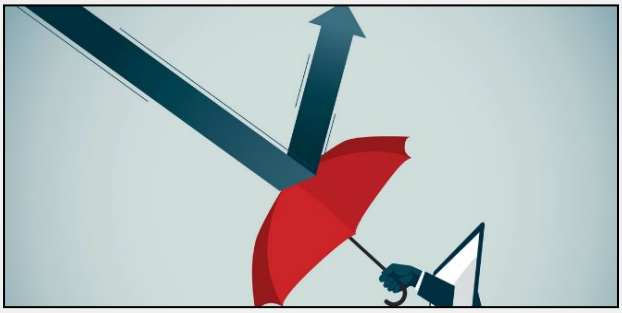
Hippogriff LLC - Vulnerability Testing Fast Look

Although risk analysis can easily be done by internal security teams, support from highly skilled technologists can be the difference between security and vulnerability. Such potent abilities are cultivated through a mindset of thinking and doing as the "bad ones" do, but with admirable intent. And in order to employ creative ways to identify problems before they occur, going beyond the use of automated tools is absolutely required to obtain thorough revelations.



Security Penetration Testing is a very intimate exercise that requires supervision by experienced and vetted computer science engineers and electronic technicians. Before any test can be initiated, a transparent scope of work must be outlined with elevated participation from organizational management. The advantages to Hippogriff's approach to testing are amplified by tangible interaction with systems, supervised by prior Law Enforcement and former Military Internal Security Associates. Attributes that are relevant to a precise testing cycle include but are not limited to:

Test Phases

- Pre-Interactions
- Intelligence Gathering
- Mapping/Modeling
- Vulnerability Analysis
- Exploitation
- Post-Exploitation
- Reporting

Tested Elements

- Active/Inactive IPs
- Gateways
- Mac Addresses
- Applications/Utilities
- Coupling Elements
- Controls
- Masking
- Monitoring
- Encryption Ciphers
- Electronic Components
- Response Readiness
- Psychological Coercion
- Physical Access

Examination Levels

- Red Teaming
- Expanded
- Compliance
- Functional

Examined Protocols

- IPv4 | IPv6
- NBT-NS
- WPAD
- DNS
- DHCP
- BGP | IPMI
- ICDP | DTP
- LLDP
- NBNS
- OSPF | LLMNR
- DTP | VLAN
- VRRP | SNMP
- UDP | VTP
- SSL | TLS
- HTTP(S)
- FTP | RDP

Not only must a formidable deterrence be designed to keep an infiltrator out, it must also have attributes which can trap that same infiltrator from escaping; if by chance they do defeat early warning detection and perimeter defense layers. By implementing such a capability and enforcing incident response policy, the odds of revealing the point of origination for a cyber attack greatly increase. This next generation counter-action is better explored when elevated levels of testing, i.e. – Expanded and Red Teaming are carried out.

"If we care about the security of our people and our data, it is the real world threat that counts the most. While compliance requirements may be a necessary evil, they do not equate to a necessarily secure environment. So much effort is spent meeting compliance requirements that sometimes actual operational security isn't assessed adequately. It is easy to forget the reasons for having security in the first place when we are running around just trying to validate compliance, instead of analyzing real world threats and risks that are the ones that lead to eventual compromise. This is called "doing the job right instead of doing the right job."

The value you gain from a penetration test is largely dependent on your choices in who you trust as a partner, what degree of freedom you entrust them to operate within, and how they cater their reporting to your organization's needs. Getting a penetration test is a bit like going to get an MRI: It's never something you want to do, and you hope the results come back negative, but you do it because you want peace of mind and you want to know what things look like in the real-world."

- Eric Basu, U.S. Navy, Sentek Global, Oct. '13

Operating systems, firmware, applications, networks, electronic components, and living people all have unknown or ignored flaws. These flaws must be illuminated and corrected in a timely manner to uphold not only user safety, but also for the integrity and promotion of ethical technological advancement. Computing and data processing/transfer product/service developers and manufacturers are not solely responsible for the prevention of exploits; those that employ such products and services are too. Test and keep testing...

Computer Technology Protection Services

1-866.273.4831
inquiry@hippogriff.tech
Hippogriff.TECH • Hippogriff.IO