

Nama : Yayang Prayoga

NIM : 09011181320006

MK : Keamanan Jaringan Komputer

SCANNING

Scanning merupakan rangkaian proses mengidentifikasi target serangan yang dilakukan attacker untuk mendapatkan informasi host, port dan service apa saja yang tersedia pada network target sebelum melakukan serangan lebih lanjut. Scanning sendiri memiliki 3 tipe, yaitu Port Scanning, Vulnerability Scanning, Network Scanning.

Berikut ini contoh hasil ujicoba pada target www.unsri.ac.id

Nmap Output	Ports / Hosts	Topology	Host Details	Scans
nmap -T4 -A -v www.unsri.ac.id				
Starting Nmap 6.46 (http://nmap.org) at 2017-02-22 19:33 SE Asia Standard Time NSE: Loaded 118 scripts for scanning. NSE: Script Pre-scanning. Initiating Ping Scan at 19:33 Scanning www.unsri.ac.id (103.241.4.11) [4 ports] Completed Ping Scan at 19:33, 0.28s elapsed (1 total hosts) Initiating Parallel DNS resolution of 1 host. at 19:33 Completed Parallel DNS resolution of 1 host. at 19:33, 2.03s elapsed Initiating SYN Stealth Scan at 19:33 Scanning www.unsri.ac.id (103.241.4.11) [1000 ports] Discovered open port 3389/tcp on 103.241.4.11 Discovered open port 113/tcp on 103.241.4.11 Discovered open port 53/tcp on 103.241.4.11 Discovered open port 21/tcp on 103.241.4.11 Discovered open port 256/tcp on 103.241.4.11 Discovered open port 22/tcp on 103.241.4.11 Discovered open port 80/tcp on 103.241.4.11 Discovered open port 554/tcp on 103.241.4.11 Discovered open port 135/tcp on 103.241.4.11 Discovered open port 110/tcp on 103.241.4.11 Discovered open port 995/tcp on 103.241.4.11 Discovered open port 5900/tcp on 103.241.4.11 Discovered open port 139/tcp on 103.241.4.11 Discovered open port 993/tcp on 103.241.4.11 Discovered open port 143/tcp on 103.241.4.11 Discovered open port 23/tcp on 103.241.4.11 Discovered open port 445/tcp on 103.241.4.11 Discovered open port 25/tcp on 103.241.4.11 Discovered open port 3306/tcp on 103.241.4.11 Discovered open port 1025/tcp on 103.241.4.11 Discovered open port 8888/tcp on 103.241.4.11 Discovered open port 199/tcp on 103.241.4.11 Discovered open port 111/tcp on 103.241.4.11 Discovered open port 1720/tcp on 103.241.4.11 Discovered open port 443/tcp on 103.241.4.11 Discovered open port 587/tcp on 103.241.4.11 Discovered open port 8080/tcp on 103.241.4.11 Discovered open port 1524/tcp on 103.241.4.11				
Nmap Output Ports / Hosts Topology Host Details Scans nmap -T4 -A -v www.unsri.ac.id Discovered open port 2702/tcp on 103.241.4.11 Discovered open port 1137/tcp on 103.241.4.11 Discovered open port 1124/tcp on 103.241.4.11 Completed SYN Stealth Scan at 19:33, 2.78s elapsed (1000 total ports) Initiating Service scan at 19:33 Scanning 995 services on www.unsri.ac.id (103.241.4.11) Completed Service scan at 19:36, 134.18s elapsed (999 services on 1 host) Initiating OS detection (try #1) against www.unsri.ac.id (103.241.4.11) Retrying OS detection (try #2) against www.unsri.ac.id (103.241.4.11) Initiating Traceroute at 19:36 Completed Traceroute at 19:36, 3.02s elapsed Initiating Parallel DNS resolution of 2 hosts. at 19:36 Completed Parallel DNS resolution of 2 hosts. at 19:36, 2.02s elapsed NSE: Script scanning 103.241.4.11. Initiating NSE at 19:36 NSE Timing: About 42.63% done; ETC: 19:37 (0:00:42 remaining) Completed NSE at 19:40, 250.59s elapsed Initiating NSE at 19:40 Completed NSE at 19:40, 0.18s elapsed Nmap scan report for www.unsri.ac.id (103.241.4.11) Host is up (0.12s latency). rDNS record for 103.241.4.11: ns4.unsri.ac.id PORT STATE SERVICE 1/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 3/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 4/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 6/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 7/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 9/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 13/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 17/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug)				

Nmap Output	Ports / Hosts	Topology	Host Details	Scans
nmap -T4 -A -v www.unsri.ac.id				
Nmap scan report for www.unsri.ac.id (103.241.4.11) Host is up (0.12s latency). rDNS record for 103.241.4.11: ns4.unsri.ac.id PORT STATE SERVICE VERSION 1/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 3/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 4/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 6/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 7/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 9/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 13/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 17/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 19/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 20/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 21/tcp open ftp vsftpd 2.0.8 or later _auth-owners: ERROR: Script execution failed (use -d to debug) 22/tcp open ssh? _auth-owners: ERROR: Script execution failed (use -d to debug) _ssh-hostkey: 23/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 24/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 25/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) _smtp-command: Couldn't establish connection on port 25 26/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 30/tcp open tcpwrapped				
Nmap Output	Ports / Hosts	Topology	Host Details	Scans
nmap -T4 -A -v www.unsri.ac.id				
_auth-owners: ERROR: Script execution failed (use -d to debug) 111/tcp open rpcbind 2.4 (RPC #100000) _auth-owners: ERROR: Script execution failed (use -d to debug) _rpcinfo: program version port/proto service 100000 2,3,4 111/tcp rpcbind 100000 2,3,4 111/udp rpcbind 100024 1 36109/tcp status 100024 1 46268/udp status 113/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 119/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 125/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 135/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 139/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 143/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) _imap-capabilities: ERROR: Failed to connect to server 144/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 146/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 161/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 163/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 179/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 199/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 211/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 212/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug)				
Nmap Output	Ports / Hosts	Topology	Host Details	Scans
nmap -T4 -A -v www.unsri.ac.id				
9998/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 9999/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 10000/tcp open http MiniServ 1.831 (Webmin httpd) _auth-owners: ERROR: Script execution failed (use -d to debug) _http-favicon: Unknown favicon MD5: 41D44C789F280528351F3236683D907E _http-methods: No Allow or Public header in OPTIONS response (status code 200) _http-title: Site doesn't have a title (text/html; Charset=iso-8859-1). _ndmp-version: ERROR: Failed to get host information from server 10001/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 10002/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 10003/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 10004/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 10009/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 10010/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 10012/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 10024/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 10025/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 10082/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 10180/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 10215/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 10243/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 10566/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug)				
Nmap Output	Ports / Hosts	Topology	Host Details	Scans
nmap -T4 -A -v www.unsri.ac.id				
53/tcp open domain 1.3.0 BIND 9.4.21 _auth-owners: ERROR: Script execution failed (use -d to debug) _dns-nsid: id.server: hkg80-009.ff.avast.com bind.version: unbound 1.4.21 70/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) _gopher-ls: 79/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) _finger: ERROR: Script execution failed (use -d to debug) 80/tcp open http nginx _auth-owners: ERROR: Script execution failed (use -d to debug) _http-favicon: Unknown favicon MD5: 105412C8FAE55AF242AD032B67CD0B9 _http-methods: No Allow or Public header in OPTIONS response (status code 405) _http-robots.txt: 1 disallowed entry _ _http-title: :: Halaman Utama Universitas Sriwijaya - Indralaya, Sumater... 81/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 82/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 83/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 84/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 85/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 88/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 89/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 90/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 99/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 100/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 106/tcp open tcpwrapped				
Nmap Output	Ports / Hosts	Topology	Host Details	Scans
nmap -T4 -A -v www.unsri.ac.id				
443/tcp open http nginx _auth-owners: ERROR: Script execution failed (use -d to debug) _http-methods: No Allow or Public header in OPTIONS response (status code 400) _http-title: 400 The plain HTTP request was sent to HTTPS port _ssl-cert: Subject: commonName=*.unsri.ac.id _Issuer: commonName=AlphaSSL CA - SHA256 - G2/organizationName=GlobalSign nv-sa/countryName=BE _Public Key type: rsa _Public Key bits: 2048 _Not valid before: 2016-06-15T12:17:00+00:00 _Not valid after: 2017-06-16T12:17:00+00:00 _MD5: necc 41e0 0274 b17b 3d70 7985 31e8 e708 _SHA-1: 0612 f33c c8c3 9914 9907 0f61 cc24 b4b4 elbf d062 _ssl-date: 2017-02-22T12:37:29+00:00; -6s from local time. 444/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 445/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 458/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 464/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 465/tcp open smtps? _auth-owners: ERROR: Script execution failed (use -d to debug) _smtp-command: Couldn't establish connection on port 465 481/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 497/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 500/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 512/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 513/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 514/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 515/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 516/tcp open tcpwrapped				
Nmap Output	Ports / Hosts	Topology	Host Details	Scans
nmap -T4 -A -v www.unsri.ac.id				
60443/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 61532/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 61900/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 62078/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 63331/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 64623/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 64680/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 65000/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 65129/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) 65389/tcp open tcpwrapped _auth-owners: ERROR: Script execution failed (use -d to debug) OS fingerprint not ideal because: Host distance (8 network hops) is greater than five No OS matches for host Uptime: Russia: 11.885 days (since Fri Feb 10 22:26:00 2017) Network Distance: 5 hops TCP Sequence Prediction: Difficulty=257 (Good luck!) IP ID Sequence Generation: Randomized TRACEROUTE (using port 1723/tcp) HOP RTT ADDRESS 1 4.00 ms 192.168.43.1 2 ... 4 5 59.00 ms ns4.unsri.ac.id (103.241.4.11) NSE: Script Post-scanning. Read data files from: C:\Program Files (x86)\Nmap OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ Nmap done: 1 IP address (1 host up) scanned in 412.80 seconds Raw packets sent: 1259 (57.940KB) Rcvd: 1390 (61.188KB)				

Dari hasil ujicoba di atas di dapatkan beberapa informasi sebagai berikut

Nama Situs	IP	Status	Service	OS
www.unsri.ac.id	103.241 4.11	21/tcp : open 22/tcp : open 53/tcp : open 10000/tcp : open 443/tcp : open 80/tcp : open 993/tcp : open 9100/tcp : open 9101/tcp : open 9102/tcp : open 9103/tcp : open 995/tcp : open 1723/tcp : close 111/tcp : open 465/tcp : open 563/tcp : open	ftp ssh domain http http http imaps jetdirect jetdirect jetdirect jetdirect pop3s pftp rpcbind smtps snews	Vsftpd 2.0.8 ISC Bind unbound 1.4.21 MiniServ 1.831 (Webmin httpd) Nginx Nginx 2-4 (RPC #100000)