Cover Letter

Respected Information Security Team,

It is with great pleasure that Oman Data Park – Cyber Security Park confirms our ability to deliver the requested red team assessment. The aim of this assessment, as we understand it, is to evaluate the effectiveness of your organization's security posture through simulated attacks and other testing methods.

We assure you that all penetration testing activities will be conducted in a manner that adheres to industry's best practices and standards, and that is both professional and ethical. The scope and objectives of the assessment will be clearly defined and agreed upon in advance, and all findings will be promptly reported to you in a comprehensive manner.

We are aware that our team will be collaborating closely with your internal security staff and other relevant parties during the duration of the assessment. To minimize any potential disruptions to your business operations, we will cooperate with your team to ensure that all necessary precautions are taken.

We are confident in our ability to provide valuable insights and recommendations based on the results of this assessment. We look forward to working with you and your team to ensure the success of this engagement. Will you have any questions or concerns, please do not hesitate to contact us.

Sincerely,

Oman Data Park – Cyber Security Park

Confidentiality Statement

This proposal is confidential to “CUSTOMER” (hereinafter referred to as “CUSTOMER”) and Oman Data Park SAOC (hereinafter referred to as “ODP”).

This proposal contains the intellectual property of Oman Data Park and other third parties with whom ODP has business relationships. It has been supplied to “CUSTOMER” on condition that it may not be disclosed, in whole or in part, to any party other than those of your employees and professional advisors who need to see it to evaluate the proposal. It may not be used for any other purpose.

Whilst every care has been taken to ensure that the contents of this proposal are complete and realistic, ODP reserves the right to change or withdraw this document in the light of further information on “CUSTOMER” specific requirements.

Executive Summary

Oman Data Park- Cyber Security Park (ODP-CSP) is pleased to submit a proposal to “CUSTOMER” for a comprehensive Vulnerability Assessment and Penetration Testing (VAPT) services. The objective of this VAPT is to identify and address potential vulnerabilities and weaknesses in “CUSTOMER”’s IT infrastructure. Our team of experienced professionals will utilize a combination of automated and manual testing techniques to provide a comprehensive evaluation of “CUSTOMER”’s network, systems, and applications.

The testing process will be performed by our highly skilled and certified ODP-CSP offensive security team, who will conduct thorough testing of the IT infrastructure. This will include testing web applications, network infrastructure, and endpoint devices. Our team will work closely with “CUSTOMER”’s relevant department to ensure that the testing process is minimally disruptive to daily operations.

Upon completion of the VAPT, ODP-CSP will provide “CUSTOMER” with a comprehensive report detailing all identified vulnerabilities, showcasing a step-by-step approach to breakdown the team’s approach and methodology, the severity of each identified vulnerability, and recommendations for mitigation. Our team will also provide detailed technical debriefing to “CUSTOMER”’s relevant team(s), including recommendations on how to implement effective security measures to address identified vulnerabilities.

Why Oman Data Park – Cyber Security Park

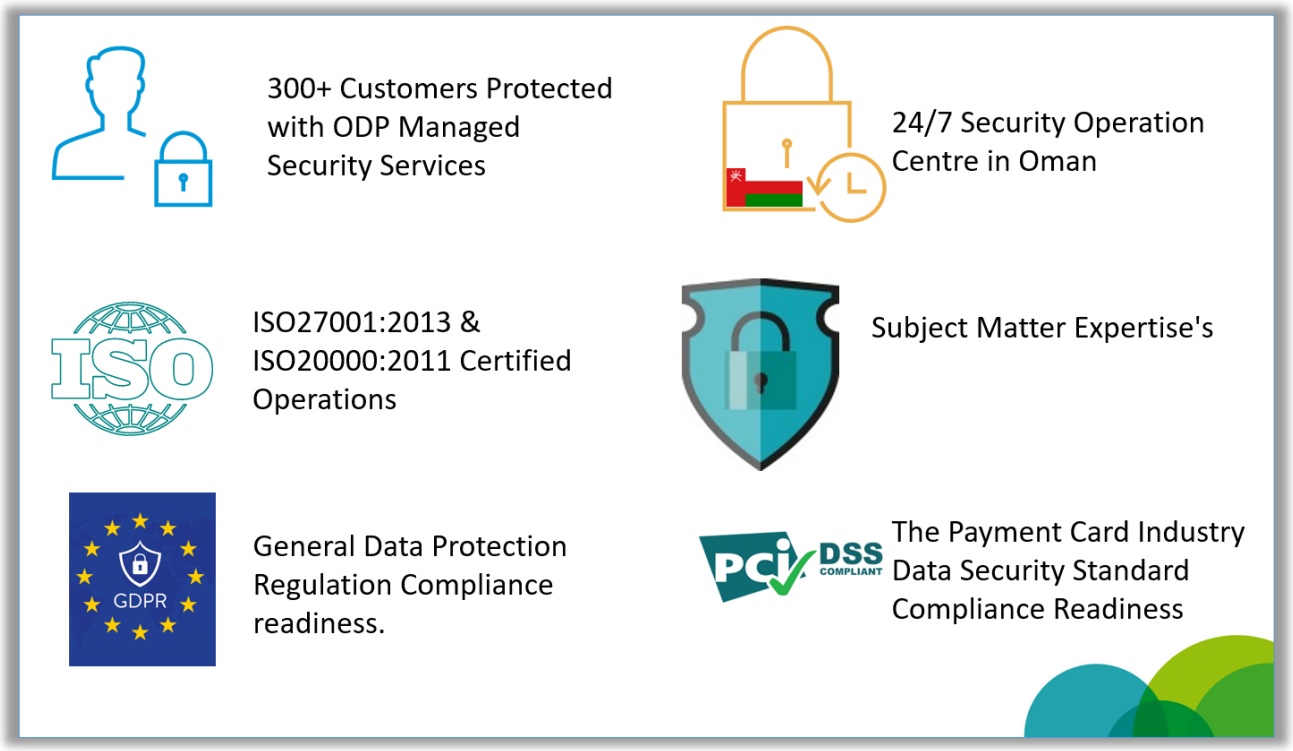
Background

Oman Data Park is a joint venture company owned by Oman Telecommunications and 4-Trust, a part of National Trading Company. The partnership brings an unrivalled combination of network infrastructure and management expertise to ensure unmatched service and reliability to its customers.

Oman Data Park has Data Centre's in Wattaya, Knowledge Oasis Muscat and Duqm. The facilities provide the highest levels of performance, simultaneously providing the most robust, fault-tolerant site infrastructure, redundant capacity systems and multiple distribution paths to serve business critical IT needs of its customers. Oman Data Park operates both 24x7x365 Security Operation Centre (SOC) and Network Operation Centre (NOC) which are ISO27001 & ISO 20000 Certified.

Oman Data Park is the first the Managed Security Services provider in Oman that provides both practice and detective security services. It operates on 24x7x365 basis. The incident response team is available across the clock to provide the assistance needed on site or remotely

Why ODP-CSP's Managed Security Services



Associations

GLOBAL CYBER ALLIANCE

عمان الرقمية
e.oman

Oman National CERT
Towards a safe cyber environment

ODP Certifications and Awards

URS is a member of Registrar of Standards (Holdings) Ltd.

Oman Banking & Finance Awards 2018
Data Centre Leader of the Year
Oman Data Park

Certified Information Systems Security Professional

Certified Cloud Security Professional

Certificate of Cloud Security Knowledge

Certified Information Security Manager

Certified in Risk and Information Systems Control

Certified Data Centre Professional

Certified Data Centre Specialist

Offensive Security Team

As Oman embarked on its digital transformation journey, Oman Data Park emerged as the pioneer company in driving the cybersecurity pillar of this transformation. An Omani company led by the industry's top leaders and experts over the last decade.

We are a 100% Omani team, with a deep understanding of the local business landscape and culture, giving us a unique edge when providing tailored security solutions and assessments for our clients.

Our team members hold multiple top leading industry-level certifications and trainings – from OffSec's OSCP, OSWE, OSEP, and OSED, to CRTO, CRTP and CRTE, as well as courses from SpecterOps' Adversary Tactics: Red Team Operations.

We have a plethora of experience across multiple industries, from finance, banking, and insurance to oil & gas, aviation, and healthcare amongst others.

All members of our team have discovered zero-day vulnerabilities within national and international applications, demonstrating their exceptional skills and abilities to identify and exploit vulnerabilities that may have been missed by other teams.

Our team provides customized solutions that fit the unique needs of each client, working closely with them to identify and mitigate potential risks before they are exploited.

We prioritize keeping our clients in the loop when conducting engagements, keeping a close communication & collaboration link to ensure that they have a full understanding of their security posture.

Our commitment to excellence is reflected in our track record of successful engagements and long-term relationships with our clients.

Proposal Overview

Scope of Work

ODP-CSP will provide “CUSTOMER” with the requested security assessment services to assess and measure “CUSTOMER”’s overall security posture. ODP-CSP will provide the knowledge and technical expertise to conduct a comprehensive security assessment service through the services specified in the table below. This is to begin upon an agreed date and last for the duration specified.

S. No	Vulnerability Assessment & Penetration Testing	Quantity
1	Number of Web application	10
2	Number of Internal IPs	15
3	Number of External IPs	8
4	Number of VMs/Physical Servers	3 - 4
5	Hosting	1 Site
6	Number of Mobile Application (Android and IOS)	10
7	Confirm the VAPT Type (Black Box or Grey Box)	BOTH

Approach

Provided that our proposal is accepted, the project will follow a structured approach, divided into distinct phases to allow for comprehensive analysis and thorough evaluation of “CUSTOMER”’s environment. The schedule will be adjusted as information is discovered in each phase and is dependent on resource availability. Each service will run on a different milestone, which may overlap, but won't hinder the work. The duration of each phase is exclusive of the final report submission. ODP-CSP will not be held to timelines for delays caused by the client.

Service	**Phase No.**	**Scope Covered**
External Penetration Test	I	Reconnaissance
	II	Enumeration
	III	Exploitation
	IV	Post Exploitation (If Applicable)
Mobile Application Test	I	Static & Dynamic Analysis
	II	Enumeration
	III	Exploitation
	IV	Post Exploitation (If Applicable)
Internal Penetration Test	I	Reconnaissance
	II	Enumeration
	III	Exploitation

	IV	Post Exploitation (If Applicable)
Reporting	V	Detailed Technical Reporting
Revalidation	VI	Validate Fixes & Produce Revalidation Report

Table 1 - Penetration Testing Approach

Client Provided Property

ODP-CSP requires the following information detailed in the table below, to be able to commence with and successfully complete the specified Scope of Work (SOW). Listed on the table below is the required information/details:

Serial No.	**Service**	**Client Provided Property**
1	Internal VAPT	Testing Site (On-Site / Off-Site)
2		Internal IP Addresses/Subnets
3		Internal URLs
4		Out of Scope Items
5	External VAPT	External/Public IP Addresses
6		External URLs
7		Number of Pages
8		Number of APIs
9	Mobile Application VAPT	Platform (Android/iOS)
10		Source Code Availability (White Box)
11		Number of Interactive Pages
12		Number of APIs
13		External URLs

Table 2 - Client Provided Property

Deliverables

ODP-CSP proposes the following testing and penetration testing and deliverable schedule to provide "CUSTOMER" with an overview of the general assessment timelines. It is anticipated that exact timeframes for assessment and consulting activities will be finalized during the planning process.

Deliverable	Due Date
Assessment Kick-Off Meeting	Within two (2) business days after notification
Begin Assessments	TBD during planning
Complete Assessments	TBD during planning
Knowledge Sharing	TBD during planning
Results Analysis	Five (5) business days after completion of active assessment activities
Execution Out Brief (if applicable)	TBD during planning
Final Report	Five (5) business days after result analysis

Table 3 - Deliverables

Penetration Testing Methodology

The Penetration Test provides a comprehensive security evaluation of the network with the goal of identifying and leveraging vulnerabilities in Internet-facing systems. ODP-CSP uses a structured methodology and publicly available information to identify and/or verify the network ranges that comprises "CUSTOMER"'s networks, identify potential vulnerabilities, and, when requested by "CUSTOMER", attempt to exploit these vulnerabilities to demonstrate their potential business impact. To present a realistic attack scenario, the test will be conducted with no prior knowledge of or access to "CUSTOMER"'s IT environment.

External Penetration Test

Methodology

The External Penetration Test consists of the following stages:

Service	Stage	Scope Covered
External Penetration Test	I	Footprinting & Reconnaissance
	II	Host Discovery & Enumeration
	III	Vulnerability Identification & Exploitation
	IV	Vulnerability Post Exploitation

Table 4 - External Penetration Testing Methodology

Stage 1 – Footprinting: ODP-CSP begins the assessment by performing some basic research on publicly available sources to verify the ownership of the provided target ranges and to search for readily available information (Open-Source Intelligence or OSINT) that would be useful to an attacker targeting a network. Such information is often useful in identifying potential usernames and passwords to try in password spraying attacks and in identifying details about the network infrastructure, such as versions of the software in use, and the types of devices on the network.

Tools Used: WHOIS, nslookup, dig, Shodan, search engines.

Stage 2 – Host Discovery & Enumeration: The purpose of this stage is to perform an inventory of all the live hosts in the target IP address ranges approved by "CUSTOMER"'s Point of Contact (POC). The primary steps of that constitute this process are:

DNS Mining: The first phase of discrete host discovery is to examine Domain Name Service (DNS) records for the target network. Using reverse and brute-forced forward DNS lookups, ODP-CSP assembles a list of hostnames in the network, along with the associated IP addresses. This list is then manually reviewed to determine likely roles and services provided by the systems based on the hostname(s) assigned. In some cases, geographic or sub-organization structures of the network can also be determined by analysis of the hostnames.

Tools Used: Nmap, Recon-NG, Shodan, Custom Scripts, Other scanning tools.

Host Discovery: The process of host discovery is initiated with ICMP ping sweeps to determine live hosts. However, this process does not always produce a comprehensive list of Internet-routable hosts. This can be attributed to the rejection of ICMP packets by most perimeter firewalls or other filtering devices. Thus, ODP-CSP augments this process by using TCP and UDP based discovery methods that query commonly available services such as HTTP, SMTP, DNS, VPN services and SNMP, to detect Internet-accessible hosts through positive responses. In addition, ODP-CSP performs source port scans to locate additional hosts that may be protected by elementary router access controls.

Tools Used: Nmap, Vulnerability Scanners, and other scanning tools.

Port and Service Enumeration: Having amassed a list of live hosts, ODP-CSP proceeds to identify services listening on TCP and UDP ports. This is achieved by executing automated and manual TCP and UDP port scans against the list of known active hosts. The types of scans include, but are not limited to, TCP connect scans, TCP SYN scans, and UDP data packet scans. Due to the time-consuming nature of port scans, the initial scans are targeted to probe only the commonly available services like HTTP,

SMTP, DNS, NetBIOS, etc. Depending on the responses received, the targeted scans are typically followed by comprehensive scans that query all 65536 (0-65535) TCP and UDP ports.

In addition to determining the open ports, ODP-CSP also attempts to map these ports to the corresponding service daemons by running automated service fingerprinting tools and evaluating the banners returned by the various service daemons by listening on the host. These banners normally yield definitive clues to the version of the service running.

Tools Used: Nmap, Vulnerability Scanners, tcpdump, WireShark, and Custom Scripts.

Operating System Identification: To build a comprehensive inventory prior to the attack and penetration phases, it is essential to determine the underlying operating system of the live hosts. ODP-CSP uses publicly available tools to accomplish operating system identification. These tools function by observing subtle variances received in response to specially crafted TCP and UDP packets directed at the live hosts. The variations in the responses arise due to the minor differences in the implementation of TCP/IP stacks of different operating systems.

In addition to using automated tools for this purpose, ODP-CSP also evaluates the banners returned by the various service daemons listening on the host. These banners normally yield definitive clues to the type of operating system deployed.

Tools used: Nmap, vulnerability scanners, netcat, sysinternals tools, and custom scripts

Network Topology Mapping: ODP-CSP uses a combination of ICMP, TCP and UDP-based route tracing methods to determine the various paths into Customer's network. The results of these network probes are collated to create a baseline network map as perceived by an outside observer. This allows ODP-CSP to properly evaluate the security of the external facing hosts in the context of the externally visible network.

Many of the tools used concentrate on soliciting information from misconfigured routing devices, allowing an outside attacker to not only determine the network architecture available to the Internet, but also to discover implemented protocols.

Tools used: ping, trace route, Nmap netmask and timestamp requests

Stage 3 – Vulnerability Identification & Exploitation: After thoroughly mapping out the target space, ODP-CSP consultants conduct testing to identify vulnerabilities and determine if they are exploitable. ODP-CSP tests each running service on each Internet accessible system to identify any security risks that could be exploited by an attacker from the Internet. Automated tools are used to perform an initial check of the environment, but most of the testing is performed using manual techniques to discover vulnerabilities and misconfigurations and to attempt to exploit those issues, where possible, to gain access to systems and/or to sensitive information.

Tools used: Nessus, Metasploit framework, Nikto, Nmap, OS commands, and custom scripts and tools

Stage 4 – Vulnerability Exploitation: When explicitly approved by "CUSTOMER", ODP-CSP proceeds to exploit any identified vulnerabilities. The purpose of this exercise may be to emphasize the impact of a potential compromise. This process entails the use of built-in operating system commands and the execution of verified exploit code to gain unauthorized access to any vulnerable machines.

Tools used: Tested exploits, native MS Windows and Unix commands, NetCat, Metasploit Framework, SQLmap and custom scripts

Red Team Execution Phases

The goal of the Red Team Assessment is to assess the effectiveness of “CUSTOMER”’s information security detection, prevention and response capabilities by leveraging real-world, objective-based adversarial techniques to attempt to penetrate the external perimeter, establish a foothold on the internal environment, and accomplish specific attack objectives mutually defined by “CUSTOMER” and ODP-CSP. Example objectives may include gaining access to “CUSTOMER”’s data, compromising internal domain administrator credentials, or demonstrating access to email or critical business systems. To present a realistic attack scenario, the test will be conducted with no prior knowledge of or access to Oman Data Park's IT environment. Additionally, ODP-CSP will utilize techniques specifically designed to evade detection by IT Security teams and controls.

Approach

In the Planning phase, ODP-CSP testers will interact with “CUSTOMER”’s stakeholders, scope the project, develop a project plan and rules of engagement, and coordinate all assessment activities.

Kick Off Meeting	Schedule project kick-off meeting within two (2) business days of specific task assignment Identify system-specific information, including but not limited to configuration settings, user accounts, IP addresses, the Uniform Resource Locator (URL), contact information, and any other system-specific information Identify testing dates/times, as well as the specific test objectives to be executed Aggregate information into a test plan and include it in the Rules of Engagement document
Scoping, Project Plan, & Rules of Engagement	Develop project schedule and assign necessary resources and ensure key stakeholder availability Develop rules of engagement for review and signature Document scope (include and exclude), target system identification, system architecture, logistics, technical approach, and identification of any exceptions or special requirements (if applicable) Establish points of contact (POCs) Document testing schedule – dates, testing window timeframes, logistics (as applicable) Document tools and techniques to be used during testing Document the required level of access to the facility and the system that the testers will need to ensure a comprehensive assessment (if applicable) Review security requirements, procedures, and risk of loss Review notification and approval to test procedures and obtain signature authorities – ROE approval by key stakeholders
In-Brief (Optional)	Ensure all key stakeholders understand the testing methodology Ensure that all key personnel have been identified before the active execution activities have been initiated
Assessment Coordination	Ensure stakeholders are aware of the assessment schedule, activities, and potential impacts the assessment may have Ensure the assessment does not take place during upgrades, new technology integration, or other times when the system’s security is being altered (e.g., testing occurs during maintenance windows or periods of low utilization) Ensure the key stakeholders are informed of any critical high-impact vulnerabilities as soon as they are discovered (if requested) Ensure the appropriate individuals are informed (e.g., assessors, incident response team, senior management) in the event of an incident. Will this occur, it is recommended that activities cease until the incident is addressed and the assessors are given approval to resume their activities in accordance with the assessment plan

Methodology

The specific methodology used during this testing may be customized during the engagement based on results and findings, but will generally follow the following stages:

Stage	Description
1	Identification
2	Exploitation
3	Post-Exploitation
4	Exfiltration Testing

Stage 1: Identification. The goal of this stage is to identify, assess, and catalogue both human and technical targets that would be most susceptible to compromise by an external adversary.

ODP-CSP may leverage both open-source intelligence collection techniques (OSINT) and active scanning tools to locate Internet-accessible systems and applications. Each potential target may be evaluated for further testing based on multiple factors, including exposed ports and services, technical architecture, functionality, potential vulnerabilities, ease of compromise, and value to an attacker.

ODP-CSP may also leverage OSINT to identify potential Oman Data Park employees for targeting using social engineering techniques. This process entails collection and analysis of data derived from publicly accessible sources such as search engines, social media, “CUSTOMER” owned websites, and other online resources that provide the information necessary to create and execute targeted social engineering attacks against specific individuals.

The outcome of the Identification stage is a master list of potential targets that will be evaluated and prioritized for exploitation.

Tools used: WHOIS, nslookup, dig, search engines

Stage 2: Exploitation. During the Exploitation stage, ODP-CSP will leverage the analysis conducted during the Identification stage to select high-potential targets, customize technical and social engineering attacks designed specifically for those targets, and execute the attacks to gain access to internal “CUSTOMER”’s networks. The Exploitation stage may include any of the following:

Technical Exploitation – Upon identification of vulnerabilities in Internet-facing systems and applications, ODP-CSP may attempt to exploit those vulnerabilities to compromise sensitive data or gain a foothold within the perimeter. Additionally, ODP-CSP may execute attacks against systems with the goal of gaining further insight into the environment to identify additional targets or gain additional targeting information. Types of attacks typically used during this activity include SQL Injection, upload and execution of web shells, and brute force attacks against login interfaces.

Social Engineering – ODP-CSP may also target “CUSTOMER”’s employees using both phone and email-based techniques. Individuals may be selected from the target list based on job function, presumed access to important internal systems, and perceived susceptibility. ODP-CSP will tailor the phone and email-based attacks to each user in an attempt to perform various potentially harmful actions, including revealing login credentials, visiting unknown websites, or executing malware on the target's corporate IT asset.

The goal of the Exploitation stage is to breach the perimeter and access internal systems. Technical exploitation is often accomplished by compromising Internet-facing systems and leveraging that access to attack adjacent systems within the environment. Social engineering exploitation is often achieved by obtaining valid credentials that can be leveraged to access the environment via remote access solutions (e.g., VPNs) or via installation of malware on the user's machine that allows ODP-CSP to operate within the internal environment under the context of the user.

Stage 3: Post-Exploitation. Upon gaining access to the internal environment, ODP-CSP will attempt to move laterally throughout the intranet and ultimately gain access to “CUSTOMER” sensitive data and critical business systems. The post-exploitation stage may involve the following:

Privilege Escalation – Upon gaining access to a system, ODP-CSP may leverage various attacks to escalate the privileges of the current user to the highest levels. This escalated privilege allows ODP-CSP to perform a variety of malicious activities, including establishing persistence, installing additional malware (e.g., key loggers), and capturing credentials.

Internal Exploitation – By leveraging the same techniques used during Identification stage, ODP-CSP may search for internal data repositories, portals, collaboration forums, and other internal sources that provide access to sensitive data and assist in locating high-value targets within the intranet. Additionally, ODP-CSP may identify internal systems that can be compromised via technical exploits to gain further access to the environment or capture additional credentials.

Credential Harvesting – Once access to internal systems has been obtained, ODP-CSP may begin collecting account credentials for valid internal users. Specific focus will be given to identifying and extracting privileged domain credentials, as these provide extensive access to the environment. Typical credential harvesting attacks include dumping hashes, Kerberos tickets, and cleartext credentials from local system memory or accessible virtual machine files and identifying accessible scripts and configuration files with hard-coded credentials.

In most attacks, post-exploitation is an iterative process that involves multiple cycles of identifying internal targets, compromising those targets, and extracting additional information and credentials for further lateral movement within the intranet. As noted above, the goal of this stage is to accomplish the predefined attack objectives. This is often accomplished by demonstrating full administrative access to critical systems (e.g. financial application servers, key databases, executive email and file shares), the internal authentication and authorization systems (e.g., Active Directory, LDAP, two-factor authentication), or the core network infrastructure (e.g., RADIUS, TACACS).

A secondary objective of this assessment is to measure the detection and response capabilities of the information security team, ODP-CSP will utilize testing and attack techniques that are specifically designed to bypass or evade security controls. The team will leverage custom malware that may not be detected by commercial anti-virus products and avoid using any scanning or exploitation techniques that are likely to be observed by system users or detected by network sensors and endpoint controls. If “CUSTOMER” information security team detects the test in progress, the ODP-CSP project manager and “CUSTOMER”’s PM will select an appropriate course of action for the continuation of testing.

Testing activities will be discussed and agreed upon by both ODP-CSP and “CUSTOMER” during the project kick-off meeting. This document may include the specific scope of the engagement (e.g., whitelisted targets, blacklisted targets), coordination and approval necessary prior to exploitation of targets, schedules and timeframes, data handling and communications plan, and escalation policy.

Stage 4: Exfiltration Testing. During this stage of testing, ODP-CSP will attempt to securely transfer test/sample data out of the Oman Data Park network environment. The purpose of this testing is to determine if network and host-based defences will identify and/or prevent such a transfer. This testing would include the transmission of simulated data created by ODP-CSP.

Offensive Tooling

The team utilizes multiple vetted tools from customized open-source tooling, as well as commercial ones to ensure comprehensive and effective engagement takes place. Tooling will usually be different per engagement as each environment is unique, though the below ones are the most used and fit the current industry standards such as OWASP and PTES.

Category	Tool	Description
	Nmap	Network Mapping & Port Scanning Tool

Network Scanning	Httpx	Fast and multi-purpose HTTP toolkit for discovering and fingerprinting web applications
	Shodan	Open-Source Intelligence Tool to discover open ports and low hanging fruit
	BBOT	Open-Source Intelligence Collection Tool
Vulnerability Scanning	Nuclei	Technology Discovery & Vulnerability Scanning
	Nikto	Technology Discovery & Vulnerability Scanning
	WPScan	WordPress Enumeration & Exploitation Tool
	SQLMap	SQL Enumeration & Exploitation Tool
Web Application Testing	Burpsuite Professional	Manual Web Application Assessment & Proxy Tool
	Nuclei	Technology Discovery & Vulnerability Scanning
	Ffuf / Dirsearch	Directory Brute Forcing
	Ysoserial	Deserialization Exploitation Tool
Mobile Application Testing	Drozer	Mobile Application Testing Tool
	Frida	Interface Server for Objection & MobSF
	Objection	Mobile Application Testing Tool
	Mobile Security Framework	Static & Dynamic Analysis Tool
	APKTools / Jadx	APK Decompiler
Exploitation & Post Exploitation	Neo-regeorg	Pivoting & Web Shell Proxy Tool
	PHPSploit	PHP Post Exploitation Framework
	Ysoserial	Deserialization Exploitation Tool
	HashCat	Password Cracking Tool

Please note that the table above includes some of the main tools that we commonly use in our engagements, but it is not an exhaustive list, and we may use additional tools or techniques depending on the specific needs of each engagement.

Sample Penetration Testing Report

Network Penetration Test

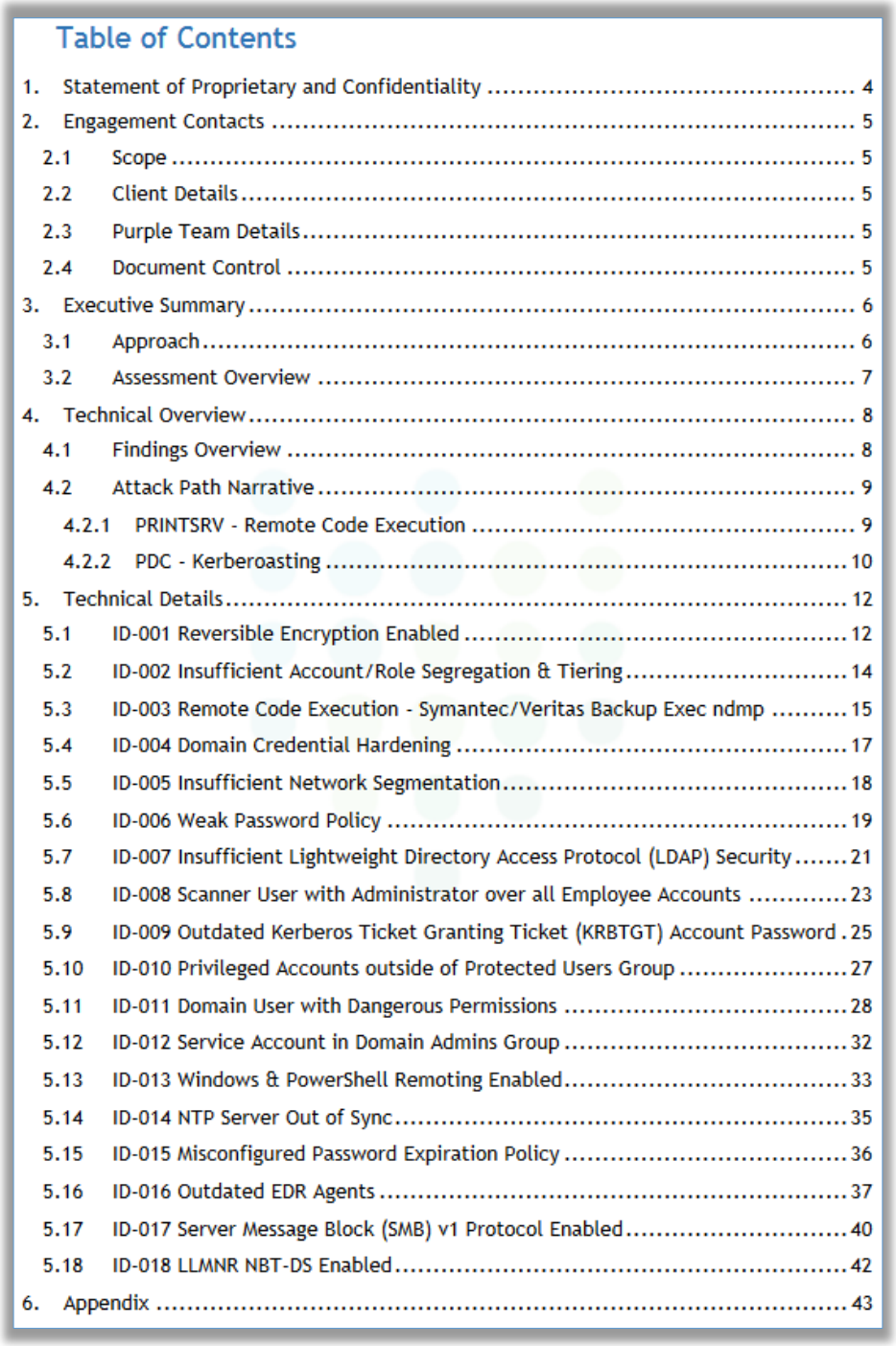
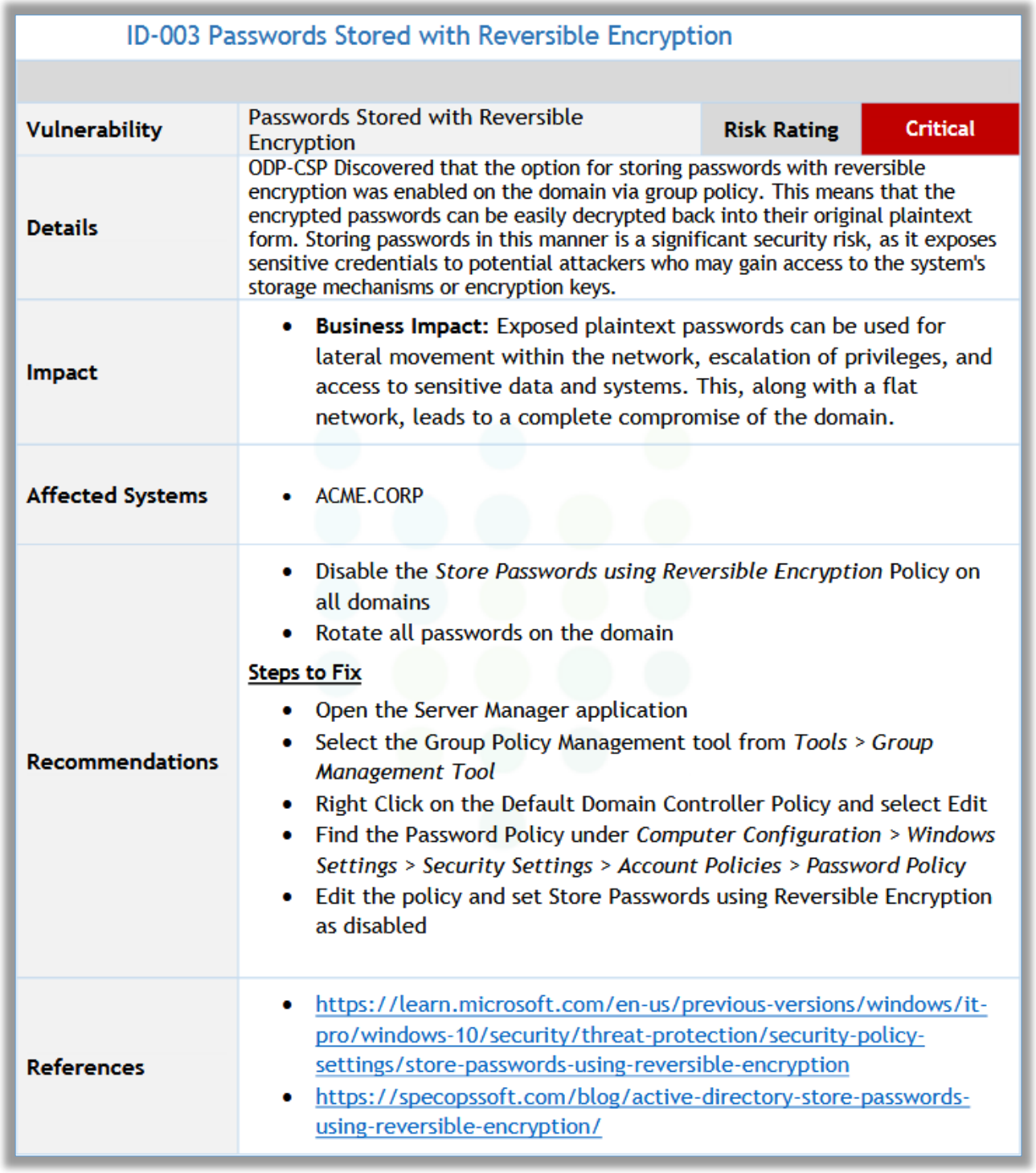


Table of Contents

Figure 1 - Network Sample Report



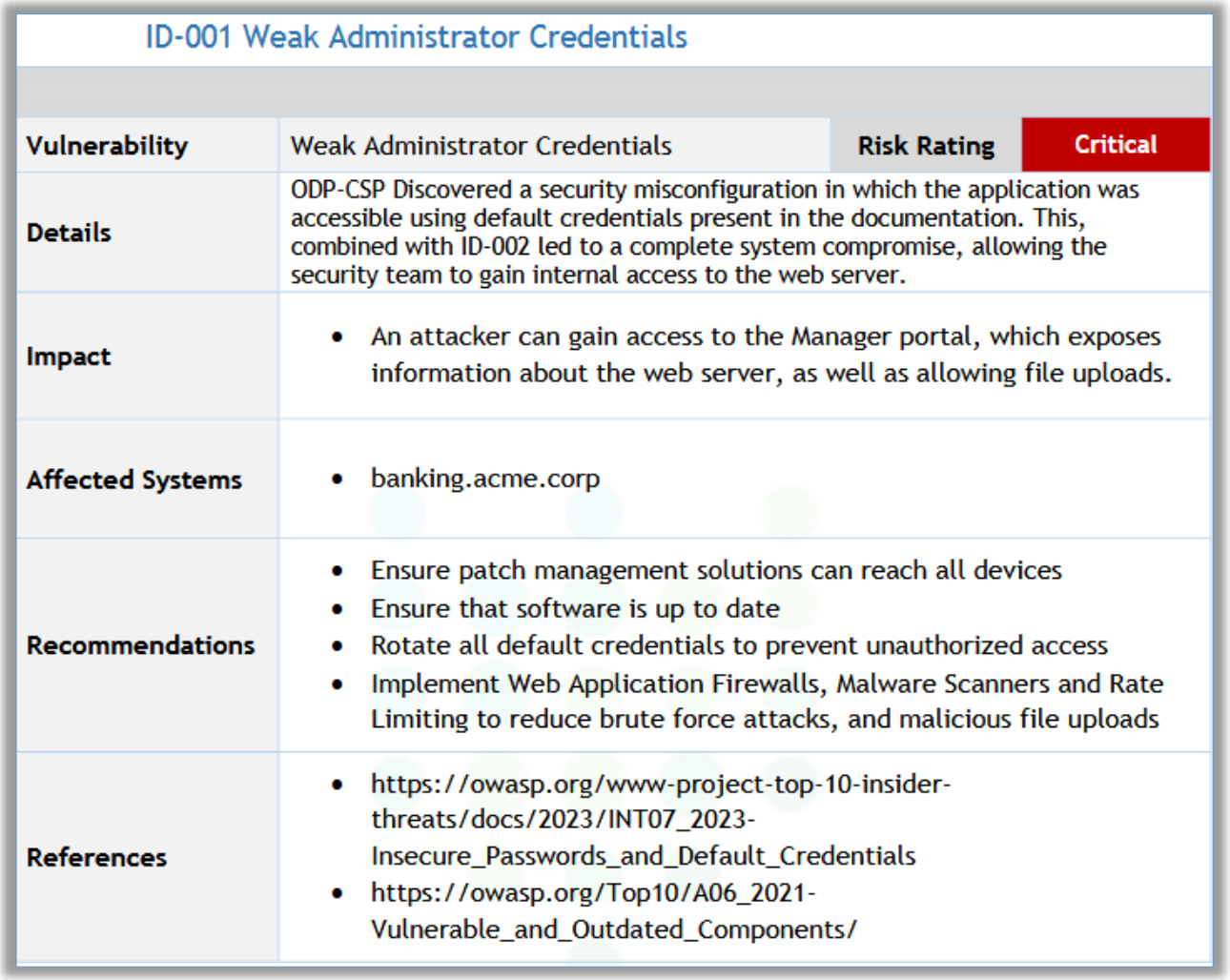
ID-003 Passwords Stored with Reversible Encryption

Vulnerability	Passwords Stored with Reversible Encryption	**Risk Rating**	**Critical**
Details	ODP-CSP Discovered that the option for storing passwords with reversible encryption was enabled on the domain via group policy. This means that the encrypted passwords can be easily decrypted back into their original plaintext form. Storing passwords in this manner is a significant security risk, as it exposes sensitive credentials to potential attackers who may gain access to the system's storage mechanisms or encryption keys.		
Impact	• **Business Impact:** Exposed plaintext passwords can be used for lateral movement within the network, escalation of privileges, and access to sensitive data and systems. This, along with a flat network, leads to a complete compromise of the domain.		
Affected Systems	• ACME.CORP		
Recommendations	• Disable the *Store Passwords using Reversible Encryption* Policy on all domains • Rotate all passwords on the domain **Steps to Fix** • Open the Server Manager application • Select the Group Policy Management tool from *Tools* > *Group Management Tool* • Right Click on the Default Domain Controller Policy and select Edit • Find the Password Policy under *Computer Configuration* > *Windows Settings* > *Security Settings* > *Account Policies* > *Password Policy* • Edit the policy and set Store Passwords using Reversible Encryption as disabled		
References	• https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/store-passwords-using-reversible-encryption • https://specopssoft.com/blog/active-directory-store-passwords-using-reversible-encryption/		

Figure 2 - Sample Network Finding

Table of Contents

Figure 3 - Sample Web Application Report



ID-001 Weak Administrator Credentials

Vulnerability	Weak Administrator Credentials	**Risk Rating**	**Critical**
Details	ODP-CSP Discovered a security misconfiguration in which the application was accessible using default credentials present in the documentation. This, combined with ID-002 led to a complete system compromise, allowing the security team to gain internal access to the web server.		
Impact	• An attacker can gain access to the Manager portal, which exposes information about the web server, as well as allowing file uploads.		
Affected Systems	• banking.acme.corp		
Recommendations	• Ensure patch management solutions can reach all devices • Ensure that software is up to date • Rotate all default credentials to prevent unauthorized access • Implement Web Application Firewalls, Malware Scanners and Rate Limiting to reduce brute force attacks, and malicious file uploads		
References	• https://owasp.org/www-project-top-10-insider-threats/docs/2023/INT07_2023-Insecure_Passwords_and_Default_Credentials • https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/		

Figure 4 - Sample Web Application Finding

Red Team Report

Table of Contents

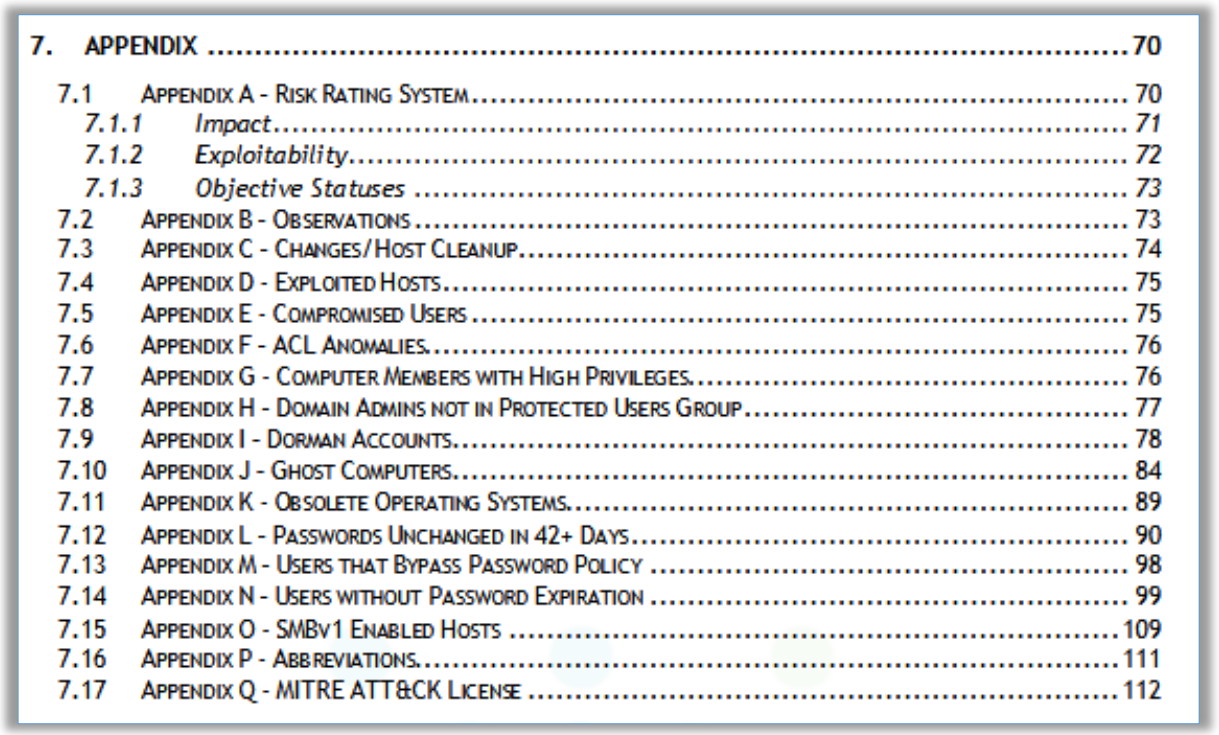


Figure 5 - Sample Red Team Report

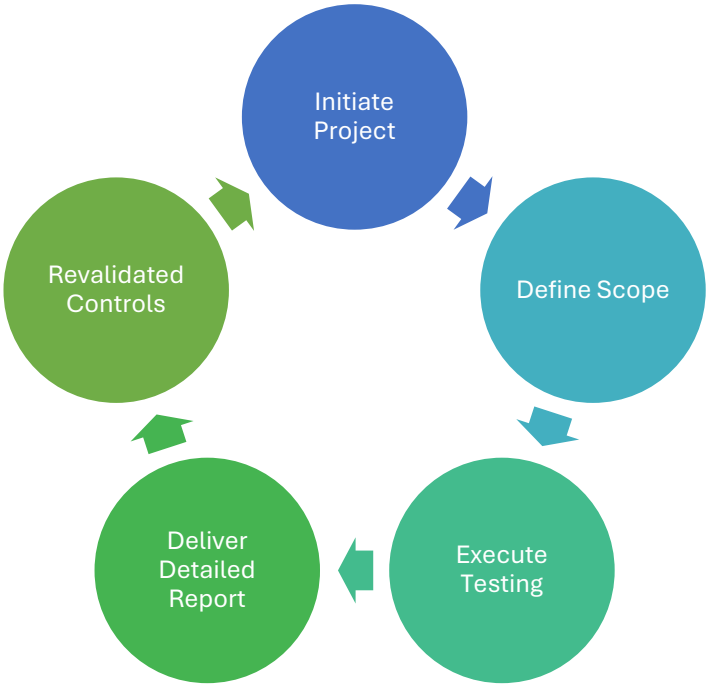
ID-004 Domain Privilege Escalation - NoPAC - Critical	
Vulnerability	Domain Privilege Escalation - NoPAC
MITRE Technique	**T1068 - Exploitation for Privilege Escalation**
Details	ODP-CSP discovered a vulnerability which allows a domain user account to create and domain administrator workstation, effectively escalating their privileges and allowing for further attacks on the affected domain. The NoPAC vulnerability works by: 1. Creating a new account in active directory with a random name (or one that you specify in the PoC tool), then renaming it to match one of the domain controllers without the usual machine account suffix (E.g. DC-SRV instead of DC-SRV$) 2. Requesting a Kerberos ticket for the created account. Once the ticket is granted, changing the name of the account back to the original name (the one you specified or the randomly generated one) 3. Using the ticket created to request an access token from the TGS for a specific service (HTTP/CIFS/HOST). Because of the absence of an account with that name, the TGS chooses the closest match and appends a "$" symbol. In this way, access to the service is granted with Domain Controller privileges
Impact	• **Privilege Escalation:** Low privileged Domain Users can possibly escalate to a higher privilege allowing an attacker to perform further, more sophisticated and damaging attacks such as ransomware deployment at scale, data exfiltration, or pivoting to other active directory domains if they are joined together. • **Insider Threat:** An employee with domain user privileges will be able to escalate to domain admin and perform internal attacks such as data exfiltration, theft of IP, and data destruction or ransomware deployment across the domains.
Affected Systems	• ACME-DC.LOCAL • CHARITON.LOCAL
Recommendations	• Ensure that all domain controllers are in the latest version where possible (2025 at the time of writing) and security patches have been applied. • Set the MachineAccountQuota value from 10 to 1
References	• http://michalszalkowski.com/security/active-directory/privilege-escalation/no-pac/ • https://www.trustedsec.com/blog/an-attack-path-mapping-approach-to-cves-2021-42287-and-2021-42278

Figure 6 - Sample Red Team Finding

Project Management

Project Management Approach

ODP-CSP follows the Iterative method when it comes to managing penetration testing projects as they follow a linear process of initiating, scoping, testing, revalidating, and delivering the project.



Initiate Project

This phase marks the beginning of the penetration testing engagement, where initial planning and alignment with “CUSTOMER” takes place. The goal is to set clear objectives, define timelines, and establish expectations for the project’s deliverables.

Define the project’s objectives, deliverables, and timeline.

Engage stakeholders to confirm scope, expectations, and responsibilities.

Allocate resources and assign roles within the project team.

Define Scope

In this phase, the project scope is clearly outlined to ensure both ODP-CSP and “CUSTOMER” have a mutual understanding of what will be tested and any constraints. This step is essential to avoid scope creep and align on specific assets or systems that require attention.

Identify assets, systems, and networks included in the testing.

Clarify boundaries and exclusions for testing activities.

Document the testing objectives, limitations, and any special requirements from the client.

Execute Testing

This is the core phase where the actual penetration testing activities are conducted. ODP-CSP leverages a mix of tools, methodologies, and manual techniques to identify vulnerabilities and potential risks within the defined scope.

Conduct penetration testing based on the defined scope and methodologies.

Identify, analyse, and document vulnerabilities, along with their potential impacts.

Use a combination of automated tools and manual testing techniques for comprehensive results.

Deliver Detailed Report

After the testing is completed, the findings are compiled into a detailed report. This report is designed to convey technical findings in a clear, actionable manner for both technical and non-technical audiences, outlining vulnerabilities and providing recommendations.

Prepare a comprehensive report with findings, including severity and potential impacts.

Provide remediation and mitigation recommendations for identified vulnerabilities.

Present findings to “CUSTOMER”’s, explaining technical issues in a clear format.

Revalidated Controls

In this final phase, the ODP-CSP retests previously identified vulnerabilities to confirm remediation efforts have been successfully implemented. This step ensures that the environment is secure and that the project objectives are fully met.

Retest vulnerabilities to confirm effective remediation.

Validate that the implemented controls meet security standards.

Close the project upon successful revalidation, ensuring all identified issues are addressed.

This structured approach helps to ensure that all aspects of the penetration testing process are handled efficiently and comprehensively, providing clear value to “CUSTOMER”

High Level Timeline

ODP-CSP proposes the following penetration testing and deliverables schedule to provide "CUSTOMER" with an overview of the general assessment timelines. It is anticipated that exact timeframes for the assessment and consulting activities will be finalized during the planning process.

High-Level Timeline Overview			
S. No	Task Description	Assets Covered	Man-Days
1	Project Start • Kick-off Meeting: initiate the project by aligning all stakeholders, settings expectations, and confirming the scope and objectives.		
2	External VAPT • Conduct Activity: Perform black box testing to identify vulnerabilities. • Submit Report: Document findings, including identified vulnerabilities and recommendations.		
3	Internal VAPT • Conduct Activity: Perform black box testing to identify vulnerabilities. • Submit Report: Document findings, including identified vulnerabilities and recommendations.		

Table 5 - High Level Overview Table

Client References

Figure 7: Client References

Experience & Qualifications

Mohammed Al Balushi – Red Team Manager

Areas of Expertise

Mastery in simulating adversarial techniques on large enterprises.
Detailed proficiency with technical report writing.
Experience across entities both locally and internationally.

Certifications

Offensive Security Web Expert (OSWE)
Offensive Security Experienced Penetration Tester (OSEP)
Offensive Security Certified Professional (OSCP)
Zero Point Security - Certified Red Team Lead (CRTL)
Zero Point Security - Certified Red Team Operator (CRTO)
Pentester Academy - Certified Red Team Expert (CRTE)
Pentester Academy - Certified Red Team Professional (CRTP)
Hackthebox Certified Dante & APT Pro Lab

Achievements

1st Place - Cyber Talents Oman National Cybersecurity Competition 2020
1st Place - Oman HUSN CTF 2021
1st Place - Cyber Talents Oman National Cybersecurity Competition 2021
2nd Place - Oman Cyber Drill 2022
2nd Place - Oman Threat Hunters (Seniors) 2020
Discovered 3 Zero days in leading banks and international applications
Conducted Country Level Scoped Red Team Assessments
HackTheBox Top 5 Worldwide

Haitham Al Siyabi – Red Team Operator

Areas of Expertise

Offensive Security
Red Teaming
Windows Active Directory
Python and Golang Programming
Bug Bounty Hunting

Certifications

Offensive Security Web Expert (OSWE)
Offensive Security Certified Professional (OSCP)
eLearnSecurity - Certified Professional Penetration Tester (eCPPTv2)
Pentester Academy - Certified Red Team Professional (CRTP)
eLearnSecurity - Junior Penetration Tester (eJPT)

Hackthebox Certified Dante & APT Pro Lab

Achievements

1st Place - Cyber Talents Oman National Cybersecurity Competition 2020.
1st Place - Oman HUSN CTF 2021.
1st Place - Cyber Talents Oman National Cybersecurity Competition 2021.
1st Place - Cybersafe Oman Incident Response Competition 2022.
2nd Place - Oman Cyber Drill 2022.
Top 1% of participating students in Python Programming Competition.
Finalist of 2021/2022 IoT challenge.
65,000+ points with 150+ training hours/CPE points.
Finalist of 2021/2022 IoT challenge.
Created custom red team tooling on GitHub: GoMugger
Tariq Al Harrasi – Red Team Operator

Areas of Expertise

Red Teaming & Adversary Simulation
Windows Active Directory
Python, Go & C/C# Programming
Offensive Development
Infrastructure Automation & Development
DevOps & CI/CD
Threat Hunting

Certifications

Offensive Security Experienced Penetration Tester (OSEP)
Zero Point Security – Certified Red Team Operator (CRTO)
Altered Security - Certified Red Team Professional (CRTP)
Cyber Warfare Lab – Certified Red Team Infrastructure Developer (CRT-ID)
SpecterOps - Adversary Tactics: Red Team Operations (AT:RTO)
White Knight Labs – Advanced Red Team Operations (ARTO)
White Knight Labs – Offensive Development (OD)
EC-Council – Certified Ethical Hacker v12 (Practical)

Achievements

Helped develop and instruct the Advanced Red Team Operations Course by WKL
Speaker @ Black Hat Oman
2nd Place – NTG Hacktivate Capture the Flag 2023
Top 50% - Cyber Safe 2021
Taught Cyber Security & Ethical Hacking in a University Capacity
Antisyphon Training – Nerd Herder
Created Custom Tooling on GitHub (d0txecute & Lavender-exe)
Wrote articles on Computer Science and Red Teaming @ blog.securescape.cc