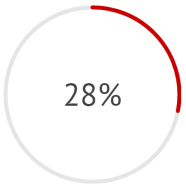
SECNAP NETWORK SECURITY

Internal Vulnerability Assessments

Mitigate Risk with Internal Vulnerability Assessments

Assess your IT risk like an insider. Vulnerabilities can arise due to misconfigured hardware, out of date software or even unpatched systems. Attacks can come from a malicious insider, viruses, malware or even an unintentional attack such as an accidental deletion of sensitive data.

The objective of an Internal Vulnerability Assessment is to safeguard the network's assets that could be exploited to interfere with the confidentiality, availability, and integrity of your network.



Percent of Breaches that Involve Internal Actors.*

Our Team's Experience

Our US-based security experts provide an insightful review of the state of all internal network assets including vulnerabilities, misconfigurations and other health indicators. Since 2001, SECNAP has been leveraging our security professionals who have extensive experience reviewing real-world exploits on a daily basis.

Attack Surface Testing

Our testing is built for the modern attack surface and leverages automation in order to test against over 100,000 potential vulnerabilities and 45,000 Common Vulnerabilities and Exposures. Those test are complimented with manual testing performed by a highly experienced security professional in order to confirm and further explore gaps in your security posture.

Assessment Report includes:

- Executive Report for the Non-Technical
- Detailed Findings and Remediations Report
- Comparison to Previous Scans if Applicable
- Screenshots of Confirmed Vulnerabilities
- HTML Detailed Data and Supporting Files

The final report will accurately identify and prioritize vulnerability remediation based on criticality, threat context and vulnerability severity. For example, a vulnerability that is easy to exploit, leads to large amounts of data loss or has potential of lateral movement, should be high priority.

Automated scans with tests for:

- Catalog all active ports/services on network
- Check for operating system vulnerabilities
- Check for web server vulnerabilities
- VoIP vulnerability testing
- Testing for malware and bots

Manual probes may include:

- Check internal services for misconfigurations
- Confirm best practice configurations for services
- Evaluation of service inherited attack vectors
- Escalate compounding low-risk vulnerabilities
- Verification of vulnerabilities detected
- Perform exploitations against target systems

*2018 Data Breach Investigations Report, Verizon

844.638.7328 | SALES@SECNAP.COM | SECNAP.COM

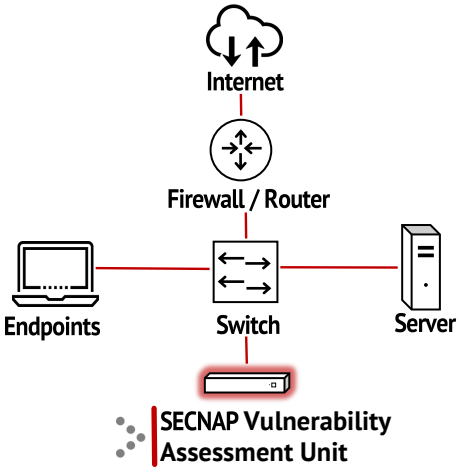
Internal Vulnerability Assessments

What happens during testing?

A Vulnerability Assessment Unit is deployed onsite where it is connected to the core switch and remains active until testing is complete. There is typically no impact on the network during installation. The assessment gives broad and deep visibility into internal vulnerabilities. It can cover over 47,000 unique IT assets such as network devices, operating systems and applications.

Authenticated scanning, is an optional part of the assessment that is highly recommended. We require administrative and regular user credentials which are used to gain a more thorough view of internal network assets.

7x More Critical and High Vulnerabilities are identified when we have full credentials.*



Vulnerability Testing	Identify and manually confirm internal vulnerabilities
Level of Expertise	Advanced
Level of Intrusion	Likely non-intrusive
Client Involvement	Conducted with approval and under cooperation of IT Department

Benefits of Regular Testing

This assessment should be used to analyze the network's current security posture. Depending on your business vertical, security maturity and sensitivity of your data, your risk appetite may vary. In general, it is recommended that testing be performed quarterly at minimum. It is particularly important after the network undergoes any significant changes as new security gaps may arise.

Proactive Security over Compliance

Numerous state and federal laws and regulations require risk assessments, of which internal vulnerability assessments are an integral part. If your business is regulated by GLBA, FINRA, NCUA, HIPAA, SOX, SSAE 18 or PCI, these assessments are critical. The FTC has stated that the identification of internal vulnerabilities is a key element in a proper security program. If a breach were to occur and legal action is being taken, assessments will be valuable when proving that reasonable measures were taken to protect and secure data.

Security teams who follow the NIST Framework understand the importance of frequently identifying vulnerabilities. Each assessment will determine the system's deficiencies for short-term analysis. Recurring assessments will provide trending data for long-term evaluation. A proactive stance in security, not just in compliance, requires an ongoing process that discovers and remediates vulnerabilities.

Still have Questions?

It's likely you have some questions you need help with. Contact us to get scheduled with a security expert.

*Based on Actual SECNAP Customer Data