SALUS

CYBER

PENETRATION TESTING SERVICES

WWW.SALUSCYBER.COM

PENETRATION TESTING SERVICES

Network Layer Penetration Testing

This phase will take elements from vulnerability scanning and verify the vulnerabilities manually. Exploitation will occur if deemed to be safe and to identify the full risk posed. Network Layer Penetration Testing is considered to be a "traditional penetration test". Targets can include network devices such as switches and routers as well as workstations and servers.

Penetration testing of infrastructure uses a wide range of testing tools by highly skilled penetration testers who are trained to deliver a range of thorough, purpose-driven tests that will identify and exploit security weaknesses.

Security testing usually is iterative in nature, with the results of one stage being fed back into earlier stages or the testing of other targets. For example, successful exploitation could lead to further scanning, enumeration, and analysis; a username and password obtained on one target would be checked on other targets because authentication credentials are often re-used on internal networks.

Internet Facing Penetration Testing

Internet-facing infrastructure penetration testing employs the same methods and tools as internal infrastructure penetration but is performed remotely over the Internet and does not require a site visit.

As part of internet-facing testing, we will perform a footprinting exercise to discover and verify the externally facing assets.

From that point forward, the penetration test's main aims are to target and compromise identified hosts and use any access gained as a gateway into internal networks.

If remote access is gained to the internal network as part of an internet-facing penetration test, the penetration test can continue as an exploration of what resources can be accessed internally, but only at the customer's discretion.

PENETRATION TESTING SERVICES

Network Vulnerability Assessment

Network vulnerability assessments, by definition, have little or no manual verification of test results. This type of assessment is useful when an organisation wishes to assess the general security posture of many devices, applications, and systems. The results of the evaluation will help consultants to create an initial view of the risk profile of the infrastructure.

Vulnerability assessments can be conducted rapidly, and can be conducted from an appliance with network access to the targeted devices, or via an agent installed on the targeted hosts. This versatility allows the client to conduct the assessment in the most convenient possible manner.

The Salus Cyber auditors' preferred vulnerability scanner is Nessus, a commercial scanner produced by Tenable Network Security. However, customer requirements may identify a need to use a different scanner. For these cases, the team has experience of using various commercial and open-source scanners, including Qualys and Rapid7 products.

Internal Vulnerability Assessment

Internal vulnerability assessments target devices on internal networks, these assessments are conducted using credentials in order to gain a complete insight into vulnerabilities visible only from a local perspective, and to fully enumerate missing patches affecting installed software and the operating system.

Internet-facing Vulnerability Assessment

Internet-facing vulnerability assessments target hosts that have exposed network services on the internet. This is a two part assessment; initially to identify vulnerabilities visible to an unauthenticated attacker on the internet, followed by an authenticated vulnerability assessment on the local device.

This second assessment can be conducted from an internal perspective to ensure no changes to the security posture are required to conduct the assessment.

PENETRATION TESTING SERVICES

Active Directory Review

Active Directory is an integral part to most businesses; with your Active Directory environment compromised, many other critical applications are often compromised as a result. This can prove a complex task to recover from, as persistent methods can allow an attacker to revisit at any stage even with remedial actions taken. Many Active Directory environments are missed or avoided during an infrastructure refresh or new project implementation, thus compounding the problem further. An Active Directory security assessment will see your domain investigated for common security weaknesses used in domain compromise. By the end of the assessment, you will have a clear understanding of the configuration required to help secure your environment further and reduce the risk. Salus Cyber will look to investigate the following key areas:

- Administrative access review.
- User account assessment.
- Exposure to credential theft attacks.
- Role based access control.
- Active Directory compromise.
- Domain Controller security.

This test should ideally be performed within the first month of the vulnerability management programme so that any insecure Active Directory issues can be treated with the vulnerability remediation plans as part of the vulnerability management programme.

Optionally, Salus Cyber can conduct an Active Directory password audit by recovering password hashes from the domain NTDS.dit file. Hashes recovered from this file will then be run through Salus Cyber's advanced password cracking system to attempt to recover user credentials. As a result of this process, Salus Cyber can provide a list of usernames for which passwords were recoverable, as well as intelligence surrounding the recovered passwords. Please note that Salus Cyber will not correlate cracked passwords and users as a result of this audit, but compromised users and an analysis of the cracked passwords is available.

PENETRATION TESTING SERVICES

IAM Review

Due to the increasing reliance on cloud services and the identity security perimeter, an increasingly common and important question to answer is around the effectiveness of an organisation's authentication and authorisation management processes and policies.

This exercise compares the authentication process used by organisations to best-practice as defined by NCSC from a practical perspective, ensuring all services within scope of the assessment conform to the expected requirements.

Traditionally this exercise is performed against all cloud services used by the client, in addition to any services that the client accesses from the internet. This may also include a review of internal authentication mechanisms such as Active Directory or internally used applications.

This exercise commonly results in the identification of disparate or decentralised authentication systems, that places a larger burden on the user to remember credentials, and increases the likelihood of credential re-use. It can also assist with compliance with external standards and best-practices.

As part of this phase, the process and policy documentation, and any associated technical features such as Azure AD Identity Governance tasks will also be reviewed.

This is to ensure that manual processes are appropriate for the level of auditing and review required.

In addition to this, Salus consultants can leverage insight into technical controls used to perform the same function.

PENETRATION TESTING SERVICES

Lost Device Testing

Data is increasingly mobile, devices can be lost or stolen, and due to the high level of data that is stored on, or accessible from, mobile devices, the potential risks of a lost device have not been larger than now.

As a result, Salus Cyber has developed a service to comprehensively explore the potential risks of losing a device. The testing iteratively progresses from a completely shut down machine, ensuring the encryption is applied and configured appropriately, through to enumerating stored passwords in each of the users' browsers to identify what cloud or web application services might be compromised through losing the device.

This testing is considered a greybox approach, where consultants use credentials only if required to progress to the next stage in testing, ensuring a realistic set of scenarios are maintained, whilst comprehensively enumerating the risks present to your organisation and data.

Vulnerability Management

Vulnerability Management is an ongoing, proactive approach to identifying, evaluating, and closing down any known security holes, before a breach happens. By using a variety of technology and processes, it helps identify any known security holes throughout your IT environments. It forms a critical component of your security posture and resilient cyber risk management strategy.

Through our customisable reporting, we pride ourselves on aligning the program with the organisation's business needs and objectives. We can then ensure the critical points around security vulnerabilities are more valuable to senior decision makers.

We will deploy an automated process to investigate any potential areas where a hacker might look to exploit a network and identify any security holes. This can be run at any intervals needed, allowing for real-time evaluation of your security posture, in addition to providing regular snapshots of your organisation to track long-term improvement. This can result in a quick win to improving your cyber eecurity posture.

PENETRATION TESTING SERVICES

Network Device Configuration Review

A network device security assessment is an in-depth review of network devices' security posture and configuration.

Salus Cyber will undertake a comprehensive review of your network devices such as routers, switches, and other network devices in a network device build review, focusing on the operating system, port security, access control, logging, and password storage.

Device review testing is used to assess configuration quality as applied to a specific network device (or group of devices). In addition, testing considers password policies, applied software updates, and management services' configuration.

Testing aims to understand any potential avenues of attack should a malicious user gain access to the system in question.

Firewall Ruleset Review

A firewall configuration review identifies issues that may permit an attacker to exploit the firewall device itself, such as through misconfiguration of network services on the device, and issues that may affect the clients making network connections through the device.

This will involve a review of each firewall rule on the device, ensuring that firewall rules are correctly formed and conform to the requirements in the design specification.

We will also compare this to best-practice, primarily to the principle of least-privilege, ensuring that clients only have access to the resources that they require.

PENETRATION TESTING SERVICES

Wireless Network Security Assessment

Wireless network assessments are provided to allow a customer to gain an understanding of the security policies applied to their internal wireless networks. Wireless networks provide a great degree of convenience when dealing with a mobile or irregular workforce. However, such networks can also provide an attacker with a simple route of attack when they are inadequately secured.

Wireless penetration testing is primarily concerned with the identification of security vulnerabilities in wireless networks and clients. Depending on the specific objectives of the test, wireless penetration testing may include some or all the following techniques:
Footprinting of wireless access points in or around the targeted building. Similar to network infrastructure footprinting, this phase is concerned with gathering information about the wireless networks located in or around the target building, such as the number of wireless access points available, and whether any unofficial or rogue Access Points (APs) have been installed.

In this phase, attempts are made to break any encryption in use on the wireless network to gain access to the internal network. An examination of the resilience of any wireless devices discovered to typical attack techniques will take place during this phase. If access is gained to the wireless network, exposure testing may follow to determine the level of access gained. For example, whether full, unfiltered access to the corporate network has been gained, or whether further protections, such as firewalls, are in place.

Embedded Device Testing

Embedded systems testing aims to evaluate the security of a specific device, both from a network and local perspective. The consultants will initially pull methodologies in from a network penetration testing and web application testing perspective where required, before beginning to look at the system itself.

Often with embedded devices the operating system and software is held on Read-only memory, requiring specific methods to extract the data. In some circumstances this is not the case, and the consultant can recover the filesystem in a straightforward method. Once retrieved, the consultant can identify the functionality of the device through analysis of the system executables and configuration.

The consultant can then investigate the device for traditional build review vulnerabilities such as insecure authentication, hardcoded credentials, and failure to adhere to best-practices.

The aim of this test is to provide a comprehensive overview of the device from a network and local perspective, and to provide assurance around the security of the device if placed in a physically accessible location.

PENETRATION TESTING SERVICES

ICS and SCADA Testing

ICS Penetration Testing differs from regular (corporate) Penetration Testing. During an ICS test, a large emphasis is put on reducing risk, test impacts and negative side-effects on production systems. Salus Cyber consultants understand that most ICS systems are either very fragile or don't have test environments. Even a misguided network packet may cause disruption or damage for production lines. Therefore it is imperative to follow a consultative approach to ICS testing rather than an intrusive approach. This means that an ICS assessment incorporates close collaboration with on-site ICS subject matter experts (SMEs).

This holistic approach to ICS testing will consist of several elements. The elements concerning the ICS environment ('shopfloor IT') directly are as follows:

Traditional IT infrastructure such as servers, desktops, workstations, routers, and switches are part of ICS environments. Testing these infrastructure components is a vital part of each Penetration Test as the compromise of those systems can lead to un-authorised control over Remote Terminal Units (RTUs) or direct access of Human-Machine Interfaces (HMIs).

Applications are a vital part of an ICS environment. Applications exist in the form of web-applications functioning as an HMI, or as a part of an execution process within a control server. The goal of testing the applications is to identify vulnerabilities that would allow an attacker access to control servers or programmable logic controllers (PLCs).

ICS environments use various kinds of network communication. An ICS Penetration Test includes the identification of vulnerabilities that would allow an attacker to control network traffic or compromise a device through manipulating a specific protocol.

This manipulation can happen on wired networks as well as on Wi-Fi and Radio Frequency (RF) networks. RF networks may include typical SCADA components such as Bluetooth (Low Energy), Near Field Communication, ZigBee, or other, proprietary RF protocols. The testing of wired network traffic covers common ICS protocols such as DNP3, Modbus, or ICCP as well as various proprietary vendor protocols.

It is a security best practice to strictly segregate all other IT systems, such as the corporate IT environment, from the ICS IT environment. If this is not done with great care, an internal attacker from the corporate IT environment may gain access into the ICS to other IT environments. Like the other tests conducted as part of a full system assessment, exposure testing will be conducted in close collaboration with SMEs. environment. To test for this risk is the task of an exposure test. It assesses how much of the ICS environment is exposed.

SALUS

CYBER

PENETRATION TESTING SERVICES

WWW.SALUSCYBER.COM
01242 374087

CYBER ESSENTIALS CERTIFIED PLUS

THE CYBER SCHEME

Assured Service Provider
in association with
National Cyber Security Centre

CHECK
IT Health Check Service

Crown Commercial Service Supplier

ISOQAR REGISTERED

UKAS MANAGEMENT SYSTEMS
0026

Certificate Number 18737
ISO 9001