Network/Infrastructure Scan Methodology

Network Footprinting

Along with the provided list of domains, IP ranges and subnets - we begin with identifying all networks, devices, and infrastructure components associated with the customer's environment. We employ various tools and techniques to discover IP ranges, subnets, network devices, and external exposure points. This step helps establish a comprehensive inventory of targets, forming the foundation for subsequent assessment phases.

Network Discovery

In this phase, we identify all live and operational network components, including servers, routers, switches, firewalls, and other connected devices. This allows us to focus the assessment on critical assets and reduce the scope of unnecessary testing.

Network Enumeration and Profiling

We utilize advanced tools and techniques to enumerate devices, services, and open ports on each identified target. Profiling is performed to gather detailed information about operating systems, services, protocols, and network configurations. This phase also includes identifying communication paths, exposed APIs, and third-party integrations.

Threat Modelling

Threat modelling involves an in-depth evaluation of the network topology, critical assets, communication flows, and access points. By analyzing these components, we create a threat matrix that maps network vulnerabilities, misconfigurations, and potential attack vectors. Special attention is given to dependencies, privilege boundaries, and external connections to define possible exploitation scenarios.

Security Control and Test Cases

Based on enumeration and threat modeling, a detailed set of security controls and test cases is created. These test cases align with industry standards to ensure coverage of common and advanced network vulnerabilities.

Sample security categories include:

- Firewall misconfigurations
- Weak authentication mechanisms (e.g., plaintext credentials)
- Network segmentation flaws
- Outdated firmware or software
- Misconfigured VPNs and remote access points
- Exposed sensitive data via protocols (e.g., SNMP, SMB, FTP)

contactus@blueinfy.net

- ARP spoofing, DNS poisoning, and MITM vulnerabilities
- Open ports and unnecessary services

Vulnerability Assessment

This phase involves identifying potential weaknesses in the network by combining automated scans and manual verification techniques. Open source and licensed tools along with custom scripts are used to detect misconfigurations, unpatched systems, and exposed vulnerabilities. Human intelligence plays a key role in validating results and reducing false positives.

Vulnerability Exploitation

Controlled penetration testing is performed to exploit identified vulnerabilities and measure their potential impact. Scenarios such as privilege escalation, lateral movement, and data exfiltration are simulated to determine the level of risk.

Mitigation Strategies

Based on the identified vulnerabilities and associated risks, a comprehensive set of mitigation strategies is proposed. These strategies prioritize addressing critical issues while following industry best practices and aligning with the customer's operational requirements**.**

Actionable Report with Zero False Positives

A key deliverable of the assessment is a highly actionable, well-structured report designed to drive immediate remediation. The report is curated to maintain zero false positives and includes the following critical components: -

- Vulnerability Descriptions: Detailed information about each identified issue
- Risk Ratings: Categorization of vulnerabilities by severity and potential business impact
- Evidence: Screenshots, logs, and step-by-step reproduction guides for validation
- Exploitation Evidence: Details of successful exploit scenarios (if required)
- Mitigation Strategies: Practical recommendations to address vulnerabilities and improve the overall network security posture
- Report Walkthrough: Guidance for stakeholders and support in implementing remediation measures

Tools and Utilities

Blueinfy uses a combination of proprietary and open-source plus licensed tools during the assessment. This includes utilities for network mapping, vulnerability scanning, exploitation, and custom scripts to identify complex vulnerabilities effectively.

