Network Security Assessment

Find critical vulnerabilities in your Infrastructure

SentryArk

Network Penetration Testing is the process of simulating real-world attacks on a network and its devices by using the same approach as the hackers do. Unlike automated vulnerability scans that only scrape the surface of your network, a network penetration test by SentryArk provides deep understanding into the security risks in your environment.

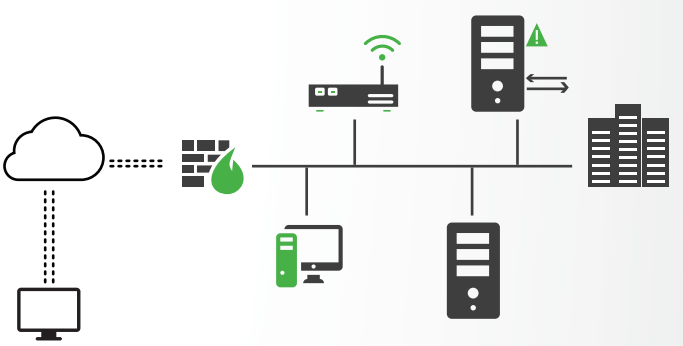
OUR CONSULTANTS CAN HELP TO DETERMINE:

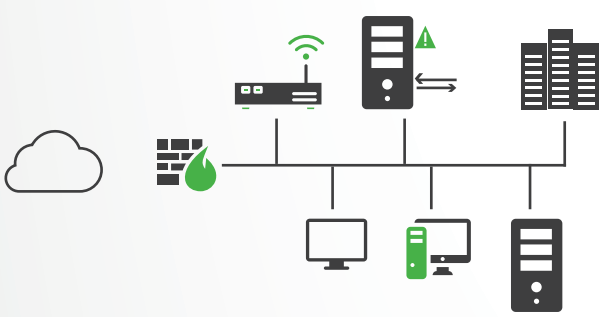
- Where vulnerabilities exist in your network.
- The total risk, exploitation likelihood, and potential impact of vulnerabilities.
- How privileged accounts might be abused internally.
- Which permissions can be escalated on compromised systems.

EXTERNAL NETWORK ASSESSMENT

External network penetration testing identifies vulnerabilities on infrastructure devices and servers accessible from the internet.

External penetration testing assesses the security posture of the routers, firewalls, Intrusion Detection Systems (IDS) and other security appliances which filter malicious traffic from the internet.





INTERNAL NETWORK ASSESSMENT

Our experts approach the local area network as an attacker on the inside. We look for privileged company information and other sensitive assets. This involves incorporating a variety of tools, uncovering user credentials, and attempting to compromise both virtual and physical machines present in the network environment.

The advantage of this engagement is in ensuring a breach of your external network will not result in a breach of your assets.

ASSESSMENT DETAILS AND METHODOLOGY

To ensure high quality, repeatable engagements at SentryArk, our penetration testing methodology follows these steps:

Planning and Information gathering

Penetration test begins with information gathering. Collecting, parsing, and correlation information on the target is key to identifying vulnerabilities.

Vulnerabillty Analysis

Once the target has been fully enumerated, SentryArk uses both vulnerability scanning tools and manual analysis to identify security flaws. With decades of experience and custom-built tools, our security engineers find weaknesses most automated scanners miss.

Exploitation

At this stage of the assessment, our consultants review all previous data to safely exploit identified vulnerabilities. Once sensitive access has been obtained, focus turns to escalation to identify total business impact

Risk Determination

In this phase Our consultants set an industry standard for clear and concise reports, prioritizing the high, medium and low risk vulnerabilities.

Reporting

Once the engagement is complete, SentryArk delivers a detailed analysis and threat report, including remediation steps.

The assessment includes the following:

- Executive Summary
- Strategic Strengths and Weaknesses
- Identified Vulnerabilities and Risk Ratings
- Detailed Risk Remediation Steps
- Assets and Data Compromised During Assessment

ABOUT SENTRYARK

SentryArk is a team of Security professionals, white-hat hackers and security enthusiasts seeking innovation in the Information security industry. We expertise and focus on providing offensive security solutions that help understand the real-world risks impacting your business. Our goal is to deliver top tier professional and innovative services and help organisations champion their cyber security initiatives.