SECNAP NETWORK SECURITY

External Penetration Assessments

Reduce Risk with External Penetration Testing

The best way to stop an attacker from succeeding is to think like one. Our security experts will simulate a remote attack on your network to find vulnerabilities in systems accessible to public network infrastructure. Our penetration test are performed by our team of certified security experts who have extensive experience reviewing real-world exploits on a daily basis.

Our testing leverages automation in order to test against over 90,000 vulnerabilities and is complimented with manual testing to further explore gaps in your security posture. Our US-based security experts will work to identify weaknesses that could be exploited to interfere with the confidentiality, availability, and integrity of your network. With our findings, we will provide a detailed report and give your team guidance towards how to minimize your network's external facing attack surface.

Benefits of Performing an External Penetration Test

A penetration test can help justify the resources needed to close the security gaps that directly impact your risk level. With our detailed report, you will be able to facilitate the compliance process and identify potential compliance violations.

Your sales team can also benefit from security. During the vetting process of new vendors, your prospects may require a copy of your most recent penetration test to ensure they are doing business with a secure company.

Our External Penetration Assessment Report includes:

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

Over 70% of Breaches Involve External Actors.*

*2018 Data Breach Investigations Report, Verizon

Top Six Benefits

1. Evaluate Effectiveness of Current Security Posture
2. Facilitate and Ensure Regulatory Compliance
3. Validate Defenses and Prioritize Remediation Efforts
4. Identify Business Risk and Help Leadership Make Informed Decisions
5. Validate the Need for Resources and Additional Budget
6. Documented Third-Party Reporting for Others Looking to do Business with a Secure Company

18.2

844.638.7328 | SALES@SECNAP.COM | SECNAP.COM

SECNAP NETWORK SECURITY

External Penetration Assessments

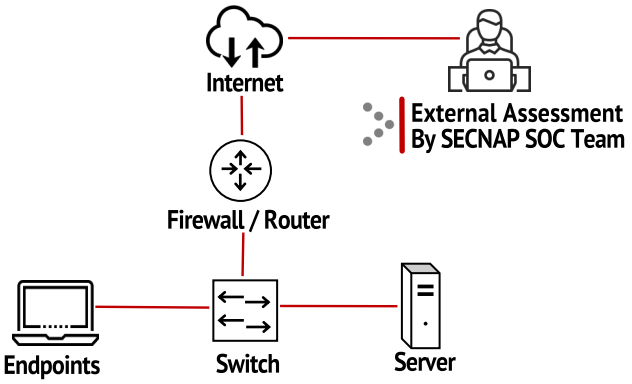
What happens during testing?

External penetration testing consists of remote scans and tests generated from our Secure Operations Center (SOC) to determine if vulnerabilities can be detected on web-facing hosts.

Over 90,000 automated tests are performed on external facing surfaces including network devices, web servers, firewalls, hypervisors, databases and operating systems.

During Level 2 testing, our security team will manually confirm vulnerabilities in a non-intrusive manner in order to prevent disruption of critical services. Exploits will be attempted with cooperation of IT Department during Level 3 penetration testing.

Once testing is concluded, our security experts will report back on what actionable remediation should be prioritized to reduce your external attack surface.



How does it get done?

During testing our US-based security experts will run a series of automated and manual probes.

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 for external services 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

Frequency of Testing

Testing is a snapshot in time of your current security posture. Depending on your business vertical, it is recommended that testing be performed monthly or at least quarterly. It is particularly important after the network undergoes any significant changes as new security gaps may arise. Compliance regulated industries may require Penetration Testing annually to ensure compliance.

SECNAP's External Penetration Program is designed so that our customers are in control of how far our security experts are expected to go. Here is a brief comparison between the levels of External Penetration Testing:

	Level 1	Level 2	Level 3
Vulnerability Testing	Identifies potential vulnerabilities	Identify and manually confirm vulnerabilities	Identify, confirm and attempt to exploit vulnerabilities
Level of Expertise	Analyst	Advanced	Expert
Level of Intrusion	Non-Intrusive	Potentially intrusive	Likely to be intrusive
Client Involvement	Minimal client involvement	Conducted with approval and under cooperation of IT Department	Conducted with approval and cooperation of IT Department. Typically performed in a replicated system

18.2