A comparison between Nessus and CyBot

Both Nessus and CyBot perform scanning of organizational networks for vulnerabilities.

The main difference between CyBot and Nessus is that scanning is Nessus' main function, whereas scanning is simply the first phase in CyBot's solution.

Nessus is a Vulnerability scanner/manager, whereas CyBot performs Vulnerability scanning powered by our patented Attack Path Scenarios, on both infrastructure and web, on a global scale with minimal impact on the network, taking into account the customer's business processes.

Creation of Attack Path Scenarios is performed by an algorithm, patented worldwide by Cronus Cyber Technologies, that shows validated routes hackers could take to reach critical assets within the network.

The CyBot scan utilizes elements similar to a human ethical hacker in order to create a more reliable shortlist of vulnerabilities with lower false positive rates.

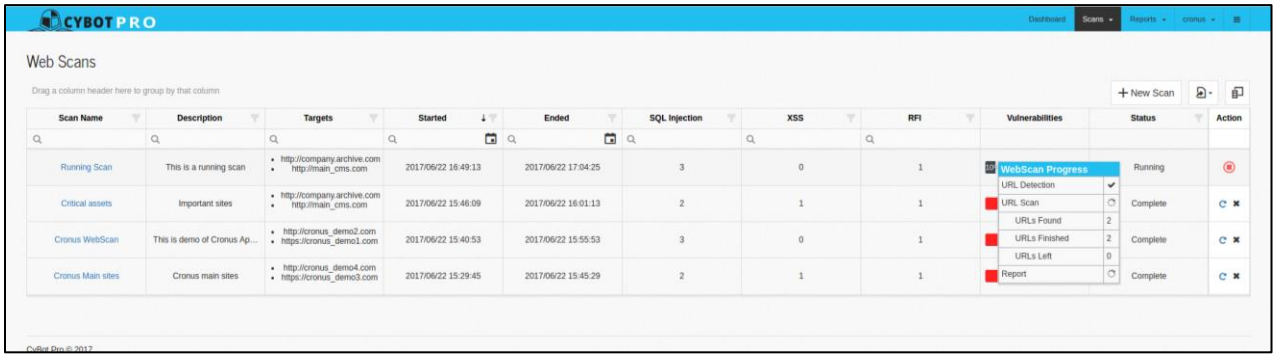
1. **Identify all the network assets.**
   The existing solutions on the market (such as Nessus) usually scan all the hosts in the network one by one, using a method called "unicast". This method is very time consuming. CyBot Pro uses "multicast" scanning which is much faster and is performed on all network assets simultaneously, which enhances asset detection and makes it 100 times faster (give or take since it depends on the network topology, network infrastructure and the assets/hosts CyBot Pro is scanning).
2. **Collect the "fingerprint" (OS, ports and services) of all the machines on the network.**
   The available infrastructure vulnerability scanners on the market heavily load the network traffic. At Cronus Cyber Technologies, we developed a sophisticated algorithm (patent registered) implemented within the CyBot Pro scan engine that performs the same type of questioning as other scanners but only uses 5% of the packets ("plugins") that are sent to the remote machines, which directly affects the scan speed and the impact that the scanning procedure has on the network traffic, reducing it greatly.
3. **Prepare a list of vulnerabilities to exploit.**
   Nessus scans for vulnerabilities and then lists them for the user, while CyBot goes further and identifies, analyzes the vulnerabilities and creates the Attack Path Scenarios, to demonstrate how a hacker can exploit the vulnerabilities and connections between the assets in the network, to reach his ultimate targets, while also providing remedial and mitigating information.
   This analysis creates a succinct result set that focuses on what is really important and urgent to be resolved, based on our exploitable Attack Path Scenarios repository. Obviously, by doing so, the user can focus on remediating and mitigating the most

significant threats, and ignore the long lists of vulnerabilities that are not always exploitable by hackers.

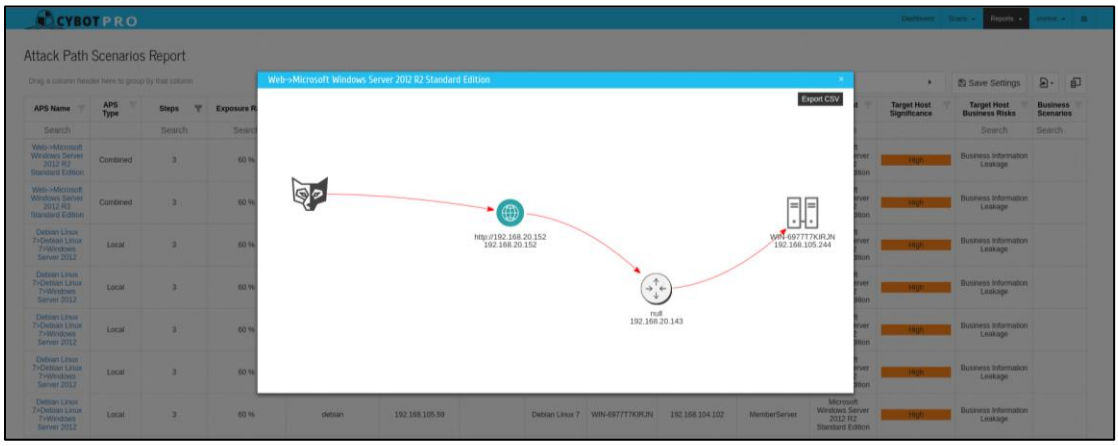
Additional advantages over Nessus

1. **Web / Infra vulnerability detection including APS**

In today's market, automated solutions, specifically in the vulnerability management segment, support either Web scanning or Infrastructure scanning. Cronus has launched the first Infra-Web scanner which combines both Web and Infra scans in order to provide actionable insights and remediation prioritization which take into account a hacker's ability to start his attack from the web, entering all the way into your critical assets or business processes. In our Web scanning we currently support 4 of the OWASP top 10.
How does it work? The customer initially provides a URL for web applications, and then CyBot performs tests on the URL.
During configuration of the web scan, the user has to approve CyBot to perform the tests, as they include a test to validate that it is truly possible to perform the exploit.



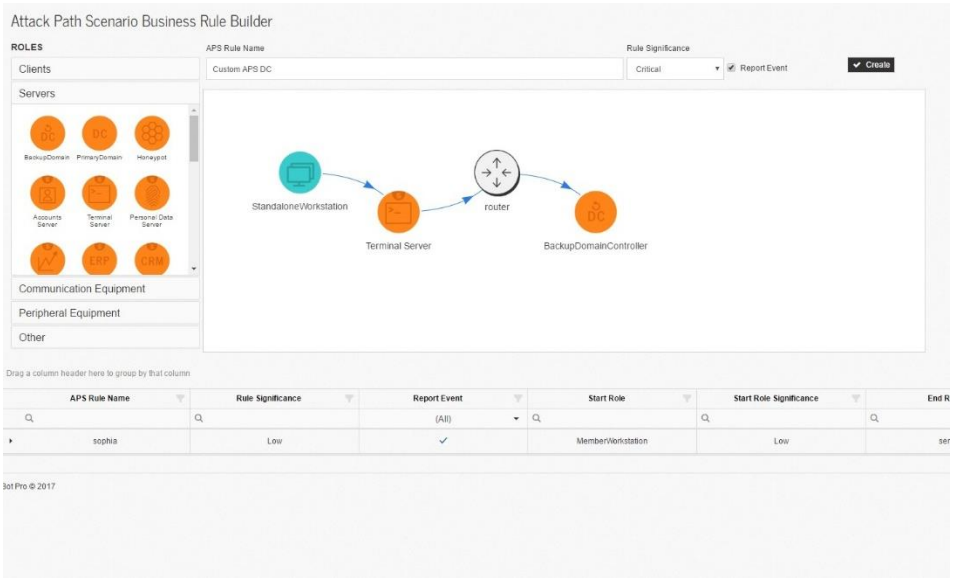
Web test results



Web -> infrastructure Attack path scenario

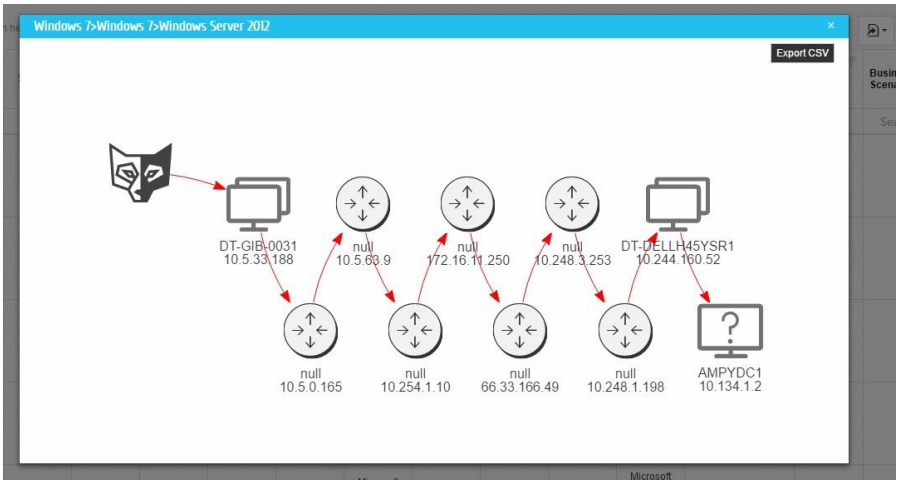
2. Business Processes

Our platform enables our users to input their business processes (such as mortgage supply flow, CRM, customer onboarding, billing process, etc.). This is used to detect Attack Path Scenarios™ that correlate with a business process. If such an attack path is found it will be highlighted as a "Business Scenario" which should be prioritized for remediation.
Business processes can be generic or specific, depending on the input from the user.



3. Global Scanning

When using our Enterprise management console, it aggregates the input from all CyBots deployed in the network (infra and web), based on the information gathered, it can display attack scenarios between the different subnets or CyBots. This shows how a potential hacker can exploit a vulnerability on a host in one subnet, and from there move within the organization to a target host, even if it’s in another subnet (lateral movement). This provides a real time snapshot of the risks to the global network.

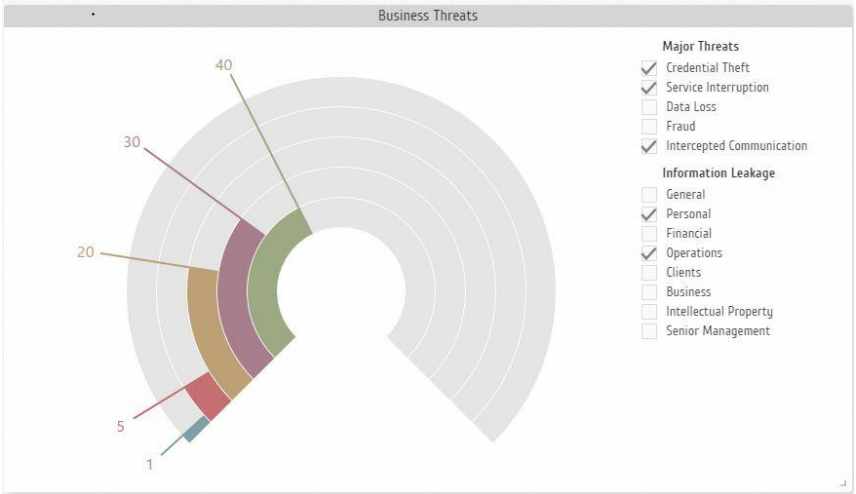


4. Continuous operation

CyBot Pro can be configured to run 24/7 since CyBot Pro scanning doesn't overload the network.

5. Business Risk View

Cronus displays risks, not just in terms of CVEs but also translates those risks to the Business Risks/Threats discovered by CyBot Pro such as Credential Theft, Service Interruption, Data Loss, Information Leakage and more.



6. **Lower false negatives**
   Today, most vulnerability scanning systems perform sample tests, especially for large systems with hundreds or thousands of virtual servers and geographically dispersed organizations. The ability to install an unlimited number of CyBot's allows to minimize the possibility of a system with vulnerabilities not being detected and false negatives. Moreover, the attack path validation process also greatly reduces the chance for a false positive and helps focus remediation on a short list of vulnerabilities that are a part of an attack path to a critical asset or business process. Since Nessus does not display attack scenarios, all the vulnerabilities displayed are at the same level, since it is impossible to know which vulnerabilities really can lead to an attack scenario or be exploited. Thus the organization receives a list with thousands of vulnerabilities and is unable to understand whether these findings are really dangerous or if these vulnerabilities could lead to real damage. Also, using credentials allows for almost 100 percent verification of the risk and reduces the risk of dealing with false positives. CyBot Pro also verifies the physical connection between the machines that participate in the attack path, thus additionally minimizing false positives.