“Finecars” Network Security Assessment

# **Information gathering & Recon**

## Nmap Scan:

## Command used: “**nmap -Pn -sV 192.168.10.0/23”**

* (-Pn) skip ping-check on systems in scope
* (-sV) get version information on discovered services if possible
* (192.168.10.0/23) the IP range of the network we are targeting
  + - 192.168.10.1 will appear in this scan, but no action will be taken against it as it is determined to be out of scope.

**4 Significant Hits (and service information):**services appearing multiple times are highlighted in green

1. **192.168.10.1**
   1. Out of scope
2. **192.168.10.10**
   1. Apache httpd 2.4.7 ((ubuntu)) – Web Server for company Site (up to date, only exploits discovered required authentication to system, which we couldn’t acquire)  
      more info at: <https://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-66/version_id-161847/year-2014/Apache-Http-Server-2.4.7.html>
      1. Port: 80/TCP
      2. Service: Http
   2. MySQL 5.5.58-0ubuntu0.1404.1 - This service is severely out of date, latest version is 8.x, various vulnerabilities have been reported in the 5.5.x release**.** for a complete list of vulnerabilities in this service please refer to: <https://security-tracker.debian.org/tracker/source-package/mysql-5.5>
      1. Port: 3306/TCP
      2. Service: mysql
3. **192.168.11.4**
   1. Microsoft Windows RPC – Password Protected (didn’t crack)
      1. Port: 135/TCP
      2. Service: msrpc
   2. Microsoft Windows netbios-ssn
      1. Port: 139/TCP
      2. Service: microsoft-ssn
   3. Microsoft Windows XP Microsoft-ds
      1. Port: 445/TCP
      2. Service: microsoft-ds
   4. Microsoft Windows RPC **(again? This is a duplicate service)**
      1. Port: 1025/TCP
      2. Service: msrpc
   5. Unidentified Service
      1. Port: 5000/TCP
      2. Service: upnp?
4. **192.168.11.10**
   1. Microsoft IIS httpd 10.0 – Another web server
      1. Port: 80/TCP
      2. Service: http
   2. Microsoft Windows RPC – Password Protected (didn’t crack)
      1. Port: 135/TCP
      2. Service: msrpc
   3. Microsoft Windows netbios-ssn
      1. Port: 139/TCP
      2. Service: netbios-ssn
   4. Microsoft Windows Server 2008 R2 – 20012 microsoft-ds (workgroup: FINECARS)
      1. Port: 445/TCP
      2. Service: Microsoft-ds

# **Vulnerability Analysis:**

It would appear, from what we could manage, your system’s security is well designed to ward off an outside entity (namely us). However some out-of-date services are weak to anyone [currently or formerly] on the inside, and any who they may slip their credentials to -knowingly or not. Various remote exploits are dependent on authentication. Your security is compromised the moment any credentials are slipped. While we didn’t have the opportunity to with the limitations of our environment, dedicated attackers have methods of squeezing these credentials out of your employees unknowingly through social engineering mechanisms, phishing emails, and any number of creatively mischievous schemes.

The best approach to resolve this fault is to remember to update the vulnerable services, noted in the above section, and to keep all services patched with the latest release. Also, if you don’t already enforce one, we recommend implementing a policy that requires updating credentials fairly frequently.

# **Report Summary:**

**Scope of Assessment:** Ip range of “192.168.10.0/23”

**Project Objectives:** gain access to the system, and any customer information possible, and report on our findings.

**Summary of Findings:** Access was not gained, no customer information was acquired, despite the flourishing environment of vulnerabilities – within the scope of the project we could not acquire the requisite information to exploit them.

**Summary of Recommendations:** Update all services, namely the MySQL server and the Apache webserver. Further, In order to minimize exploitation of the vulnerabilities which are currently prevalent it is recommended that you implement a credential expiration policy, enforcing that employees to update and change their credentials regularly.