SECURITY DOCUMENTATION

Submitter’s ID: 1121

SYSTEM OVERVIEW

Briefly describe the overall system (in 200 words or less).

One cannot secure a system when its purpose and scope are unknown.

An Ubuntu machine hosts the basic interface for end users to interface with the system. It contains information from a MySQL database, access to the HMI on the Winserv2012 machine at 10.0.94.9, and an admin page that lets the database be edited. The Winserv2016 machine handles DNS and time. An email server is available on the 10.0.94.7 machine in addition to an FTP server. The Ubuntu machine at 10.0.94.8 and the Winserv2012 machine at 10.0.94.9 make up the machines that interface with the windfarm as a PLC and HMI to the wind turbines, respectively. A VPN machine serves as the interface to this network from the outside world.

ASSET INVENTORY

List all of the system's devices, by name, and their key attributes in the following table.

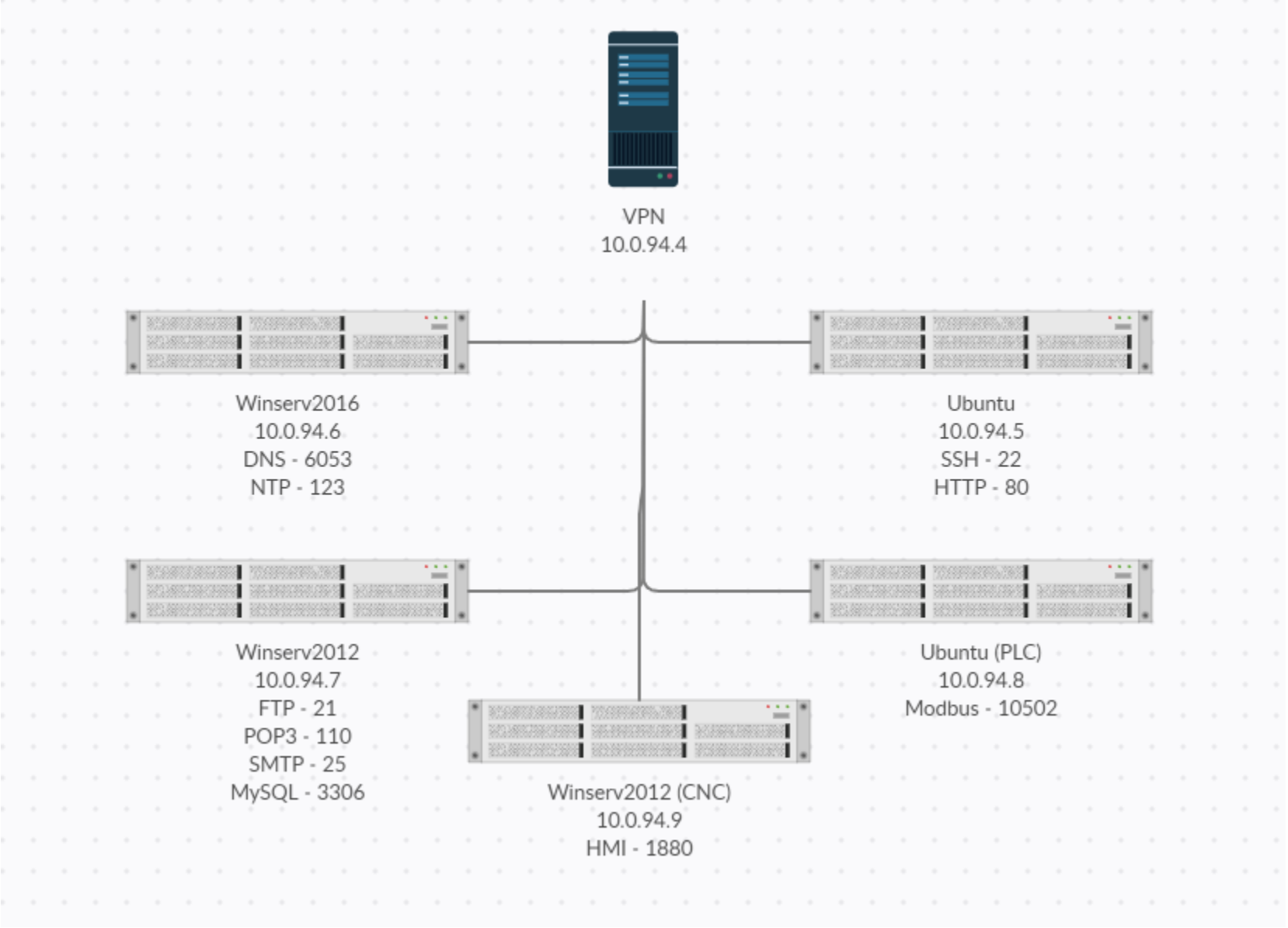
Asset management is a critical component of operational technology security. One cannot secure a network when one does not know what devices and services are running on the network.

Host	OS	IP Address	Port	Service
SSH	Ubuntu	10.0.94.5	22	SSH
Website	Ubuntu	10.0.94.5	80	HTTP
DNS	Winserv2016	10.0.94.6	6053	DNS
NTP	Winserv2016	10.0.94.6	123	NTP
FTP	Winserv2012	10.0.94.7	21	FTP
Email Server	Winserv2012	10.0.94.7	110	POP3
Email Server	Winserv2012	10.0.94.7	25	SMTP
Modbus	Ubuntu	10.0.94.8	10502	Modbus
HMI UI	Winserv2012	10.0.94.9	1880	HMI
Database	Winserv2012	10.0.94.7	3306	MySQL

NETWORK DIAGRAM

Provide a network diagram for your system. All hosts, network appliances, and services should be identified.

Current and detailed network diagrams facilitate enhanced situational awareness, especially for new staff that may be responding to a cyber security incident.



PLEASE LIST ALL VULNERABILITIES YOU FOUND AND THE MITIGATIONS YOU TOOK FOR EACH

The CyberForce competition environment was "seeded" with many vulnerabilities. List each vulnerability that you were able to identify. For each vulnerability, also list the mitigation(s) that you were able to enact (e.g., system hardening, software patch, compensating control, operational procedure).
Security documents often include a section of known issues—both those that have been resolved as wells open issues that may or may not yet have mitigating controls.

Example: Add a row to the table for each unique vulnerability per host. For example, if Alice, Bob, and Carol all have weak passwords on host Foo, this merits one line in the table. If Alice, a network admin, has weak passwords on three hosts, then three lines should be added to this table.

Host/System	Vulnerability	Mitigation(s)
10.0.94.5	CVE-1999-0170	Reconfigure to disallow remote hosts to mount NFS shares
10.0.94.6	CVE-1999-0519	Update sharing permissions for SMB shares
10.0.64.7	CVE-1999-0519	Update sharing permissions for SMB shares
10.0.64.6	SMB Signatures not Required	Require SMB security signatures server side
10.0.64.7	SMB Signatures not Required	Require SMB security signatures server side
10.0.64.9	SMB Signatures not Required	Require SMB security signatures server side
10.0.94.5	CVE-1999-0103	Disable `echo` service
10.0.94.5	CVE-1999-0524	Disallow ICMP timestamp request responses
10.0.94.6	CVE-1999-0524	Disallow ICMP timestamp request responses
10.0.94.7	CVE-1999-0524	Disallow ICMP timestamp request responses
10.0.94.8	CVE-1999-0524	Disallow ICMP timestamp request responses
10.0.94.5	Daytime Service Detection	Disallow `daytime` service to make timed auth attacks more difficult
10.0.94.5	CVE-1999-0632	Disable RPC portmapper
10.0.94.7	Microsoft KB2696547	Disable SMBv1
10.0.94.5	Malicious Script `evilsh`	Remove malicious script
10.0.94.5	Admin password visible	Change password verification to compare to a hash

SYSTEM HARDENING

In 1250 words or less, please explain ALL additional defensive steps you took (or are taking) to harden your system? Provide justification for each action you took and any actions you may have considered but chose not to take.

Cybersecurity professionals must proactively harden and defend their systems. It is not enough to just mitigate known vulnerabilities.

With the scope of this system setup and architecture requiring us to largely modify systems in place and not change the methods used to access them, the first step that has been taken to harden the system is to disallow communication that isn't expected. This will mean that, even if an attacker is able to get into a single system, there will be far more work required for them to compromise another machine. A couple options explored for this were using some firewall system like pfsense or client-side rules such as iptables. At the end of the day, for simplicity sake and to ensure some system is actually implemented, iptables are setup with pfsense being a goal to establish before the competition. Next, user provided code is being checked throughout all the public facing systems to find any possible issues that could arise from their design. For instance, a file from the webserver on 10.0.94.5 had the login credential visible in plaintext which would allow any agent to bypass the login and modify a database of data that had been collected.

After seeking to harden these systems, the next step is to ensure that intrusions can be detected and properly addressed. Adding snort to the environment will allow us to monitor the network as it is actively attacked and respond to any changes that may be introduced to the system. This intrusion detection system plays a key role in the defensive strategy since, without the information about what is changing and what has been done to our system, there is no possible way to properly ensure their security.