# HOW NOT TO GET HACKED

## TIPS TO PROTECT YOUR ORGANIZATION FROM A CYBERATTACK

By Brandyn Fisher

((CENTRIC))

# EXECUTIVE SUMMARY

Overseeing cybersecurity is a daunting task. While the role is maturing across multiple industries, it heavily relies on internal teams such as audit, technology and risk.

Meanwhile, the media seems to focus on which organization was hacked and how it was hacked, which is a public relations nightmare. As a chief information security officer (CISO), the following thoughts may continuously consume your mind:

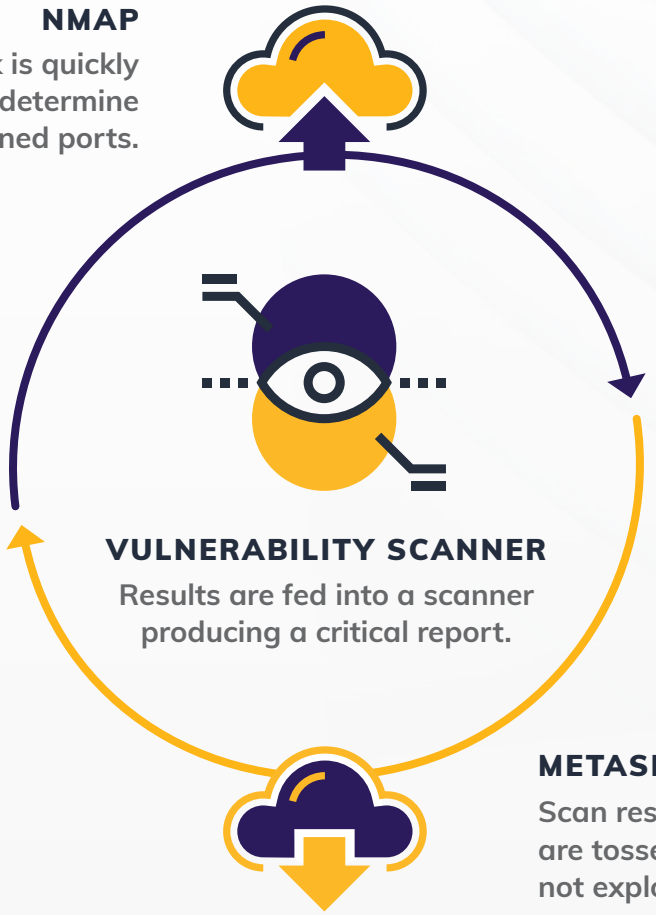
*"If we have a breach, I'll lose my job. We'll end up all over the news. I think I'm doing enough, but am I? It doesn't matter how much we spend; it doesn't matter how many devices we buy; we can still get hacked. I just can't get peace of mind about whether we're secure enough."*

Over the past few years, penetration tests have provided temporary peace of mind for organizations. Afraid of landing in tomorrow's news headlines, organizations hire third parties to assess and test their network for vulnerabilities. While organizations understand the significance of a penetration test, they continue selecting vendors with the intention of making a limited-scope or reduced investment.

But you need something more than that if you're going to manage your network security risk in the most effective way possible. Below, we'll explain how to do just that, and attempt to reveal "how not to get hacked."

## COMMON NETWORK TESTING

**Below is an example of a vulnerability scan that acts as a penetration test, but doesn't go far enough to examine vulnerabilities and identify weaknesses.**



**NMAP**

Network is quickly mapped to determine most opened ports.

**VULNERABILITY SCANNER**

Results are fed into a scanner producing a critical report.

**METASPLOIT**

Scan results from report are tossed aside and not explored.

---

**RESULTS**

**A raw formatted report filled with errors and missing critical warnings.**

# YOU SHOULD EXPECT MORE

## BREAKING DOWN THE PROCESS

Organizations that fall victim to these routine penetration tests often find they are paying for a penetration test but receiving a vulnerability scan. The tools listed in the graphic above are essential for performing a penetration test, especially under tight time constraints.

However, these tools should not become a crutch for the assessment. There is no magic button to fully automate a penetration test, nor a magic scan that will provide the same level of thoroughness as a true penetration test.

Penetration testing, by nature, requires the penetration tester to manually examine each vulnerability to identify the weakness and ascertain how it fits into the larger picture.

## A DIFFERENT PERSPECTIVE

A symbiotic relationship exists between cybersecurity and malicious threat actors. As the skills, abilities and knowledge of threat actors increase, you must enhance cybersecurity safeguards.

This in turn forces threat actors to find new ways to circumvent modern technologies and controls. Without this relationship, the cybersecurity field would become stagnant. You should not assume an attacker will rely solely on network-based attacks for network entry.

## CYBERATTACK

### RATHER THAN CIRCUMVENTING MULTIPLE NETWORK SECURITY CONTROLS:

Attackers desire the highest reward

For the least amount of effort

### ADDITIONAL AVENUES OF ENTRY – EASY TARGETS

- Physical entry
- Wireless networks
- Bluetooth and peripheral devices
- Email phishing
- USB thumb drives

## A FALSE SENSE OF SECURITY

Network security vendors typically provide organizations with a report that includes a laundry list of vulnerabilities and guidance that states they will be protected from attacks once they correct those vulnerabilities. But that is almost never the case.

A holistic penetration test must examine all the avenues through which an attacker may attempt to penetrate security defenses, not just network defenses. It's imperative that your cybersecurity vendor takes an overarching approach, looking beyond any narrowly defined threat to encompass a broad range of security needs and potential weaknesses.

Threat actors look for the weakest point to attack, which is rarely your perimeter. Modern enterprise firewalls, if kept up to date, do an excellent job of protecting your network from the outside. But that makes no difference if your operating systems are not fully patched, as a threat actor could walk into your office unimpeded and boot a workstation from a USB thumb drive. Or an attacker could trick users into providing their usernames and passwords over the phone.

**The scary part is that these scenarios are not difficult or uncommon.**

# WHAT TO LOOK FOR

A mature assessment will focus on a full penetration test rather than a network-only one. A penetration test should be multifaceted and address all the possible violations of the confidentiality, integrity and availability of the organization's data and network.

Organizations do not possess the luxury of limiting what a threat actor can and cannot attempt. Therefore, penetration tests must consider as many attack avenues as possible to fully understand and measure the organization's risks.

**When reviewing the scope of a penetration test, consider the following targets commonly exploited by threat actors:**

- Wireless networks
- Mobile devices
- Bluetooth devices
- I/O devices
- Employees
- Physical devices

**In addition, you should consider including the following types of assessments within the scope of work with third-party service providers:**

- External network penetration
- Voice phishing (vishing)
- Internal network penetration
- Physical social engineering
- Wireless penetration testing
- Web application testing
- Bluetooth device testing
- Peripheral device testing
- Email phishing
- Cyber footprint analysis

# RAISING THE BAR

When selecting a security penetration testing vendor, it is crucial that you review the full scope of work to ensure the penetration test is comprehensive. Vendors that market and sell vulnerability scans as penetration tests lower the perceived value by making penetration testing a commodity rather than a service.

And, to ensure that you develop and implement a comprehensive penetration test that can successfully pre-empt cyberattacks and the hackers who plot them, it's important to establish a scalable, reusable penetration process.

You should ensure the service provider's assessment is not dependent on a single set of tools. Instead, the vendor should have the ability and skillset to use a large, customized set of tools. Just like a mechanic does not rely on a single socket wrench to repair a car, a penetration test should not rely on a single tool to assess the organization's overall security.

Vendors should carefully select and customize tools based on the risk, as described below, to meet your organization's individual needs.

# RAISING THE BAR (CONTINUED)

## NETWORK RISK

An external and internal network penetration test, which should consist of more than just a few NMAP port scans, focuses on finding vulnerabilities on the network and methods of exploiting software and services on the various systems. Vulnerability scans assist in speeding up the discovery process, but can be riddled with false positives and negatives that vendors should investigate further during the exploitation and vulnerability confirmation phase of testing.

Nonetheless, the most important aspect of any penetration test is information gathering, as it is instrumental to the outcome of subsequent testing phases. In addition, conducting an analysis of the organization's public footprint, which is the platform hackers use to obtain what they need to gain entry, is advisable and incredibly useful in ascertaining a complete picture of how the organization operates.

## WEB APPLICATION RISK

As technology has become an immensely vital part of the business world, the number of web applications has grown exponentially. Web application penetration testing attempts to violate security controls and program logic to access unauthorized parts of an application or perform actions not intended by the developer.

It looks past the server on which the application resides and into the program or application being hosted. Short development cycles and complex application requirements have led to an increasingly high number of application vulnerabilities waiting to be exploited.

# RAISING THE BAR (CONTINUED)

## WIRELESS RISK

Wireless testing assesses the security controls around the organization's WLAN. Often offered as a convenience to employees and visitors, WLANs provide an easy avenue for attackers to infiltrate the network without a physical presence, since they could be miles away and still access an organization's network resources.

## HUMAN CAPITAL RISK

Vishing, email phishing and physical social engineering focus heavily on vulnerabilities in the workforce and assess employees' willingness to perform tasks that violate organizational policy. Human behavior is the most difficult vulnerability to remediate, which is why it's often the most exploited one. Through a few simple social tricks, it's possible to accomplish almost anything.

## PERIPHERAL DEVICE RISK

Bluetooth and peripheral device testing are reserved for mature penetration tests, as they attempt to access information and systems through mobile and third-party devices, such as cell phones, headsets, mice and keyboards.

Peripheral devices often are an afterthought during a penetration test and not regarded as legitimate attack avenues. Attackers hope organizations adopt this line of thinking so they may skate by unnoticed in a single mouse-click.

# A REAL-WORLD CASE STUDY

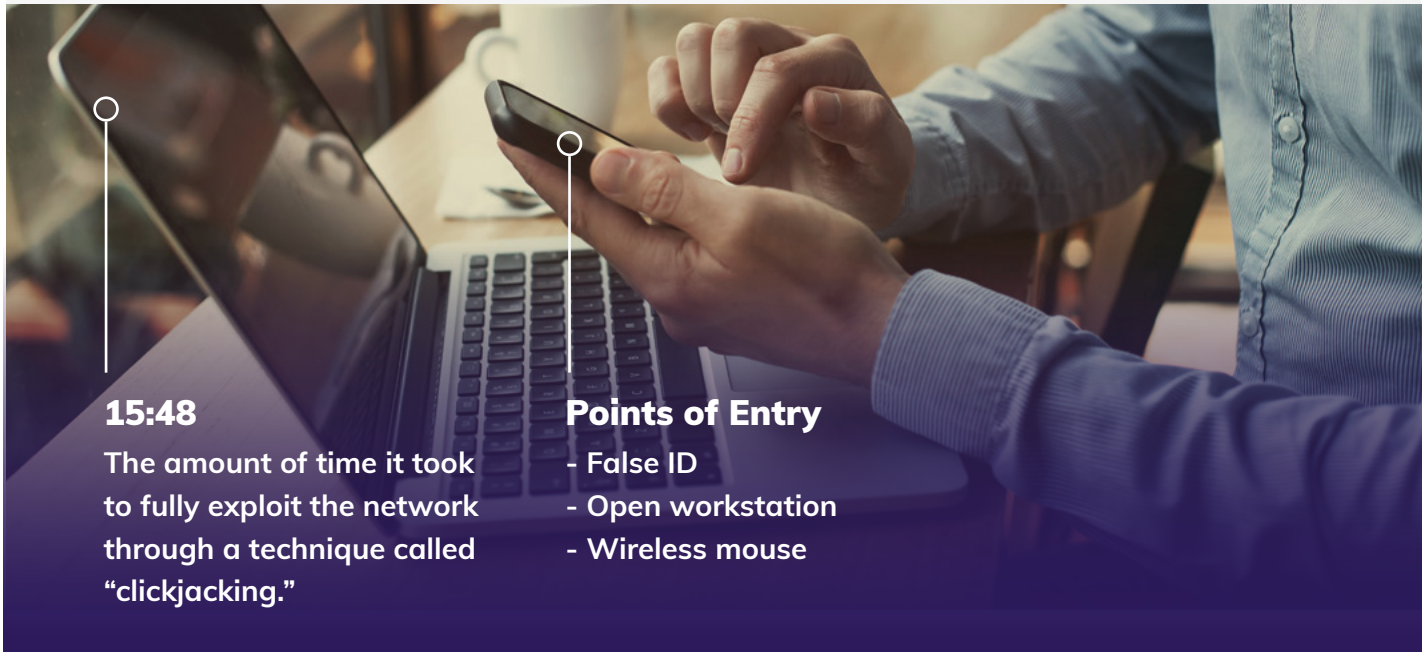
During a recent project with a major healthcare organization, a full penetration test performed over expansive attack avenues revealed that many servers were missing several third-party software and operating system patches on the internal network. Further exploitation of these vulnerabilities required access to the management VLAN, which was restricted to authorized devices via port security. Therefore, the network portion of the penetration test did not enable access to the organization's network.

In sharp contrast, the physical social engineering portion of the penetration test allowed network access. The testing team was able to enter the facility under false pretense and reboot a workstation to Kali Linux from a USB thumb drive. From this point, it was extremely easy to locate password hashes and exploit network vulnerabilities to obtain local administrator access on the network.

To further illustrate weaknesses in the organization's environment, the testing team searched for wireless peripheral devices. In an attack known as "clickjacking," the testing team was able to create an account on a workstation by sending commands to a wireless mouse receiver. After escalating the account's privileges to domain administrator using the same attack tactic, the network was fully exploited.

## PHYSICAL SOCIAL ENGINEERING

A critical component of penetration testing often overlooked.
Includes attempting to enter a facility and gain control of a network.



**15:48**

The amount of time it took to fully exploit the network through a technique called "clickjacking."

**Points of Entry**

- False ID
- Open workstation
- Wireless mouse

## ABOUT THE AUTHOR

**Brandyn Fisher | Senior Manager**
Cybersecurity Practice

Brandyn has an extensive background in cybersecurity with more than 10 years of professional experience in the area, an extensive list of security certifications, a Bachelor's in computer security and investigation, and a Master's in cybersecurity and information assurance. Most recently, Brandyn managed a penetration testing and security team as well as led vCISO services for The Mako Group, a cyber risk management firm acquired by Centric Consulting. With a diverse background across multiple industries, Brandon oversaw enterprise projects to bolster the security posture of large financial institutions, hospitals, municipalities and manufacturing entities.

**Want to keep your brand reputation and financial impact safe? Our Cybersecurity team can help address your security concerns.**

**Talk to an expert**

((CENTRIC))

## ABOUT US

Centric Consulting is an international management consulting firm with unmatched expertise in business transformation, AI strategy, cyber risk management, technology implementation and adoption. Founded in 1999 with a remote workforce, the company has established a reputation for solving its clients' toughest problems, delivering tailored solutions, and bringing in deeply experienced consultants centered on what's best for your business. In every project, you get a trusted advisor averaging over 15 years of experience and the best talent from across the United States and India. Centric deliberately builds teams that can scale up or down quickly based on client needs, industry and desired outcome.

Headquartered in Ohio, with 1,400 employees and 14 locations, Centric has been honored over the years with over 100 awards for its commitment to employees, clients and communities. Most recently, it was recognized by Forbes, for the eighth consecutive year, as one of America's Best Management Consulting Firms.

**Visit http://www.centricconsulting.com to learn more.**