8 Tips for Penetration Testing
TEST WELL OFTEN

At least one per quarter or any time there is a significant change to your IT infrastructure.

If this seems like it is too often, remember attackers are testing your IT infrastructure every single day.
THINK RISK
Define your goals. Step back and ask, “What am I trying to protect? What are my critical assets?” What if email goes down? How would it impact your business?
CHOOSE WISELY
There are many capable, powerful tools out there, but some are easier to use than others. Buy one your team can use.
If a test takes your system down, you’ll want to ensure you were acting within company policy and are prepared to implement a security incident response plan.
BE A KNOW-IT-ALL
Identify devices, applications, databases, etc. The more you know about a target, the better chance you have of breaking in.
REMEDIATION ✓
The attack path.
A breach usually occurs when multiple vulnerabilities connect across vectors. Start remediation efforts here.
E-Z SELF ASSESS

If you pay a contractor to scan your website, you’re throwing out money. If your team doesn’t know how to do this, you have a problem a consultant can’t fix.
BE PARANOID

Better to be safe than sorry. Take a look around your physical workspace, consider every potential event and procedures that could put assets at risk.
LEARN MORE ABOUT ATTACK INTELLIGENCE

Visit www.coresecurity.com to learn more about pen testing and how we are reinventing vulnerability management.

GET MORE INFO