Penetration Test Capstone

Introduction

I proudly work for **Mindful Moments Security Consulting**, **(MMSec)**, a fictitious US-based cybersecurity consulting firm specializing in penetration testing, vulnerability assessments and regulatory compliance. As part of MMSec Consulting, I've been tasked with leading a structured walkthrough for a simulated external penetration test of **Artemis Gas, Inc.**, a multinational industrial gas provider headquartered in Paris, France serving 1.7 million customers. This walkthrough is designed to prepare a new team of penetration testers before the actual engagement begins. The goal?

1. Align expectations across the team.
2. Maximize test time efficiency.
3. Deliver actionable insights to the client.

This formal report is organized around five key phases of the penetration test, each building on industry standards including: NIST SP 800-115, OWASP Testing Guide. The five phases are:

1. Perform simulated reconnaissance of the client.
2. Simulate target identification and scans against the external network.
3. Simulate the identification of vulnerabilities.
4. Based on the above, assess the threats and make recommendations.
5. Create two mock reports for the client: An Executive Summary for the client's senior management, and a Detailed Technical Report for the client's IT staff.

Phase 1: Reconnaissance

Objective

The goal of Phase 1 is to simulate passive intelligence-gathering efforts using Open Source Intelligence (OSINT) techniques to profile Artemis Gas, Inc. effectively. This includes identifying public-facing infrastructure, domains, subdomains, exposed employee information, outdated technology, and any security weaknesses that could become exploitation vectors in later phases.

Given Artemis's hybrid infrastructure (AWS + on-prem data centers), complex employee structure, and quick growth curve, reconnaissance will help our firm paint a clearer picture of the external attack surface. Overall, we're figuring out what the world can see about Artemis (and what an attacker might do with that information).

Recon Profile

Reconnaissance: Artemis Gas, Inc.		
Tools	**Rationale**	**Findings**
Google Dorking	Reveal sensitive indexed pages (login portals, docs, etc.)	site:artemisgas.com filetype:xls returned spreadsheets containing inventory codes
Shodan	Identify exposed services and devices	Found outdated Cisco ASA appliance at a public IP with a known vuln
Whois Lookup	Identify domain registrar info, DNS, and expiration	whois artemisgas.com showed registrar emails and admin contacts
DNSDumpster	Subdomain enumeration and DNS mapping	Revealed subdomains: vpn., controlcenter., dev.
Censys	Advanced host/device lookup by fingerprinting	Discovered TLS configs showing weak ciphers on dev environments
Hunter.io	Email harvesting and format detection	Confirmed email pattern: first.last@artemisgas.com
HaveIBeenPwned	Check if employee emails have been involved in public breaches	3 emails appeared in 2023 ransomware dump; indicates weak email hygiene
FOCA	Extract metadata from public documents	Metadata revealed Office 2010 + usernames like itadmin_john
Wayback Machine	Capture past versions of websites and tech stack evolution	Older version of controlcenter.artemisgas.com listed exposed version numbers
LinkedIn	Discover org chart, roles, and possible shadow IT	Found employees listing outdated tech in skills (e.g., Joomla, outdated SAP versions)
ZoomInfo	Find employee contact details and job functions	Used to confirm that Artemis has a growing DevOps team leveraging AWS
Recon-ng	Automate data collection across multiple sources	Used modules for WHOIS, email harvesting, and SSL cert scraping

Maltego	Map digital relationships between assets (people, systems, emails)	Built a visual map connecting domain names, emails, and infrastructure
SpiderFoot	Deep OSINT automation (domain monitoring, leaks, breaches)	Showed Artemis's IP ranges and Github commits by devs
crt.sh	Certificate Transparency logs for subdomain and cert discovery	Showed new cert registered to staging.artemisgas.com

Recon Findings

1. **Subdomains**: vpn.artemisgas.com, controlcenter.artemisgas.com, dev.artemisgas.com, staging.artemisgas.com
2. **Leaked Metadata**: Found usernames (e.g., itadmin_john), document authors, and outdated Microsoft Office versions
3. **SSL Weakness**: Weak TLS configurations using Censys on dev.artemisgas.com
4. **Breach History**: At least 3 corporate emails have been involved in credential stuffing attacks per HIBP
5. **Org Chart Insight**: Employees publicly list experience in insecure/outdated systems on LinkedIn
6. **Visual Mapping**: Maltego revealed connections between Artemis's public-facing infrastructure and employees' personal GitHub repos

MMSec Consulting Conclusion

Reconnaissance is like cybersecurity people-watching. With patience and the right tools, we uncovered the shadowy corners of Artemis—such as: misconfigured TLS, forgotten subdomains, and even metadata breadcrumbs left by IT admins. These might seem small individually, but collectively they reveal a map for potential attackers.

References

1. Bott, A. (n.d.). *Maltego: Transform Data into Intelligence*. Maltego Technologies. https://www.maltego.com

2. Censys. (n.d.). *Search Engine for Internet-Connected Hosts and Devices*. https://censys.io/
3. Have I Been Pwned. (n.d.). *Check if your email or phone is in a data breach*. https://haveibeenpwned.com
4. Recon-ng. (n.d.). *Recon-ng Framework*. GitHub. https://github.com/lanmaster53/recon-ng
5. crt.sh. (n.d.). *Certificate Transparency Search*. https://crt.sh
6. ElevenPaths. (n.d.). *FOCA*. https://www.elevenpaths.com/labstools/foca/index.html
7. OWASP. (n.d.). *Information Gathering*. https://owasp.org/www-community/Information_Gathering
8. Shodan. (n.d.). *The search engine for the Internet of Things*. https://www.shodan.io