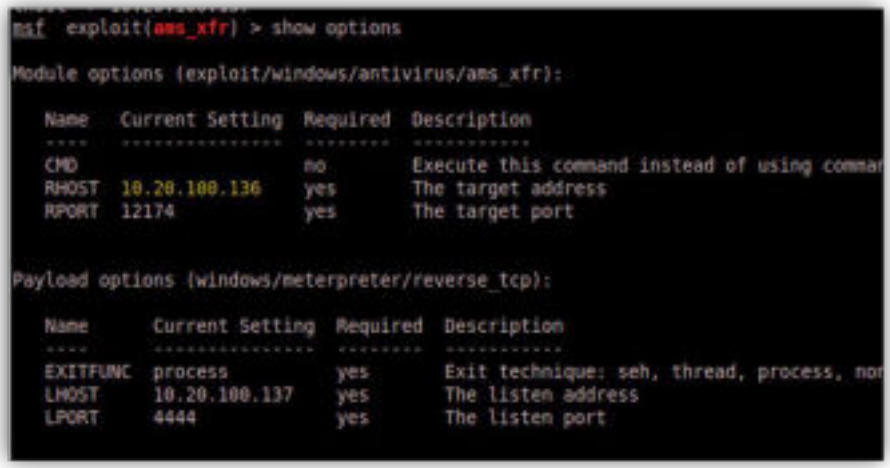
Rhodian prioritized the results of our testing, and the most significant vulnerabilities exploited or discovered are described below. A list of all discovered vulnerabilities can be found in the vulnerability scan report provided separately.

SIGNIFICANT VULNERABILITIES

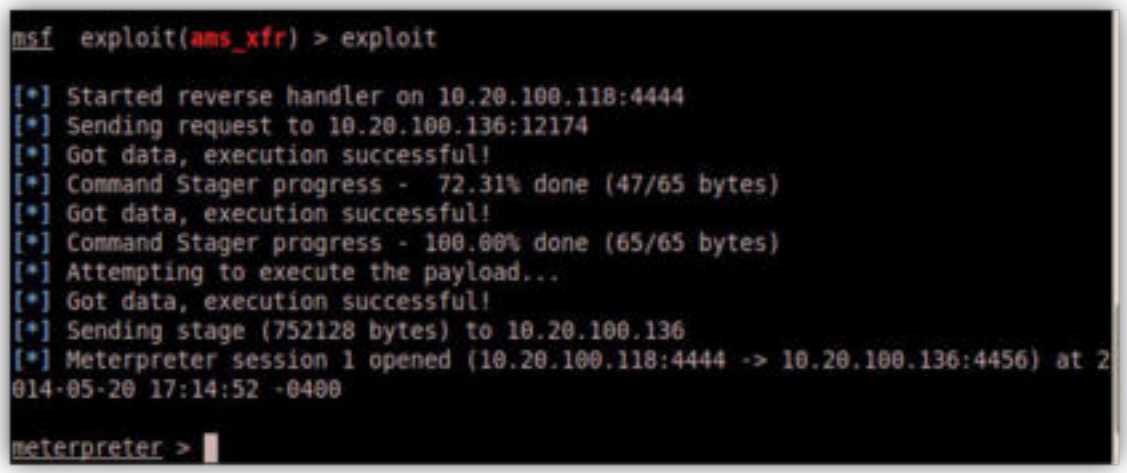
Rhodian discovered the following vulnerabilities and strongly recommends that each be remediated, as they represent an unnecessary and potentially significant risk to the overall security posture.

02 – Intel Common Base Agent CreateProcessA() Function Remote Command Execution	
CRITICAL RISK	
Description and Impact	The remote host is running a version of the Intel LANDesk Common Base Agent (CBA) that allows the contents of a specially crafted packet to be passed as an argument to 'CreateProcessA()' to be executed on the remote host with SYSTEM privileges. By exploiting this vulnerability, Rhodian was able to gain not only admin access on the vulnerable machine, but full admin access on the ACME domain. With this level of access, everything on the domain, including workstations, servers, files, and databases, can be considered compromised.
Vulnerable Systems	x.x.x.x
Recommend-ations	If using Symantec AntiVirus Corporate Edition, Symantec Client Security, or Symantec Endpoint Protection, apply the appropriate update as described in Symantec's advisory, SYM09-007.

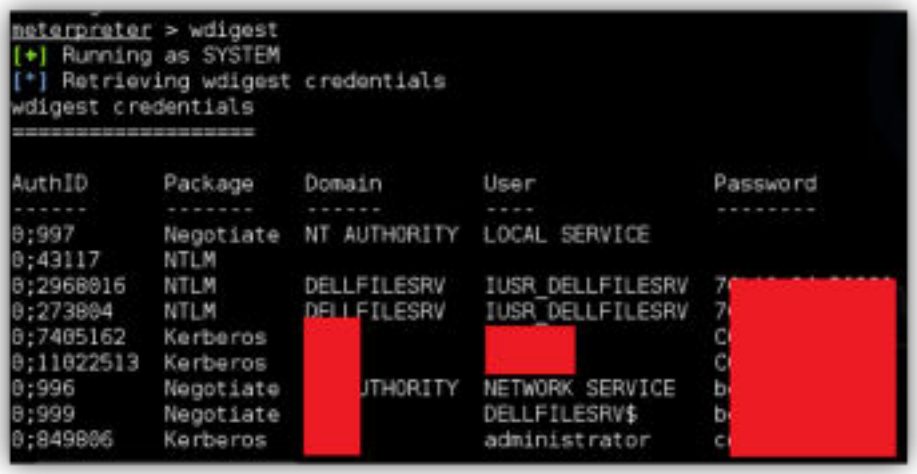
Using Metasploit, Rhodian was able to exploit the vulnerability using a publicly available exploit.



The exploit is successful, and a remote shell is gained.



Once the remote shell is established, Rhodian obtained clear-text passwords stored in memory by Windows Digest Authentication. A domain administrator password was discovered in memory.



By logging into the Domain Controller, we can verify that the administrator credentials are valid. At this point, everything on the ACME domain can be considered compromised.
<SENSITIVE IMAGE REMOVED>

RHODIAN

Based in Colorado, Rhodian provides cybersecurity services to businesses nationwide. Over the past decade, our staff has supported hundreds of clients across diverse industries. As your trusted security advisor, we provide valuable insight to prevent attacks and can respond immediately to cybersecurity events. Utilizing a real-world approach, we combine information security best practices, human intelligence, and our vast experience to ensure your business is protected against the ever-evolving threat landscape. Our proven approach and experience has enabled us to become the preferred vendor for IT providers, MSPs, and various other organizations.

HIPAA

Rhodian is HIPAA compliant and understands the needs of businesses striving to meet compliance for different industries, States, and Federal regulations.

QUALIFICATIONS

Rhodian is committed to supporting the information security community by being involved in industry events and organizations. All Rhodian staff maintain industry-recognized certifications and constantly pursue cutting-edge training. Some of our certifications include:

- GPEN - GIAC Penetration Tester
- OSWP - Offensive Security Wireless Professional
- OSCP - Offensive Security Certified Professional
- CEH - Certified Ethical Hacker
- CPT - Certified Penetration Tester
- CRISC - Certified in Risk and Information Systems Control

ASSOCIATIONS

Rhodian and its staff are proud members of the following associations:

- ISSA - Denver Chapter
- ISACA - Denver Chapter
- GIAC Advisory Board
- Longmont Chamber of Commerce
- Colorado Technology Association
- Independent Insurance Agents & Brokers of America (IIABA)
- Independent Insurance Agencies of Texas (IIAT)
- Professional Independent Insurance Agents of Colorado (PIIAC)
- Agents Council for Technology (ACT)