CyBot FAQs

Release Version: 4.1

Release Date: July, 2020

Copyright

The "original instructions" of this manual are published in the English language.

The information conveyed in this document has been carefully checked and is believed to be reliable at the time of printing. However, Orchestra Group Ltd makes no warranty regarding the information set forth in this document and assumes no responsibility for any errors or inaccuracies contained herein. Orchestra Group Ltd is not obligated to update or correct any information contained in this document. Orchestra Group Ltd reserves the right to change products or specifications at any time without notice.

Mention of third-party products or services is for informational purposes only and does not constitute an endorsement or recommendation.

CyBot FAQs

This document contains the most frequently asked questions about the CyBot application.

How are the risks that are shown on the Business Risks and Business Impact reports calculated?

The algorithm takes into consideration several factors including:

- Is this a critical resource?
- How many steps are needed to reach the goal?
- Is the source of the attack from outside the organization and then continues inside?

How does CyBot use machine learning?

The use of machine learning is reflected in the ability of the system to learn what is the most convenient attack path from all the existing possibilities. In addition, the system can join different track segments into one track. Therefore, depending on the type of critical resource, the system will independently learn all the options and choose the relevant combination. If a track is blocked, the system will try to select an alternate route.

What other tools are available to check infrastructure security besides penetration testing?

Vulnerability scanners can check infrastructure security, but they cannot prioritize the results, they make noise on the network, and they might yield false-positive results.

What is the relationship between business size and the number of vulnerabilities?

Clearly there is a connection, but today even medium-size companies can have thousands of servers. This is because cloud computing makes rolling out new servers cheap and easy. Small- and medium-size companies are also being attacked more easily because of the lack of budget and manpower for system security. Such companies might be interested in receiving security services from an MSSP and our product fills that need precisely.

How does Attack Path Scenario (APS) work?

Attack Path Scenario represents a path of vulnerabilities that a hacker can exploit to reach his target. Keep in mind that servers are typically located on the most secure part of a network. Therefore, it is often impossible to attack them directly. The clever thing to do is to pass through several points on the way to the server. Since networks are large and complex today, there are hundreds and thousands of penetration possibilities. It is simply not possible to cover all the

possibilities by using manual penetration tests. The solution is our APS system that can check millions of paths and prioritize them appropriately.

Why do we require a domain admin user?

CyBot is a white-box tool. This means that every scan requires the correct connection to the scanned environment. Scanning with credentials dramatically reduces the chance of receiving false-positive results. In addition, it enables CyBot to gather as much data as possible from scanned servers to build accurate attach path scenarios.

Is it possible to run CyBot without AD credentials?

CyBot is a white-box tool that must have credentials prior to scanning since this allows us to collect as much information as possible to build the APSs.

If the PC (or a group of machines) is not in AD, the system can use the local admin of a particular machine. Bottom line, we need credentials for every machine/laptop/server in organization.

How we can scan VLANs without router/switch admin credentials or without disabling the endpoint firewall?

There are few scenarios to scan different networks. For example, we can install CyBot on every network or open specific firewall rules to allow scanning of remote machines.

What should I do after I fix the APS vulnerabilities?

After initial scanning and reporting of the vulnerabilities, the security team should remediate the issues. After remediation, the same scans should be run again to verify that the APS is no longer present.

What are the top vulnerabilities that are currently supported?

The infrastructure vulnerabilities are the latest CVE's that exist on the market. The web scanning vulnerabilities are currently SQL-Injection, RFI/LFI, and XSS.

How frequently do you update the list of vulnerabilities?

The infrastructure vulnerabilities are updated weekly. The web scans are the top vulnerabilities from OWASP.

Does CyBot detect vulnerabilities in the routers and other network devices?

CyBot has the ability to check vulnerabilities of Cisco routers. Unfortunately, we cannot check vulnerabilities of routers and other network devices from other providers such as HP or Juniper. CyBot can only identify their host name and OS.

Is it advisable to open port 445 and to lower the firewall settings?

There is always the remote chance that an attacker is waiting to get into the network via EternalBlue, or some other SMB vulnerability, and will attack as soon the firewall is opened. If this is truly a concern, you can use port 139 instead of 445 if this one is closed in your firewall or blocked by your AV. Alternatively, you can open port 445 or 139 only for CyBot's specific IP towards the scanned environment and for the specific time of the scheduled scan.

Why must Linux devices be set up as a Critical Asset?

Linux devices, by default, are not configured as critical resources, even if it is a server. Therefore, Linux devices must be set up as assets with a significance level of "critical."

Why there is no APS while scanning only a subnet of similar workstations or servers?

If there are many identical workstations or servers, there will be no attack scenarios because, by default, they are the same level of importance and there is no target. Therefore, one or more of the assets must be set up with a significance level of "critical" so that the APS has a target?

How can I perform an external scan?

If you want an external scan, ports must be opened, and many customers rightfully oppose this. Therefore, a good solution is to place CyBot in the DMZ, so that it is in complete control of the organization (as opposed to placing CyBot in AWS).

Should the PoC be performed on both Windows and Linux devices?

To show the full power of CyBot, it is strongly suggested that your PoC environment contain different versions of Windows and Linux.

Can CyBot scan IoT devices?

CyBot scans servers and workstations. Our Harmony IoT offering scan IoT devices.

Is the domain admin user hardcoded in CyBot?

No. You must manually enter the domain admin credentials.

Can CyBot integrate with PAM solutions such as CyberArk?

Currently, CyBot does not have active integration with PAM systems. We hope to have this available in a future release.

Does the infrastructure scans test all IP/TCP/UDP/ICMP ports?

Yes, the infrastructure scan tests all of those ports.

Is there a way to limit the range of ports scanned?

There is no need to limit the range of ports. During scanning, CyBot discovers open ports on scanned machines, however only checking connectivity through the relevant ports of a specific CVE. Therefore, CyBot does not stress the scanned environment and there is no need to limit the ports.

Can ports discovered during an infrastructure scan be automatically added in Web Scan/PT if those ports belong to web applications?

Yes. If during an infrastructure scan an active web server was detected, it will be automatically added as a valid IP for web scanning.

Is there a way to tune the infrastructure/web scan's velocity and to manage the stress on the targets and the network?

In both scans, the overall network footprint of CyBot is less than 3%. This is due to CyBot's white-box solution and its unique scanning methodology. Therefore, there is no need to be concerned about stressing your network during scans.