SecureTeam

G-Cloud 13 Service Definition Document

information. secured.

1.1 WEB APPLICATION PENETRATION TESTING

Using a combination of automated and manual testing, our consultant(s) will conduct a thorough assessment of the web application(s), identifying vulnerabilities that may be exploitable by unauthenticated users.

All application testing will be conducted in line with the current standards and methodologies produced by the Open Web Application Security Project (OWASP). At a minimum, we will concentrate on the following OWASP Top-10 vulnerabilities that commonly affect web applications:

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control
- Security Misconfiguration
- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Using Components with Known Vulnerabilities
- Insufficient Logging & Monitoring

In addition to the common vulnerabilities listed above, we also conduct testing around the following areas:

- Information Gathering
- Configuration & Deployment Management
- Identity Management
- Authentication
- Authorisation
- Session Management
- Input Validation
- Error Handling
- Cryptography
- Business Logic
- Client-Side Scripting

The use of automated tools & scripts combined with an in-depth manual testing approach, allows us to efficiently & accurately test your application and maximise the level of testing that can be performed in the time available.

1.2 MOBILE APPLICATION PENETRATION TEST

Using a combination of automated and manual testing, our consultant(s) will conduct a thorough assessment of your mobile application(s), identifying vulnerabilities that may be exploitable by malicious users.

All application testing will be conducted in line with the current standards and methodologies produced by the Open Web Application Security Project (OWASP). Using OWASP's Mobile Application Security Verification Standard (MASVS), we will concentrate on the following OWASP Top-10 vulnerabilities that commonly affect mobile applications:

- Improper Platform Usage
- Insecure Data Storage
- Insecure Communication
- Insecure Authentication
- Insufficient Cryptography
- Insecure Authorisation
- Client Code Quality
- Code Tampering
- Reverse Engineering
- Extraneous Functionality

In addition to the common vulnerabilities listed above, we also conduct testing around the following areas:

- Architecture, design and threat modelling
- Data Storage and Privacy
- Cryptography
- Authentication and Session Management
- Network Communication
- Platform Interaction
- Code Quality and Build Settings
- Resiliency Against Reverse Engineering

The use of automated tools & scripts combined with an in-depth manual testing approach, allows us to efficiently & accurately test your application and maximise the level of testing that can be performed in the time available.

1.3 EXTERNAL NETWORK PENETRATION TEST

Using a combination of automated and manual testing, our consultants will inspect your Internet-exposed services to assess if vulnerabilities are present that could allow them to be exploited by a malicious user.

Our external penetration testing comprises the following stages, which are representative of a real-life attack:

- Passive Reconnaissance
- Network Enumeration
- Active Testing

Passive Reconnaissance

During the initial stages of a real-life attack, malicious users will spend time performing reconnaissance, so that a profile or 'footprint' of the target organisation can be obtained. Information such as the IP addresses in use, hostnames and employee information can greatly assist an attacker in choosing an effective attack method and may help identify areas of the target organisation's infrastructure that would render the highest impact if compromised.

Public databases and information services can contain a wealth of information that may prove useful to an attacker. Most these information sources can be freely and passively accessed and with these information sources residing in the public domain, there is no chance that the searches performed by an attacker will trigger alerts that may notify the target organisation that an attack is being planned.

During this phase of the testing, the following public information sources will be accessed to obtain further information about the target organisation:

- RIPE Database
- WHOIS Database
- Domain Name Servers

Network Enumeration

Once an attacker has built a profile of the organisation through passive information gathering, they will attempt to identify 'live' hosts and services within the IP address range. Once an understanding of the exposed ports and services is obtained, this will give the attacker more information on potential vulnerabilities that may allow them to gain a foothold on the network and further their attack.

During this phase of the test, a full TCP and UDP port scan of all 65,535 ports will be conducted over the in-scope IP range. An ICMP scan will also be conducted, to identify which hosts would disclose their presence to an attacker who performs a simple 'ping' scan.

Active Testing

Based on the results of the Network Enumeration phase, a vulnerability assessment and targeted penetration test will be conducted on all Internet-exposed services. All results of the vulnerability assessment will be manually verified to ensure that no 'false positive' results are present.

All exposed services will be manually inspected by connecting to them and attempting to gain access through known exploits.

At the end of the test, you will be provided with a full report that explains the vulnerabilities in full and the corrective actions that should be taken. A risk-based approach is used throughout the report and all vulnerabilities are scored in line with CVSS (Common Vulnerability Scoring System). This allows the contents of the report to be fed into your own internal risk assessments and allows a plan to be developed to address the vulnerabilities which present the highest risk to your environment.

Subnet Discovery Scan

As part of the agreed testing scope, an automated subnet discovery scan will be conducted over all Internet-facing subnets that are in use by the organisation. The purpose of this assessment is to identify ports and services which may be open to the Internet that may not be known about or authorised by the organisation. This allows the organisation to check for unauthorised network services that may be exposed on the Internet and modify firewall rules to reduce the organisations attack surface.

1.4 INTERNAL NETWORK PENETRATION TEST

An Internal Penetration Test is crucial in identifying the vulnerabilities that may be present to a malicious user who has gained access to your corporate network.

Using a combination of automated and manual testing, our consultants will inspect your internal servers, workstations and other network hosts to assess if vulnerabilities are present that could allow them to be exploited by a malicious user.

Manual testing will be conducted against all vulnerabilities that are identified to determine the level of access that an attacker could obtain if the vulnerabilities were to be exploited in a real-life scenario.

Typical vulnerabilities which may be identified during an Internal Penetration Test include the following:

- Missing Security Patches
- Outdated Software & Operating Systems
- Unauthorised Software Installation
- Weak or Default Passwords
- Weak Encryption Ciphers & Protocols
- Weak File Permissions
- Vertical & Horizontal Privilege Escalation
- Vulnerable System Services
- Network Protocol Vulnerabilities (e.g. SMB, SNMP & SSH)
- Unencrypted Network Traffic
- Information Disclosure
- Microsoft Remote Desktop Vulnerabilities
- Firewall Bypass Vulnerabilities
- Lack of Data Leakage Protection (DLP)

Usually, the ultimate goal of a malicious insider is to locate vulnerabilities that could allow them to obtain Domain Administrator rights on the corporate Windows Domain. During the assessment, specific tests will be conducted that represent the latest techniques that an attacker is likely to use in enumerating information and then exploiting services that could allow for a full Domain compromise.

At the end of the test, you will be provided with a full report that explains the vulnerabilities in full and the corrective actions that should be taken. A risk-based approach is used throughout the report and all vulnerabilities are scored in line with CVSS (Common Vulnerability Scoring System). This allows the contents of the report to be fed into your own internal risk assessments and allows a plan to be developed to address the vulnerabilities which present the highest risk to your environment.

If we have been able to compromise your Active Directory Domain during the test, a full, step-by-step process will be documented which allows you to identify the combination of vulnerabilities that allowed the compromise to take place.

1.5 WIRELESS PENETRATION TEST

Due to the fact that wireless networks can often be accessed from outside of an organisation's physical premises, wireless networks can introduce a significant risk into organisations if not configured correctly.

Typical vulnerabilities that are often found in wireless networks include:

- Easily-guessable user credentials or Pre-Shared Keys (PSK)
- Poor segregation between wireless clients
- Lack of network segregation between multiple SSIDs
- Sensitive information exposure
- Weak network traffic encryption
- Wireless clients susceptible to rogue wireless access points

A penetration test will be conducted against the organisation's wireless network(s). The purpose of this assessment is to identify the level of access that a malicious user could achieve if they have been able to position themselves within range of the organisation's wireless access points.

Depending on the types of wireless networks in use, our consultants will use a combination of automated and manual testing, with the goal of achieving network connectivity to your organisations network through vulnerabilities that may be present.

During the assessment, a 'rogue' wireless access point will be deployed to identify if wireless clients are susceptible to connecting to a malicious access point that has been set up by an attacker.

For wireless networks that use WPA-Enterprise authentication, a configuration review will be performed on a sample wireless client (such as a laptop), as weaknesses in WPA-Enterprise authentication are not always apparent from passive information gathering.

1.6 SERVER BUILD REVIEW

A build review of your organisations servers is a 'white-box' assessment which provides you with a rigorous benchmark of the operating system configuration – comparing the results against industry-recognised security hardening standards.

Using a combination of automated compliance tools and manual inspection our consultant will perform an in-depth review to assess your server's resilience to attack.

In addition to the hardening guidance from the Center for Internet Security (CIS) and Microsoft Security Baselines, we include additional configuration checks during the build review that have been derived from our own experience of environments and specific attack vectors that have been identified by our consultants during penetration tests.

Specifically, the following areas of the Windows server are covered by this review:

- Anti-Virus Protection
- Password Policy
- Account Lockout Policy
- Audit Policy
- Interactive Logon
- Network Security Settings
- User Account Control
- User Accounts
- Passwords
- Services
- File Shares
- Microsoft Operating System Patches
- Vulnerability Assessment
- Windows Firewall
- Network Port Scan

1.7 CLOUD SERVICES CONFIGURATION REVIEW

A configuration review of your Cloud environments provides assurance that the environment has been configured securely and does not contain configuration vulnerabilities that may result in data leakage or exposure to known vulnerabilities and threats.

Our Microsoft 365 configuration review is based on the current Microsoft security best practice guidelines. This ensures that your organisations emails and data is protected with a high level of security and ensures that you are taking advantage of the latest protective mechanisms that Microsoft has available at the time of the assessment.

During the review, our consultant(s) will conduct a thorough assessment of the following areas of your organisations Microsoft 365 environment:

- Azure Active Directory
- Endpoint Manager (InTune)
- Microsoft Teams
- Exchange Online
- Data Loss Prevention

Our configuration review is based on the Microsoft Azure security hardening benchmark which is produced by the Center for Internet Security (CIS), alongside the current Microsoft security best practice guidelines. This provides a rigorous assessment of your Azure environment and ensures that it has been configured in line with industry-recognised security standards.

Using a combination of automated and manual testing, our consultant(s) will conduct a thorough assessment of your Azure environment, which covers the following areas:

- Identity & Access Management (IAM)
- Security Center
- Storage Accounts
- Database Services
- Network Controls
- Logging & Monitoring
- Encryption
- Certificate & Key Management
- Network Segregation
- Perimeter Network Security
- Data Backup
- Virtual Machine Configuration
- Operational Security Practices
- AppService Configuration

1.8 OPEN SOURCE INTELLIGENCE (OSINT) ASSESSMENT

Open Source Intelligence gathering will be conducted to ascertain the information that is available in the public domain on the target organisation.

Specific information, such as email addresses and telephone numbers will be obtained for staff, as these are useful to an attacker when performing a remote social engineering exercise.

Sources of public information that will be checked during the assessment will include:

- LinkedIn
- Facebook
- Twitter
- Organisations website
- Publicly-available documents (including hidden metadata)
- Professional forums
- WHOIS & RIPE Information

At the end of the assessment, we will provide a full and complete report that highlights the information that could be obtained about the organisation in the time available and suggestions on how sensitive information can be restricted from the public domain.

1.9 PHYSICAL SOCIAL ENGINEERING

Physical Social Engineering provides an assessment of your organisation's physical perimeter to assess how resilient your staff and the access-control methods are to a social engineering attack by a malicious 3rd party.

After an initial reconnaissance phase (and very often combined with Open Source Intelligence (OSINT) gathering), attempts will be made to obtain access into the physical office space of your organisation through a range of creative methods.

Typical access methods that might be employed during the assessment may include 'tailgating' through external doors behind staff members, cloning access cards or setting up appointments with members of staff within your organisation that could grant the consultant a legitimate reason for being within the building.

Sensitive areas would be specifically targeted (such as HR & Legal departments or server rooms), as these are considered by malicious users to contain high value assets.

At the end of the assessment, you will be provided with a report which outlines the security weaknesses that were identified within your organisations internal security processes or through staff negligence. Where a perimeter security breach was successful, we will provide you with a timeline of the events leading up to and during the breach, so that you can pinpoint where your processes require strengthening or where staff require security awareness training.

1.10 TELEPHONE SOCIAL ENGINEERING

Despite the fact that the majority of social engineering attacks originate through email, a large percentage of online scams are facilitated through telephone social engineering. This could be an attacker calling a user and requesting access to their computer or asking them to divulge their credentials over the phone.

During a Telephone Social Engineering assessment, our consultancy team will make telephone calls to users within your organisation in an attempt to get them to divulge information which could be considered confidential. Based on the information obtained, we will then attempt to further the attack on your organisation, so that it is representative of a real-life scenario. For example, if our consultants are able to obtain usernames and passwords, we may attempt to connect remotely to your organisation's network through a VPN gateway.

At the end of the assessment, you will be provided with an understanding of the conversations that took place and a report which individuals are susceptible to social engineering by telephone.

1.11 EMAIL PHISHING ASSESSMENT

Over the past few years, spear-phishing attacks are the number one method that attackers are using to infiltrate the perimeter defences of an organisation with malware or as a method in which to coerce employees into divulging sensitive information.

An email phishing assessment is a highly effective way in assessing if individuals within your organisation are susceptible to targeted spear-phishing attacks, through a number of attack scenarios that have been observed to be in use by attackers and criminal gangs in real life.

While we are extremely versatile in this area, the following are some example scenarios that could be delivered in the time scoped for the testing:

1. Emails may be sent into organisation that pretend to be from the organisation's IT department. The email will request that users log into a fake web portal to check that a newly built email server is working correctly. The portal would be hosted on our servers and would harvest the credentials that were input by the user. Harvested credentials would then be used to attempt access to externally-facing services such as Outlook Web Access, VPN, Citrix etc.

2. Emails may be sent that inform staff that an employee discount portal has been set up to get discount vouchers from top brands. The portal requests the users Domain credentials and again is used to harvest credentials for further attacks. The portal can be configured to use client-side exploits against the user's browser, so that when they visit the page an attempt is made to compromise their workstation remotely.

In addition to these credential harvesting scenarios, we also have the ability to send malicious files into your organisation, which if opened on a vulnerable workstation, would allow for us to gain remote access to the user's workstation and allow a method of pivoting an attack into the surrounding infrastructure. We can also generate custom scenarios for the phishing assessment, if you feel that you would like to test for a specific area of susceptibility.

Prior to the phishing assessment taking place, we will consult with you around the type(s) of scenario that we believe to be most effective for your organisation. You have the option of providing us with a list of email addresses that you wish to be used for the assessment, or alternatively you may wish to combine this with email addresses obtained through the Open Source Intelligence (OSINT) Assessment, making the engagement more representative of a real-life spear-phishing attack.

Once the assessment has been completed, you will be provided with a full report which shows the users who opened the email, those who clicked on the malicious link or opened the malicious file and timestamped event log that also shows the IP address that the users accessed the malicious website from.

STAGGERED EMAIL PHISHING CAMPAIGN (OPTIONAL)

Sending phishing emails in bulk to multiple individuals within an organisation has the potential to trigger security alerts and can often not prove representative of a real-life attack. As an option, we can stagger the email phishing campaign over several months, using different scenarios and payloads. This allows you to identify how your organisation would respond to a real-life phishing assessment that may take place over several months.

1.12 ISO 27001 GAP ANALYSIS

An ISO 27001 Gap Analysis allows you to benchmark your organisation's policies and technical controls against the ISO/IEC 27001:2013 standard, before you apply to an ISO 27001 Certification Body to become accredited. The Gap Analysis allows you to identify areas in your organisation's processes, policies and technical controls, which may prevent your organisation from achieving ISO 27001 accreditation – enabling you to implement the necessary control measures and be fully-prepared for the final audit.

The following elements make up the overall assessment process:

- Cyber Risk Assessment
- Gap Analysis Workshop
- Documentation Review

1.12.1 CYBER RISK ASSESSMENT

A Cyber Risk Assessment identifies the level of risk that is associated with the types of threats which affect your organisation's information assets.

Using a workshop-based approach, our consultant(s) will help your organisation identify the types of information assets that you have, such as workstations, servers, database or cloud-based services such as Microsoft 365. For each of your information asset categories, we provide insight into the real-world threats that can affect the confidentiality, integrity or availability of your organisation's data or services.

When used in the context of ISO 27001 certification, a cyber risk assessment enables a risk treatment plan to be created in the form of a Statement Of Applicability (SOA), which shows the Annexe A controls that can be applied to reduce the overall risk to an acceptable level.

1.12.2 GAP ANALYSIS WORKSHOP

Through a one-day workshop, one of our ISO 27001 Certified Lead Auditors will cover each of the following control topics, as required by the latest ISO/IEC 27001:2013 standard:

- Information Security Policies
- Organisation of Information Security
- Human Resource Security
- Asset Management
- Access Control
- Cryptography
- Physical & Environmental Security
- Operations Security
- Communications Security
- System Acquisition, Development & Maintenance
- Supplier Relationships
- Information Security Incident Management
- Information Security Aspects of Business Continuity Management
- Redundancies
- Compliance

Each of the above controls (and any relevant sub-controls) will be discussed throughout the workshop, to ascertain if your organisation is compliant with what is required by the standard, or if additional work is required before you initiate the accreditation process.

1.12.3 DOCUMENTATION REVIEW

With documented policies and procedures forming a large part of ISO 2700 certification, it is imperative that your organisations documentation is written and structured in a way that clearly outlines your organisation's cyber security controls in a way which can be easily understood by your employees and stakeholders.

Our consultancy team will conduct a detailed review of your existing documentation that is relevant to ISO 27001 certification – providing recommendations and suggestions that will both satisfy the certification requirements and will further strengthen your organisations policy controls.

1.13 HARDWARE SECURITY ASSESSMENT

A targeted Hardware Security Assessment will be performed against a device. The purpose of this assessment is to identify vulnerabilities that may be compromised by an attacker if they have physical access to one of the wristband devices.

During the scoping phase, the following attack vectors were identified in the wristband device that may be targeted by an attacker:

- Device Firmware & BIOS
- Boot Process
- JTAG Debugging Interface(s)
- Smart-Card Interface
- Disabled or Unused Functionality
- Storage Devices
- Physical Device / Enclosure
- Printed Circuit Board(s)
- Communication Interfaces

The following sections cover each of the above hardware attack vectors that may be targeted by a malicious user:

1.13.1 DEVICE FIRMWARE & BIOS

The device firmware and BIOS (Basic Input Output System) will be inspected to identify potential attack vectors that could allow the device to be compromised. Typical attacks may include forcing the device to boot into a different operating system to allow specialised tools to be used by an attacker or attempting to reflash the BIOS if the device to allow malware or backdoor trojan applications to be inserted into the BIOS software. The firmware(s) and BIOS versions will also be assessed to identify if published vulnerabilities are available that may allow the firmware or BIOS to be compromised through specially-crafted exploit code.

1.13.2 BOOT PROCESS

The device boot process will be analysed to identify ways in which this may be bypassed or exploited by a malicious user who has access to the device. Checks will be made to identify ways in which the boot process may be halted or interrupted in such a way that may allow malicious code to be inserted into the process memory space of the device, that could assist the attacker in compromising the device or the encryption used by it to communicate with accessories or remote web services.

1.13.3 ON-CHIP DEBUGGING INTERFACE

All On-Chip Debugging (OCD) debugging interfaces (such as JTAG) will be identified on the device PCB(s) and assessed to identify the level of access that this could provide to an attacker. Attempts will be made to dump the memory and program code from the device, to identify ways in which this may be bypassed. Using the On-Chip Debugging interfaces, attempts will be made to inject code into the memory space of the device to identify if the hardware could have a backdoor application installed in it.

1.13.4 SMART-CARD INTERFACE

The SmartCard reader and access cards will be assessed to identify potential security flaws in their implementation and the way in which they are used to provide access to the device and store patient information. A sample SmartCard will be examined to identify if data is being encrypted “at-rest” and if the SmartCard is used in conjunction with PKI authentication, the certificate-based authentication process will also be examined.

1.13.5 DISABLED OR UNUSED FUNCTIONALITY

The physical device will be examined to identify if there are any features that may not be implemented at the time of testing that may prove useful to an attacker. This could include “engineering” or diagnostics modes that may be exploited by an attacker to gain further information or access to the device or that may allow for administrative functionality.

1.13.6 STORAGE DEVICES

All storage devices that are used by the device will be examined to ensure that data is encrypted and that it is not possible for an attacker to obtain sensitive information from the storage devices that may relate to personal medical information or data that would allow an attack to be further on the device or the environment to which it connects.

1.13.7 PHYSICAL DEVICE / ENCLOSURE

The physical properties of the device will examined to ascertain if it provides sufficient protection against an attacker who has been able to obtain physical access to the device. If the enclosure contains tamperproof seals, these will be checked to identify ways in which these may be circumventable. The enclosure fixings will also be assessed to see if they allow access with readily available hand tools.

1.13.8 PRINTED CIRCUIT BOARDS

Once the device has been dismantled, the PCBs (Printed Circuit boards) will be examined to identify if there are any disabled ports or functionality that could be easily enabled or accessed. All ICs

(Integrated Circuits) will be examined to identify ways in which they may be reverse engineered or bypassed and an inspection of the circuit board will be performed to locate serial numbers or engineering revisions that may assist an attacker in locating publicly-known exploits.

1.13.9 COMMUNICATION INTERFACES

All communication interfaces on the device will be enumerated and assessed to find out if they permit connectivity to the operating system or the wider control system on the device. Typical interfaces that will be examined include, UART (RS-232), Ethernet, CAN Bus, Bluetooth, I^2C, SPI and Wireless (802.11). Attempts will be made to connect to all identified interfaces and checks will be made to identify the level of access that may be achievable by an attacker.