



INTERNAL SECURITY TESTING

Can one of your employees steal your private data and damage your computer system?

An Internal Security Test (IST) is what you need to answer this question. This test's main purpose is to expose the vulnerabilities threatening your system. It is offered in two different options: blind and assisted. The blind IST consists of **Virtual Guardian's** experts trying to log on directly onto your company's network without the use of passwords. They will try, by using several known techniques, to compromise the confidentiality, integrity and availability of your system and its data. As for the assisted version of the test, the approach is similar with the exception that the system's administrators give **Virtual Guardian** direct access to their network. This allows our experts to dig deeper into the network as they now have the same access level as a company employee.

This test will also allow you to quickly obtain a list of all vulnerabilities in order of importance i.e., from most to least critical. Following the test, **Virtual Guardian** will present you with a complete comprehensive report with this list of vulnerabilities and recommendations on how to correct the situation. As an option, **Virtual Guardian** also offers a "VIP" report that can be prepared for your company's board of directors that can be a very useful tool when evaluating yearly budgets for example. This report is written in layman's terms and will describe the risks and impacts on the business if the vulnerabilities go untreated.

OUR METHODOLOGY

You will find below the five main steps of the methodology that **Virtual Guardian** uses for all its internal tests.

Step 1: Security environment evaluation

Before all else, **Virtual Guardian** will take note of the organization's policies. These should describe the organization's security objectives and the ways it chose to reach them. This step is necessary in order to compare the gap between those objectives and reality. To achieve this, **Virtual Guardian** will use ISO 27002 (17799) and COBIT as references bases to analyze corporate objectives.

Here are the main categories of elements that will be verified:

- IT security policies;
- General organization of internal IT security measures;
- Informational asset management;
- Security linked to human resources;
- Physical and environmental security;
- Operations and communications security;
- Access control management;
- Development and maintenance of informational systems;
- Security-linked incidents management;
- Business continuity management;
- Legal conformity policy.



Step 2: Automatic port scanning

This step is slightly intrusive and will probably be detected by your company's IT department due to the high number of attempted connexions **Virtual Guardian** will generate. From its headquarters, **Virtual Guardian** employees will use different tools to scan all 65535 ports (TCP and UDP formats) looking for available services. This type of scanning also allows to verify the configuration(s) of the firewall(s) that the company uses. Furthermore, this process allows:

- To obtain the list of every open port, which are considered potential entry points (i.e. vulnerabilities);
- To obtain service and software identification through the open ports. This can tell us if a specific port is linked to a website;
- To look for software version numbers used by the company, which in turn will alert our experts because some vulnerabilities are directly linked to specific software version numbers;
- To try to circumvent the firewall.

Step 3: Automatic vulnerability scanning

This second scanning process delves much deeper than the first and as such, is considered as very intrusive. Not only will this process attempt to identify the services which are accessible but it will also try to take control of them using known attack techniques. This process will allow us to quickly test more than 10,000 potential software vulnerabilities. Due to the intrusive nature of this step, **Virtual Guardian** will always seek the customer's explicit authorization before proceeding as there is the possibility that the information systems experience a brief interruption of service that may require the client to restart certain applications.

VULNERABILITY SUMMARY

Zone	Vulnerabilities/ Threat level					Vuln. Total
	0	1	2	3	4	
WORKSTATIONS	0	3	11	26	6	46
SERVICES / SERVERS	0	26	39	26	6	97
TOTALS	0	29	50	52	12	143

This summary is included in the final report.

Step 4: Manual intrusion testing

This phase is a complement to the results of steps 2 and 3. In essence, the manual intrusion testing is the application of well known techniques to try to exploit the vulnerabilities that were discovered. Also, these techniques used are not automatic due to the fact that human analysis is required. For example, a computer will be able to identify two benign individual vulnerabilities but will not be able to tell you that when combined, those two vulnerabilities become a dangerous threat. Here are a few examples of the information we look for during the manual verification:

- Validation of false positives, i.e. identified vulnerabilities that aren't really threats;
- Validation of false negatives, i.e. vulnerabilities we know exist but were not pick up in step 3;
- Additional access to confidential information using a combination of found exploits and other informations
- Weaknesses or problems related to applications that can be found through more intense web research;
- Weaknesses or problems related to IT systems that must be regularly updated.

Step 5: Technological architecture analysis

Corporate culture is a factor that will vary from one company to another. The technological choices the company makes influences this culture and vice versa. In this final step, **Virtual Guardian** will evaluate the strengths and weaknesses for these choices and of the overall informational architecture in place. Virtual Guardian will also evaluate the security risks linked to your overall network. This evaluation will include:

- Verification of firewalls and filtering rules;
- Evaluation of restrictions and network separations;
- Evaluation of restrictions and verification of protocols to see whether they are allowed or forbidden as per the company's security policies;
- Access control and user authentication, attempt to obtain passwords, replay attacks etc.;
- Validation of protocols (NTP, SNMP etc.) used to manage networks;
- Evaluation of surveillance systems, system logs and general organizational security in place.

Do you need to **evaluate your IT system's defenses?**
Contact **Virtual Guardian** today to get a free evaluation!