****

|  |  |
| --- | --- |
| **Project Name** | **NCIIPC** |
| **Tested App Version** | **register.eshram.gov.in** |
| **Start & End Dates** | **11/25/2021 - 11/25/2021** |
| **Analyst Name** | **Krishanu Chakraborty** |

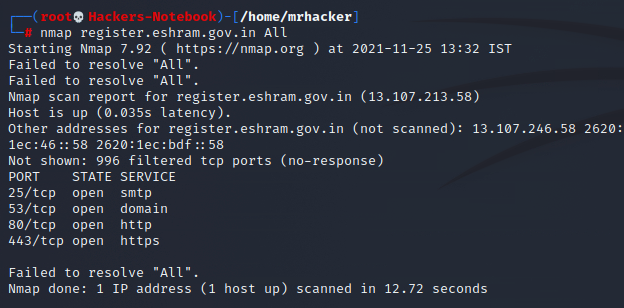
**SUMMARY OF FINDINGS**

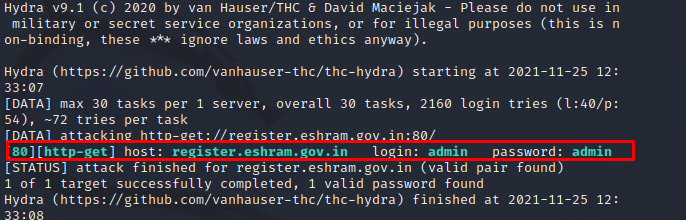
|  |  |
| --- | --- |
| **Risk** | **Count** |
| **Critical** | **0** |
| **High** | **1** |
| **Medium** | **0** |
| **Low** | **0** |
| **Total** | **1** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Vulnerability or Condition Type** | | **Risk** | **Severity** |
| **1** | **SENSITIVE INFORMATION DISCLOSURE** | **High** | **High** |

**DETAILED FINDINGS  
Finding #1: SENSITIVE INFORMATION DISCLOSURE**

|  |
| --- |
| **Risk** |
| High |
| **Severity** |
| High |
| **Details** |
| Information disclosure, also known as information leakage, is when a website unintentionally reveals sensitive information to its users. Depending on the context, websites may leak all kinds of information to a potential attacker, including:  1. Data about other users, such as usernames or financial information  2. Sensitive commercial or business data  3. Technical details about the website and its infrastructure |
| **Suggested Remediation** |
| Remove the sensitive information exposed on Port 80 i.e, Username and P |

**Proof of Exploit  
Screenshot: 1  
  
*Screenshot: 2***

****