Compiled Application Security Assessment

External Infrastructure Assessment

In an external infrastructure assessment, NCC Group's team of consultants will focus on retrieving as much data as possible about your systems. Various tools will be used to actively gather information about the systems under review. Information such as OS identification and software used, along with associated potential vulnerabilities, will be collated and researched.

Appropriate attempts will then be made to exploit the systems, and the results noted. At the end of an external infrastructure assessment, NCC Group will have an attacker's-eye view of your systems and will be able to advise you on the best ways to protect your systems from external attackers. With an external infrastructure assessment from NCC Group, you will have the assurance you need that your systems are free fromcommon exploitable vulnerabilities.

What we do

Open information check:
Accessing websites, news groups, social networks and other forms of publicly- accessible information, to discover information which could be of use to attackers. In this stage we might discover information such as names of employees, possible passwords they might use and other information which could be useful in a social engineering attack.

Automotated discovery:
Using a variety of automated scanning techniques, we will perform port scans, fingerprint operating systems, identify services, map the network and, where appropriate, enumerate users. In this stage we might discover problems such as the use of insecure protocols. Use of such protocols as Telnet and FTP may increase the risk of compromise and any use of these protocols will be highlighted.

Manual assessment:
Once the automated discovery is completed, the results will be investigated in a manual test to identify possible attack vectors.

Remote attack:
Attempting to attack visible servers with no valid user credentials or trust. Attack scenarios will use a combination of exploits including, where agreed with the client, memory corruption vulnerabilities and system misconfiguration.

Authentication attempts:
Authentication processes are attacked both directly and indirectly, using a combination of brute force and password guessing techniques.

Brute force attacks are not used where there is a risk of account lockout. In this stage we might discover problems with the configuration of authentication services, which may allow attackers to gain unauthorised access, or to gain privileged access to systems to which they have access as a normal user.

Perimeter circumvention:
Circumventing the firewall or router perimeter security, to directly access and exploit other components of the system.

In this stage we might discover problems which allow attackers to gain access to corporate networks from the public Internet, or which allow VLAN-hopping attacks, in which access to one private network is used to gain access to other networks, due to insufficient boundary protections. Unless specifically stated, theassessment will take place fromNCC Group offices.

Other flaws we look for include:

Host and service configuration:
Misconfigurations and poor build processes can leave insecure services available. These often allow a trivial route to achieve system compromise.

Poor password policy:
Default and easy-to-guess passwords will be attempted and their use identified.

Patching vulnerabilities:
Lack of a stringent patching strategy can leave hosts vulnerable; efforts will be made to locate out-of-date services and operating-system-wide missing patches.

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

+44 (0)161 209 5200

bidteam@nccgroup.com