

OPEN FOR BUSINESS OR OPEN FOR ATTACK?



MANAGED SECURITY SERVICES LTD

TEL: +44 (0)1628 675854

info@mss-ltd.net

www.mss-ltd.net

About Extrusion Testing

Traditionally penetration testing is used to establish whether a system, network or web site is secure from external attack. MSSL in conjunction with Encode, our security consultancy partners, have launched a new concept in security testing.

We have termed this new concept "Extrusion Testing" as we identify the potential for leakage or theft of internal data rather than the ability of a hacker to penetrate the network via a vulnerability.

Hackers have recently moved away from trying to batter down the door and are employing more productive means by adopting social engineering techniques. We have developed a service using a combination of e-footprinting and e-social engineering, along with malicious code attacks and state-of-the-art Remote Access tool (RAT) technology.

The "Extrusion Testing" service closes the gap between network and application penetration services. We not only tell you about your network vulnerabilities we can also tell you exactly what data can be extracted.

Your organisation's access/content security, endpoint security, data leak prevention and intrusion detection/prevention capabilities are all put to the test.

Extrusion testing is fast becoming an essential element of any security portfolio whether to assess implementation of new security systems or to identify where additional measures are required.

The Objective:

Demonstrate external access to internal system(s)/network(s)

Demonstrate external access to specific data/services

Puts the organization's security controls & capabilities to the test against the professional attacker:

Web access/content security

Endpoint security

Data leakage prevention

Network/Security Monitoring

Internal Security in general

Methodology

e-footprinting & e-Social Engineering

Profile users in the organisation

Develop e-Social Engineering scenarios (e.g. spear phishing)

Trick users to access a specific web-site, open an attachment...

Web/Mail-born Attack

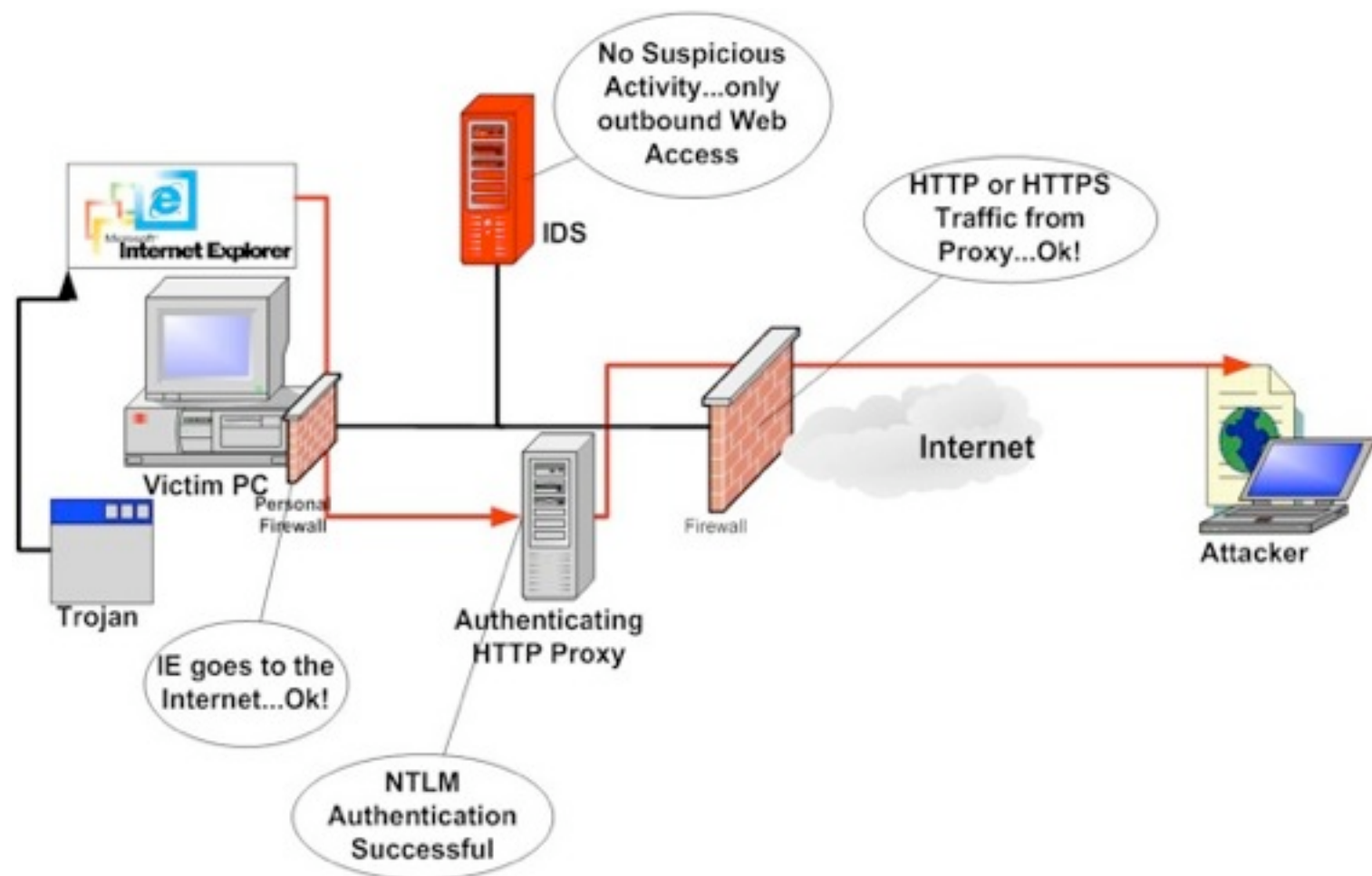
Use mobile code exploits to get access on internal user system (endpoint)

Full-blown Extrusion Testing

Escalate attack to compromise internal business system(s) and/or network

Demonstrate ability to obtain specific critical data

Demonstrate ability to take control of critical business services



It doesn't take long for a determined cyber criminal to succeed...

a couple of days to e-footprint an organisation and launch an e-social engineering attack between 1 hour to a few days to take control of an internal endpoint...depending on level of determination

...and then a few days, or even hours, to "stealthily" take control of critical internal business systems and data, or worst case scenario, the entire network,

and then successfully being able to conduct fraud, industrial espionage and sabotage, whatever they want!

FIND OUT MORE CALL US: +44 (0)1628 675854