Aptekmas
Jurnal Pengabdian Kepada Masyarakat

Volume 7, Nomor 3, (2024)
http://dx.doi.org/10.36257/apts.vxix
pp 06-11

SOSIALISASI DAN SIMULASI KEAMANAN SERVER KERBEROS DAN OPENLDAP DI SMK NEGERI 4 PALEMBANG

Lindawati[1)], Mohammad Fadhli[2)], Sopian Soim[3)], Salwa Deta Mediana[4)]
[1,2,3,4] Teknik Elektro, Politeknik Negeri Sriwijaya
email: lindawati@polsri.ac.id, mohammad.fadhli@polsri.ac.id, sopiansoim@gmail.com, meidiana.slw@gmail.com

Abstract

Computer networks are essential to daily life in the digital age because they link devices and provide distant information access. But technological progress also poses serious concerns to data security. Threats like viruses, malware, and hacker attacks put data's confidentiality and integrity in danger. For this reason, cybersecurity technicians must comprehend and use strong security frameworks. Kerberos, a security protocol that enables entities in a network to safely verify their identities, is one of the solutions that are presented. On the other side, directories are managed via Lightweight Directory Access Protocol (LDAP). In this context, teachers and students at the Vocational High School (SMK) with a focus on computer and network engineering receive instruction and training on network security. It is hoped that by doing this outreach, the community would see how important network security is and take the necessary precautions to safeguard data from intrusions. The outreach efforts were conducted at SMK Negeri 4 Palembang, which is the subject of this study. The findings demonstrate that students are able to test exploitation techniques on the framework used in the apache2 service and have a solid understanding of Kerberos, LDAP, and Firewalld.

Keywords: *Kerberos, OpenLDAP, SSH, Apache2, Debian.*

Abstrak

Jaringan komputer memiliki peran penting dalam kehidupan sehari-hari di era digital karena mampu menghubungkan berbagai perangkat serta menyediakan akses informasi jarak jauh. Namun, perkembangan teknologi juga membawa tantangan serius terhadap keamanan data. Ancaman seperti virus, malware, dan serangan peretas dapat mengancam kerahasiaan maupun integritas data. Oleh karena itu, teknisi keamanan siber perlu memahami serta menerapkan kerangka keamanan yang kuat. Salah satu solusi yang digunakan adalah Kerberos, yaitu protokol keamanan yang memungkinkan entitas dalam jaringan melakukan verifikasi identitas secara aman. Sementara itu, pengelolaan direktori dilakukan dengan menggunakan Lightweight Directory Access Protocol (LDAP). Dalam kegiatan pengabdian masyarakat ini, guru dan siswa di Sekolah Menengah Kejuruan (SMK) dengan konsentrasi keahlian Teknik Komputer dan Jaringan mendapatkan pelatihan mengenai keamanan jaringan. Melalui program ini, diharapkan warga sekolah semakin menyadari pentingnya menjaga keamanan jaringan serta mampu melakukan langkah-langkah pencegahan untuk melindungi data dari ancaman. Kegiatan dilaksanakan di SMK Negeri 4 Palembang sebagai lokasi utama pelaksanaan pengabdian. Hasil kegiatan menunjukkan bahwa siswa mampu melakukan uji coba teknik eksploitasi pada kerangka kerja yang digunakan dalam layanan Apache2, serta memiliki pemahaman yang baik mengenai Kerberos, LDAP, dan Firewalld.

Kata kunci : *Kerberos, OpenLDAP, SSH, Apache2, Debian.*

Aptekmas
Jurnal Pengabdian Kepada Masyarakat
Volume 7, Nomor 3, (2024)
http://dx.doi.org/10.36257/apts.vxix
pp 06-11

1. PENDAHULUAN

Dalam era digital saat ini, jaringan komputer menjadi sangat penting dalam kehidupan sehari-hari. Internet atau jaringan luas menghubungkan banyak perangkat dan memungkinkan komunikasi juga akses informasi jarak jauh. Namun, dengan semakin canggihnya teknologi juga membawa resiko keamanan data yang semakin besar juga. Ancaman keamanan seperti virus, malware, dan serangan hacker dapat mengganggu integritas, kerahasiaan, dan ketersediaan data di jaringan komputer. Oleh karena itu diperlukan suatu upaya untuk meningkatkan keamanan jaringan komputer (A. Aryanti et al. 2021).

Dalam menghadapi ancaman cyber yang semakin meningkat, memahami dan menerapkan framework keamanan yang kuat bukanlah pilihan melainkan keharusan bagi seorang teknisi keamanan cyber (cyber security). Pertama-tama, Kerberos adalah sebuah protocol keamanan yang memungkinkan entitas dalam sebuah jaringan (seperti pengguna/user atau server) untuk membuktikan identitas mereka satu sama lain dengan cara yang aman. Kerberos menggunakan sistem token yang disebut dengan "Ticket" untuk memverifikasi pengguna dan memberikan akses terbatas ke sumber daya yang disediakan oleh server (D. Pengajar and B. Rahardjo. 2004). Di sisi lain, LDAP adalah protokol aplikasi yang digunakan untuk mengakses dan mengelola direktori (Askari Azikin. 2011).

Pelatihan dan edukasi ini akan diberikan kepada siswa dan guru di Sekolah Menengah Kejuruan (SMK) jurusan Teknik Komputer dan Jaringan. Tujuannya adalah memberikan pemahaman yang lebih baik tentang pentingnya keamanan jaringan, risiko keamanan jaringan yang ada, serta cara untuk melindungi jaringan dari serangan pembobolan data. Dengan adanya sosialisasi dan edukasi tentang cara meningkatkan keamanan jaringan, diharapkan masyarakat dapat memahami betapa pentingnya keamanan jaringan dan dapat mengambil tindakan yang tepat untuk melindungi jaringan dari serangan kebocoran data. Dengan demikian, data dan informasi yang sensitive dapat terlindungi dengan baik dan aman dari serangan *cyber*.

SMK Negeri 4 Palembang merupakan salah satu lembaga kejuruan dimana tidak hanya membahas *hardware* (perangkat komputer), namun juga bagaimana mengelola suatu jaringan komputer dan server terutama di bagian security systemnya apakah aman dari bahaya cyber atau belum sama sekali memiliki perlindungan pada database dan arsipan data lainnya sehingga bisa diakses oleh semua user tanpa enkripsi lanjutan. Terkait masalah tersebut maka tim peneliti dan pengabdian dari Politeknik Negeri Sriwijaya merasa perlu diadakannya sosialisasi untuk keamanan jaringan pada SMK Negeri 4 Palembang dalam bentuk kegiatan pengabdian kepada masyarakat. Selain memberikan informasi umum tentang sistem keamanan jaringan dengan *Kerberos Authentication Protocol* dan *Lightweight Directory Access Protocol* (LDAP) kepada siswa, juga diharapkan pihak sekolah dapat menerima dan diterapkan pada data penting guna menghindari penyusupan data dan dapat diakses oleh orang tertentu saja.

2. IDENTIFIKASI MASALAH

Keamanan jaringan merupakan isu penting yang perlu diperhatikan oleh para pengembang jaringan karena teknologi dalam lalu lintas jaringan atau internet tidak terjamin aman dan dapat ditembus oleh penjahat *cyber* seperti *hacker* dan *cracker*. Oleh karena itu, sistem keamanan jaringan harus dibuat sebaik mungkin agar keamanan sumber daya pada server dapat terjamin. Para *administrator* jaringan harus memikirkan cara untuk meminimalkan terjadinya kebocoran data dan serangan terhadap jaringan yang dibuatnya.

Agar jaringan terhindar dari penyadapan dan serangan oleh pihak lain, *administrator* jaringan perlu membatasi hak akses atau otoritas terhadap layanan yang ditawarkan oleh server. Ketika *administrator* ingin membatasi penggunaan layanan oleh seorang klien, maka ia akan memeriksa identitas atau otoritas yang dimiliki oleh klien tersebut untuk menentukan layanan mana yang bisa diakses dan dibatasi. OpenLDAP *Directory Services* adalah layanan direktori terpusat yang menggunakan protokol LDAP untuk

Aptekmas
Jurnal Pengabdian Kepada Masyarakat
Volume 7, Nomor 3, (2024)
http://dx.doi.org/10.36257/apts.vxix
pp 06-11

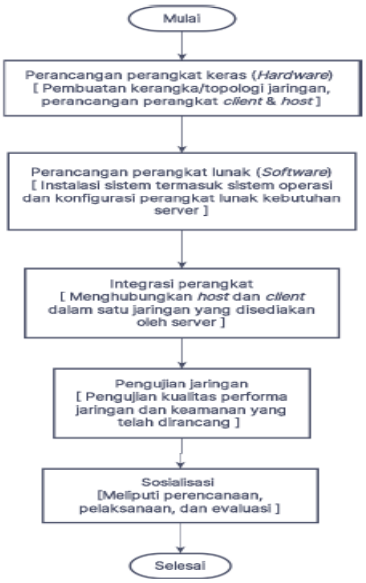
mengakses dan mengelola informasi direktori. Protokol LDAP menggunakan *password* untuk autentikasi.

Adapun teknologi keamanan *cyber* yang digunakan untuk mengenkripsi data adalah penggunaan protokol Kerberos. Kerberos memungkinkan pengguna untuk terhubung ke server layanan autentikasi yang sesuai dengan protokolnya. Protokol Kerberos dirancang untuk melakukan autentikasi dua arah, dimana *client* membuktikan identitasnya ke server dan server juga membuktikan identitasnya ke *client*. Kerberos didasarkan pada Needham-Schroeder protocol yang dikembangkan oleh *Massachusetts Institute of Technology* (MIT) dalam proyek Athena untuk jaringan komputer modern.

3. METODELOGI PELAKSANAAN

Target dari pengabdian masyarakat ini adalah siswa dan guru di SMK yang memiliki jurusan teknik komputer dan jaringan. Siswa diharapkan dapat meningkatkan pemahaman tentang keamanan jaringan dan teknologi yang berkaitan dengan topik penelitian kerjasama dosen mahasiswa, serta keterampilan praktis dalam mengimplementasikan solusi keamanan jaringan. Selain itu, guru diharapkan dapat meningkatkan pemahaman tentang keamanan jaringan dan teknologi yang berkaitan dengan topik penelitian kerjasama dosen mahasiswa dan dapat mengajarkan materi ini secara efektif kepada siswa.

Kerangka kegiatan pengabdian dilakukan melalui tahapan-tahapan serperti dalam blok diagram ini:



Gambar 1. Tahapan Kegiatan Sosialisasi

3.1 Perancangan *Hardware*

Kebutuhan sistem perangkat keras yang diperlukan untuk server diidentifikasi selama tahap perancangan perangkat keras. Tahap ini melibatkan penyusunan infrastruktur fisik, konfigurasi arsitektur jaringan, dan pemilihan komponen yang akan mendukung aplikasi penelitian keamanan pada server. Dalam penelitian ini, digunakan topologi jaringan *client-server* sebagai metode. Beberapa komponen perangkat keras yang digunakan meliputi server, penggunaan kabel *Unshielded Twisted Pair* (UTP) untuk koneksi *client-server* di dalam jaringan area lokal, dan penggunaan *router* sebagai *gateway* untuk menghubungkan jaringan lokal dengan jaringan publik (internet).

Volume 7, Nomor 3, (2024)
http://dx.doi.org/10.36257/apts.vxix
pp 06-11

3. 2 Perancangan *Software*

Pada jaringan ini, PC *host* adalah pusat pengendali. PC *host* memiliki otoritas tertinggi dan dapat mengatur layanan yang dapat digunakan oleh *client*, memonitor, dan melakukan *remoting* pada *client*. OpenLDAP adalah penyedia layanan direktori yang mengontrol akses pengguna ke aplikasi dan data lainnya. Kerberos *protocol authentication* digunakan untuk keamanan kerahasiaan dan kredensial pengguna. DHCP digunakan untuk alokasi IP *client* secara otomatis.

Untuk desain arsitektur pengimplementasian perangkat lunak *protocol* Kerberos dan LDAP adalah sebagai berikut:



Gambar 2. *Design* Arsitektur Implementasi *Framework*

3. 3 Pelaksanaan Sosialisasi

1. Perencanaan Sosialisasi

   Tahap ini adalah tahap perencanaan kegiatan sosialisasi yang akan dilakukan, mulai dari koordinasi dengan pihak mitra penentuan waktu, tempat, serta target peserta sosialisasi.

   Selain itu, perlu persiapan dan penentuan materi yang akan disampaikan pada saat sosialisasi agar peserta dapat memahami tujuan dan manfaat dari *framework* keamanan jaringan yang ditawarkan.

2. Pelaksanaan Sosialisasi

   Kegiatan sosialisasi akan dilakukan dengan memulai pendahuluan dan mengenalkan topik kepada peserta. Materi yang telah disiapkan pada saat perencanaan disampaikan dengan jelas dan terstruktur sehingga peserta dapat memahami konsep dan penerapan dari *framework* keamanan jaringan yang ditawarkan. Demonstrasi bagaimana *framework* bekerja akan diberikan dalam bentuk video ilustrasi dan memberikan diskusi dan tanya jawab untuk memberikan kesempatan pada peserta terkait hal-hal yang kurang dimengerti atau memerlukan penjelasan lebih lanjut.

4. HASIL DAN PEMBAHASAN

Kegiatan sosialisasi ini telah dilaksanakan pada tanggal 24 November 2023 dengan target peserta pelatihan 20 siswa dari 4 (empat) kelas dan 2 (dua) orang guru SMK Negeri 4 Palembang yang berasal dari jurusan Teknik Komputer dan Jaringan (TKJ). Kegiatan dilaksanakan di laboratorium TKJ SMKN 4 dari pukul 09.00 WIB sampai pukul 15.00 WIB sesuai dengan jam sekolah siswa dan guru SMKN 4 Palembang.

Kegiatan sosialisasi dilakukan dengan mensosialisasikan hasil karya penelitian kerjasama dosen dan mahasiswa dalam hal ini ialah *Framework* Keamanan Server yang telah dirancang, melalui penjelasan materi dengan media presentasi dalam bentuk *powerpoint*

Sosialisasi dibuka bersama dengan penyampaian kata sambutan oleh Wakil Kepala Sekolah SMKN 4 Palembang dan juga kata sambutan dari ketua jurusan Teknik Komputer dan Jaringan (TKJ) SMKN 4 Palembang. Setelah acara dengan resmi dibuka oleh wakil kepala sekolah, sosialisasi dilanjutkan dengan pengisian materi oleh perwakilan dari tim pengabdi yang hadir pada saat acara sosialisasi.



Gambar 3. Dokumentasi Pembukaan Acara

Aptekmas
Jurnal Pengabdian Kepada Masyarakat
Volume 7, Nomor 3, (2024)
http://dx.doi.org/10.36257/apts.vxix
pp 06-11

Pada saat kegiatan penyampaian materi, adapun pokok inti dari materi yang disampaikan adalah sebagai berikut:

1. Latar belakang dan pengenalan mengenai pentingnya menjaga keamanan jaringan baik internal maupun jaringan eksternal.
2. Memberikan beberapa contoh kasus kebocoran data yang terjadi sepanjang tahun 2023 dan memberikan kesempatan bagi siswa untuk menanggapi kasus tersebut.
3. Memaparkan tujuan dari sosialisasi.
4. Memberikan materi teori dasar yang menyangkut framework keamanan.
5. Memberikan gambaran terhadap uji demonstrasi yang akan dilakukan peserta pada saat sesi praktik uji coba keamanan produk framework.

Setelah pengisian materi sosialisasi selesai dilakukan, para peserta akan dibagikan buku manual dan guide yang akan menjadi pedoman peserta dalam melakukan demo uji coba terhadap produk *framework* keamanan yang telah dirancang.

Peserta 20 orang siswa dibagi menjadi 4 (empat) kelompok dimana masing-masing kelompok akan melakukan praktikum dengan metode yang berbeda sesuai dengan pedoman yang telah disiapkan oleh tim pengabdi. Buku pedoman ini berisi tata cara dan langkah demi langkah untuk melakukan uji demo terhadap produk yaitu framework keamanan dalam bentuk virtual machine (vm).



Gambar 4. Dokumentasi Penyampaian Materi Sosialisasi

Pada 30 menit pertama setelah pemaparan materi dan pembagian buku pedoman untuk setiap tim, para peserta dipersilakan untuk menyiapkan perangkat dan alat yang akan digunakan sebelum masuk ke tahap pengetesan produk. Pada tahap persiapan ini tiap kelompok dibagikan masing-masing satu buah *flashdisk* sebesar 32 *giga bytes* yang berfungsi sebagai media distribusi server dalam bentuk *virtual machine* yang akan dijalankan dalam perangkat lunak vmware versi 17 pro. Selain itu, disediakan juga vm (*virtual machine*) untuk host client dengan system operasi kali-linux sebagai mesin tambahan pada saat uji coba melakukan eksploitasi terhadap ketahanan dan kerentanan dari produk *framework* keamanan server.

Selanjutnya, para peserta dipersilakan untuk langsung melakukan uji coba praktikum, adapun pembagian tugas untuk masing-masing kelompok adalah sebagai berikut ini:

1. Kelompok 1: Melakukan eksploitasi dengan metode Nmap (*Network Mapping*) terhadap *port-port* terbuka dari server.
2. Kelompok 2: Melakukan eksploitasi dengan metode *Brute Forced Attack* dengan *tool* Nmap terhadap layanan SSH yang ditanamkan pada mesin server.
3. Kelompok 3: Melakukan eksploitasi dengan metode *Brute Forced Attack* dengan *tool* Metasploit terhadap layanan SSH yang ditanamkan pada mesin server.
4. Kelompok 4: Melakukan ekslploitasi dengan metode DDoS (*Distributed Denial-of-Service*) terhadap keamanan dan keandalan layanan web server apache2 yang ditanamkan pada mesin server.

Volume 7, Nomor 3, (2024)
http://dx.doi.org/10.36257/apts.vxix
pp 06-11



Gambar 5. Dokumentasi Sesi Praktikum Uji Coba

Setelah setiap kelompok selesai melakukan tugas praktikum, tiap kelompok akan melakukan presentasi untuk memaparkan hasil praktikum yang telah dilakukan. Pada sesi ini semua peserta akan diberikan kesempatan untuk memberikan pendapat dan komentar terhadap presentasi yang dilakukan oleh kelompok lain.

Setelah sesi praktikum dan presentasi kelompok peserta selesai, sesi acara selanjutnya adalah sesi tanya jawab dan sharing seputar materi sosialisasi, lalu acara selesai dan ditutup oleh moderator dari tim pengabdi.

5. KESIMPULAN

Berdasarkan sosialisasi yang telah dilaksanakan, dapat disimpulkan bahwa program pengabdian kepada Masyarakat ini berjalan lancar. Tujuan pengabdian, yakni peningkatan kesadaran dan keamanan digital, meningkatkan pengetahuan teknis, mendorong adopsi praktik keamanan tersampaikan sepenuhnya kepada siswa-siswa SMK Negeri 4 Palembang. Siswa dapat memahami definisi *Kerberos Authentication Protocol*, OpenLDAP, dan Firewalld. Siswa juga telah melakukan demo uji coba pada *framework* yang telah dikembangkan dengan mencoba untuk melakukan 3 (tiga) metode eksploitasi yang cukup familiar di kalangan pengembang sebuah jaringan. Adapun 3 metode tersebut adalah *network mapping* (*Nmap*) untuk mendeteksi kerentanan berupa *port* terbuka yang bisa diakses pada server, *brute forced attack* ke layanan *ssh* untuk mencoba melakukan eksploitasi akun user, dan juga *DoS* (*Denial of Service*) ke web server untuk menguji performa framework yang diimplementasikan pada layanan *apache2*.

6. UCAPAN TERIMA KASIH

Terima kasih kepada seluruh pihak yang terlibat dalam pengabdian kepada masyarakat ini. Berlangsungnya kegiatan ini tidak luput dari kerja keras dan kontribusi besar tim, Dosen, dan pihak SMK Negeri 4 Palembang yang telah menerima serta menjadi wadah untuk kami melaksanakan pengabdian masyarakat.

7. REFERENSI

[1] A. Aryanti, A. S. Handayani, I. Ziad, I. Mekongga, and F. J. Abiyyu, “Compatibility of Linux Architecture for Diskless Technology System,” 2021.

[2] D. Pengajar & B. Rahardjo, “Laporan Proyek Akhir Ec 5010 Keamanan Sistem Informasi Sistem Autentikasi Kerberos Pada Jaringan Komputer Itb,” 2004.

[3] Z. Wang and Y. Wang, “Research and design of campus network unified identity authentication system based on Kerberos,” in Advanced Materials Research, 2012, pp. 1086–1089. doi: 10.4028/www.scientific.net/AMR.546-547.1086.