No jargon, no compromise*

*Reassuringly dull cyber security

Penetration Testing Services

Norm's Penetration Testing Services provide security assessments of your computer networks, systems, applications and people to identify and address security weaknesses.

Through our highly trained security analysts, we will help your organisation manage cybersecurity risks by identifying, safely exploiting, and helping to remediate weak points in your environment that could otherwise lead to data and assets being compromised, lost to malicious attackers and possibly leading to other direct and indirect collateral damages/losses.

Norm's Penetration Testing Services are comprised of the following key security assessment services:

- External Penetration Testing
- Internal Penetration Testing
- Web Application Penetration Testing
- Vulnerability Assessments

This service module focuses on, reinforces, and actively tests the three elements of Norm's holistic trinity of cybersecurity - People, Process and Technology.

Its purpose is simple:

* Deployment of Cyber Security Experts to identify, exploit weaknesses in your corporate environment(s) through a combination of vulnerabilities, exploits and people social engineering

* Final Incident report provided detailing findings from the assessment(s) and recommendations to prevent similar incidents in the future

Service Offerings

Penetration tests (pen tests) are part of an industry-recognised approach to identifying and quantifying risk. They actively attempt to 'exploit' vulnerabilities and exposures in a company's infrastructure, applications, people, and processes. Through exploitation, Norm can provide context around the vulnerability, impact, threat, and the likelihood of a breach of an information asset.

It is frequently possible for a pen tester to gain remote access to operating systems, application logic and database records. Through active exploitation of direct and interconnected systems, Norm can provide strategic guidance on risk and tailored advice on countermeasures.

Norm's Red Team Testing skills and experience:

- Industry-leading testers
- Management and technical reports
- Proven testing methodology
- Vulnerability assessment services
- Internal assessment testing
- External assessment testing
- Web application testing
- Mobile application testing
- Full security audit services
- PCI compliance services

External Infrastructure Testing

External Infrastructure tests will provide an organisation with a review of its IT infrastructure, conducted through the eye of an Internet user. The external tester tests any network attached to the Internet and will determine if they can penetrate through weak Internet-facing security controls.

The types of tests that these assessments include: -

- DNS Servers
- Internet Routers
- Firewalls
- IDS/IPS
- VPN Servers
- FTP Servers
- HTTP/HTTPS Servers
- Web Services
- Mail Servers
- Extranet Servers
- External Switching Fabric

External tests will assess the security controls configured on access routers, firewalls, Intrusion Detection Systems (IDS) and content scanners to protect the perimeter of the network. External tests will also evaluate security controls for published applications through the Internet.

Norm recognises that there is increasing logic being built into web services to deliver extranet, e-commerce and supply chain management functions to Internet users. Therefore, we pay attention to these resources and perform granular assessments on their build and configuration, as well as interaction with other data sources that sit in your protected network segments.

The testing will conform to the requirements defined in the scoping phase of the assessment.

Daily debriefs can be arranged for clients who want to be informed about the discovery of critical vulnerabilities as they are found.

Internal Infrastructure Testing

Internal infrastructure tests will provide an organisation with a review of its security conducted through the eye of an internal user, a temporary worker, or an individual that has physical access to the organisation's buildings.

These types of assessments will focus on: -

- Wireless Infrastructure
- Wired LAN Infrastructure
- Network Switches
- Network Routers
- Firewalls
- IDS/IPS
- Proxy Servers
- Windows Server Machines
- Unix Server Machines
- IP Telephony
- File/Print Services
- Application Services
- Shared Storage Resources
- Native Internet Connectivity
- Ability to gain remote access to the infrastructure through the Internet/PSTN
- Ability to steal data
- Extranet Servers

Norm conducts tests from within an organisation, over its Local Area Network (LAN). Tests will observe whether it is possible to gain access to privileged company information, including sensitive application databases, HR information, and ERP type resources using techniques common amongst hackers.

Internal tests will reveal whether a user can escalate their network privileges and gain copies of usernames, and passwords of other business users. Internal tests will also evaluate whether it is possible to remove data from the corporate environment without triggering alarms or an audit trail.

Internal tests will assess whether a user can circumvent existing security controls to grant themselves inbound access to the infrastructure via remote access mechanisms, along with assessing the potential impact of modern malware threats.

No jargon, no compromise*

*Reassuringly dull cyber security

Web and Mobile Application Testing

The number of businesses transacting online is at an all-time high and shows no sign of slowing down. Whether it is online retailers selling direct to consumers, or businesses giving extranet type services to their trading partners, there is a growing trend to bring increased functionality to the Internet browser. Many of these transactions are over secure HTTPS connection streams. Although this brings more security to the end-user, it does mean that a malicious user can send encrypted traffic to the webserver that cannot be seen by many traditional security controls.

Web server tests evaluate all types of web servers, ranging from static brochure-ware websites to all-encompassing transactional e-commerce environments. Norm focuses on how application logic is built into the website and pays attention to any aspect of the environment that allows a user to enter input.

Web server tests will assess an environment for server- side attacks such as SQL injection and Blind SQL injection. Additionally, tests will review an environment for client-side attacks, such as Cross-Site Scripting (XSS) exposures which could allow an attacker to manipulate the clients that access your infrastructure. Norm will assess the design of web infrastructure, including the use of cookies and log-in forms. We will also determine how data is encrypted, how content is displayed, the presence of error messages, and the entry style of commands/input.

Norm's experienced web application testers can accurately test all manner of web applications, from feature-rich fully-fledged dynamic applications to slimline API calls, IOS and Android mobile applications. Norm's web application tests are designed around OWASP's web application testing guidelines and standards, ensuring that web applications are continually tested against the latest threats. These threats include: -

- Tests for database injection (SQL injection, NoSQL injection)
- Tests for logic flaws, indirect object references
- Authentication weaknesses
- Code injection, both on client and server-side
- Cross-site request forgeries.
- File upload vulnerabilities
- IOS and Android vulnerabilities

Social Engineering

Norm delivers highly tailored social engineering engagements, designed to help aid organisations increase their security posture and reduce the risk of insider threat attacks.

What is social engineering?

The phrase social engineering; covers a multitude of different types of analysis, ranging from services conducted over the Internet, through to services over the phone or physically on site.

We firmly believe that an element of social engineering is conducted in all penetration tests, because humans are involved in all security processes and to focus on the technology alone, results in an incomplete analysis.

The intent behind a penetration test should be to identify the risk to an asset, a connection, or an activity. Therefore, to address all the elements that feed into that risk, Norm believes that this also includes any human aspects.

Social Engineering and Spear Phishing Services

Through conducting spear-phishing attacks and other social engineering tests, an organisation can obtain a feel for how susceptible its employees would be to this type of attack. In almost all instances, employees will provide the weakest link in an organisation's security arsenal.

Consequently, social engineering tests that feed directly into security awareness training programs provide a direct mechanism for organisations to tackle this vulnerability.

Vulnerability Assessment

The Vulnerability Assessment reviews your corporate environment through scanning and monitoring all the devices connected to your internal and external networks as well as your web-facing applications/services. Each device/application's scan information is scrutinised & analysed for vulnerabilities. Those identified are then scored based upon their criticality.

The assessment provides visibility and detection of weaknesses and vulnerabilities throughout your organisation's corporate environment such as:

- Internal Network(s) monitoring your corporate network-connected devices for known weaknesses and vulnerabilities. This will not only scan and scrutinise all connected devices from Laptop, Desktops, Servers but other infrastructure & IoT devices such as routers, firewalls, switches, CCTV, printers, phones including rogue devices.
- External Network(s) monitoring your corporate network traffic for known weaknesses and vulnerabilities. This will scan and scrutinise all externally facing devices from servers, routers, firewalls, VPN gateways etc.
- Web Application(s) focuses on all the corporate business applications in your network including new and unknown ones. It provides dynamic deep scanning, covers all apps on your perimeter, in your internal environment and under active development, and even APIs that support your mobile devices. The scanner will detect OWASP's top 10 risks such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF) and unvalidated redirection. Authenticated, complex and progressive scans are supported. With programmatic scanning of SOAP and REST API services, this scanner tests IoT services and APIs used by mobile apps and modern mobile architectures.

How does it work?

Once your order is received, a member of our customer experience team will take ownership of your order and contact you to introduce themselves. We will then:

- Arrange a technical scoping call between a member of our Red Team and your organisation's IT team (or your managed service provider (MSP)) to confirm the configuration of your network and your exact requirements.
- Document the scope of the penetration test assessment service and ask you to agree and sign off.
- Agree a testing window with you in which the test(s) will be conducted. The testing team will be on call throughout the testing, and available for any questions that may arise during the test.

Once the assessment has been completed, we will provide you with a report detailing the findings of the above tests, as well as remediation steps and/or best practice recommendations to address any issues found.

We will offer you the opportunity to review the results of your test with the testing team to help you understand exactly what vulnerabilities were discovered, how they could be taken advantage of, and how to remediate these vulnerabilities.

If requested, will offer a free re-test on all 'Critical' and 'High' category vulnerabilities to ensure that they have been remediated. The service only includes re-tests that occur within 90 days of the date the report is provided.

Service Availability

The Penetration Testing services are available during UK business hours, Monday to Friday 9:00 to 17:30hrs, excluding public holidays.

The Customer Experience and Red team will be on hand to provide technical advice and assistance on any queries or issues should this be required.

Customer Responsibilities

- Customer will be responsible for confirming the scope and systems for the Penetration test.
- The Customer will be required to authorise access for Norm's testers to access the systems in scope (and obtain approval from affected 3rd parties for external systems) before the commencement of the assessment(s).