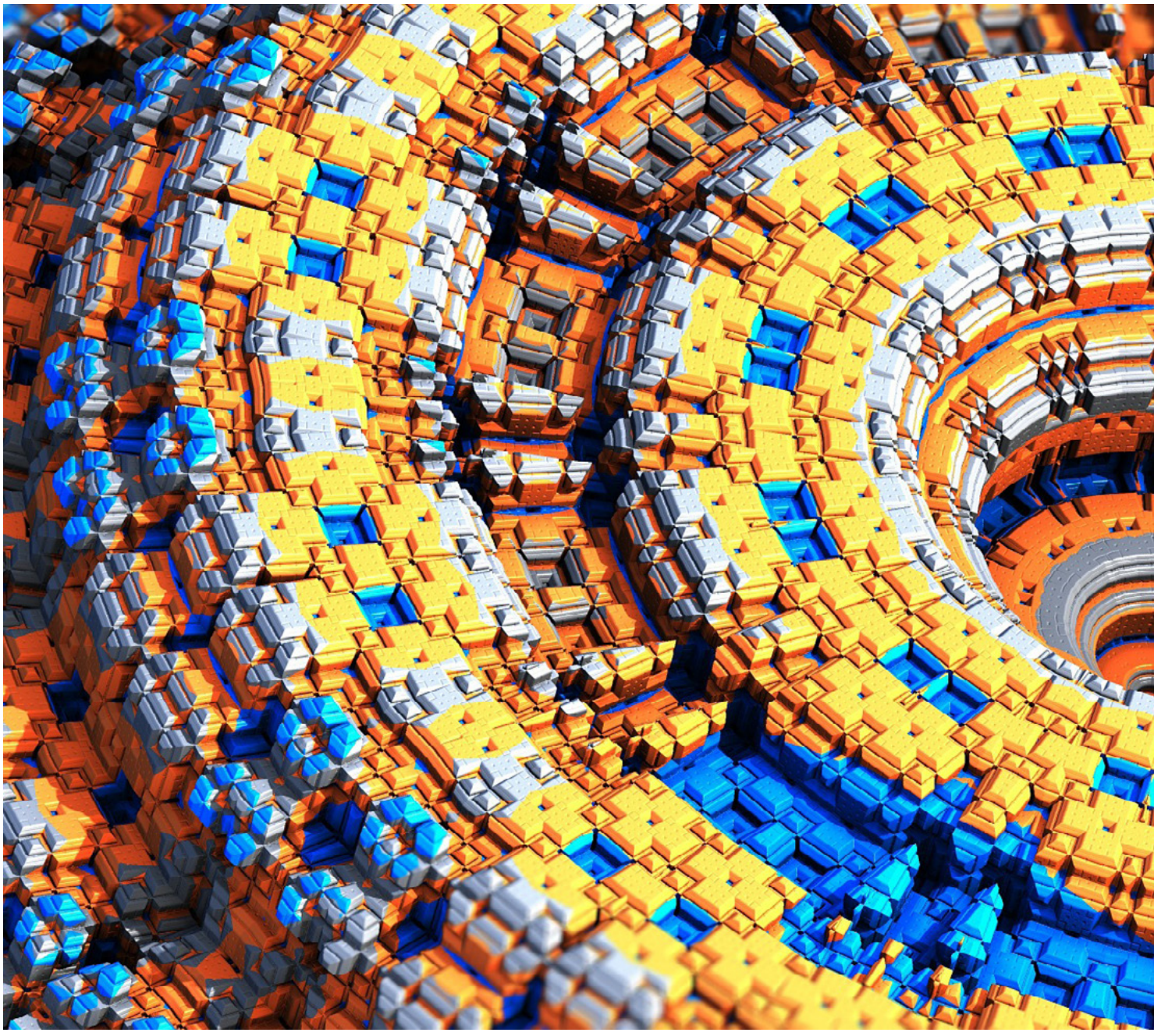
Audit • Advisory • Tax

BDO IN SOUTH AFRICA

CYBER LAB SERVICES

Vulnerability assessments and penetration tests



CONTACT US

Graham Croock
gcroock@bdo.co.za
T 011 488 1700

Georgia Adams
gadams@bdo.co.za
T 011 488 1700

OUR METHODOLOGY

BDO CYBER AND FORENSICS LAB MIMICS AN ATTACKER SEEKING TO ACCESS SENSITIVE ASSETS BY EXPLOITING SECURITY WEAKNESSES EXISTING ACROSS MULTIPLE SYSTEMS.

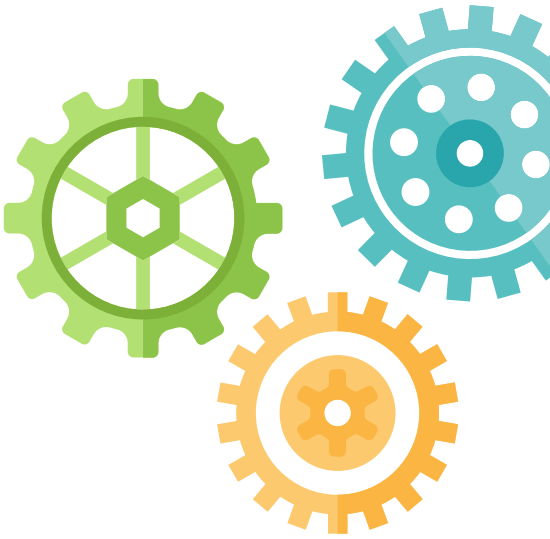
WHILE WE ARE GUIDED BY BEST PRACTICE STANDARDS SUCH AS NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), SYSADMIN, AUDIT, NETWORK AND SECURITY (SANS), AND OPEN WEB APPLICATION SECURITY PROJECT (OWASP), OUR VULNERABILITY AND PENETRATION TESTING APPROACH HAS BEEN TESTED, REFINED AND CUSTOMISED OVER TIME. THE METHODOLOGY NOTED BELOW PROVIDES A HIGH-LEVEL OUTLINE OF OUR PROVEN PENETRATION TESTING PROCESS.

THIS METHODOLOGY CAN BE AUGMENTED BY ADVANCED THREAT MODULES (ATM) THAT INCLUDE, BUT ARE NOT LIMITED TO, OUR STEALTH TESTING MODULE, MANAGED SECURITY SERVICE PROVIDER TESTING MODULE, INTRUSION DETECTION SERVICES OR INTRUSION PROTECTION SERVICES EFFECTIVENESS AND TUNING MODULE, PSEUDO-MALWARE MODULE, DISTRIBUTED METASTASIS MODULE, SOCIAL ENGINEERING MODULE, AND MANY MORE.

BDO Cyber and Forensics Lab's penetration testing services identifies vulnerabilities and reveals how networks designed to support normal business operations can provide attackers with pathways to back-end systems and data. During the engagement, we begin by assessing your network or application infrastructure's weakest links and other possible vectors of attack. We then determine the ramifications of each compromise by attempting to escalate privileges on the entry points and pivoting to determine whether any other systems can be subsequently targeted and breached.

STEP 1
Logistics and controls

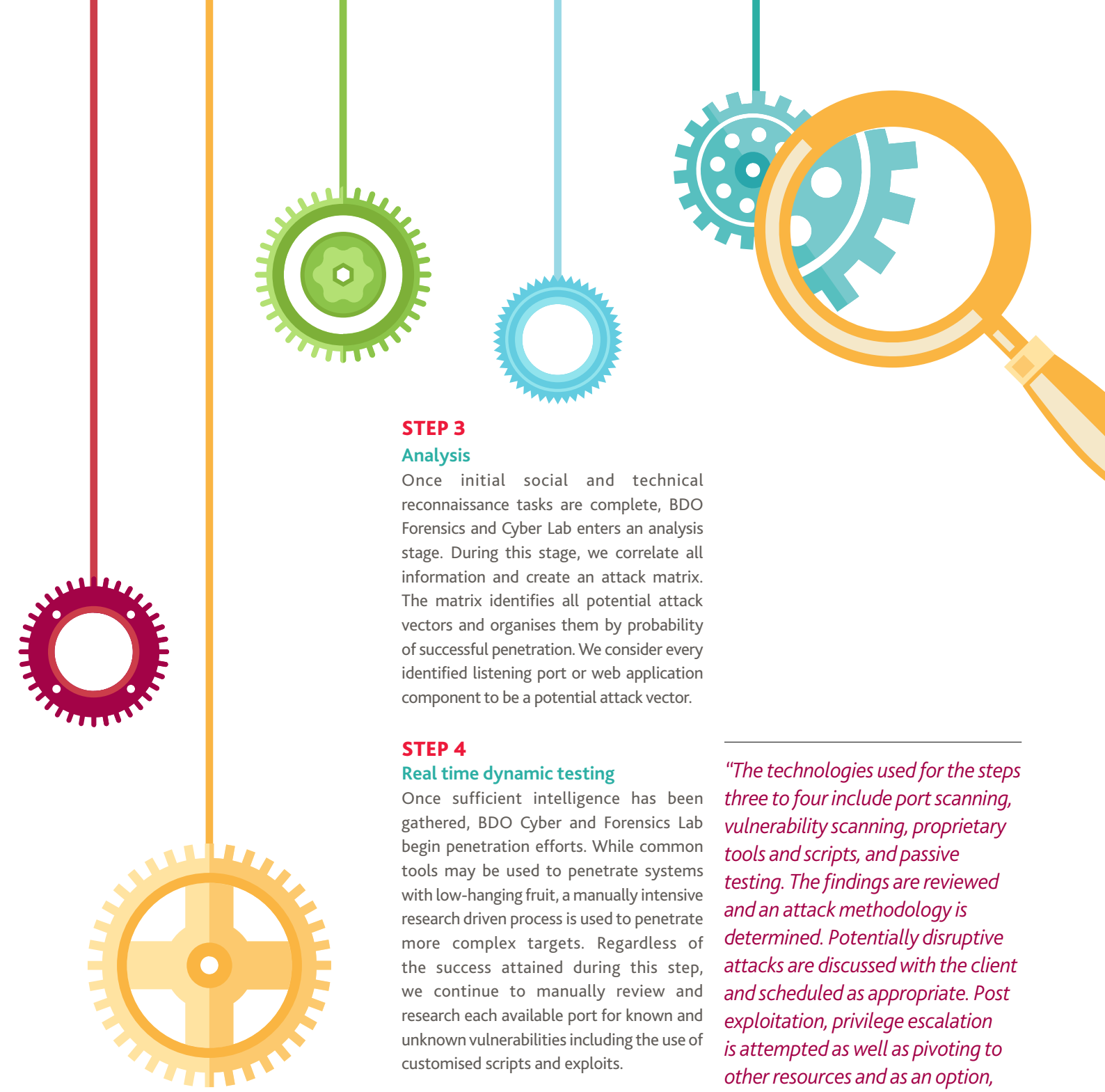
Logistics and controls are important yet often overlooked components of delivering quality penetration tests. They aim to reduce the rate of false positives and false negatives by making proper adjustments to all testing modules prior to its launch. This module is perpetual by continuing to run during the entire course of testing in order to identify any issues that may exist before testing, or to identify network or system state changes during testing.



STEP 2
Advanced reconnaissance

We begin all penetration tests with a combination of social and technical reconnaissance. Social reconnaissance (not to be confused with social engineering) is focused on extracting information from personal websites, social networking sites (like LinkedIn and Facebook), technical forums, internet relay chat rooms, company job opportunities, documents that have been leaked or published, and more. The goal is to identify information that might assist in compromising the target. Historically, this information has included source code, confidential files, passwords, and troubleshooting questions about IT issues, amongst other sources of information.

Technical reconnaissance focuses on the discovery of hosts, service fingerprinting, configuration analysis, web server directory enumeration, the identification of administrative and customer portals, the identification of hidden endpoints, such as cable modems or DSL lines, the use of third party services provided by hosting providers, managed security service providers, and much more. Technical reconnaissance may or may not use port scanners, web application scanners, vulnerability scanners, and others depending on the threat and intensity levels of the service being provided.



STEP 3

Analysis

Once initial social and technical reconnaissance tasks are complete, BDO Forensics and Cyber Lab enters an analysis stage. During this stage, we correlate all information and create an attack matrix. The matrix identifies all potential attack vectors and organises them by probability of successful penetration. We consider every identified listening port or web application component to be a potential attack vector.

STEP 4

Real time dynamic testing

Once sufficient intelligence has been gathered, BDO Cyber and Forensics Lab begin penetration efforts. While common tools may be used to penetrate systems with low-hanging fruit, a manually intensive research driven process is used to penetrate more complex targets. Regardless of the success attained during this step, we continue to manually review and research each available port for known and unknown vulnerabilities including the use of customised scripts and exploits.

STEP 5

Reporting

To conclude the project, a collation of all the findings are submitted for review.

"The technologies used for the steps three to four include port scanning, vulnerability scanning, proprietary tools and scripts, and passive testing. The findings are reviewed and an attack methodology is determined. Potentially disruptive attacks are discussed with the client and scheduled as appropriate. Post exploitation, privilege escalation is attempted as well as pivoting to other resources and as an option, persistent backdoor access is created as proof of concept."

OUR SERVICES

When conducting vulnerability and penetration tests, the objective of the BDO Cyber and Forensics Lab is to:

- Identify and prioritise known security vulnerabilities
- Test your organisation's ability to detect and respond to attacks
- Identify and address vulnerable attack vectors
- Assess the operational impact of successful attacks
- Review regulatory compliance
- Review effectiveness of current security spending
- Test and advise the client on a layered security approach

The components of our testing service include the following:

INTERNAL WHITE-BOX TESTING OF THE ENTIRE INFRASTRUCTURE

- All servers (physical and virtual)
- All client machines (a random selection, and all client machines to be considered in scope)
- All networking devices including routers, switches, IDS/IPS, VOIP servers/VLANs etc
- Password cracking of current server hashes as proof of concept (POC) and test of password policies
- Deep packet inspection to find anomalous packets/PII/passwords transmitted in plain text

EXTERNAL WHITE-BOX TEST OF UP TO 20-IP ADDRESSES

- All internet facing ports
- All support infrastructure, including databases (MSSQL/MYSQL) and hosting software (Apache/IIS)
- Denial-of-service attacks at a mutually agreed upon time as POC

DEEP PACKET INSPECTION

The test team connects a machine to the network which captures all packets flowing through the switch for a period of 24 to 48-hours. We then review those packets in our lab looking for unencrypted sensitive information, including:

- Login credentials
- Plain text emails
- Sensitive data being sent unencrypted across the network and onto the internet
- Anomalies (such as back-doors) on the network

This will allow the client to prove with data, which intended systems are transmitting packets using encryption and that best practices are being practically implemented.

CRYPTOGRAPHY

Using supplied administrative credentials, the test team pulls password hashes from the server and attempts to crack those passwords in our lab. This testing is conducted in two phases: firstly, dictionary attack to locate poor passwords; secondly, brute force of all passwords with 9-characters or less. This allows administrators to gauge the effectiveness of password policies and whether users are following best practice guidelines when choosing passwords.

SOCIAL ENGINEERING

Social engineering is a technique that relies on the manipulation of people to gain access to resources that should be off limits to the attacker. These attacks rely on helpful human nature to succeed and are exceptionally popular with knowledgeable attackers.

External

The test team endeavours to mislead users into clicking email links, downloading files or by other means execute software which allows us to gain access to those client machines. We have the ability to use either active (live) payloads or passive (POC) payloads as per client preferences. Phishing attacks are conducted at 5-levels of increasing legitimacy to allow accurate assessment of current staff training.

Internal

The test team endeavours to gain physical access to the infrastructure, bypassing access control and security, and place a device on the network, plug it in and execute software on unlocked workstations and gain access to sensitive information.

OUR SERVICE PACKAGES

AS A COST EFFECTIVE INFORMATION SECURITY SERVICE, BDO CYBER AND FORENSICS LAB HAS INTRODUCED A NEW SERVICE WHICH AFFORDS YOUR ORGANISATION CONTINUOUS INFORMATION SECURITY MONITORING FOR A PERIOD OF TWO YEARS.

THREE SEPARATE PACKAGES HAVE BEEN DEVELOPED, EACH WITH DIFFERENT SERVICES THAT BEST SUIT YOUR RISK APPETITE. A DESCRIPTION OF EACH SERVICE FOLLOWS. SPEAK TO US ABOUT PRICING ON THESE PACKAGES, SHOULD YOU PREFER TO SECURE YOUR ORGANISATION MORE VIGILANTLY OVER A CONTRACTUAL PERIOD OF TWO YEARS INSTEAD OF A ONCE-OFF VULNERABILITY/ PENETRATION TEST.

	Bronze	Silver	Gold
New Risk Notification	√	√	√
External Vulnerability Scan	√	√	√
Internal Vulnerability Scan	√	√	√
Consultation Services		√	√
Training		√	√
Forensic Audits		√	√
External Penetration Test			√
Internal Penetration Test			√

NEW RISK NOTIFICATION

New risks and vulnerabilities are continually being discovered by the security community at large. Our research team not only keeps abreast of these discoveries and notifies our clients immediately as these new risks are identified but also set up labs to test those exploits in an effort to better understand the scope and limitations of those exploits. All this is done in order to be able to explain, in detail, to our clients how the new risk affects them and how to manage that risk until such time as software developers release updates to address the problem.

EXTERNAL VULNERABILITY SCANS

Once every two weeks the external (internet) facing network is scanned by multiple industry leading vulnerability scanners. The external facing network is the most likely target for hackers since it is relatively easy to remain anonymous across the internet while attacking companies. There is very limited risk to the attacker in these situations if the attacker is knowledge and because of this, it is the most common attack vector.

INTERNAL VULNERABILITY SCAN

BDO scans the internal network every three months to identify risks from inside the Local Area Network (LAN). We notify the client of what information is available on the network with different levels of authentication. We also check the infrastructure for viruses, malware, back-doors, misconfigured devices, and devices that are not currently with software and firmware updates. BDO scans the client infrastructure with multiple industry leading vulnerability scanners. These scans assist in preventing attacks by identifying vulnerabilities and configuration issues that hackers could use to penetrate the infrastructure. A few of the many possible issues that are detected include:

- Viruses and malware
- Botnets
- Open ports
- Known vulnerabilities
- Web services serving malicious content
- Back-doors
- Unknown processes
- Missing patches and updates
- Misconfigurations

These scanners are continually updated to identify the newest risks and vulnerabilities as they are discovered by researchers. By scheduling these scans on a mutually agreed upon time and date we avoid operational impact and allow technical staff to identify scans originating from BDO as opposed to other malicious vectors. Our security experts review every report and will contact the responsible person directly if a serious issue is detected.

EXTERNAL VULNERABILITY SCAN

A full external penetration test is conducted every six months. A red team tries to exploit every part of the internet facing network. We not only try to breech the firewall, but also attempt to gain access to the internal network. External testing includes Social Engineering tests conducted during external penetration tests, as well as at random times during the agreement period, keeping staff "on their toes". Testing may include all supporting infrastructure (unless indicated otherwise by the client) including but not limited to:

- Web research
- Databases
- Access control
- VPN access
- Firewalls
- Routers
- Connectivity
- Mobile devices
- Applications
- Client computers

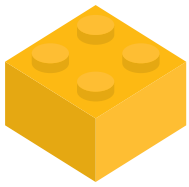
Denial of service testing will be conducted (unless specified otherwise by the client) after hours to limit the collateral impact of these tests. Please note that we require a technical staff member on site to verify the tests and resolve any unexpected occurrences (usually restarting a router or firewall). A penetration test takes testing a step further than a vulnerability scan. Instead of simply identifying risks for the client to resolve, the pentest team actively tries to exploit those risks and vulnerabilities, simulating what a knowledgeable black hat (or bad guy) hacker could potentially access. Every single open port of every single IP address is actively tested with the goal of bypassing security systems and gaining access to unauthorised systems and infrastructure. This is a time intensive process, heavily dependent on expertise in information security and many different fields within the information technology field.

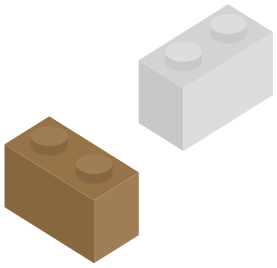
GOALS

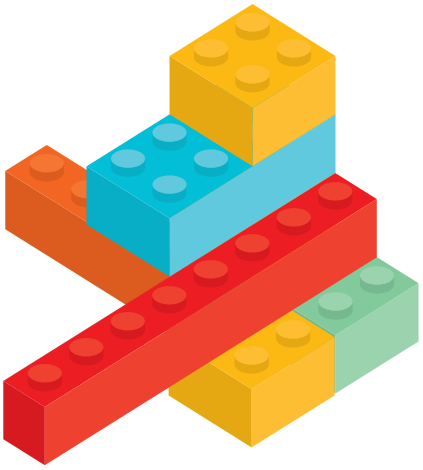
- Identify and prioritise known security vulnerabilities
- Test ability to detect and respond to attacks
- Identify and address vulnerable attack vectors
- Assess operational impact of successful attacks
- Review regulatory compliance
- Review effectiveness of current security spending
- Test and advise on layered security approach

BENEFITS

- Superior risk management
- Increased business continuity
- Reveal security flaws
- Protect clients, partners, third parties and staff
- Minimise and limit client side attacks
- Evaluate security investment
- Protect public relationships and brand continuity







INTERNAL PENETRATING TESTING

Every 6-months, BDO conducts a full internal penetration test. We attempt to gain access to resources without any access (simulating a wireless or plug-in breach), with user-only access (what can a knowledge attacker, posing as a new staff member, access on the infrastructure), or as an administrator (are systems configured optimally).

Every branch and satellite office should be tested from within its local network. The report produced from these tests provides an exceptionally detailed view of the infrastructure. Internal penetration testing includes social engineering exercises, deep packet inspection and password cracking. Testing may include all supporting infrastructure that use IP-addresses including research, servers and databases, access control, MD5 hashes, firewalls, routers, UPS and inverter devices, connectivity devices, mobile devices, applications (limited internal app testing), routers and switches, printers, client computers, social engineering, denial-of-service attacks.

TRAINING

It is generally understood by the security community that staff members are the weakest link of any security posture. We can spend a wealth of time and money on security only to have a user bypass it all by giving away crucial information. At BDO we believe that training is of critical importance for all staff members that have access to computers, and with that in mind we offer training for general staff members.

Our immensely popular "Meet the hacker" presentation is a 1-hour training session that aims to teach all staff members the basics of keeping information safe, both within the company, and in t heir personal capacity. Presented from the point of view of the "hacker", we illustrate with examples, different exploits used in order to gain unauthorised access. While heavily focused on social engineering, it also covers many of the other vulnerabilities users face. Included in this agreement is a training session per year for every staff member, including satellite offices with ten or more staff members within South Africa.

FORENSIC AUDIT

Even the most diligent, security conscious companies have been breached due to zero day attacks. These are vulnerabilities that have been uncovered by black hat hackers but have not been discovered by the information security community. Should a breach occur, despite our best efforts, BDO will provide a well-trained, respected authority in the security community to conduct a forensic audit at no additional cost. The auditor will attempt to:

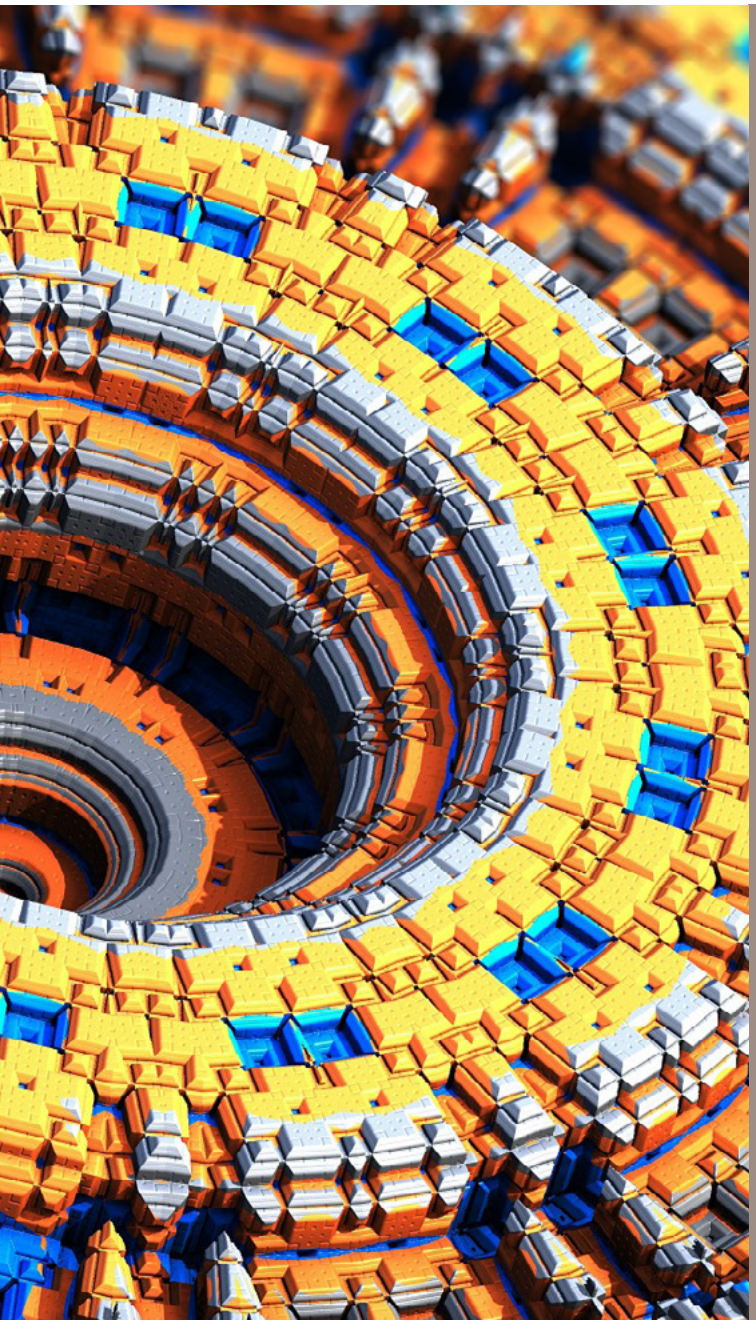
- Identify attackers
- Identify the means and the time span of the breach
- Determine the impact to the organisation
- Collect evidence in such a way as to be admissible in legal proceedings should the organisation wish to prosecute
- Advise on corrective action regarding controls that may have failed

ON-GOING CONSULTATION SERVICES

BDO offers limited additional consultation services including:

- 24/7 telephonic support related to information security
- 24/7 email support related to information security
- Review or creation of information security policies, such as:
  - End-user security policy
  - Acceptable use policy
  - Clean desk policy
  - Email policy
  - Ethics policy
  - Password construction guidelines
  - Password protection policy
  - Software installation policy
  - Technical security policy
  - Security response plan
  - Remote access policy
  - Wireless communication policy
  - BYOD
  - Server security policy
  - Router and switch policy
  - Firewall policy
  - Information logging standards
  - Change control policy
  - Disabling accounts for users who have left

Unfortunately, additional services like data loss prevention and security framework implementation cannot be included by default and will need to be managed separately.



WE TAKE IT PERSONALLY. FOR FURTHER INFORMATION, PLEASE CONTACT US:

GRAHAM CROOCK
Director
gcroock@bdo.co.za
T 011 488 1700

GEORGIA ADAMS
Senior Manager
gadams@bdo.co.za
T 011 488 1700

/BDOSouthAfrica /bdoafrica /bdo_sa /company/bdo-south-africa

BDO

www.bdo.co.za