



Psiframe Network Security Services

- ❑ Network Vulnerability Assessment, External and/or Internal (eNVA / iNVA)
What does my network look like from an attacker's perspective? What systems, services and data are exposed and exploitable? What could a rogue employee do if he or she were disgruntled, or worse, "planted"? The best way to validate the security of a network is to try to break into it. Our "Red Teams" examine networked systems "in the blind" by leveraging sophisticated expertise and **Acumen™**, Psiframe's proprietary interrogation, data collection and reporting suite. All Internet-connected systems, packet switching networks and dial-up devices are meticulously probed for insecurities over a period of several weeks. Our highly regarded interactive **RiskPoints™** eDeliverable, a Psiframe exclusive, includes a Network Map, Risk Analysis and Lockdown Guide with step-by-step instructions for mitigating all vulnerabilities found throughout the network infrastructure.

- ❑ Wireless Network Vicinity Assessment (wNVA)
How secure are wireless LANs? Do we even know if one is operating without our authorization? According to Gartner Inc., at least 20 percent of enterprises have "rogue" wireless LANs in place that were installed by users, not by IT staff, and 30 percent of large firms will be hacked through wLANs in 2002. "War Driving" and "Drive-by Hacking" have become the latest watchwords among IT Security concerns as network attackers trade cracking tools for the flawed WEP encryption standard. Using sophisticated scanning and monitoring techniques, we document an outsider's ability to detect, collect and decrypt data from 802.11b Wireless Access Points and associated mobile devices – often at distances far greater than expected by those who installed them. Access Points operating in nearby buildings are also identified to determine risks of inadvertent network bridging.

- ❑ Social Engineering Assessment (SEA)
How easy is it for impostors to get confidential information? Can they get user names and passwords? What's at risk? How can we stress to our employees and management the importance and urgency of following our security policies? "Social Engineering" is commonly employed by hackers as a simple way to circumvent complex roadblocks. Regularly testing and documenting the degrees of organizational awareness and staff discretion in dealing with dubious requests promotes compliance with policies and procedures.

- ❑ PBX and Voice Mail (PBX/VM)
Can unauthorized users access privileged messages from our voice mailboxes? Could our corporate telephone networks be used as diverters that mask locations and identities of criminals for illicit activities? Psiframe analysts test the back-line security of corporate telephone switches in attempts to discover exploitable vulnerabilities. Our findings reveal scenarios whereby attackers may compromise telecommunications equipment and services. Deliverables include detailed documentation of methodologies used, results found, and expert advice.

- ❑ Vulnerability Management Program (VMP)
How can we have testing and analysis performed regularly to ensure that our network remains secure? Once Psiframe's prerequisite eNVA and iNVA engagements have been performed, we offer an ongoing service available on a quarterly basis that leverages industry best practices in managing the *process* of good security. Standards such as GLBA, HIPAA, IS-17799, and SAS-70 are supported enabling simplified certification processes.

- ❑ Server Security Review (SSR)
If we want to focus an assessment solely on a specific server or group of servers, is there a way to do that on a stand-alone basis? Yes. While many security vulnerabilities are external in nature, those that present the greatest risks may exist within a server's operating environment. The Psiframe SSR is designed for organizations that require a higher level of security for critical servers. Psiframe's auditors identify vulnerabilities including misconfigured operating systems, unpatched services, improper permissions, and unsound logging practices. Psiframe analysts provide recommendations for hardening affected operating systems. Extensive documentation is provided including a server hardening guide that addresses the security of each system individually.

- ❑ Application Security Analysis (ASA)
What is the best way to assess the security of applications we've developed in-house? The Psiframe ASA is designed to help mitigate the risks of deploying and using custom software applications. The ASA is also used by Psiframe clients who wish to validate the security of their consumer software applications before releasing them to the public. During an ASA, Psiframe application security experts review critical e-business, groupware, and custom software applications to identify security weaknesses and provide recommendations.



What clients are saying about Psiframe Network Security

"Your group is very professional and detailed. I look forward to working with your team in the future."

– Network Manager

"A well-done [findings] presentation."

– Vice President, COO

"I like the format of the report and I like how you tie back the threats to vulnerabilities."

– IT Director

"The way you communicated with us during the assessment process was great."

– Manager, Systems & Networks

"We were extremely relieved when you came in. You actually knew what you were talking about. We had to sit through three other meetings with clueless people trying to sell auditing services."

– Security Manager

"This was well worth our time."

– Vice President, IS Director

"I was really pleased with the process. It was good to be in regular contact with you throughout."

– Vice President

"It went very well. We would like to use you again."

– Sr. Vice President, IS Manager

"We would like to see more banks do penetration testing like this."

– FDIC Examiner

"Wow! I'm really impressed. Very good!"

– Sr. Network Engineer

"You are masters of your craft. Congratulations! Well done."

– IT Director

"I found it fascinating! It was like a spy movie - pretty cool!"

– COO

"I WAS BLOWN AWAY! Great job! I can't wait for the next opportunity."

– Psiframe Channel Partner

"I was very happy to see how much diligence you put into it."

– IT Administrator

"I got the information I needed and I believe the management team got what it needed."

– CFO

"What this has shown me is how fast [the technology] moves and how difficult it is to keep on top of everything."

– Network Manager

"I'm very happy with the quality of your report and the level of detail you put into it."

– Founding Partner

"I was impressed by the elegance of how you got in! It speaks to the quality of what you do."

– Vice President

"It was quite enlightening for our client and will prove to be an excellent investment towards averting future security breaches."

– Psiframe Channel Partner

"The whole process has been very eye-opening for me."

– IS Administrator

"I think it was a very useful exercise."

– Vice President

"I was very impressed with the amount of work you did. What I don't understand is how you learn all this stuff without going to jail!"

– Network Administrator

"You and your people did an excellent job of presenting the results of the assessment in a manner that was technical enough for the technical people and high level enough for the CxO personnel."

– Psiframe Channel Partner

"We received real VALUE from this engagement. We learned what we are doing well, and where we can make improvements, especially with internal controls."

– Vice President

"I have gained invaluable knowledge and experience working with you and your team on this very sensitive assignment."

– Vice President