Infrastructure Security

Contents

Our Approach to Securing Your Environment 4

Infrastructure Security Assessment: External 5

Infrastructure Security Assessment: Internal 6

Focused Infrastructure Security Assessments: 7

Infrastructure Security

NCC Group's Infrastructure Security services include three key offerings:

External Infrastructure Testing

a remote penetration test performed across the Internet or other untrusted network targeting your accessible systems. This offering is ideal to form a baseline threat profile and gives you the "hacker's eye view" of your systems.

Internal Infrastructure Testing

similar in concept to the external test however the source for all testing is within your data centre or cloud environment. This is ideal for gaining a more comprehensive view of your threat profile as internal findings are typically more comprehensive than external. This testing will identify issues exploited by malicious insiders and external attackers who have gained a foothold within your environment.

Focused assessments

a series of in-depth assessments of key services and infrastructure devices, performed with administrative rights to identify all potential issues and reduce false positives. Typically, these are combined with either an external or internal infrastructure test but can be performed in isolation in many cases. These consultancy offerings are further supported by application testing, automated scanning, training and Escrow services in our wider portfolio.

Whatever your need, a traditional penetration test of your network or a more focused review of your business-critical systems, NCC Group has an offering to assist you in securing your infrastructure and supporting services.

Expert Security Testing

Infrastructure security testing by NCC Group is delivered by our large team of expert penetration testers. Our extensive experience assessing clients across all sectors means we are able to assess the findings in the context of your organisation's operations. NCC Group can therefore provide an accurate view of the likelihood of exposure and the threat posed of each vulnerability.

Key benefits of NCC Group's infrastructure security assessment offerings include:

Comprehensive and efficient:
Manual expert analysis augmented with automated tools to ensure thorough coverage of your infrastructure whilst keeping test durations to the minimum.

Safe:
All activities are performed to pre-agreed rules of engagement, minimising the risk of any adverse operational impact.

Comprehensive Reporting:
Executive level summary of the business risks you face along with appropriate mitigation strategies, supported with remediation advice.

About NCC Group

NCC Group is a global expert in cyber security and risk mitigation, working with businesses to protect their brand, value and reputation against the ever-evolving threat landscape.

With our knowledge, experience and global footprint, we are best placed to help businesses identify, assess, mitigate & respond to the risks they face.

Our Approach to Securing Your Environment

Location of Test

Traditionally the location of testing was a binary choice between remote and on-site, with remote testing conducted across the Internet and on-site from within a trusted and protected network, typically a data centre or office location. The advent of cloud has blurred this distinction considerably, however the concept remains useful when considering the level of access a would-be attacker or NCC Group consultant would have:

On-site Testing

the ability to assess the entire target unimpeded by network level security controls such as a firewall. Whilst firewalls and other mitigating controls are an essential component in a defence-in-depth strategy, many organisations wish to identify the true level of exposure of an individual target system should the network control fail or the attacker have trusted access behind the control.

Software defined networks and virtual security appliances allow cloud environments to mimic traditional networks and as such the same considerations apply, albeit the controls are implemented differently, for example Conditional Access Policies within cloud environments.

Remote Testing

predominantly this testing takes place across the Internet and its intention is to mimic the level of access the majority of threat actors would have, be it a cybercriminal or hacktivist. Certain technologies may support remote testing across mediums other than the Internet, such as testing of wireless access points or remote access solutions over PTSN.

Firebase

an internally developed testing platform, Firebase is preconfigured to drop into your chosen network location, whether as a virtual machine or physical appliance. You have sole control of when
the Firebase connects via a VPN using digital certificates to NCC Group's secure operations centre in the UK. All traffic is encrypted.

Once connected, NCC Group consultants can conduct security testing as if they were physically in your office, data centre or cloud environment. Firebase allows for the level of testing associated with on-site engagements with the flexibility in scheduling and consultant support of remote engagements.

Level of access

A key consideration when commissioning a security test is the level of access and information you provide the testing team. The information can range from next to nothing though to everything available; this ranges from closed box, through partial box to open box testing:

Closed box testing
this is the minimal information necessary to conduct the test. In extreme cases this may consist solely of the target's organisational name with technical findings being confirmed at each stage prior to proceeding with the test plan. It is however more common for a confirmed list of target IP addresses and URLs to be provided prior to testing. This mimics the majority of common threat actors.

Partial box testing –
additional information is supplied, yet not to the degree that test results may lose the context of a "hackers eye view". This type of testing is often used when assessing applications where valid user accounts are provided to the test team prior to the engagement. This mimics a malicious yet authorised user of the system.

Open box testing
considerable information is supplied to the test team, with the goal of finding as may issues as possible in as efficient a manner as possible. The information supplied can vary considerably depending on the target but would typically consist of administration level user accounts, full system documentation, access to previous test reports, issue trackers and internal threat intelligence.

A greater level of access also enables you to gain a higher level of assurance in a given time period, for example five days of partial box testing may identify the same issues as an invested attacker who spends ten days attempting their attack, which is effectively a closed box assessment.

Infrastructure Security Assessment: External

Organisations have historically hosted systems and applications within internal networks and 3rd party data centres, increasingly these are migrating to the cloud. It is now more important than ever to accurately identify the assets to be protected and significant threats they face; the most likely methods by which those assets will be attacked; and the best means of protecting them from those attacks.

This purpose of an external infrastructure test is to simulate the access an Internet based threat actor may be able to achieve should they undertake a concentrated and professional attack against your cloud and Internet facing systems.

This phase of testing across the Internet will focus on retrieving as much publicly available data as possible about the hosting environment. After this passive research, various tools will be used to actively gather information about the systems under review and their topology.

Information such as OS identification and software type or version information, along with associated potential vulnerabilities, will be collated and researched. Where appropriate and agreed, attempts will be made to exploit the systems.

This assessment will typically include the following phases:

- **Initial assessment** – conducting an external black-box security assessment on hosts associated with the infrastructure, identifying devices and potential vulnerabilities. This will give a hacker's-eye view of the environment.
- **Active attack** – attempting to attack visible servers with no valid user credentials or trust.
- **Perimeter bypass** – circumventing the cloud conditional access controls, firewall and router perimeter security to directly access and exploit other components of the system. This phase will typically involve the chaining of vulnerabilities.

Unless specifically stated, the assessment will take place from NCC Group offices.

Optional add-ons:

It is common should the environment contain particularly sensitive systems for there to be additional and more focused tests conducted as detailed in "Focused Assessments". Systems typically selected for this further testing include:

- Routers
- Firewalls
- Email servers
- Web servers

Testing in-depth

Information retrieval activities include:

- Domain-based discovery
- Viewing the customer's website (if available)
- Review of Network Solutions and RIPE databases
- DNS zone transfer attempts to listed DNS servers
- Open information source vulnerability checks
- Web, newsgroup, IRC searches, company databases, social networks

Automated identification and enumeration activities include:

- UDP and TCP port scanning
- Operating system fingerprinting
- Service identification
- User enumeration
- Network mapping

Manual assessment of all live hosts and exposed services focuses on:

- Host and service configuration.
- Patching vulnerabilities
- Use of insecure credentials or protocols

NCC Group use all information gathered to date to attack the services exposed. All exploitation is done in strict accordance with agreed rules of engagement and is highly dependent on circumstances.

Once exploits have succeeded, we use any access and privileges gained to attempt to escalate access rights to the highest level possible.

All exploits are risk-assessed to minimise disruption to live systems.

Infrastructure Security Assessment: Internal

Organisations have historically hosted systems and applications within internal networks and 3rd party data centres, increasingly these are migrating to the cloud. It is now more important than ever to accurately identify the assets to be protected and significant threats they face; the most likely methods by which those assets will be attacked; and the best means of protecting them from those attacks.

This purpose of an internal infrastructure test is to simulate the access a local threat actor, be they a legitimate user of the environment or an external attacker who has gained a foothold, may be able to achieve should they undertake a concentrated and professional attack against your internal systems.

This phase of testing will focus on gathering information about the systems under study and their topology. Information such as OS identification and software type or version, along with associated potential vulnerabilities, will be collated and researched. Where appropriate and agreed, attempts will be made to exploit the systems. This phase is planned to include:

- **Initial assessment** – conducting a network-based black-box security assessment on hosts associated with the infrastructure, identifying devices and potential vulnerabilities. This will give a hacker's-eye view of the environment under review.
- **Active attack** – attempting to attack visible servers with no valid user credentials or trust.
- **Perimeter bypass** – circumventing the cloud conditional access controls, firewall and router perimeter security to directly access and exploit other components of the system.

Testing will be conducted from one or more subnets within the environment. Multiple connection points are utilised in order to assess the target systems unobstructed by firewalls, as such the number required is heavily dependent upon the topology of the environment.

Optional add-ons:

It is common should the environment contain particularly sensitive systems for there to be additional more focused tests conducted as detailed in "Focused Infratructure Security Assessments".

Testing in-depth

Discovery:

- All address ranges are scanned across most typically used protocols
- (TCP, UDP, & ICMP) to identify live hosts.
- Active Directory domains and forests are identified, and account information is enumerated.
- UNIX servers are scanned for running services such as Telnet, SSH, X11, r-services, SNMP, and NFS.
- Web, database and other key services are identified.

Connectivity and Network Architecture:

- The connections to and from the servers, including firewalled segments are reviewed.
- Network appliances such as routers and switches are identified.
- Ingress and egress connectivity is evaluated to determine the effectiveness of proxies and outbound firewall rules.

Research Phase

- During this phase we will research any weaknesses in the identified services using up-to-the-minute vulnerability databases.

Assessment

- We use all information gathered to attack the services, subject always to agreed rules of engagement.
- Privilege escalation techniques are used to elevate access levels.
- Local and domain password files are obtained and cracked where possible.
- Database services are reviewed for default or weak account credentials, the presence of dangerous stored procedures and SQL injection.
- Authentication processes are attacked in a safe manner using both default credentials and bruteforce techniques.
- All exploits are risk-assessed to minimise disruption to live systems.
- All remnants of any attack are removed.

Focused Infrastructure Security Assessments

This purpose of an NCC Group focused assessment is to dig deeper into the configuration of particular systems.

These engagements are performed with interactive access to the device, typically as either the Administrator or root user, such privileged access allows NCC Group to comment on configuration elements we would not otherwise be able to from an unauthenticated network perceptive.

Focused assessments have further advantages, firstly they have a lower false positive rate as it possible to cross reference potential issues against several configuration sources; and secondly, they can be more efficient in the case of voluminous or difficult to enumerate sources such as a firewall rule base.

During these targeted assessments, we will undertake a comprehensive review of the operating system builds and the configuration of key components. This will focus on assessing the build security quality of the device, encompassing areas such as:

- Installed OS components
- System services running
- Core security configuration (firewall, automatic updates, etc.)
- Patch levels
- User accounts
- Password policies (strength, expiration, lockout policies, etc.)
- Registry configuration / permissions
- User rights assignments
- Audit policies
- Event log management
- Kernel settings
- Boot services
- Network services
- User accounts and rights, password policies system access, authorisation, and authentication
- Application security settings (Email service configuration, firewall rule base or IDS rules etc.)

Dedicated Testing Methodologies

NCC Group are capable of reviewing all devices against security best practice and have formalised methodologies for the more commonly encountered:

- Systems – Windows,
- Apple Mac and all variants of Linux
- Network devices – switches,
- routers, Wi-Fi access points & load balancers
- Security devices – firewalls, IDS/ bIPS, anti-virus, content filtering and security proxies
- Application services – Email server, web server, SharePoint, Hadoop, Jenkins and SAP etc.
- Active Directory
- Database servers – RDBMS,
- NoSQL, key value stores, and graph databases
- Infrastructure services – DNS, NTP and DHCP
- Remote working assessments - VPN/RAS, BYOD & mobile device, MDM, RDP breakout and stolen laptop

For more information from NCC Group on our G-Cloud 15 service, please contact:

+44 (0)161 209 5200

bidteam@nccgroup.com