|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Host** | **Ip address** | **Open Ports** | **Issues/Notes** |  |
| Attacker's Machine | 203.0.113.100 |  |  |  |
|  |  |  |  |  |
| Vyos Switch 1 |  |  | Vulnerable to ARP poisoning |  |
|  |  |  |  | Can capture VoIP call using G.711 codec which gives VNC credentials to "Windows 10", which is in the internal network |
|  |  |  |  | Captures an email from bob to amanda @ treetown.t211 capturing bob's credit card details, phone number, and pc credentials of "Lab:sparky1" |
|  |  |  |  | (Theoretical) - Intercept traffic to and from "Web Server", giving away credentials and secret data |
|  |  |  |  |  |
|  |  |  |  |  |
| pfSense | 203.0.113.10 | 53/tcp, 80/tcp, 5900/tcp | The credentials for the web interface are the default of "admin:pfsense" | |
|  | 172.16.20.1 (Office) | 53/tcp, 80/tcp | Traffic between subnets can be captured | |
|  | 192.168.100.1 (Server) | 53/tcp, 80/tcp | Configuration can be changed to allow access to the internal network | |
|  | 192.168.101.1 (Generator) | 53/tcp, 80/tcp |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Representation Of T | h203.0.113.1, 203.0.113.20, 203.0.113.21 | 22/tcp, 25/tcp, 53/tcp, 2000/tcp |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| Windows 10 | 172.16.20.2 | 135/tcp, 139/tcp, 445/tcp, 5900/tcp | Weak password "Password1", which is spelt out in the password hint | |
|  |  |  | VNC password "abc123" is obtained from a phone call | |
|  |  |  | Provides a pivot into the internal network | |
|  |  |  |  |  |
|  |  |  |  |  |
| Phone 1? | 172.16.20.100 | 286/tcp, 1312/tcp, 1416/tcp, 2259/t | Downloads configuration data using HTTP | |
|  |  |  |  |  |
|  |  |  |  |  |
| Camera | 172.16.20.103 | 22/tcp | Vulnerable to packet capture, gives ftp credentials "user:test" to connect to "SecServer" | |
|  |  |  | Uses plaintext ftp to send camera data | |
|  |  |  |  |  |
|  |  |  |  |  |
| Phone 2? | 172.16.20.104 | 22/tcp | Makes a plaintext call using G.711 codec which gives credentials for remote access to "Windows 10" | |
|  |  |  |  |  |
|  |  |  |  |  |
| Bob's PC | 172.16.20.105 | Nothing | Downloads calc.exe split into 459 parts, encoded in base64, from txt dns queries | |
|  |  |  | Plaintext email with credit card details | |
|  |  |  | Information about Bob being away, and how often Amanda will check Bob's PC (could do less stealthy attacks without being detected) | |
|  |  |  | Information about a new sensor being ordered (perhaps the old one will be offline during installation - meaning no security system) | |
|  |  |  |  |  |
|  |  |  |  |  |
| Sensor | 172.16.20.106 | Nothing | Sends plaintext MQTT data to "EnvServer" including temperature readings and alarm/security system states | |
|  |  |  |  |  |
|  |  |  |  |  |
| Other 2 | ???? | ???? | Not visible on the network - 172.16.20.101 and 172.16.20.102 don't respond on any port from both Kali & Bob's PC. Maybe 172.16.20.107? | |
|  |  |  |  |  |
|  |  |  |  |  |
| Web Server | 192.168.100.2 | 22/tcp, 80/tcp | Vulnerable to SQL Injection |  |
|  |  |  |  | Can bypass the login system, getting access to the admin account (credentials "Admin:myDBPass") |
|  |  |  |  | Can exfiltrate the entire database using classic injection, or blind injection for a stealthier attack, including all account credentials, and credit card details |
|  |  |  | phpinfo has the root "DatabaseServer" credentials "root:myDBpass" | |
|  |  |  | Passwords are stored in plaintext |  |
|  |  |  | The admin user can view the passwords of all users | |
|  |  |  | Uses plaintext HTTP to transmit credentials and secret data | |
|  |  |  | Passwords are case-insensitive |  |
|  |  |  |  |  |
|  |  |  |  |  |
| DatabaseServer | 192.168.100.3 | 3306/tcp | Can login to the sql server using the root credentials found on the website via "SecServer", access to everything in the database | |
|  |  |  |  |  |
|  |  |  |  |  |
| EnvServer | 192.168.100.5 | 1883/tcp | Uses plaintext MQTT with no security, sensor readings can be sent from any device | |
|  |  |  |  |  |
|  |  |  |  |  |
| Store | 192.168.100.201 | 22/tcp, 111/tcp, 3260/tcp, 42397/tc | piSCSI drive with sensitive company data has no authentication/authorisation | |
|  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
| SecServer | 192.168.100.202 | 21/tcp, 135/tcp, 139/tcp, 445/tcp, 1 | Vulnerable to metasploit "windows/dcerpc/ms03\_026\_dcom", allows access to CLI | |
|  |  |  | Credentials "user:hwlab" are stored in plaintext on the desktop | |
|  |  |  | Can reconnect a disconnected iSCSI drive with sensitive company data | |
|  |  |  | Provides a pivot into the server subnet | |
|  |  |  | ftp config including credentials "user:iyzz" | |
|  |  |  |  |  |
|  |  |  |  |  |
| Generator | 192.168.101.103 | Nothing | Turns off if "temp/coolingPlant" exceeds 158 | |
|  |  |  |  |  |
|  |  |  |  |  |
| Misc | Misc | Misc | Web Server admin password is the same as the root database password | |