

internet2.0

MILITARY-GRADE

CYBER PROTECTION

Internet 2.0

Cloaking Firewall

Author

Internet 2.0 team

Table of Contents

Introduction.....	2
Reconnaissance.....	2
Public Scanning Subscription Services.....	3
Cloaking Firewall – Obfuscation by Design.....	4
Conclusion.....	7

Introduction

The purpose of this white paper is to discuss the innovation, tactical implementation and impact of a new technology created and patented by Internet 2.0. This technology is called a 'Cloaking Firewall' and it has been researched, designed, and developed by Internet 2.0.

In essence, a Cloaking Firewall defeats network scanning. According to N. Hoque from *Network attacks: Taxonomy, tools and systems*' a network scanning tool aims to identify active hosts on a network, either (a) to attack them, or (b) to assess vulnerabilities in the network'. It provides an overall status report regarding network hosts, ports, IPs, etc.'

Scanning is important for attackers because it provides them with all the network information they need to interact and possibly attack your network over the internet. The military have a specific definition for this type of capability. Scanning is a critical capability for an attacker's ability to conduct reconnaissance, find their target and identify weaknesses (including open ports and unpatched operating systems). In the Military Appreciation Process language scanning technology is a critical capability to any cyber attacker's centre of gravity.

Internet 2.0's Cloaking Firewall denies the ability for attackers to see or ping your network, rendering many of the avenues they traditionally use to interact with your network unavailable. In other words, we have worked out how to defeat scanning.

Reconnaissance

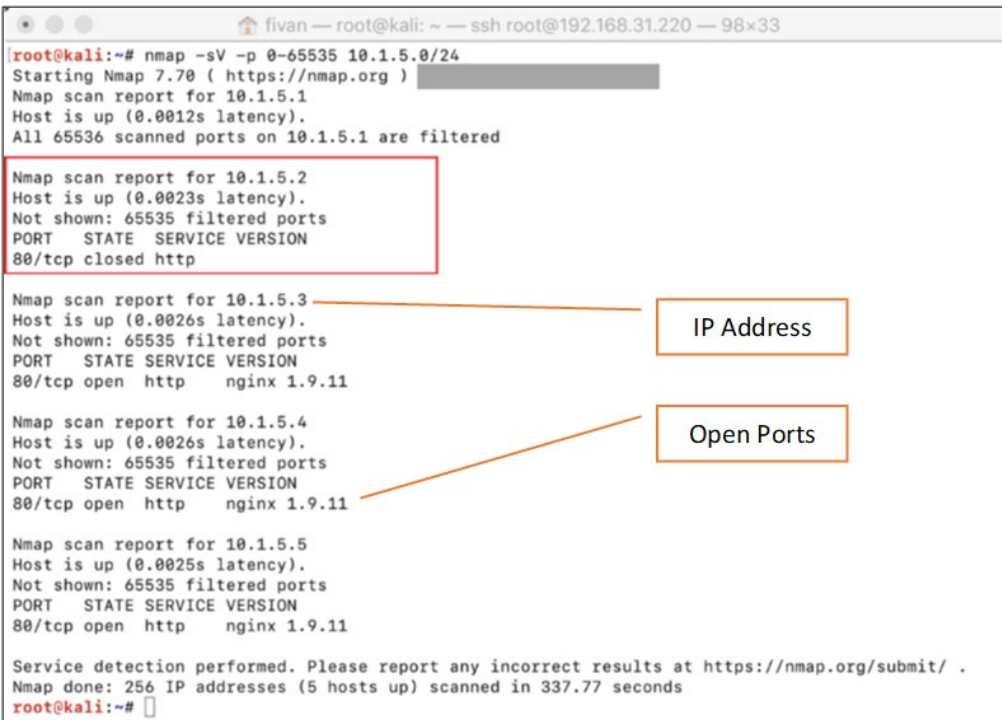
The MITRE ATT&CK framework is the industry accepted framework for layout threat modelling. In this framework reconnaissance is the very first stage in the MITRE ATT&CK.¹ Active scanning is the very first technique listed under reconnaissance. In every cyber attack the attacker needs to be able to not only identify their target but identify specific technical information about their target. Specific information that private scanning or public scanning subscription services can provide are:

- IP addresses
- The status of the open and closed ports on a firewall or switch
- The operating system in use
- Applications in use
- Certificates

The above technical information is needed in computer networking as packets need the intended address and routing information to communicate with the network. Without it the Domain Name System servers or telecommunications providers do not know where to route your packets. Attackers need to know this information if they are to interact with their target network, otherwise it would be as if their target does not exist on the internet. Basically, without scanning they cannot interact with your network.

¹<https://attack.mitre.org/#>

Secondly, the status of open ports and operating systems on your network is extremely valuable to attackers. This is because when communicating between networks most operating systems, applications or protocols require communication through the same open port. By seeing which port is open, or in use, it is easier to determine which application or protocol is being used by the target (see the example in Figure 1). An attacker will then go about the process of gathering victim network information which is the fourth technique in the reconnaissance stage under the MITRE ATT&CK framework. This information is valuable because it informs the next stage of the attack.



```
[root@kali:~# nmap -sV -p 0-65535 10.1.5.0/24
Starting Nmap 7.70 ( https://nmap.org )
Nmap scan report for 10.1.5.1
Host is up (0.0012s latency).
All 65536 scanned ports on 10.1.5.1 are filtered

Nmap scan report for 10.1.5.2
Host is up (0.0023s latency).
Not shown: 65535 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    closed http

Nmap scan report for 10.1.5.3
Host is up (0.0026s latency).
Not shown: 65535 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   nginx 1.9.11

Nmap scan report for 10.1.5.4
Host is up (0.0026s latency).
Not shown: 65535 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   nginx 1.9.11

Nmap scan report for 10.1.5.5
Host is up (0.0025s latency).
Not shown: 65535 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   nginx 1.9.11

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 337.77 seconds
root@kali:~#
```

Figure 1: Port scan courtesy of Nico Surantha.

Public Scanning Subscription Services

Publicly available commercial services that conduct scans everywhere on the internet are becoming more mainstream, cheaper to access and more detailed in providing information. The best example is of this is Shodan.io, which can be seen in Figure 2. This service, for a subscription, can filter all publicly available network information on a graphical interface accessible through a standard web browser. The technology Shodan uses is a commercially confidential scanning technology application. The service provides information on ports, IP addresses, applications in use, the Intrusion Prevention System, Autonomous System Number, Hostname, Secure Sockets Layer certificates and existing potential vulnerabilities. Most of the information provided is enough to enable attackers to conduct a significant part of the reconnaissance stage. In fact, of the ten techniques offered in the reconnaissance stage of the MITRE ATT&CK framework eight are covered by a monthly \$300 subscription to Shodan.

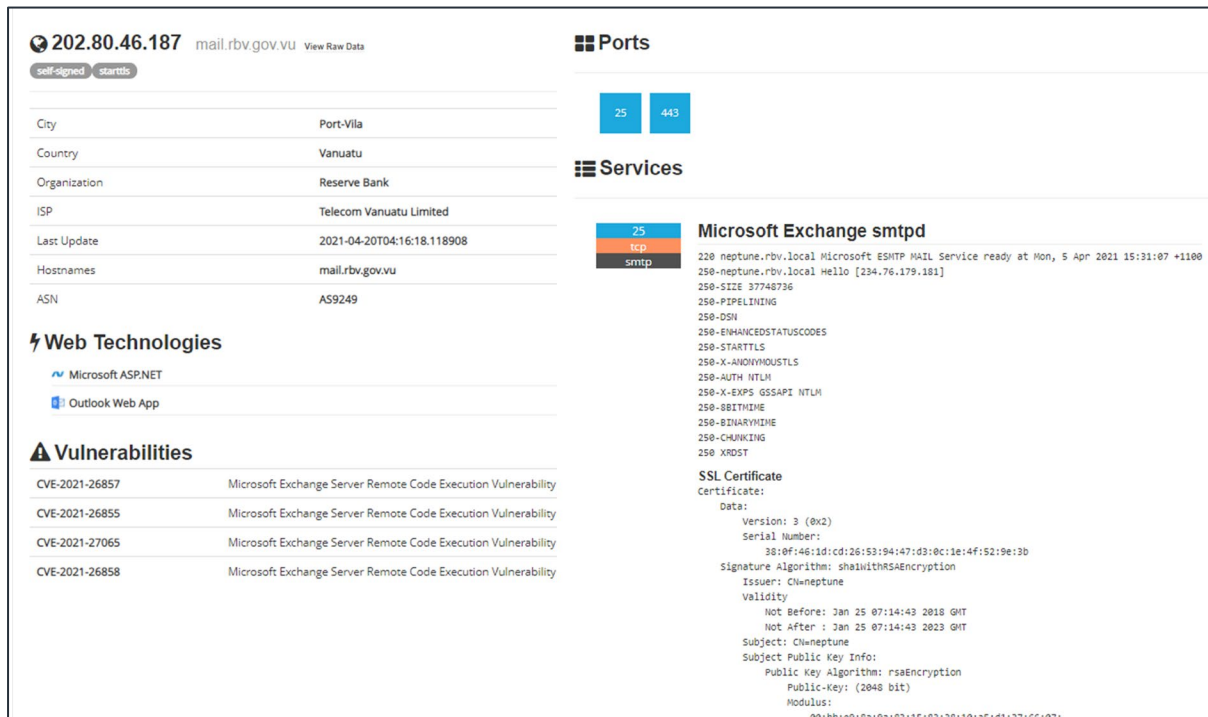


Figure 2: Shodan interface courtesy of Shodan.io.

It is a significant problem that easily accessible services like Shodan provide access to sensitive information to low skilled cyber attackers. Previously a sophisticated attacker would be required to find the above information in the reconnaissance stage using private scanning tools. This highlights the necessity to account for such publicly available sophisticated techniques by cyber defenders and the importance of defeating scanning tools.

The Cloaking Firewall is the answer to this problem. Internet 2.0 developed the Cloaking Firewall specifically to resolve the risk of this information being provided by our networking equipment. If you have a firewall, a static IP address or a domain name as part of your network then all this information is scanned daily by dozens of companies, governments, and threat actors on the internet.

Cloaking Firewall – Obfuscation by Design

Internet 2.0 has developed a technology that defeats scanning technology without any significant degradation in network performance. Based on tests conducted by Internet 2.0 we assess the Cloaking Firewall engine has less than 1ms of impact on network performance and reduces all network visibility from scanning technology.

This Cloaking Firewall is a commercial technology under patent by Internet 2.0. It is currently deployed via the Internet 2.0 operating system, and available on major cloud providers such as AWS and Azure.

When scanned no visible open ports or other sensitive information is available. Figures 3 to 5 are examples of tests conducted by Internet 2.0.

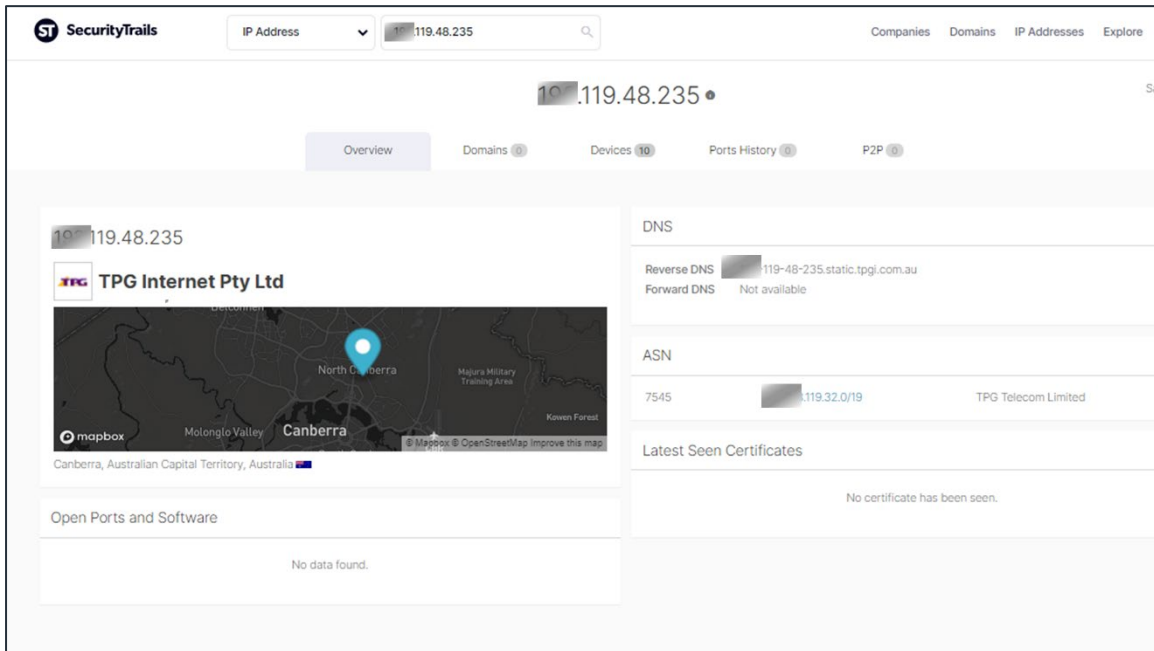


Figure 3: Network history April to July 2021.

Figure 3 is a good representation of our network over three months. It is a historical view over a 90-day window. As you can see in Figure 3, the SecurityTrails historical view picks up the device count from when the Cloaking Firewall technology was disabled for the Shodan scan but it cannot detect any open ports. Figures 4 and 5 are a direct comparison of Shodan scans three months apart as we deployed the Cloaking Firewall technology onto our network. As you can see Shodan cannot even recognise the existence of the network after the Cloaking Firewall was enabled.

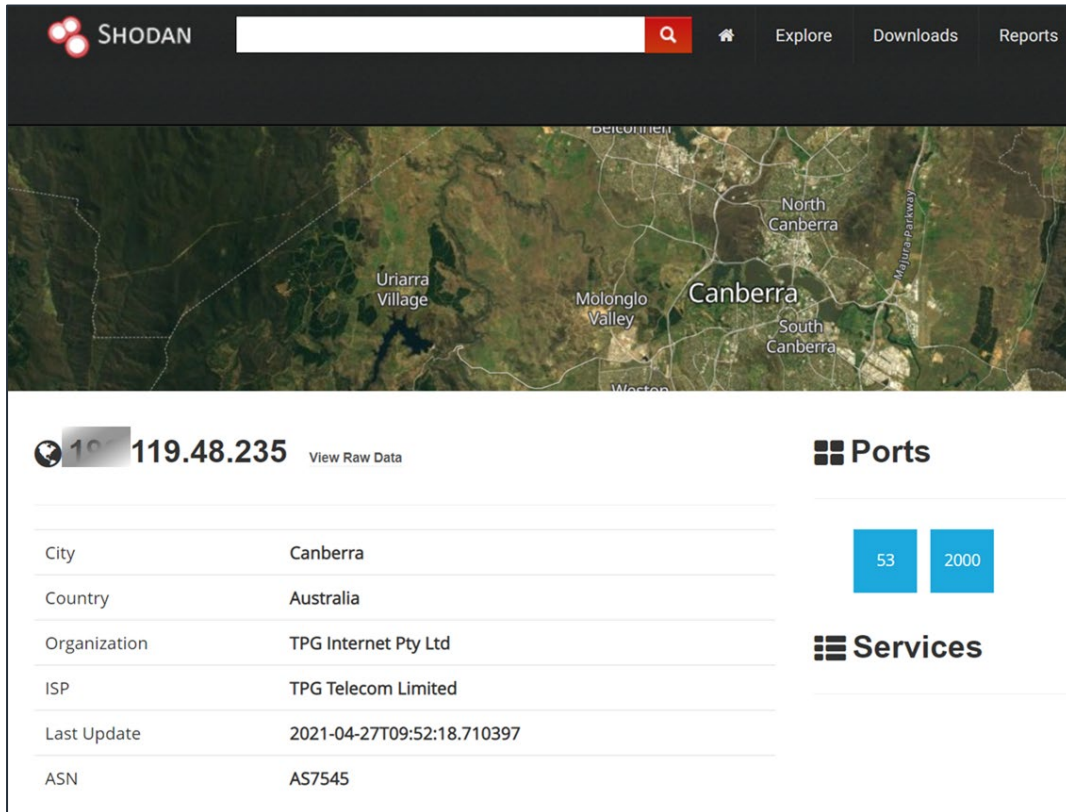


Figure 4: Normal network April 2021.

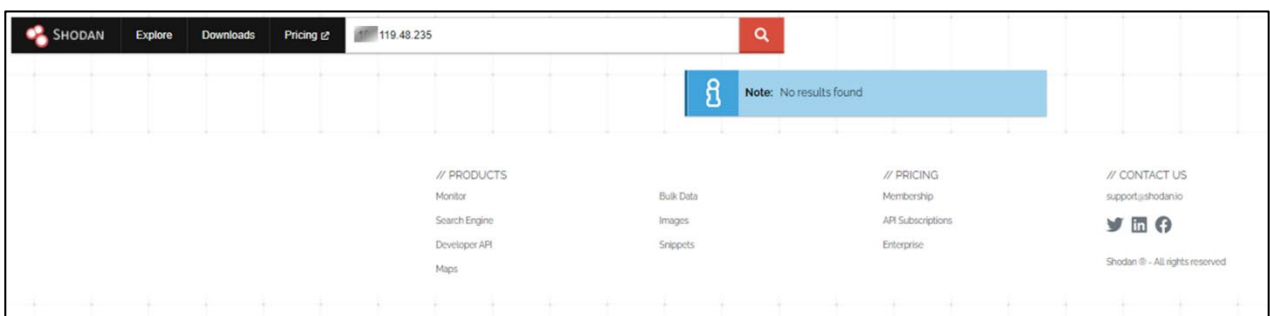
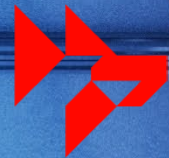


Figure 5: Internet 2.0 Cloaking Firewall engine July 2021

Conclusion

As we can see the Cloaking Firewall will be a critical technology going forward to protect networks and their administrators from malicious attackers gaining critical intelligence, and mitigate the ever increasing financial, organisational and reputational impacts of a cyber attack on your business. It will add to defenders' ability to protect their network and will reduce the risk profile that public scanning subscription services impose on network administrators.

internet2.0



MILITARY-GRADE

CYBER PROTECTION

Australia

Level 1

18 National Circuit

Barton ACT 2600

ABN: 17 632 726 946

United States

Suite 100

211 N Union St

Alexandria 22314

EIN: 86-1567068

contact@internet2-0.com