



## Network and Application Testing Methodology

### Testing Methodology

The methodology used by Yacc Labs to perform audits is a combination of industry best practice, together with frameworks provided by the SANS Institute, PCI DSS, OWASP and ISC<sup>2</sup> and generally falls into the following iterative process: Reconnaissance, Mapping, Discovery and Exploitation.

These steps then fall into the following activities:

- Scanning and Identifying resources
- Vulnerability scanning and probing
- Application scanning and Information disclosure
- Policy and procedural review
- Remedial recommendations

In our experience we find that by iterating this process, it provides a thorough and constructive approach to ensuring a full assessment of an organisation's infrastructure and system is carried out.

When performing tests on Websites and Applications, we follow guidelines specified by OWASP to help ensure a structured approach. Tests for flaws in application logic which may allow SQL injection and cross-site scripting (XSS) vulnerabilities are performed, together with ensuring software and systems are patched correctly up to date.

### Tools

Yacc Labs use publicly available Open Source tools, combined with Commercial products and our own specially developed in-house software, during our audits. Using exactly the same tools as potential hackers might use themselves provides us with the same view of the targets as they have. Combining these with professional feeds, plus many years of software development and networking experience, gives us an excellent advantage in discovering any flaws before hackers do.



## Exploitation of Vulnerabilities

When a potential vulnerability is identified, the cause and effect is fully reviewed and the findings are reported immediately to the client. Detailed information about the issues are provided to enable our client to make an informed judgement as to whether to attempt to exploit the vulnerability, or just to provide proof of concept that there is an issue

Yacc Labs take security and system integrity equally seriously. At no point will we ever attempt to exploit a vulnerability if we feel that doing so could cause damage, data loss or system downtime; (unless specifically instructed to by the client) to any system area but particularly if it is a production system.

There may be times where the client may wish to instruct work to be undertaken where there is a risk of all or some of the above issues occurring, but YACC Labs would only ever do this upon instruction from the client, ideally after a collaborative evaluation of the risks and benefits of taking this action had taken place.

In addition, depending upon the vulnerability and with the necessary authorisation, we may attempt to insert data into a system. All stages of the exploit will be fully documented so that records can be removed afterwards by the client's own technical staff and the results analysed in order to determine a suitable fix.

## Documentation and Recommendations

Throughout each phase of the audit, the actions carried out and outcomes from these are fully documented. Where a new system is discovered and it is within scope of the audit, the same audit processes as above is followed. This ensures that a complete picture of the system environment, including issues uncovered, is developed.

Some clients prefer to simply receive our findings at the end of the audit, whereas others prefer a slightly more collaborative approach. We strongly recommend the latter, as then we can report back any issues immediately which, if remedied during the audit and if time allows, may then be re-tested to maximise the benefit of our time and experience.

The issues found drive our recommendations, but generally they may fall into the following areas:

- 1) Network design and firewall infrastructure changes
- 2) Application and authentication enhancements
- 3) Policy and procedural improvements



Our team has the skill and experience to work with client's technical staff to help develop new designs or suggest improvements in any areas at risk and will provide as much information as we can to allow them to undertake any remedial work necessary. This may be formally, via a report, or informally via telephone or email as required.

## **Back out Procedures**

Generally, Yacc Labs will not carry out any invasive testing activities unless expressly instructed to by the client. However, when we do, we ensure that:

- a) Full system backups have been taken immediately prior to beginning tests
- b) Client's technical staff are on-hand should anything untoward occur
- c) Test data we insert will be obviously marked as such
- d) Client notified when testing complete
- e) Any extraordinary behaviour or system failure notified immediately.

Ideally, such activity should be performed whilst the system is in test or off-line, however live systems should be tested during off-peak periods where possible.

We are manually involved with all tests we undertake and observe results as they happen. In the unlikely event that we do spot an issue, we will immediately halt the test, review the situation to determine what may have happened and alert the client immediately so a resolution can take place.

## **Other Test Activities**

As part of the initial information gathering stage, we will carry out DNS zone transfers and other IP audit techniques in order to discover as much information about the target environment as we can.

We will also utilise the power of the main internet search engines and other resources so we can build up a picture of what information is publicly available to us, and use this as the basis of further 'client specific' tests. It's amazing how much information you can quickly gather that can provide useful details such as potential usernames and passwords.

All information discovered will be provided in the full audit report, with just the main highlights detailed in the executive summary.