PREPARED BY
HACKER TARGET

PREPARED
JULY 2021

MODERN THREATS & THE ATTACK SURFACE

A WHITEPAPER

JULY 2021

HACKER TARGET PTY LTD

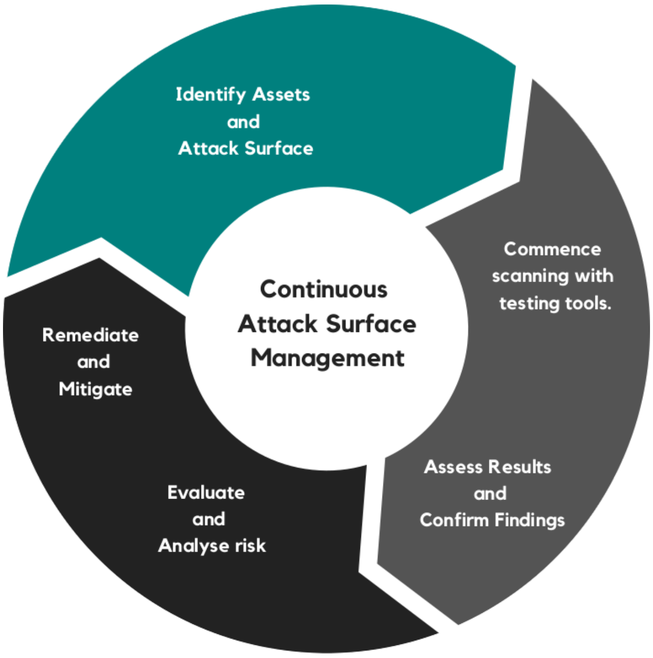
MODERN THREATS & THE ATTACK SURFACE >_

KNOW YOUR NETWORK FOOTPRINT.
KEEP YOUR DATA AND ASSETS SECURE.

The trend of moving infrastructure into cloud providers makes an organisation's network more dynamic than ever.

Vulnerability scanning and analysis are essential. Equally important is knowing what services, networks, and systems are exposed..

**Know your network footprint.
Keep your data and assets secure.**


Identify Assets and Attack Surface
Commence scanning with testing tools.
Assess Results and Confirm Findings
Evaluate and Analyse risk
Remediate and Mitigate
Continuous Attack Surface Management

AN ATTACKER ONLY HAS TO BE SUCCESSFUL ONCE.

Security teams need to deflect and block multitudes of attacks from all areas of their attack surface daily.

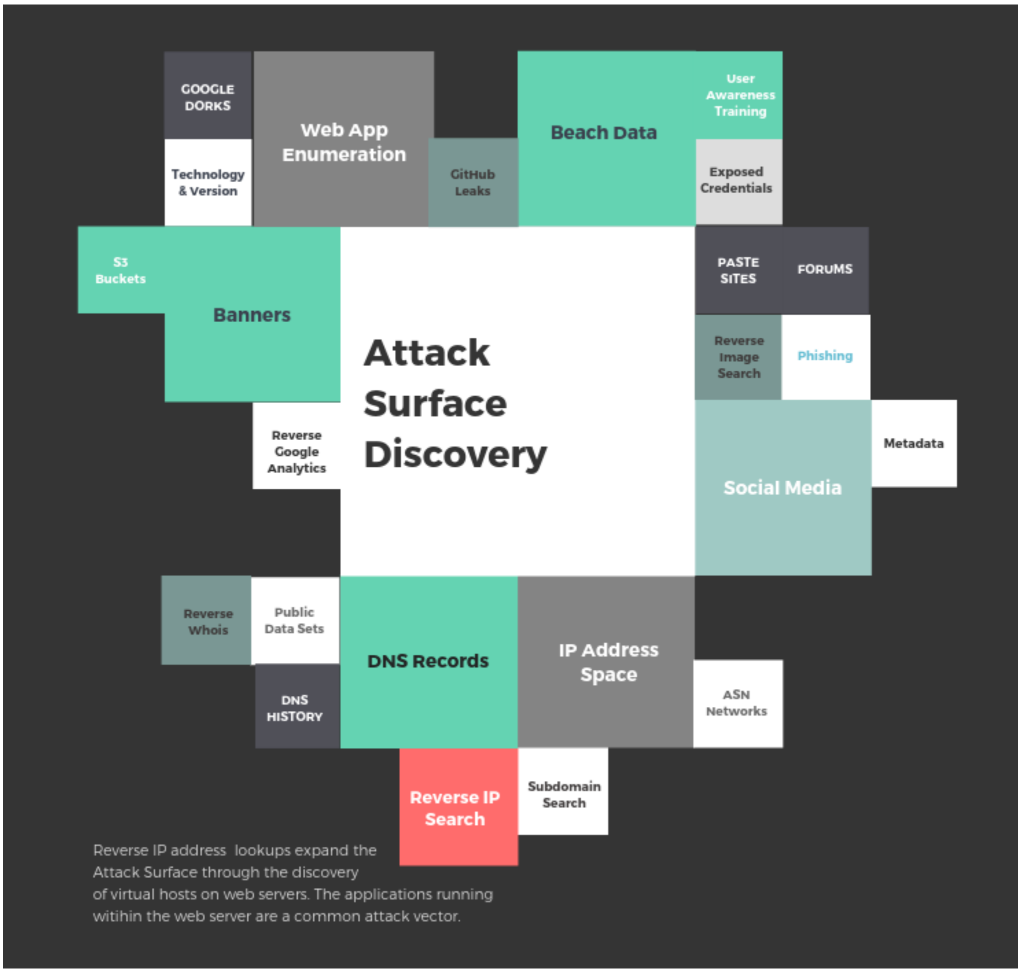
This white paper details the advantages of employing Open Source Vulnerability Analysis tools to protect your Internet facing servers.

Acknowledging vulnerability analysis is only part of the solution to staying secure. It is clear that reliable attack surface mapping and vulnerability identification is essential for any sized organisation.

According to the SANS Institute : "...Regular scanning ensures new vulnerabilities are detected in a timely manner, allow them to be remediated faster. Having this process in place greatly reduces the risks an organization is facing."

Attacks against infrastructure and services are increasingly common. For years attackers and penetration testers had free reign against the end user; attacking client systems that were soft and squishy. Adobe Acrobat, Flash, Browsers, and Office were the go-to exploits. As client systems have become more hardened, the pendulum has swung back towards attacks against Internet facing systems.

Organisations face very different threats now than a few years ago, with a pivot to the cloud, a jump in remote working, and increasing connectivity through the Internet of Things (IoT). Future-proofing the possibility of a hybrid style of work, businesses will need to re-work security that covers remote and in-house.



Reverse IP address lookups expand the Attack Surface through the discovery of virtual hosts on web servers. The applications running witihin the web server are a common attack vector.

INCREASING THREAT LANDSCAPE

As far back as 2002, there were Google Dorks. Security researchers discovered specific Google queries revealed Internet-connected devices. It is still possible to find thousands of unsecured, remotely accessible security cameras and printers via simple Google searches. Search engines such as Shodan.io and Censys.io are tools commonly used to passively discover open services and devices on the Internet.

THE WORLD IS DIGITISED

Digital convergence and innovation has been accelerating exponentially over the years. The global pandemic of 2020 and beyond became the landscape for the necessity to integrate technology in all areas of business, social, and home life. The integrations have expanded the attack surface, and opportunities and vectors for attackers have increased.

SHARED TECHNIQUES

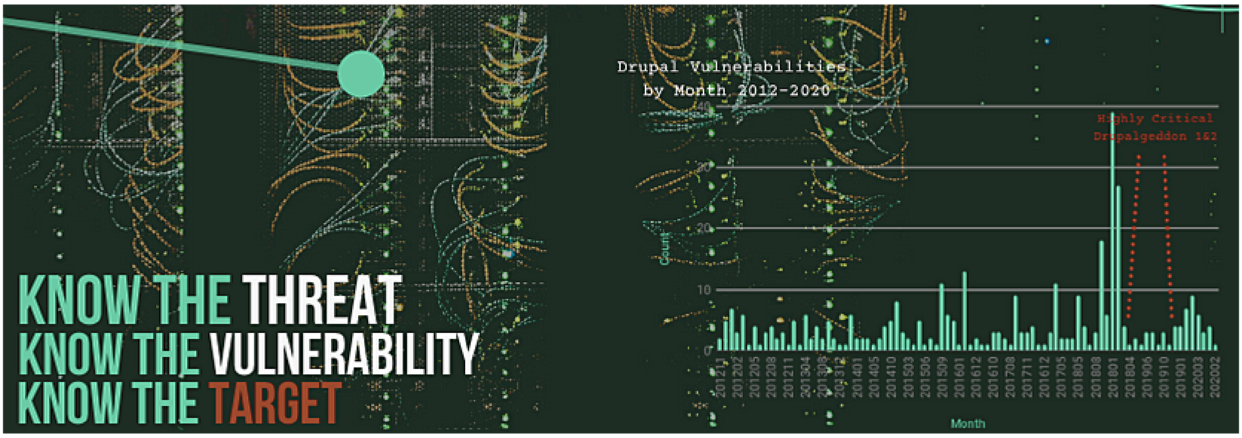
New attack techniques are shared within the security community for the benefit of Red & Blue Teams. These same techniques inevitably make their way into threat actor capabilities.

DARK WEB

The rise of the Dark Web makes it easy to distribute, trade, and locate data. Endless breaches seemingly provide an unlimited amount of data for sale to those wishing to use it for malicious means.

APT : ADVANCED PERSISTENT THREATS / HACK FOR HIRE GROUPS

APT's aim for long-term presence on a network most often used for data theft. These groups are becoming more common. Previously within the realm of state actors and the stealing of nation's secrets, these days, state sponsored hacking techniques are being used for monetization.



EASY ACCESS TO ADVANCED TOOLS

A proliferation of easily available hacking tools with advanced red team capabilities are being deployed against under resourced blue teams. The financial incentive, and ease of trading information has resulted in an explosion of financially motivated threat actors.

CYBER SECURITY BUDGET CONSIDERATIONS

An intelligent application of the cyber security budget is essential. Flash marketing and rack mounted pizza boxes with flashing lights do not solve security fundamentals.

Adequate training for technical staff and access to tools that solve known problems. Know the network, know the vulnerabilities and know the threats.

NEGLIGENT OR MALICIOUS INSIDERS

Humans are often the weakest link when it comes to cybersecurity. Lack of training for employees on cybersecurity threats, what to look out for, what to not do, what and how to report. On the other end are disgruntled employees who may leak information for personal or monetary gain.

INSUFFICIENT LOGGING & MONITORING

Good visibility into an organisation's network and systems has been a known problem for years. There have been expensive commercial solutions that make promises but are often unusable in day-to-day operations.

The future is looking better. Many high-quality open-source tools are filling this capability gap. OSQuery, Zeek, Arkime, and the ELK stack just touch the surface of what's now possible. Being open-source they can be stitched together into a powerful solution.

COMMON ATTACK AREAS

MIS-CONFIGURED SERVERS

Whether it is bad permissions, a mis-configured web, mail or remote access server, or a temporary fix that was done when the clock was ticking - a simple mistake can result in a vulnerable system.

SOFTWARE NOT UPDATED / PATCHED

Server operating systems, applications and plugins all need to be updated when security updates and or patches are released. There are many hosts that get overlooked leaving the service vulnerable to a variety of attacks. It really is only a matter a of time until a vulnerable service is discovered and the system is compromised.

WEB APPLICATIONS

PHP, Python, ASP applications, and the latest JS frameworks are a great way to get websites working quickly and dynamically, But they aren't set and forget. Like operating systems and software, these must be updated when security updates are made available.

Updates are constant and easily overlooked - until the day your blog is compromised and starts serving up malicious iframes to your unsuspecting audience.

PASSWORD REUSE

Using the same password over multiple accounts is a disastrous idea. It is one of the major contributors to data breaches. Clients re-using identical passwords over different accounts give attackers opportunities to use valid credentials to breach a corporate network and access customer or corporate data.

REMOTE ACCESS SERVICES

Remote access for work is on the rise, and with it comes more opportunities for attackers to probe for weak access points. Enterprise VPN and personal VPN usage have increased.

POOR SSH PASSWORD SECURITY

The use of strong passwords and two factor authentication on all internet-facing hosts is crucial.
View the ssh log for any internet-facing host and see how often the system is being hit by brute force ssh attacks

SOCIAL ENGINEERING

A broad term used to describe the technique where hackers trick humans to discover information for which they can then use in a cyber attack.

PUBLICLY AVAILABLE INTERFACES

Exponential increase in cloud infrastructure, storage and usage. This relatively new technology creates a huge set of vulnerabilities. One of which is publicly available interfaces.

ACTIVE DIRECTORY

Securing active directory is complicated. Active directory is increasingly integrated with cloud services, which has both positive and negative aspects. A simple example is the compromise of a user's Office365 password. This password may also provide access to AD services within the corporate network.

USES OF A COMPROMISED RESOURCE

RANSOMWARE

Increasingly Ransomware is the go-to for financially motivated actors. Compromise of one host enables a pivot into the network. Followed by deployment of ransomware and controlling access to devices, data, and network until payment is made.

DISTRIBUTION OF MALWARE

Using your web server to serve up content - just what it was made for right? What if the content is malicious? Loading and exploiting your customers or users, spreading key logging malware that is further compromising their desktops and eventually emptying their bank accounts.

PHISHING SITES

Fake pages used to collect credentials from users of the site. Commonly these are widely distributed in spam campaigns going after banking access or other services.
Alternatively a phishing site can be deployed tactically against your organisations users in a much more targeted approach to gain full access to the network and systems.

BACK-DOOR

Providing persistent access to the network, a compromised system may be simply used as a jump point into the network. This access may stay dormant for months or even years, ready and waiting for when the attacker wants to access the machine and pivot into the network.

SPAMMING HOST

A straight up spamming operation. Using your server to send out hundreds of thousands of spamming emails is a profitable use of your compromised host. This will go on until you stop it or you get blacklisted and the spammer finds another use for your server.

NOW IS A GOOD TIME TO SCAN YOUR INTERNET FACING NETWORKS

It is clear from the data, research, and increasingly high profile cyber attacks, security by obscurity was never a great strategy. Open services listening on the Internet will be found. Consequently, if they can be found, they will be attacked.

WHY USE HACKER TARGET

- Non-intrusive scan of your network / host perimeter.
- Identify security issues on your internet server and web site.
- Find security holes with trusted open source tools.
- Expertise in cyber security in a team with over 20 years experience.
- Simple Interface : launch scans with a simple form.
- Find forgotten assets and poorly maintained endpoints across the organisations Attack Surface.
- Schedule network and port scans for ongoing vulnerability detection and firewall monitoring.
- As a hosted service there is no installation or maintenance.

Learn More: **Hackertarget.com**

REASONS TO STAY SECURE

The impact of cyber attacks are far ranging and long lasting. After the initial attack, the clean up and costs associated with repairing affected systems, devices, and networks can be huge.

With the obvious financial impact, there are other major damages to you and your business,

WHY STAY SECURE:

- Prevent data loss and / or theft.
- Prevent costly **downtime** resulting in network being unavailable to users.
- Avoids loss of **reputation** and trust in the event of a security breach.
- **Compliance** Failure
- Provides assurance to customers that information security is valued.

Exercising added actions for security and continual updates is time-consuming and costly.

But never assume vulnerabilities won't affect you or your business.

Everyone is a target.

Scan and protect your data.

MODREN THREATS & THE ATTACK SURFACE

A WHITEPAPER

HACKER TARGET PTY LTD