CORE4CE

ADVANCED CYBER SOLUTIONS

Network Vulnerability Assessment

Core4ce's Network Vulnerability Assessments help validate your organization's investments in network security, reduce risk, and enhance your resilience against threats. Our vulnerability assessment services include comprehensive external and internal penetration testing to identify and assess vulnerabilities across your entire network infrastructure. By utilizing a combination of open-source and proprietary tools, our experts analyze your network infrastructure to uncover potential cascading vulnerabilities. This means that not only does our team uncover individual vulnerabilities, but our highly experienced engineers also manually verify each finding to eliminate false positives and assesses the potential for adversaries to create complex attack chains which can amplify the overall security impact of each vulnerability.

Our penetration testing methodology is focused on emulating adversarial activities—from attacking external-facing systems and attempting to breach the perimeter, to assessing the internal enterprise network emulating insider threat or external attackers with an internal foothold. We validate the security posture of all networked assets—ensuring that both your perimeter defenses and internal systems are thoroughly evaluated for any gaps in existing cybersecurity controls.

Our network vulnerability assessment methodology is generally comprised of four phases: discovery, detection, exploitation, and analysis. The detection and exploitation phases are usually done from both external and internal perspectives. The external portion emphasizes the identification of vulnerabilities that allow unauthorized entry into the target environment, while the internal portion focuses on opportunities to exceed authorized access once inside. There is, of course, a close relationship between internal and external results: if an external attacker successfully gains access to the internal network all of its vulnerabilities become exploitable as well.

DISCOVERY

The discovery phase is focused on finding all points of external connectivity to the customer's network. This generally includes open-source intelligence gathering to determine the breadth and distribution of the customer's network. If requested, wireless LAN connectivity at customer locations will also be examined.

DETECTION

During the Detection Phase of the process, our consultants identify potential vulnerabilities in network services running on discovered hosts, as well as inherent vulnerabilities in equipment and operating systems. Having discovered the network content and points of connectivity, an exhaustive search of hosts and available network services is conducted to pinpoint possible vulnerabilities. Information is gathered on each network host, including the operating system type and version, hardware platform, and active services. Particular attention is paid to “high-risk” common services such as TELNET, SSH, HTTP(s), etc. Services running on unregistered ports are also noted. Specialized equipment such as virtual machine hypervisors, VoIP switches, biomedical equipment and building automation devices are subjected to the same level of analysis as any other networked system.

Three classes of tools are used in the detection phase:

PROPRIETARY TOOLS	Several tools used by our team are developed internally by our engineers. These include tools for decrypting various protocols, brute-force authentication attacks, and exploitation of system services. Our team members continually discover novel exploits and have numerous CVE credits.
PUBLIC DOMAIN TOOLS	Many of the tools used by our teams have been obtained either directly from the internet or from other security specialists. Such tools are generally highly focused and may have testing algorithms that are superior in their specific area of focus. Each public domain tool undergoes extensive testing in our labs to ensure that its behavior is consistent and that it causes no damage to the target environment.
COMMERCIAL TOOLS	In some cases, we will make use of commercial tools when required. Usually these are limited to clients for specific protocols such as GUI-based remote control or clients for access to specific database types but may include best-of-class security tools like Burp Suite Professional. Our team does not utilize commercial network scanning tools such as Nessus or Nexpose as part of our methodology as we expect our customers to use these tools as a part of the internal security program.

EXPLOITATION

The exploitation phase is designed to provide a level of assessment beyond the capability of commercially available network scanning tools. This phase includes simulated attacks, reflecting vulnerability both to authorized users exceeding their permissions, and to outsiders penetrating over the Internet.

We use a combination of public domain and proprietary tools in the Exploitation Phase. These tools are selected based upon the vulnerabilities identified in the Detection Phase. In certain engagements attack techniques may be sequenced from “quietest” to “noisiest”, providing an opportunity to test the detection capabilities of any installed intrusion detection systems, users, and system administrators. A wide range of external attack scenarios are simulated, combining discovered information with known vulnerabilities to provide the most realistic possible threat profile.

The results of a “successful” attack are pre-determined by consultation with the client’s point of contact. In most instances we can establish susceptibility to potentially harmful vulnerabilities without running an actual attack, thus avoiding any damage to data or interruption of service. When requested, however, denial of service attacks can be run against a designated target. Such tests are closely coordinated with client system administrators, and are most often conducted during designated third-shift hours

ANALYSIS

Once the active phases of the assessment have been completed, prioritized final recommendations are made regarding vulnerabilities, insecure computing practices, configuration management and network design. These are compiled in a final report and delivered to the customer.

Our reports outline each vulnerability, successful attack paths, and provide prioritized recommendations for effective remediation. Additionally, we provide "tech-on-tech" consulting, where we collaborate directly with your engineers or security personnel to review the report. This ensures a deeper understanding of how vulnerabilities were identified and validated, their business impact, and the recommended mitigations. Our assessment reports can also be used to prove adherence to cybersecurity-based Governance/Risk/Compliance requirements.

Each report package includes:

- Detailed explanations of successful attacks and their overall risk
- A breakdown of all discovered vulnerabilities
- Prioritized recommendations for addressing all identified security issues
- A database of devices and their network service versions

Given the evolving complexity of the threat landscape, we recommend our clients have a network vulnerability assessment at least annually. Our team performs a combination of manual and automated testing in an attempt to gain access to critical systems or data identified during the scoping phase, assessing potential business impact.

ADVANCED CYBER SOLUTIONS AT CORE4CE

Core4ce is a data-minded company that serves as a trusted partner to the national security community. Our mission is twofold: protecting data to safeguard national interests and applying innovative strategies to enhance security capabilities for our clients.

With a combination of seasoned security experts, proprietary methodologies, and unique access to cyberthreat intel, Core4ce is well positioned to address the complex and constantly changing cybersecurity challenges faced by modern organizations. In addition to identifying cyber vulnerabilities, we work with customers to efficiently mitigate issues, enhance defensive postures, and fortify enterprises. The geographic and functional diversity of our combined clientele contributes greatly to our breadth of expertise and holistic understanding of security threats.

Ready to join forces?
Contact our team at CyberSolutions@core4ce.com.