
SAPPHIRE
VULNERABILITY TEST AGREEMENT

External Network Security – Unannounced Penetration Test

FACILITY: CUSTOMER NAME (properties field)

DATE:

OBJECTIVE: To provide an assessment of the site's external security profile of networked computer systems and intrusion detection capabilities.

SCENARIO: Testing will consist of three stages plus reports, during which various tools and techniques will be used to gain information and identify vulnerabilities associated with the site's computer systems and subsequent attempts to penetrate the network. These stages discussed in detail below are: data collection and planning; systems search; systems test; and reporting.

Data Collection and Planning

Sapphire will obtain much of the required information regarding the site's network profile, such as IP address ranges, telephone number ranges, and other general network topology through public information sources, such as Internet registration services, web pages, and telephone directories. More detailed information about the site's network architecture will be obtained through the use of domain name server (DNS) queries, ping sweeps, port scans, and connection route tracing. Informal inquiries, not linked to Sapphire, may also be attempted to gather information from users and administrators that could assist in gaining access to network resources. Once this general network information is compiled and analysed, Sapphire will begin identification of individual system vulnerabilities.

Systems Search

During this stage, Sapphire will attempt to associate operating systems and applications with identified computers on the network. Depending upon network architecture, this may be accomplished using automated tools, such as nmap and queso, or using manual techniques, such as telnet, ftp, or sendmail login banners. Using this information, Sapphire will create a list of probable vulnerabilities associated with each potential target system. Also, at this point, automated scripts will be developed or compiled to attempt exploitation of vulnerabilities.

Systems Test

During this stage, system and user information will be used to attack the authentication processes of the target systems. Example attack scenarios in this stage include, but are not limited to: buffer overflows, application or system configuration problems, modems, routing issues, DNS attacks, address spoofing, share access and exploitation of inherent system trust relationships. Potential vulnerabilities will be systematically tested in the order of penetration and detection probability as determined by the members of the Sapphire vulnerability testing team. The strength of captured password files will be tested using password-cracking tools. Individual user account passwords may also be tested using dictionary-based, automated login scripts. In the event that an account is compromised, Sapphire will attempt to elevate privileges to that of super user, root, or administrator level.



SAPPHIRE

Since the goal of Sapphire testing is to determine the extent of vulnerabilities, and not simply penetrate a single site system, information discovered on one system may be used to gain access to additional systems that may be "trusted" by the compromised system. Additionally, host-level vulnerabilities may be exploited to elevate privileges within the compromised system to install "sniffers" or other utilities. Sapphire will insert a small text file at the highest level directory of each compromised system. In those cases where Sapphire is unable to gain sufficient privilege to write to the system, a file will be copied from the system. In either case, additional files may be copied during testing if further review is required to determine sensitivity of information contained on the system.

Sapphire will maintain detailed records of all attempts to exploit vulnerabilities and activities conducted during the attack stage.

Reporting

Sapphire will provide an on-site briefing of results. These results will also be documented in a management level report provided to the CUSTOMER NAME (properties field) Headquarters that will cover the unannounced penetration testing. Specific details on vulnerabilities will also be provided to site technical personnel.

SPECIAL CONSIDERATIONS:

Sapphire will co-ordinate testing activities with a "project supervising officer" in the CUSTOMER NAME (properties field). The CUSTOMER NAME (properties field) should identify an individual to be designated as the project-supervising officer. More than one officer may be identified at the CUSTOMER NAME (properties field), however, the number should be kept to an absolute minimum. All personnel who are informed of the testing will maintain strict confidentiality to ensure the validity of test results.

The Sapphire Project Team will co-ordinate with officers on-site to identify critical systems that should be excluded from testing activities (e.g., safety systems, major applications undergoing upgrades or other special systems). Specific network addresses and reasons for exclusion should be provided as an attachment to the signed test.

While Sapphire will not attempt to exploit "denial of service" vulnerabilities (unless specifically requested by the CUSTOMER NAME (properties field)) and every attempt will be made to prevent damage to any information system and the data it holds, some penetration attempt scenarios have the possibility of causing service interruption. In the unlikely event that such an event occurs, Sapphire will work with the CUSTOMER NAME (properties field) on-site to determine the nature of the problem and restore the system to its desired state of operation.

All information obtained by Sapphire will be protected to the best of our efforts from unauthorised access.

It is the CUSTOMER NAME (properties field)'s responsibility to restore network computer systems to a secure configuration after Sapphire testing. Sapphire will co-ordinate with and provide assistance (as requested) to system administrators during this period of "cleaning up" network computer systems. Clean-up may consist of removing added programs and files,



SAPPHIRE

identifying systems whose password files were compromised, and restoring systems to a secure configuration so that no systems are left in a compromised condition.

As evidenced by their signature on this test agreement, the CUSTOMER NAME (properties field) have, as a result, granted positive consent to this type of activity. CUSTOMER NAME (properties field) agrees to indemnify Sapphire from all liabilities for damage to or loss of equipment or information caused by the activities as described in this agreement.

APPROVALS:

I confirm that I am duly authorised by CUSTOMER NAME (properties field) to consent to the activities as described in this agreement

[Customer] [Name and Title]

[Customer] [Signature]

[Customer] [Date]

Sapphire [Name and Title]

Sapphire [Signature]

Sapphire [Date]