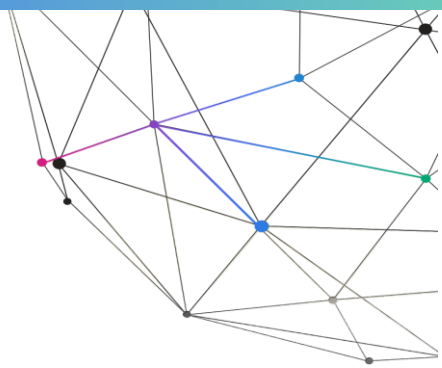


CRONUS
CYBER TECHNOLOGY

CyBot Pro
POC Guide

V2.9
June 2020

Table of Contents

1 Introduction ____ 3

2 Installing CyBot Pro ____ 5

3 Accessing the CyBot Pro GUI ____ 8

4 License ____ 9

5 Credentials ____ 10

6 Setting up Critical Assets ____ 11

7 Scans ____ 12

8 Appendix A: Add User as Local Administrators on all PC's connected to Domain ____ 14

9 Appendix B: Stand Alone Servers 2008 and above – UAC configuration ____ 15

10 Appendix C: Minimal Requirements ____ 16

11 Appendix D: Success Criteria ____ 17

12 Appendix E: Recommended Pre installation questions for customers ____ 18

1 Introduction

The document is designed to provide Cronus's clients with the details of preparing the network for CyBot Pro and Enterprise and how to conclude that the Proof of Concept (PoC) was successful. The first chapter contains requirements information needed for a successful PoC, including hardware, software, environments, installation methods, and network topology.

Note: For any problem that occurs during the PoC, do not hesitate to contact your Cronus representative.

1.1 Minimal Requirements

1.1.1 Detail of minimal HW & SW requirements – See appendix C

1.1.2 In order to deploy CyBot (all editions), the following information is required, for installation:

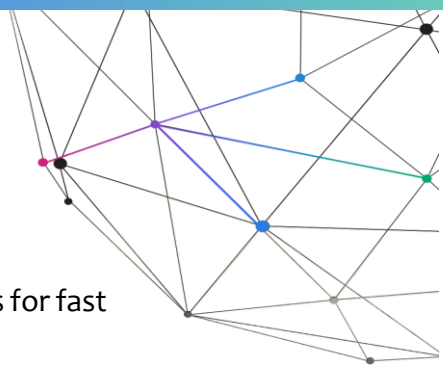
- Desired IP Address
- Desired subnet
- Desired Gateway
- Desired DNS servers
- Account for WMI credentials (member of Server Operators and
- Local Administrators groups in AD/DA)
- Account for SSH credentials (root)
- If using CyBot Enterprise, please verify that ports 443 & 6432 are open from CyBot Pro to CyBot Enterprise.

Note: Cronus supplies a VM template, preconfigured with the minimum requirements.

1.1.3 PoC Environment Requirements

Design the PoC environment so it includes at least 50 machines (physical or virtual) with the following criteria:

- At least 50% of the network should be comprised of workstations.
- At least one Domain Controller (DC).
- At least 10% of the network should include servers.
- Workstations and servers should include both Linux and Windows operating systems. It is recommended to employ various Windows and Linux based operating systems, in order to maximize the efficiency of the PoC.



Notes:

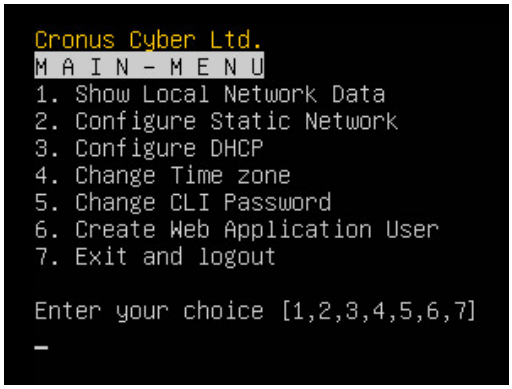
- It is required to supply CyBot with the WMI and SSH credentials for fast and efficient scanning.
- All hosts scanned must meet the minimum requirements as outlined by the specific vendor.
  i.e. – Windows machines must meet the requirements outlined in TechNet, etc.

2 Installing CyBot Pro

To install CyBot Pro, run the virtual machine that you received.

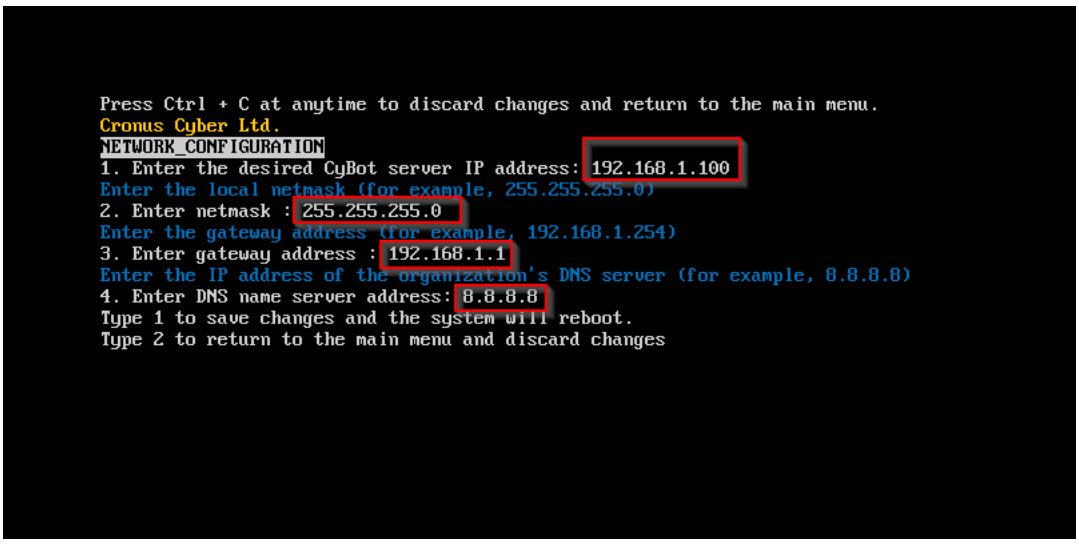
2.1 On the console Login using the following credentials:

- Username: client
- Password: CrΘnu5$$$



2.2 When prompted, select the network configuration that you prefer:

- To configure a specific static IP address for the CyBot Pro server, enter 2, followed by the IP address. This is the recommended configuration.



- To configure an IP address using the DHCP server, enter 3.

1. Save the configuration changes. The VM automatically restarts.
2. Log in again and enter 1 to check your IP address.

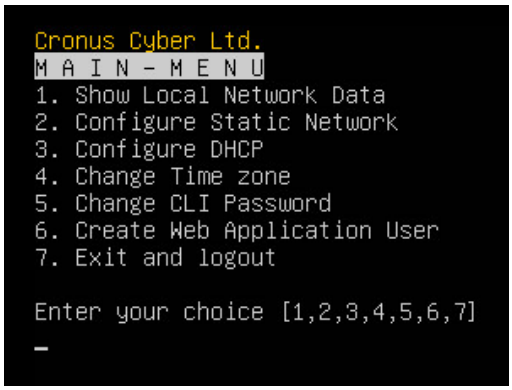
A window is similar to the following will appear. Use the IP address listed to connect to the web interface of CyBot MSSP.

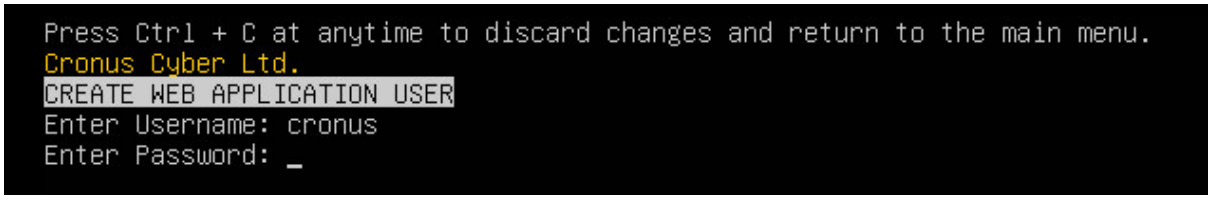
2.3 Defining Username and password for first use:

1. Login CLI using following credentials

- Username: client
- Password: Crϴnuƽ$$$

2. Once loaded choose option 6 and ser username and password for web access.



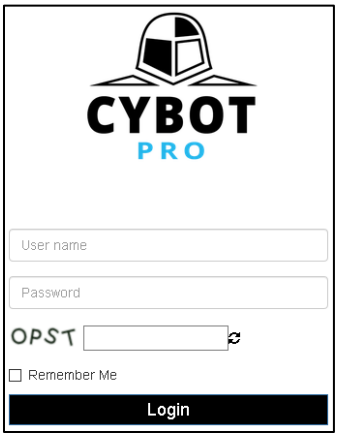


3 Accessing the CyBot Pro GUI

All CyBot GUI's are supported with **Google Chrome.**

1. Enter the CyBot Pro IP in the URL of Chrome.
   - **https:**//X.X.X.X
2. Once loaded, a screen will load saying that your connection is not private.
   a. Click **ADVANCED** on the bottom of the screen.
   b. Click **Proceed to XXX.XXX.XXX.XXX (unsafe)**.
   c. The CyBot Pro login page will load.
3. Enter the default CyBot Pro credentials when the login screen appears:

Username: **as defined in section 2.3**
Password: **as defined in section 2.3**
NOTE: The credentials can be changed and/or deleted once the initial setup is complete.



4 License

1. To upload a license to CyBot Pro:
2. Select the Common Functions button ≡ and select Licensing
3. 

4. Click on the Add license and proceed with the license installation wizard.
5. Read and agree to the "Terms and Conditions"
6. Upload the license file, by clicking on Select file or by drag-and-dropping the license file.
7. After successfully uploading your license file, please select method of license activation, it is preferred to use the "Online Activation", but if there is no active Internet connection available, use the "Offline Activation" method.
8. Offline Activation:
9. Click on "Offline Activation".
10. Click on "Copy to Clipboard".
11. Log in to Cronus portal at: https://portal.cronus-cyber.com
12. Click on "Activate Product" from the top right menu.
13. Paste the copied key to the "Unique Machine Key".
14. Click "Activate" button and copy the "Activation Key"
15. Go back to CyBot Pro window and click on 

16. Paste the copied activation key from the Portal and click "Activate now".

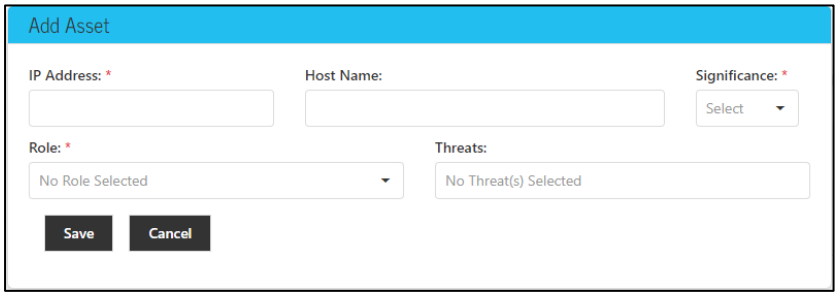
5 Credentials

1. Select the Common Functions button and select Credentials
2. Account for WMI credentials (member of Server Operators and Local Administrators groups in AD or Domain Admin)
3. Account for SSH credentials (root)
4. SSH Certificate

6 Setting up Critical Assets

1. Select The common functions button and select Asset Management.

2. Press on "+Add Asset" Button, and fill in the following data:



Critical Asset should be set prior to scanning especially Linux based servers since server information that being collected from the machines during scanning is not enough to define server Role which is one of the basic things for building of APS.

7 Scans

3. Navigate to scans main menu and click on “Infrastructure Scan”.
4. Click On 

5. The Setup Scan menu has the option to schedule a scan or to scan it right away by checking “Scan Now” option.
6. Schedules can be made hourly, daily, weekly, and monthly at a set time.
7. A CSV file of IP’s can be uploaded to speedup management with multiple CyBot Pro’s or when adding IP’s to a new scan by clicking the 

button.
8. Insert the scope of scan by clicking the + button
9. Save each “Range “ or\and “CIDR” and click “Scan”
10. Information about the scan status can be found under the Infrastructure Scan menu

APPENDIXES

8 Appendix A: Add User as Local Administrators on all PC's connected to Domain

This procedure need to be created on the DC (Domain Controller) and it will be replicated to all computers that are members in the Domain.

On the DC (Domain Controller):

Define a security group in AD users and computers. In this example I am creating a security group called IT_Admins

1. Log onto a Domain Controller 2. Right click Users, New->Group->Security Call it IT_Admins 3. Add the proper members that you want them to have the appropriate security permissions on the local computers.

Create the User

1. Create a User that will be the Local Administrator privileges 2. Go to the user properties 3. Go to member of 4. Add groups called "Server Operators", "IT_Admins" 5. Set the "IT_Admins" as primary group

Next you need to create a group policy or use the default Domain Policy (not recommended).

1. Create a separate policy called "Local Administrators" 2. Open Group Policy Management Console 3. Right click your domain or OU 4. Click Create a GPO in this domain, and link it here 5. Call it "Local Administrators" now you should see the policy in the tree

Here you will add the IT Admins group to the local administrator's policy and put them in the groups you wish them to use. 1. Right click "Local Administrators" Policy 2. Expand Computer configuration\Policies\Windows Settings\Security Settings\Restricted Groups 3. In the Right pane of Restricted Groups, Right click and hit "Add Group..." Type IT Admins and hit 'OK" 4. Click Add under "This group is a member of:" 5. Add the "Administrators" Group 6. OK Wait 15 minutes, or log on to a PC and type upgrade /force and check the local administrators group. You should see IT Admins in the group now. The user you created now access all PCs remotely as a local administrator. Link to YouTube Explanation: https://youtu.be/n2dDOKUIFI0

9 Appendix B: Stand Alone Servers 2008 and above – UAC configuration

Following Microsoft UAC hardening on Server Operating System 2012 and up, the default windows shares access are allowed only after popup security agreement even for Administrators group.

Working with Automated Penetration Tools require full access to default shares for Administrator level. There is no risk to the system when allowing and managing properly Administrators group and allow full access to Administrators group for default shares.

This level of security is achieved by the following policies:

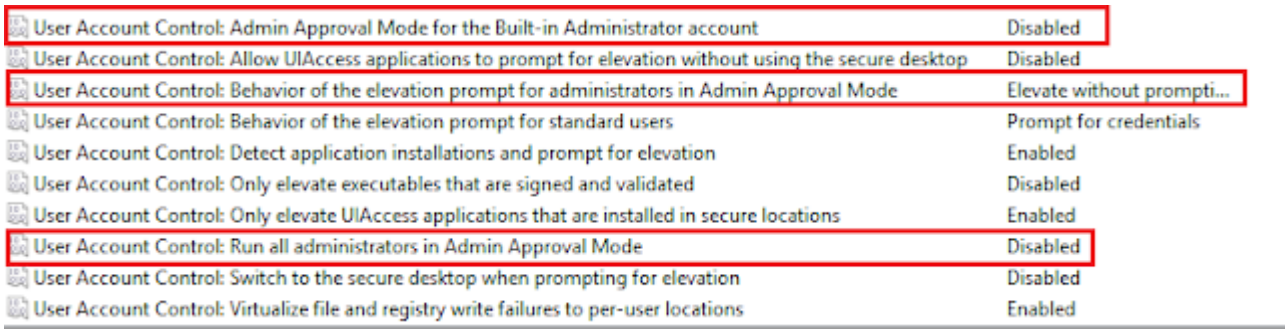
Computer Configuration --> Windows Settings --> Security Settings --> Local Policies --> Security Options

- User Account Control: Admin Approval Mode for the Built-in Administrator account
- User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode
- User Account Control: Run all administrators in Admin Approval Mode

To allow Administrators Group Only access without prompting please follow this steps:

Set the policies settings as follows in the following order as per the screenshot below:

- Disabled
- Elevate without prompting
- Disabled



10 Appendix C: Minimal Requirements

The VM's of CyBot Pro and Enterprise require the following minimal hardware and software properties:

10.1.1 Minimal Hardware and Software Requirements for CyBot Pro

- **RAM**: 8 GB
- **Free Disk Space**: 120 GB
- **Processor**: 4 cores processor
- **Network**: 1 Ethernet card 100 Mb
- **Platform**: VMware ESX v5.5 /Hyper-V 3.0 or higher.

10.1.2 Minimal Hardware and Software Requirements for CyBot Enterprise

- **RAM**: 8 GB
- **Free Disk Space**: 1000 GB
- **Processor**: 4 cores processor
- **Network**: 1 Ethernet card 100 Mb
- **Platform**: VMware ESX v5.5 /Hyper-V 3.0 or higher.

10.1.3 Minimal Hardware and Software Requirements for CyBot MSSP

- **RAM**: 16 GB
- **Free Disk Space**: 1000 GB
- **Processor**: 8 cores processor
- **Network**: 1 Ethernet card 100 Mb
- **Platform**: VMware ESX v5.5 /Hyper-V 3.0 or higher.

11 Appendix D: Success Criteria

This chapter describes the success criteria for evaluating CyBot Pro and Enterprise. Each section in this chapter includes a different test for the PoC. The advancement to the next section is performed only when the test is successful and the criterion is met.

11.1.1 Network Hosts Identifications

The first success criterion CyBot Pro is a system designed to identify and detect the scanned network's topology. A success is achieved when **at least 85%** of the hosts and devices in the scanned range are correctly identified:

- Operating System
- Role
- Services
- Open Ports

11.1.2 Vulnerabilities Detection

CyBot Pro and Enterprise should perform a scan on the system and produce a report on the critical findings. Each host, which contains critical findings, should be manually tested and verified that the vulnerability does exist on the system. Verification of the vulnerability's existence can be performed by searching the CVE number on the OS manufacturer's site and check if the patch that fixes the vulnerability **is not installed** on the host. A success criterion for this step is verification of **at least 85%** of the critical findings.

11.1.3 Attack Path Scenario (APS) Detection

CyBot Pro and Enterprise should perform a scan on the system and produce a report on the Attack Path Scenarios. Every APS with a factor of 80 and above should be tested for verification. The verification process is performed by checking each step (host) of the APS route and acknowledge the following factors:

- Each APS-related CVE finding exists on the host.
- Each APS-related CVE finding enables an attacker to take control over the host.
- All steps of the APS route are viably connected in the network.
- The final step (Target host) of each APS is considered a valuable asset (for example, DC, SQL server, etc.).

A success criterion of the step is verification of **at least 85%** of the APSs.

12 Appendix E: Recommended Pre installation questions for customers

- Overview of Hypervisor - VMware / Hyper-V: Verify how much resources are available?
- What is the current version of ESXi / Hyper-V running (and are there any plans to upgrade)?
- Are there any vNet restrictions or bandwidth limitations on the network.
- Check NIC configuration and speeds to find optimal network setup for CyBot VM – ask the customer if they have 1GB/10GB NIC.
- Intranet restrictions, connectivity & gateway rules – discuss if there are any FW or gateway setups that could limit and/or affect scans, also check if VMs pass-through Distributed Switch inside VMware.
- Overall active network setup – Which and How many - Routers, Switches, Firewalls.
- List active devices that are connected to the network – Printers, time clocks, IP phones, Smart-TVs, Consoles, etc.
- Check for any running network monitoring services.
- Ask for port whitelist / blacklist - confirm that CyBot's ports aren't being blocked / filtered / forwarded.
- Confirm & check retrieved credentials that will be used.
- Ask if there is any NLB enabled, Also ask for Ideal time for running scans (when the network is load)
- Brief network topology sketch.
- Is the Port that the ESX's Connected to in the Switch is in Trunk Mode and is it permits all VLAN's
- Ports need to be opened: 445/139,22 (WMI, SSH)
- PRO+ENT+MSSP need Ports: 443, 6432 open between them, if they are on a different segment, need to check if there is internal FW.
- Is the ESX connected to the backbone?
- What kind of Switches' in the floors?
- Is the network segmented?
- What are the VLAN's?
- What is the networks to be scan and in what classes are they, A, B, C?