BAB IV
HASIL PENELITIAN DAN PEMBAHASAN

4.1. Penentuan Ruang Lingkup (*Scope*)

Peneliti menerapkan ruang lingkup penelitian pada Web KRS Daring untuk menjadi target pengujian merujuk pada daftar hasil penilaian risiko pada penelitian sebelumnya (Yuhaz, 2018). Hasil yang ingin dicapai peneliti adalah pencarian akun milik mahasiswa.

4.2. Pengintaian Sistem (*Reconnaissance*)

Tahap pengintaian ini dilakukan untuk mencari informasi dasar target dan melakukan *port scanning* menggunakan *Nmap*. Pada *Nmap* terdapat dua cara dalam melakukan *port scanning* yaitu yang pertama dengan *command prompt / terminal* atau yang kedua dengan *Zenmap* yang memiliki GUI untuk mempermudah peneliti melakukan *port scanning*. Peneliti hanya tinggal mengetikan target pengujian dan memilih *profile scan* yang diinginkan. Pada pengujian ini memilih menggunakan *profile scan "slow comprehensive scan"* di mana *Zenmap* akan melakukan pemindai secara menyeluruh untuk mendapatkan informasi tentang *port* seperti pada **Gambar 4.1**.

Nmap Output | Ports / Hosts | Topology | Host Details | Scans

Port	Protocol	State	Service	Version
80	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
135	tcp	open	msrpc	Microsoft Windows RPC
139	tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
443	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
445	tcp	open	microsoft-ds	
3389	tcp	open	ms-wbt-server	
49155	tcp	open	msrpc	Microsoft Windows RPC

Gambar 4. 1 *Port* yang terbuka

4.3. Pencarian Kerentanan Keamanan (*Vulnerability Detection*) Menggunakan *Tools Software* OWASP ZAP

Pada tahap pencarian kerentanan keamanan akan dilakukan *Vulnerability Scanning* menggunakan OWASP ZAP (*Open Web Application Security Project*