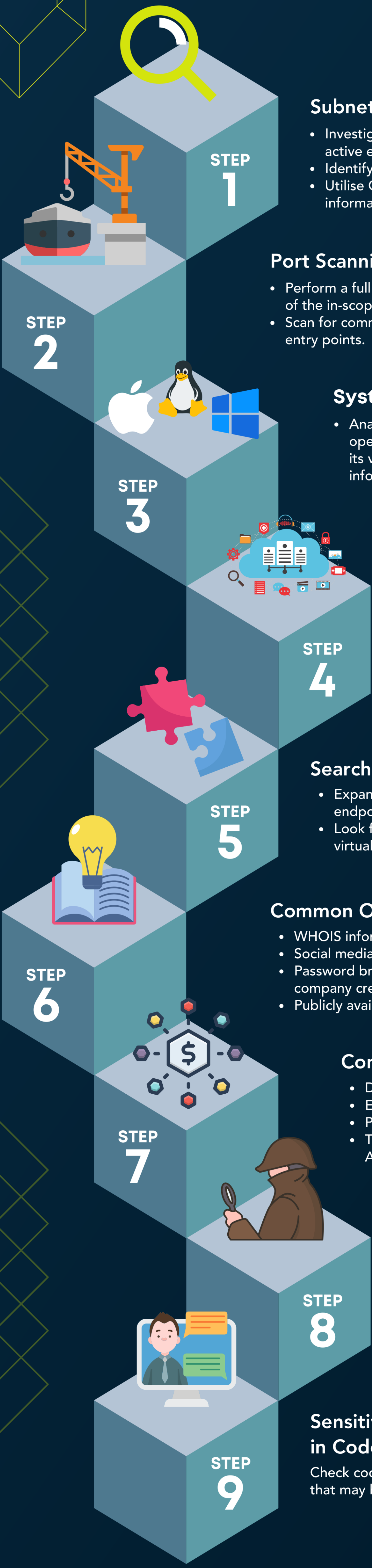
Enumeration methodology for external penetration testing



Subnet Scanning and Active Enumeration

- Investigate the subnets in scope using scanning methods and active enumeration.
- Identify systems and services accessible from the internet.
- Utilise Open Source Intelligence (OSINT) for additional information gathering.

Port Scanning

- Perform a full TCP and UDP port scan on the entirety of the in-scope subnet.
- Scan for common open ports to identify potential entry points.

System Information Gathering

- Analyse accessible systems to determine the operating system (Microsoft Windows or Linux) and its version, including build or service pack information.

Service Enumeration

- Enumerate open services and ports to identify running services.
- Gather information about the services, including version, banner details, and third-party plugins/modules.

Search for Hidden Assets and Endpoints

- Expand the attack surface by searching for hidden assets and endpoints.
- Look for non-linked admin/high-value pages, websites behind virtual hostnames, and UAT pages with live data.

Common OSINT Sources Investigation

- WHOIS information
- Social media platforms (Twitter, Facebook, LinkedIn)
- Password breach sites containing previously compromised company credentials
- Publicly available websites

Consideration of Other Assets

- DNS
- Email infrastructure
- Publicly available code repositories (GitLab, GitHub, Bitbucket)
- Third-party hosting and SaaS providers (Microsoft 365, AWS, Azure Cloud)

Identification of Publicly Accessible Sensitive Information

- Use common OSINT techniques to identify publicly accessible sensitive data.
- Look for potential leakage of sensitive information on public platforms.

Sensitive Data and Credentials in Code Repositories

Check code repositories for sensitive data, secrets, or credentials that may be publicly accessible.

visit

handbook.volkis.com.au

for our full external penetration testing methodology