



CRONUS
CYBER TECHNOLOGIES

CyBot Pro

About Cronus Cyber Technologies

Cronus Cyber is a software product company that develops software solutions for the Automated Penetration Testing market place. Cronus Cyber is a leading provider of an integrated solution that includes software technology that enables real-time penetration testing using autonomous Agents (CyBot pro) designed to operate complex hacking scenarios. A Reasoning Engine and an underlying Knowledge-Base that includes hacking scenarios is continually defined by our hacking experts and updated into the product – CyBot Pro.

Cronus Cyber mission statement is to protect organizations with a solution that anticipates and prevents Cyber Attacks before they occur – using unique and innovative algorithms that imitate the behavior of human hackers continuously, 24/7 365 days a year.

Cronus Cyber was established in 2014 by veteran security experts Doron Sivan & Matan Aguzi. Cronus Cyber employs over 30 employees in the software development and hacking scenarios definition.

The company was successful in acquiring a large customer base including Nilit, Migdal Insurance, Mellanox and Eureka.

CyBot Pro - Provides actionable Insights to enterprise vulnerabilities

CyBot Pro is an autonomous hacking robot that imitates human hacker operating practices and performs continuous Penetration Tests on enterprise networks in order to find vulnerabilities in real-time and prevent future attacks.

In addition to Automated Penetration Testing, CyBot Pro provides extensive security business intelligence complete with real-time relevant information about the identified vulnerabilities and the required measures to be taken to close these gaps. With CyBot Pro's intelligence capabilities, IT personnel can immediately access an accurate road map of how to mitigate future intrusions and most effectively utilize existing security tools and protocols.

CyBot Pro conducts Automated Penetration Testing around the clock on a company's entire IP-based system, including Cloud, ERP, Wi-Fi, Cellular, Web, VoIP, as well as Servers and Controllers.

CyBot Pro was designed for hassle-free operations and can be easily implemented by IT personnel without a need for deep technical experience. The system is downloadable from the Cloud and installed as a virtual machine (VMware-based) behind the firewall of the organization.

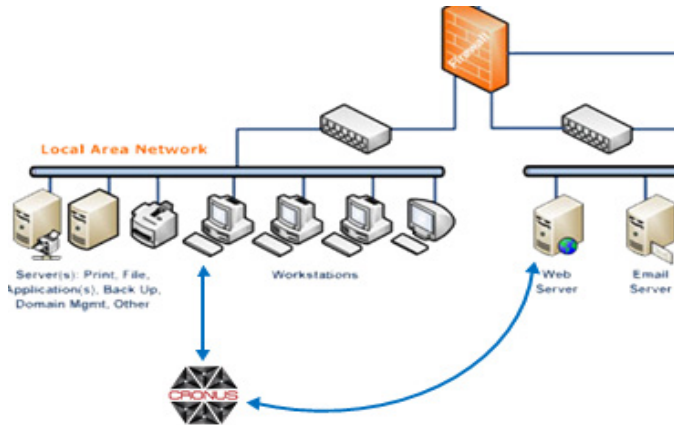
Unique to CyBot Pro is the system's ability to be updated regularly with new potential vulnerabilities thereby enabling the scanning of the most up to date vulnerabilities via updated attack scenarios.

CyBot Pro provides 24/7 Automated Penetration Testing, but it also offers recommendations for fixing identified vulnerabilities within the system.

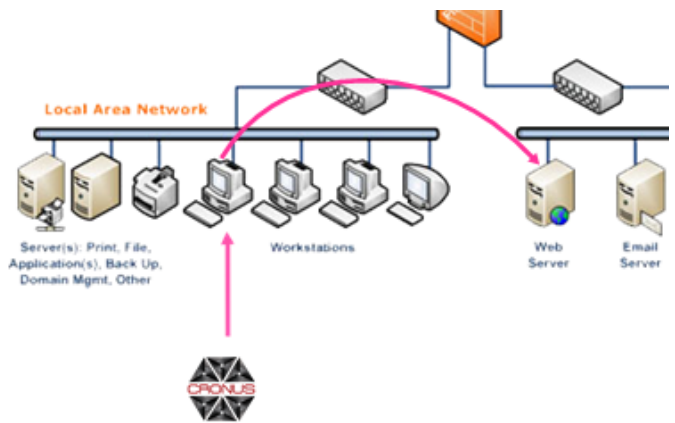
The technology enables multi-level, dynamic, complex scenarios based on real-time data collection, by proprietary Reasoning Engine (patent pending).

Technology

A depiction of a multi stage hacking scenario executed by CyBot Pro.



Vulnerability scanning continuously

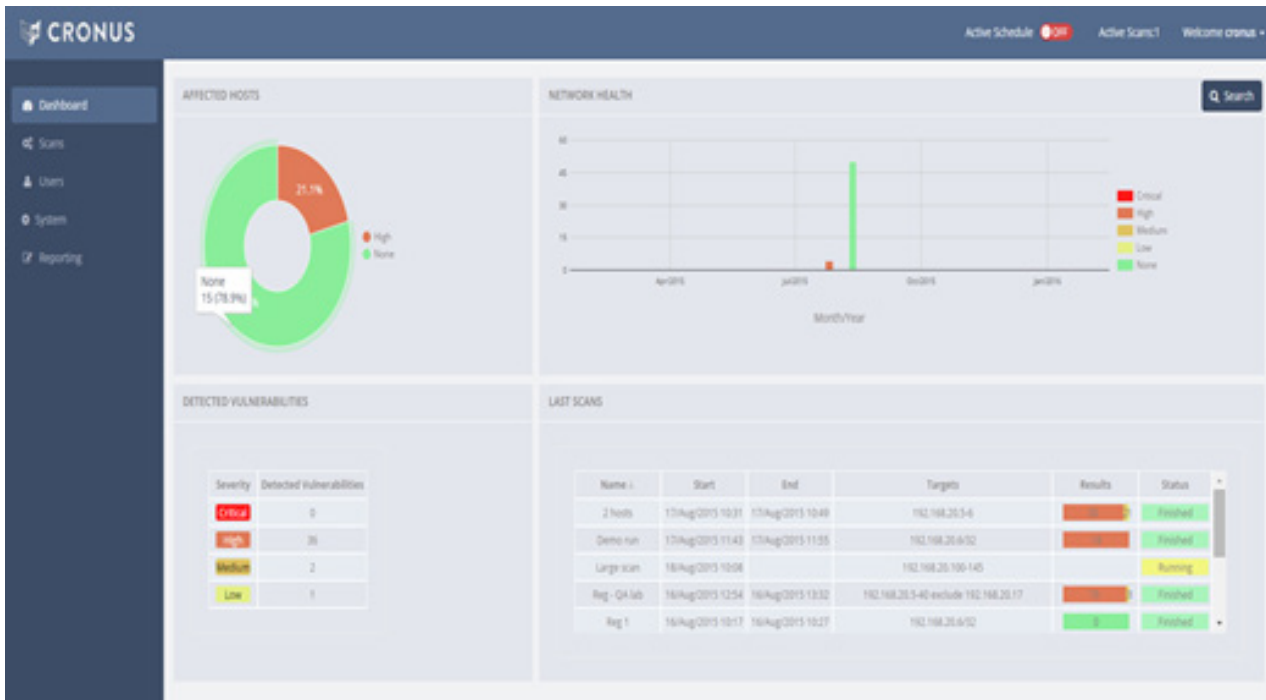


Immediate identification of a Cyber event scenario



Blocking and warning in real time

Product Capabilities



CyBot Pro Dash- Board provides a high level view of current vulnerabilities and enables drill down to specific problems, their origin and how to deal with them.

VULNERABILITIES

Code	Severity	Commonality	Age	Hosts
CVE-2003-0661	Medium	1	1	192.168.20.5 ,
CVE-2003-0717	High	1	1	192.168.20.5 ,
CVE-2005-0045	High	2	1	192.168.20.21 , 192.168.20.5 ,
CVE-2005-0050	High	1	1	192.168.20.5 ,
CVE-2005-0051	High	1	1	192.168.20.21 ,
CVE-2005-1206	High	1	1	192.168.20.5 ,
CVE-2005-1981	Low	1	1	192.168.20.5 ,
CVE-2005-1983	High	2	1	192.168.20.21 , 192.168.20.5 ,
CVE-2005-1984	High	2	1	192.168.20.21 , 192.168.20.5 ,
CVE-2006-0012	Medium	2	1	192.168.20.21 , 192.168.20.5 ,
CVE-2006-1314	High	2	1	192.168.20.21 , 192.168.20.5 ,
CVE-2006-2370	High	1	1	192.168.20.5 ,
CVE-2006-2373	High	2	1	192.168.20.21 , 192.168.20.5 ,
CVE-2006-2379	High	1	1	192.168.20.5 ,
CVE-2006-3439	High	2	1	192.168.20.21 , 192.168.20.5 ,
CVE-2006-4688	High	2	1	192.168.20.21 , 192.168.20.5 ,
CVE-2007-1748	High	1	1	192.168.20.6 ,
CVE-2007-2228	High	3	1	192.168.20.6 , 192.168.20.21 , 192.168.20.23 ,
CVE-2007-5351	High	1	1	192.168.20.23 ,
CVE-2008-4037	High	3	1	192.168.20.6 , 192.168.20.21 , 192.168.20.23 ,

Sample of Drill-Down information on the vulnerabilities and their origin. Defined by level of severity from Critical (Breached), to low.

CVE-2005-0045: High

Synopsis:
The Server Message Block (SMB) implementation for Windows NT 4.0, 2000, XP, and Server 2003 does not properly validate certain SMB packets, which allows remote attackers to execute arbitrary code via Transaction responses containing (1) Trans or (2) Trans2 commands, aka the "Server Message Block Vulnerability," and as demonstrated using Trans2 FIND_FIRST2 responses with large file name length fields.

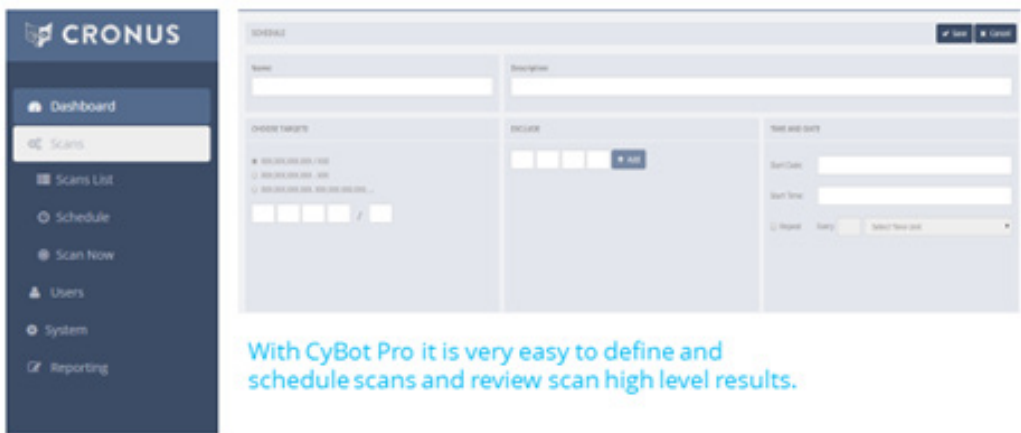
Description:
The Server Message Block (SMB) implementation for Windows NT 4.0, 2000, XP, and Server 2003 does not properly validate certain SMB packets, which allows remote attackers to execute arbitrary code via Transaction responses containing (1) Trans or (2) Trans2 commands, aka the "Server Message Block Vulnerability," and as demonstrated using Trans2 FIND_FIRST2 responses with large file name length fields. BUGTRAQ:20050209 EYE: Windows SMB Client Transaction Response Handling Vulnerability | URL:http://marc.theaimsgroup.com/?i=bugtraq&m=110792638401852&w=2 | NTBUGTRAQ:20050209 EYE: Windows SMB Client Transaction Response Handling Vulnerability | URL:http://marc.theaimsgroup.com/?i=ntbugtraq&m=110795643831169&w=2 | BUGTRAQ:20050309 Update: MS05-011 EYE: Windows SMB Client Transaction Response Handling Vulnerability | URL:http://marc.theaimsgroup.com/?i=bugtraq&m=111040962600205&w=2 | MS:MS05-011 | URL:http://www.microsoft.com/technet/security/bulletin/ms05-011.mspx | CERT:TA05-039A | URL:http://www.us-cert.gov/cas/techalerts/TA05-039A.html | CERT-VN:VU#652537 | URL:http://www.kb.cert.org/vuls/id/652537 | BID:12484 | URL:http://www.securityfocus.com/bid/12484 | OVAL:oval.org.mitre.ovaldef:1606 | URL:http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.ovaldef:1606 | OVAL:oval.org.mitre.ovaldef:1847 | URL:http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.ovaldef:1847 | OVAL:oval.org.mitre.ovaldef:1889 | URL:http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.ovaldef:1889 | OVAL:oval.org.mitre.ovaldef:4043 | URL:http://oval.mitre.org/repository/data/getDef?id=oval.org.mitre.ovaldef:4043 | XF:win-smb-code-execution(19089) | URL:http://xforce.iss.net/xforce/xfdb/19089 Assigned (20050111) None (candidate not yet proposed)

Fix:

CyBot Pro vulnerability drill down to a specific issue providing:

- Vulnerability Level
- Synopsis – high level Description
- Detailed Description
- Fix – How to solve – when relevant

CYBOT PRO – SAMPLE SCAN DEFINITION & EXECUTION



With CyBot Pro it is very easy to define and schedule scans and review scan high level results.

With CyBot Pro it is very easy to define and schedule scans and review scan high level results.

ANS

Name	Start	End	Targets	Results	Status
2 hosts	17/Aug/2015 10:31	17/Aug/2015 10:49	192.168.20.5-6	20/21	Finished
Daily run	18/Aug/2015 12:49		192.168.20.5/32		Running
Demo run	17/Aug/2015 11:43	17/Aug/2015 11:55	192.168.20.6/32	19	Finished
Large scan	18/Aug/2015 10:08	18/Aug/2015 12:48	192.168.20.100-145	20/21	Finished
Night run	18/Aug/2015 12:35	18/Aug/2015 12:36	192.168.20.6/32	0	Aborted by user
Reg - QA lab	16/Aug/2015 12:54	16/Aug/2015 13:32	192.168.20.5-40 exclude 192.168.20.17	20/21	Finished
Reg 1	16/Aug/2015 10:17	16/Aug/2015 10:27	192.168.20.6/32	0	Finished
Reg 2	16/Aug/2015 12:16	16/Aug/2015 12:32	192.168.20.6/32	19	Finished
Sanity run	17/Aug/2015 17:49	17/Aug/2015 18:25	192.168.20.5-40 exclude 192.168.20.17	20/21	Finished
host 5-6	17/Aug/2015 12:37	17/Aug/2015 12:54	192.168.20.5-6	20/21	Finished
host 6	18/Aug/2015 09:26	18/Aug/2015 09:38	192.168.20.6/32	19	Finished
sched test	17/Aug/2015 09:57	17/Aug/2015 10:15	192.168.20.5-6	20/21	Finished

CyBot Pro Dash-Board Scan Execution Status