Text

Description automatically generatedCyberhawks CCDC State 2/4/2022

Team10        Lake Superior College

NISE Website: ccdcadmin1.morainevalley.edu

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Players | NISE Username | NISE Password | NETLAB Login (VMs) | NetLab init PW |
| Ryan | team10a | kLMQ8sZwc2 | v10u1 | ENRNY92k |
| Tyler | team10b | YeHshWz4US | v10u2 | ENRNY92k |
| Carter | team10c | zSP6WKNF8T | v10u3 | ENRNY92k |
| Caleb | team10d | zwUekMdNFp | v10u4 | ENRNY92k |
| Jalen | team10e | vM9CmfPmaj | v10u5 | ENRNY92k |
| Jeremy | team10f | EDytMznwgH | v10u6 | ENRNY92k |
| Martin | team10g | S3BzFXd7WE | v10u7 | ENRNY92k |
| Josh | team10h | TXTbYfqEN6 | v10u8 | ENRNY92k |

NETLAB Website: ccdc.cit.morainevalley.edu

Accounts    v10u1 – v10u8 init pwd = ENRNY92k (ECHO – NOVEMBER – ROMEO – NOVEMBER – YANKEE – NINE – TWO – KILO)

**Functional Services**

Certain services are expected to be operational at all times or as specified throughout the competition. In addition to being up and accepting connections, the services must be functional and serve the intended business purpose. At random intervals, certain services will be tested for function and content where appropriate. Precise services to be scored are configured by the scoring management team, but will be delineated via the ISE/Team Portal.

**HTTP**

A request for a specific web page will be made. Once the request is made, the result will be stored in a file and compared to the expected result. The returned page must match the expected content for points to be awarded.

**HTTPS**

A request for a page over SSL will be made. Again, the request will be made, the result stored in a file, and the result compared to the expected result. The returned page needs to match the expected file for points to be awarded.

**SMTP**

Email will be sent and received through a valid email account via SMTP. This will simulate an employee in the field using their email. Each successful test of email functionality will be awarded points.

**POP3**

POP3 connections will be performed against the system using usernames from Active Directory. Once connected a series of commands will be run and the output examined. Correct responses will be awarded points.

**DNS**

DNS lookups will be performed against the DNS server. Each successfully served request will be awarded points.

|  |  |  |
| --- | --- | --- |
| INTERNAL | Local IP | 'Public' IP |
| Docker/Remote | 172.20.240.10 | 172.25.20+team#.97 |
| Debian 8.5 DNS/NTP | 172.20.240.20 | 172.25.20+team#.20 |
| USER |  |  |
| Ubuntu 14 Web | 172.20.242.10 | 172.25.20+team#.23 |
| 2012 AD/DNS/DHCP | 172.20.242.200 | 172.25.20+team#.27 |
| Ubuntu Wkst | dynamic | dynamic |
| PUBLIC |  |  |
| Splunk | 172.20.241.20 | 172.25.20+team#.9 |
| CentOS 7 E-Comm | 172.20.241.30 | 172.25.20+team#.11 |
| Fedora 21 Webmail/WebApps | 172.20.241.40 | 172.25.20+team#.39 |

|  |  |  |  |
| --- | --- | --- | --- |
| Team | Palo Alto e1/3 Outbound to Core | Core connection to Palo Alto | "Public" IP pool |
| 1 | 172.31.21.2/29 | 172.31.21.1 | 172.25.21.0/24 |
| 2 | 172.31.22.2/29 | 172.31.22.1 | 172.25.22.0/24 |
| 3 | 172.31.23.2/29 | 172.31.23.1 | 172.25.23.0/24 |
| 4 | 172.31.24.2/29 | 172.31.24.1 | 172.25.24.0/24 |
| 5 | 172.31.25.2/29 | 172.31.25.1 | 172.25.25.0/24 |
| 6 | 172.31.26.2/29 | 172.31.26.1 | 172.25.26.0/24 |
| 7 | 172.31.27.2/29 | 172.31.27.1 | 172.25.27.0/24 |
| 8 | 172.31.28.2/29 | 172.31.28.1 | 172.25.28.0/24 |
| 9 | 172.31.29.2/29 | 172.31.29.1 | 172.25.29.0/24 |
| 10 | 172.31.30.2/29 | 172.31.30.1 | 172.25.30.0/24 |
| 11 | 172.31.31.2/29 | 172.31.31.1 | 172.25.31.0/24 |
| 12 | 172.31.32.2/29 | 172.31.32.1 | 172.25.32.0/24 |
| 13 | 172.31.33.2/29 | 172.31.33.1 | 172.25.33.0/24 |
| 14 | 172.31.34.2/29 | 172.31.34.1 | 172.25.34.0/24 |
| 15 | 172.31.35.2/29 | 172.31.35.1 | 172.25.35.0/24 |
| 16 | 172.31.36.2/29 | 172.31.36.1 | 172.25.36.0/24 |
| 17 | 172.31.37.2/29 | 172.31.37.1 | 172.25.37.0/24 |
| 18 | 172.31.38.2/29 | 172.31.38.1 | 172.25.38.0/24 |
| 19 | 172.31.39.2/29 | 172.31.39.1 | 172.25.39.0/24 |
| 20 | 172.31.40.2/29 | 172.31.40.1 | 172.25.40.0/24 |

Banner

"UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED

You must have explicit, authorized permission to access or configure this device.

Unauthorized attempts and actions to access or use this system may result in civil and/or criminal penalties.

All activities performed on this device are logged and monitored."

Password Policy

Minimum length 12 Enforce password history 6

Maximum Age 60 Enable Complexity

Minimum Age 5

Diagram

Description automatically generated

Table

Description automatically generated