Home Network Scans

Each week, BlackCloak provides external network penetration tests of the public IP addresses for your home network. We scan for open ports that make your devices accessible to the Internet (e.g., security cameras, home automation systems, routers, etc.), and thus potentially vulnerable to compromise. We also assist with providing remediation guidance as necessary.

Our home network scans consist of 5 phases:

1. We port scan the public IP addresses for your home network;
2. For any open ports or services we find, we assess whether the service may be vulnerable to well-known issues;
3. For any open ports or services we find, we also manually test the service to assess whether the service is misconfigured (authenticates with easily compromised credentials, exposes sensitive data about your family, etc.);
4. For all weaknesses we find, we validate the findings with a second analyst, and develop remediation guidance;
5. We deliver the results and provide any relevant remediation guidance to you

Port scan of your public IP addresses

To find all your devices that are accessible to the Internet, and thus potentially vulnerable to compromise, we scan your public IP addresses for all 65,535 possible ports. We use industry-recognized and open source tools to perform this scan. For all ports we identify as open (accepting connections from the Internet), we move onward to the next step of our testing.

Vulnerability assessments and manual validation

For any open ports or services we find, we perform automated and manual testing. Our tests are designed not to disrupt your devices, and we never destructively "hack" your home network. Our goal behind these tests is to identify potential vulnerabilities or misconfigurations in your home before a bad actor can. Examples of findings we identify during this phase are: home camera systems with weak (or no) authentication, home automation software running out-of-date (and therefore vulnerable) software, IP telephones on the home network, and other common misconfigurations or vulnerabilities.

Delivering the results

When we make our findings, we validate them to increase your peace of mind, and develop remediation guidance that enables you to get back to a secure state. Occasionally, we will find misconfigurations or vulnerabilities on your home's public IP address that warrant an urgent alert. Examples of this would include cases where we find a bad actor in your network or privacy-impacting information disclosure (such as accessible camera/NVR systems).

Further, whenever our findings require an immediate response, we will notify you that we have discovered an issue that warrants your attention, and invite you to schedule time to discuss with us at your convenience. During these sessions we:

- walk through our findings with you, and
- discuss possible solutions to our findings, and
- deliver our guidance in written form

If authorized by you, we are happy to work with your chosen IT provider to coordinate the remediation of our findings. Once the issue is remediated, we validate through follow-up scans to ensure the fix was effective.