

Services Datasheet

Network Penetration Testing

OBJECTIVE

- Create a snapshot of your current security posture.
- Identify and attempt to compromise all internet facing computers in the target range.
- Attempt to use compromised hosts to probe deeper into your network (with prior approval).
- Document findings in a comprehensive report.

BENEFITS

- We find holes in your networked infrastructure, web applications, firewalls, IDS, routers, and other networked components.
- We do manual testing for accuracy and effectiveness.
- We offer to our customers active knowledge transfer of techniques, issues and remediation.
- We address your regulatory security requirements.
- We improve your security awareness in technical and non-technical staff

DELIVERABLES

- Penetration Test Executive Summary.
- Penetration Test Technical Report, containing for each flaw the detailed reasons, consequences and remediation.
- Technical support on the remediation techniques.
(All reports can be written either in English or in French).

RELATED FMA SERVICES

- Application Vulnerability Assessment.
- Source Code Security Assessment.
- Operating System Vulnerability Assessment.
- Writing Secure Code (Java, C/C++, ASP, PHP).

HACKERS and other criminals continually develop new tools to gain access and disrupt networks, staying even with or ahead of the technological curve. Your IT infrastructure is always at risk, and will most probably continue to be. The best you can do, then, is minimize your exposure to external threats. Research shows that the more difficult it is to successfully exploit your systems, the more likely an attacker will simply move on to their next target. Vigilance is effective, and can prevent attacks on your network.

FMA conducts professional Penetration Tests against systems within your LAN, WAN, intranet and internet sites in order to expose hosts that lack adequate security, and then attempts to gain control of them. A Penetration Test is a simulation of a real-world outside attack against a system in order to identify security weaknesses before they are exploited by hackers. Some like to call it Ethical Hacking, we prefer calling things by their logical name.

Although systems may be encroached during the Penetration Test, FMA will never attempt to erase, alter or harm any of your company's systems or data. This test is done with absolute safety of your infrastructure in mind. Engagements typically range from a few days to three weeks.

Why FMA Professional Services?

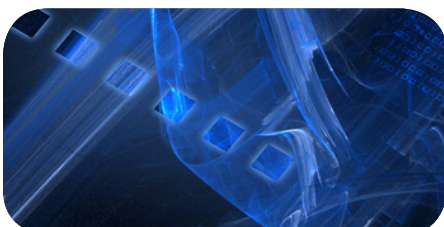
- Exclusively focused on IT security services.
- Advanced Methodology compliant with best security testing practices defined in OSSTMM, OWASP and IBTRM guides.
- FMA is more than 6 years old and has an extensive track record.
- Jargon-free detailed findings and recommendations.
- Reasonable ongoing technical support at no additional cost.
- We can perform testing on-site or remote and can work 24/7.
- We can test within given change control windows and during quiet periods.

Premier IT Security Professionals

When recruiting consultants, FMA's first priority is security expertise. Members of our team are passionate about security and have diverse IT security backgrounds. All our consultants are premier professionals with extensive IT security experience (more than 8 years) and are among the most technically proficient in the industry. Additionally, most of them are regular speakers at international IT security conferences.

Methodology

A large part of FMA effectiveness comes from having developed a thorough technical methodology that is reliable, repeatable and that definitely goes well beyond automated tools.



<http://www.fma-rms.com/>
info@fma-rms.com



Network Penetration Testing

FMA Risk Management Solutions

10 Anson Road,
#15-14 International Plaza,
Singapore 079903,
Republic of Singapore
Tel: (+65) 92997327
Fax: (+65) 67220785

Additionally to operating in Singapore, we often provide IT security services to organisations located in Indonesia, Malaysia, Hong Kong, Thailand and China.

We perform Penetration Test engagements either on a one-time basis, or on a subscription basis (e.g. quarterly or biannually).



Thorough Manual Testing

Because of the significant limitations of automated testing tools like network vulnerability scanners, almost all of our testing is performed and verified manually using a well-defined, repeatable and consistent methodology.

Automated tools are used in areas of the assessment only where they are proven to be accurate and effective (less than 5 percent of a typical engagement).

Footprinting: gathering information on the target independently of what is provided for the assessment.

Scanning: inventory of devices on the network and the identification of listening services. This allows the penetration team to focus on the best avenues of entry.

Enumeration: performing more intrusive probes. May involve establishing null sessions, getting user account information, identifying poorly secured devices, computers, shares, default configurations, etc.

Gain access: using information gathered from previous stages vulnerabilities are exploited (no harm approach).

Escalate privileges: attempting to gain full control of information assets on the network by obtaining root passwords, domain admin, database admins, etc...

Harvest: collecting sensitive and valuable information that can be stolen. Major targets are payroll databases, client listing, HR records, accounting information, legal documents, etc.

Reporting: a comprehensive report, listing vulnerabilities and recommended countermeasures is prepared. In addition, a database with each device, vulnerabilities detected, risk level, access gained, services listening, etc. is provided for the administrators to action.