NOPSEC

NopSec Pentesting Services FAQ

Uncover the exploitable areas of risk in your infrastructure, applications, and employees.

Get the Answers You Need to Improve Your Cyber Risk

What types of pentesting do you do?

We can deliver network, mobile application, social engineering, internet footprint, gap analysis, and web application pentesting.

Do you pentest the entire network, or can you focus on specific segments?

We can perform a full network pentest or focus on areas you select.

What pentesting tools do you use?

We leverage a number of tools and methods such as, but not limited to, nmap, burp, metasploit, smbmap, crackmapexec, nessus, openvas, responder, mimikatz, powershell empire, bloodhound, hashcat, sqlmap, dirsearch, rubeus, impacket, enum4linux, proxychains, sshuttle, eye witness and many, many more.

How much does a penetration test cost?

This is largely dependent on the scope of the test and the number of assets involved. We can get you in contact with a NopSec representative to build an estimate.

Do you do code or war dialing as part of your pentesting?

We do not currently offer code review or war dialing (analog modem) services.

Do you use blue, red, or purple team pentesting?

We primarily do red team pentesting, but we will work with our clients for a purple team approach if they have an internal or other external blue team for the engagement.

NopSec helps security professionals simplify their work, effectively manage and prioritize vulnerabilities, and make better informed decisions. NopSec's Unified VRM is an innovative threat and vulnerability management solution that addresses the need for better prioritization and remediation of security vulnerabilities in a single platform.

NopSec Inc. • www.nopsec.com • sales@nopsec.com