If You Give a Hacker a Host

Written by:

GYTPOL

If you give a hacker a host,
he's going to want to dig.

If he finds something good, he'll settle in...

Biding his time and looking for ways to move deeper into your network.

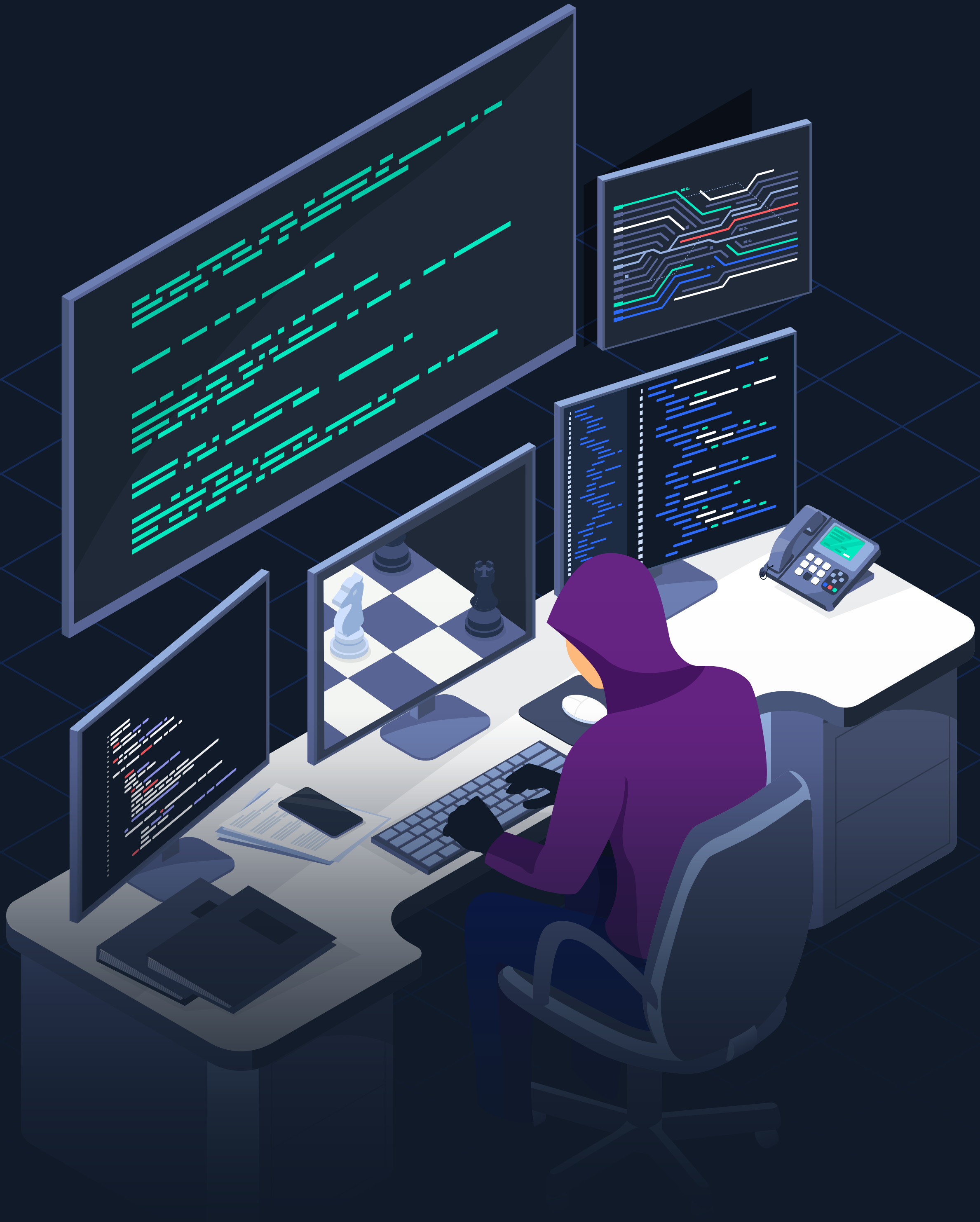
He’ll study your network
and see how it all connects.

He’ll look for weak spots.
And he’ll find them.
Because nobody’s perfect.

If your network is like most, he’ll have plenty of insecure configurations to work with.

Using each endpoint as another entry point, he'll worm through your network, going deeper and deeper.

As he goes, he'll take it all
in and make plans for later.
And you'll be none the wiser.



Once he has the run of the place, he'll look for ways to parlay access into control. It won't be too hard either...

It just takes an open SMBv1 here, a vulnerable Log4J instance there, and maybe some excessive permissions or default passwords for good measure.

When he gains control,
he'll want to play.

But that may draw attention.
So he'll probably open a backdoor
before getting started. Just in case.

Then he'll get to it. He might monitor traffic and steal a token, inject some scripts, or carry out a denial of service attack. Just for fun.

He'll extract financial records, customer information, and trade secrets. Whatever looks good.

After he's tuckered himself out chasing all that data, he'll probably want a break. So he'll call a timeout.

He'll shut everything down—locking you out until you pay up. You'll scramble to regain control as operations screech to a halt.

With each tick of the clock feeling like a punch to the gut, you'll probably cave to his demands. But even then, it won't be over...

Only 8% of ransom-payers ever get all their data back. And recovery costs typically exceed the actual ransom by 4X!

So even after the hacker calls it a day, you'll still be stuck cleaning up.

With time, maybe you'll move on.
But the hacker won't forget you.

He'll think of you often and
reflect on all the fun he had.

One day, he'll grow bored of his other playthings and he'll want to play with you again.

When that happens, he'll need a host to get things going again. He'll remember that back door he opened and he'll walk right back in.

If you give a hacker a host,
he's going to want to dig...
And that's just the beginning!

About GYTPOL

With 1 in every 3 breaches and over 80% of ransomware attacks targeting device misconfigurations, GYTPOL is on a mission to secure the most overlooked and oft-exploited stretch of the attack surface.

Offering automated detection and push-button remediation of insecure configurations, GYTPOL keeps you a step ahead. From Windows to macOS, servers to cloud instances, GYTPOL works to ensure businesses never give a hacker a host. Mapping dependencies to highlight hardening opportunities that carry no risk of business disruption, GYTPOL streamlines, simplifies, and error-proofs endpoint posture management.

With over 3 million devices protected, GYTPOL is trusted by organizations across the globe to keep their environments productive, resilient, and secure.

To learn more, visit www.GYTPOL.com or email us at contact@GYTPOL.com.

GYTPOL