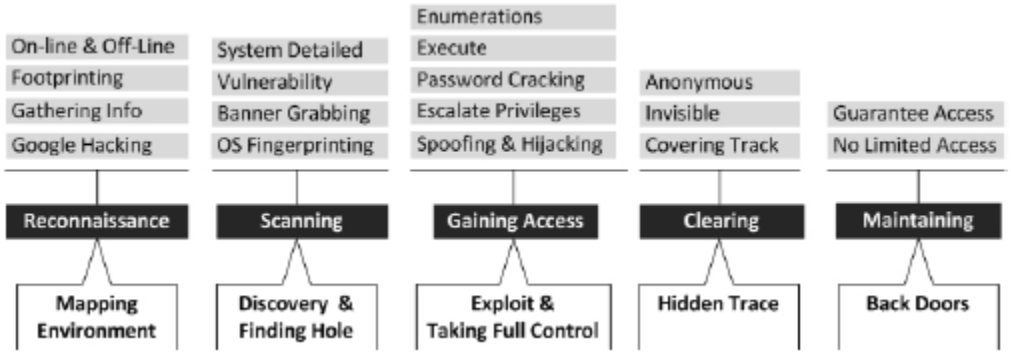
TUGAS KEAMANAN JARINGAN KOMPUTER
SCANNING pada PT. Semen Batu Raja

NAMA: EDI SUKRISNO
NIM: 09011181320043

UNIVERSITAS SRIWIJAYA
FAKULTAS ILMU KOMPUTER
JURUSAN SISTEM KOMPUTER

Scanning

Scanning merupakan yang merupakan fase pra-serangan untuk menemukan informasi dasar.



Gambar.1 langkah penyerangan dan teknik penyerangan

Server mempunyai fungsi melayani client dengan menyediakan service yang dibutuhkan. Server menyediakan service dengan bermacam-macam kemampuan, baik untuk lokal maupun remote. Server listening pada suatu port dan menunggu incomming connection ke port. Koneksi bisa berupa lokal maupuan remote.

Port sebenarnya suatu alamat pada stack jaringan kernel, sebagai cara dimana transport layer mengelola koneksi dan melakukan pertukaran data antar komputer. Port yang terbuka mempunyai resiko terkait dengan exploit. Perlu dikelola port mana yang perlu dibuka dan yang ditutup untuk mengurangi resiko terhadap exploit. Ada beberapa utility yang bisa dipakai untuk melakukan diagnosa terhadap sistem service dan port kita. Utility ini melakukan scanning terhadap sistem untuk mencari port mana saja yang terbuka, ada juga sekaligus memberikan laporan kelemahan sistem jika port ini terbuka.

Port Scanner merupakan program yang didesain untuk menemukan layanan (service) apa saja yang dijalankan pada host jaringan. Untuk mendapatkan akses ke host, cracker harus mengetahui titik-titik kelemahan yang ada. Sebagai contoh, apabila cracker sudah mengetahui bahwa host menjalankan proses ftp server, ia dapat menggunakan kelemahan-kelemahan yang ada pada ftp server untuk mendapatkan akses. Dari bagian ini kita dapat mengambil kesimpulan bahwa layanan yang tidak benar-benar diperlukan sebaiknya dihilangkan untuk memperkecil resiko keamanan yang mungkin terjadi.

Beberapa Tools dan cara scanning ke sistem :

- **Netstat** merupakan utility yang powerfull untuk menngamati current state pada server, service apa yang listening untuk incomming connection, interface mana yang listening, siapa saja yang terhubung.
- **Nmap** ("Network Mapper") merupakan sebuah tool open source untuk eksplorasi dan audit keamanan jaringan. Ia dirancang untuk memeriksa jaringan besar secara cepat, meskipun ia dapat pula bekerja terhadap host tunggal. Nmap menggunakan paket IP raw dalam cara yang canggih untuk menentukan host mana saja yang tersedia pada jaringan, layanan (nama aplikasi dan versi) apa yang diberikan, sistem operasi (dan versinya) apa yang digunakan, apa jenis firewall/filter paket yang digunakan, dan sejumlah karakteristik lainnya. Meskipun Nmap umumnya digunakan untuk audit keamanan, namun banyak administrator sistem dan jaringan menganggapnya berguna untuk tugas rutin seperti inventori jaringan, mengelola jadwal upgrade layanan, dan melakukan monitoring uptime host atau layanan.

Percobaan Scanning pada PT. Semen Batu Raja,berikut hasil scanning dengan nmap :

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

Port	Protocol	State	Service	Version
21	tcp	open	ftp	ProFTPD or KnFTPD
80	tcp	open	http	OpenResty web app server
443	tcp	open	http	OpenResty web app server
8080	tcp	open	http	OpenResty web app server
9100	tcp	open	jetdirect	
9104	tcp	open	jetdirect	
9113	tcp	open	unknown	
9117	tcp	open	unknown	
60412	tcp	open	http	Apache httpd 2.2.16 ((Debian))
65002	tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)

Gambar 2. Layanan yang terdapat pada PT. Semen Batu Raja.

Vulnerabilities dari layanan pada PT. Semen Batu Raja berdasarkan CVE (Common Vulnerabilities and Exposures) yaitu:

1. Pada FTP menggunakan aplikasi atau sofaware ProFTPD or KnFTPD

CVE-2016-3125	The mod_tls module in ProFTPD before 1.3.5b and 1.3.6 before 1.3.6rc2 does not properly handle the TLSDHParamFile directive, which might cause a weaker than intended Diffie-Hellman (DH) key to be used and consequently allow attackers to have unspecified impact via unknown vectors.
CVE-2015-3306	The mod_copy module in ProFTPD 1.3.5 allows remote attackers to read and write to arbitrary files via the site cpfr and site cpto commands.

2. Pada http/Web server menggunakan aplikasi atau sofaware OpenResty web app server

CVE-2016-6850	An issue was discovered in Open-Xchange OX App Suite before 7.8.2-rev8. SVG files can be used as profile pictures. In case their XML structure contains iframes and script code, that code may get executed when calling the related picture URL or viewing the related person's image within a browser. Malicious script code can be executed within a user's context. This can lead to session hijacking or triggering unwanted actions via the web interface (sending mail, deleting data etc.).
CVE-2016-6847	An issue was discovered in Open-Xchange OX App Suite before 7.8.2-rev8. SVG files can be used as mp3 album covers. In case their XML structure contains script code, that code may get executed when calling the related cover URL. Malicious script code can be executed within a user's context. This can lead to session hijacking or triggering unwanted actions via the web interface (sending mail, deleting data etc.).

3. Pada http/Web server menggunakan aplikasi atau sofaware Apache httpd 2.2.16 (Debian)

CVE-2016-6801	Cross-site request forgery (CSRF) vulnerability in the CSRF content-type check in Jackrabbit-Webdav in Apache Jackrabbit 2.4.x before 2.4.6, 2.6.x before 2.6.6, 2.8.x before 2.8.3, 2.10.x before 2.10.4, 2.12.x before 2.12.4, and 2.13.x before 2.13.3 allows remote attackers to hijack the authentication of unspecified victims for requests that create a resource via an HTTP POST request with a (1) missing or (2) crafted Content-Type header.
CVE-2016-2168	The req_check_access function in the mod_authz_svn module in the httpd server in Apache Subversion before 1.8.16 and 1.9.x before 1.9.4 allows remote authenticated users to cause a denial of service (NULL pointer dereference and crash) via a crafted header in a (1) MOVE or (2) COPY request, involving an authorization check.

4. Pada SSH menggunakan aplikasi atau sofaware OpenSSH 5.3 (protocol 2.0)

CVE-2008-5161	Error handling in the SSH protocol in (1) SSH Tectia Client and Server and Connector 4.0 through 4.4.11, 5.0 through 5.2.4, and 5.3 through 5.3.8; Client and Server and ConnectSecure 6.0 through 6.0.4; Server for Linux on IBM System z 6.0.4; Server for IBM z/OS 5.5.1 and earlier, 6.0.0, and 6.0.1; and Client 4.0-J through 4.3.3-J and 4.0-K through 4.3.10-K; and (2) OpenSSH 4.7p1 and possibly other versions, when using a block cipher algorithm in Cipher Block Chaining (CBC) mode, makes it easier for remote attackers to recover certain plaintext data from an arbitrary block of ciphertext in an SSH session via unknown vectors.

5. Pada SSH menggunakan aplikasi atau sofaware jetdirect

CVE-2011-4785	Directory traversal vulnerability in the HP-ChaiSOE/1.0 web server on the HP LaserJet P3015 printer with firmware before 07.080.3, LaserJet 4650 printer with firmware 07.006.0, and LaserJet 2430 printer with firmware 08.113.0_I35128 allows remote attackers to read arbitrary files via unspecified vectors, a different vulnerability than CVE-2008-4419.
CVE-2009-2684	Multiple cross-site scripting (XSS) vulnerabilities in Jetdirect and the Embedded Web Server (EWS) on certain HP LaserJet and Color LaserJet printers, and HP Digital Senders, allow remote attackers to inject arbitrary web script or HTML via the (1) Product_URL or (2) Tech_URL parameter in an Apply action to the support_param.html/config script.