



## EXTERNAL SECURITY TESTING

### ***Can a malevolent person get into my computer system?***

The external security test (EST) is your best option to get an answer to that question. Probably one of the most common tests in the industry, it is also one of the most important. The EST allows you to measure your infrastructure's capacity to resist to hackers or even motivated competitors. Our specialists will try to penetrate your company's perimeter defenses using a wide array of techniques and tools.

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 external tests. These steps are based on the recognized OSSTMM principals (Open Source Security Testing Methodology Manual). The ISECOM group also recognizes **Virtual Guardian** as a GOLD member which certifies that we respect the industry's best practices and remain constantly on the cutting edge of exploit, virus and malware detection.

### ***Step 1: Network reconnaissance***

This first step is *non-intrusive* which means that it will not affect the client and will have no impact on the company's systems. A reconnaissance process will be employed to find out the maximum of corporate information readily available on the Internet and determine if it can ultimately be used to gain access to the company's sensible information.

In order to simulate an attack, it's important for the experts at to know the company it was hired to protect. This will enable them to find every trace of information on your company that lingers on the Internet. Here is a partial list of the type of information that we will look for to complete step one:

- Corporate information such as internal practices, company policies, confidential documents etc preserved in Google "cache" memory.
- Lists of key personnel, customer details, product prices etc. With a list of company employees, we can easily begin testing system accesses and passwords.
- Traces of conversations left by your employees on web forums and through email exchanges. This information can be highly sensitive due to the perception that the information is safe. For example, technicians have been known to discuss system vulnerabilities, version numbers and other such information.
- In the event of a successful DNS information attack, it's important to obtain domain name configuration validation because it's possible to lose control of it. A typical negative consequence is the ability for the hacker to be able to read all email exchanges for a particular domain.
- When reading and revising web pages, validation of best practices such as passwords stored in a website's HTML files or comments containing confidential information left by programmers.



## **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 will generate. From its headquarters, 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. It will allow us to quickly test more than 10,000 potential software vulnerabilities. Due to the intrusive nature of this step, 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.

## **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: Logical service analysis (Web, FTP, etc.)**

Every Internet service has its own vulnerability type linked to it. The experts at are aware of all vulnerability types and use the information to their advantage to try to discover even more vulnerabilities. Here is a series of tests targeted towards a website:

- Web programming practices analysis;
- Web architecture analysis;
- Vulnerabilities due to phishing;
- Cross Site Scripting (XSS);
- SSL, Secure Socket Layer;
- Error message management;
- Session reconstruction;
- Circumvent function authorization;
- User authentication verification;
- IT Security policy verification (password choice, data storage etc.);
- Data files access management;
- Web sessions management (Token, Cookies etc.);
- Cookie modification;
- Hidden fields analysis;
- URL and HTML encoding;
- Buffer overflow;
- Service denial;
- Manual SQL injection;

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