Jurnal Nasional Teknologi Komputer
Vol.2; No: 3; Juli 2022
Website: publikasi.hawari.id/index.php/jnastek
E-ISSN: 2808-4845; P-ISSN: 2808-7801

Makalah Penelitian

Perbandingan Berbeda Alat Keamanan Untuk Mendeteksi Risiko Dalam Jaringan

Rahmat Iriyanto

[1]Teknik Informatika, Fakultas Teknik, Universitas Muhammadiyah Jakarta

Corresponding Author: Rahmat Iriyanto

ABSTRACT

Today, maintaining network security is a significant challenge. Data that has crossed a network is not regarded as secure. There are many risks, including snipping, phishing, spyware, hacking, and spoofing. Various network threats were covered in this article. There are numerous open-source technologies available to defend against these attacks. This study has examined tools like Acunetix and Intrusion Prevention System (IPS).

Keywords:

ABSTRAK

Saat ini, menjaga keamanan jaringan merupakan tantangan yang signifikan. Data yang telah melewati jaringan tidak dianggap aman. Ada banyak risiko, termasuk snipping, phishing, spyware, hacking, dan spoofing. Berbagai ancaman jaringan dibahas dalam artikel ini. Ada banyak teknologi open-source yang tersedia untuk bertahan dari serangan ini. Studi ini telah memeriksa alat seperti Acunetix dan Intrusion Prevention System (IPS).

Kata Kunci:

1. Pendahuluan

Keamanan Jaringan adalah seperangkat aturan dan konfigurasi yang dirancang untuk melindungi Kerahasiaan, Integritas, dan Ketersediaan jaringan komputer. Ini adalah perlindungan akses ke file dan direktori dalam jaringan komputer terhadap peretas atau penyusup untuk menyalahgunakan data dan juga mengubah data. Tujuan dari keamanan jaringan adalah untuk memberikan otentikasi kepada pengguna. Ini memberikan perlindungan terhadap data rahasia, memastikan integritas data, dan layanan data yang berkelanjutan. Ada cara lain untuk melindungi data menggunakan Intrusion Prevention System (IPS). Sistem ini terus memantau jaringan, mencari insiden berbahaya, dan menangkap informasi..

2. Tinjauan Pustaka

Saat ini ada banyak alat gratis yang tersedia untuk phishing konflik dan cheat yang diprediksi web lainnya, alat detektif, dll.

Nabanita Mandal dan Sonali Jadhav [2], dalam beberapa tahun terakhir memberikan keparahan pada jaringan dalam opensource telah menjadi tantangan besar. Karena informasi yang melewati jaringan tidak aman. Sudah berbagai jenis pemerasan telah ada di sistem seperti sniffing, hoaxing, dan phishing.

Dalam tulisan ini, penulis memaparkan beberapa ancaman yang merupakan serangan terhadap jaringan. Juga, ada beberapa teknik pencegahan terhadap masalah semacam itu. Penulis membahas berbagai jenis perintah pengintaian, juga pemindai keamanan, dan teknik pencegahan dalam artikel ini. Semua perintah ini berjalan di sistem operasi Ubuntu. Singkatnya, artikel ini terutama berfokus pada perintah semacam itu, alat sniffing, dan firewall untuk lebih memahami berbagai ancaman, serangan, dan kerentanan dalam jaringan.

Himani Sharma, et al [7], menjelaskan phishing adalah jenis serangan di mana phisher menggunakan email palsu dan situs web berbahaya untuk mencuri data sensitif orang. Sekarang berbagai jenis alat keamanan tersedia untuk mendeteksi phishing, penipuan. Artikel ini, pilih total delapan alat detektif untuk penelitian ini dan cari tahu alat mana yang lebih baik. Untuk pemindaian ini, penulis menggunakan dataset untuk menemukan hasilnya. Setiap alat diuji terhadap kumpulan data yang berisi phishing dan mengautentikasi situs web. Penulis melakukan survei di antara lima puluh siswa dan menyimpulkan bahwa sebagian besar pengguna internet tidak menyadari serangan semacam itu.

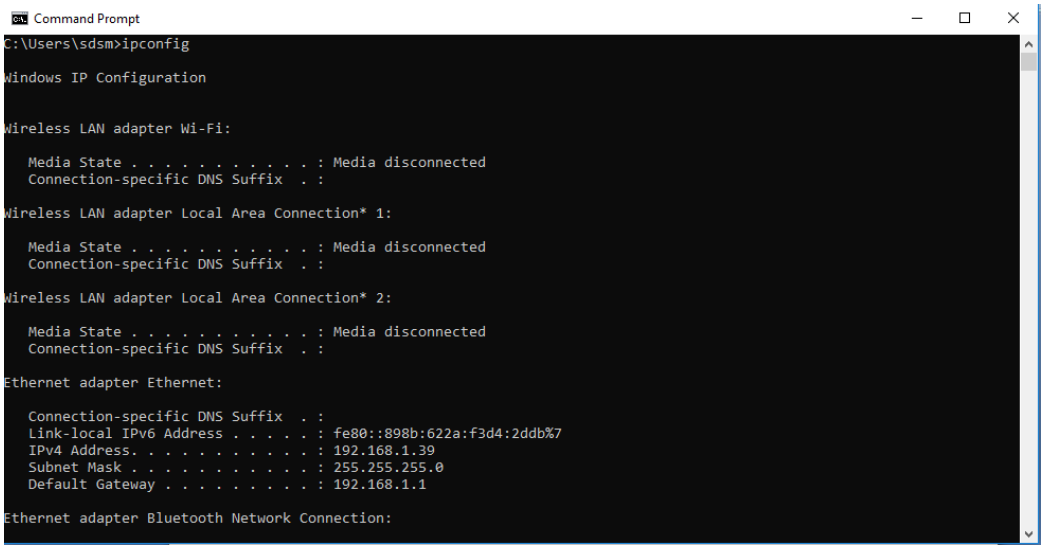
Inderjit Kaur, dkk [9], dewasa ini perluasan jaringan berkembang pesat dengan penerimaannya. Tetapi perlu untuk melindungi jaringan dari serangan luar. Ada salah satu teknik untuk mengamati data online yang dikenal sebagai packet sniffing. Ada banyak alat sniffing yang tersedia untuk memantau informasi seperti Wireshark, Tcpdump, Nmap, Zenmap, Capsa, dan banyak lagi.

Dalam artikel ini, penulis terutama berfokus pada berbagai alat sniffing dengan kapasitas analisisnya untuk menangkap lalu lintas jaringan di dalam jaringan. Beberapa dari mereka hanya digunakan untuk menangkap informasi tanpa menyelidiki lalu lintas. Jadi, penulis akhirnya menyimpulkan bahwa beberapa alat digunakan untuk deteksi intrusi dan sedikit yang digunakan untuk pengujian pena.

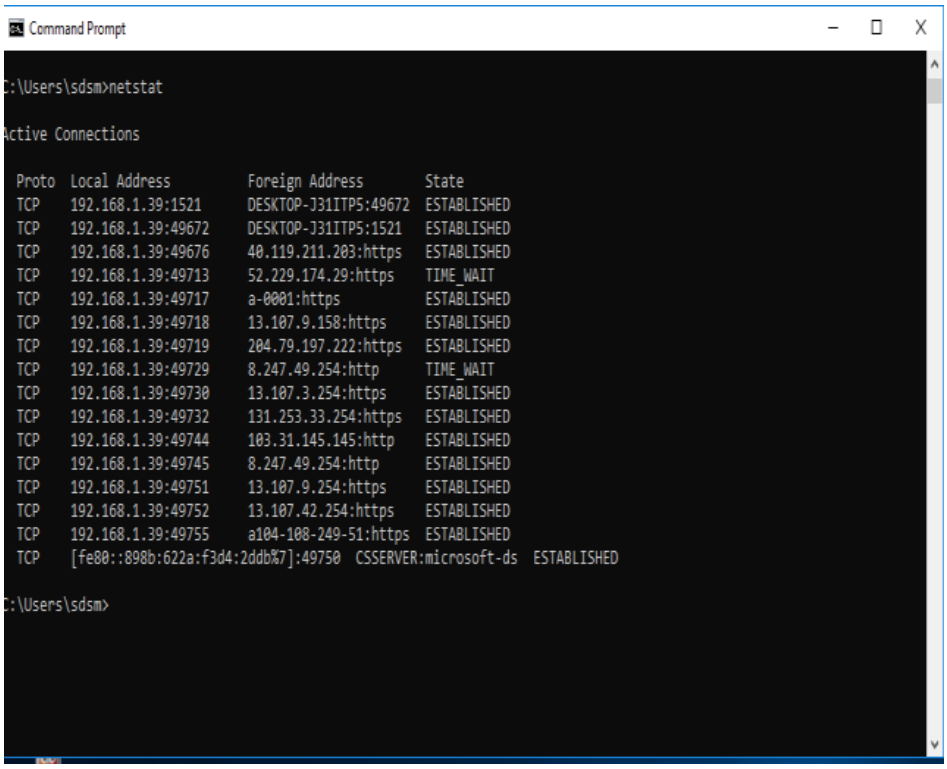
3. Metode

Ini adalah kelemahan yang dapat dimanfaatkan oleh penyusup untuk melakukan tindakan jahat dalam sistem komputer. Itu bisa jenis apa saja seperti Bug, kata sandi yang lemah, enkripsi data yang hilang, otorisasi yang hilang.

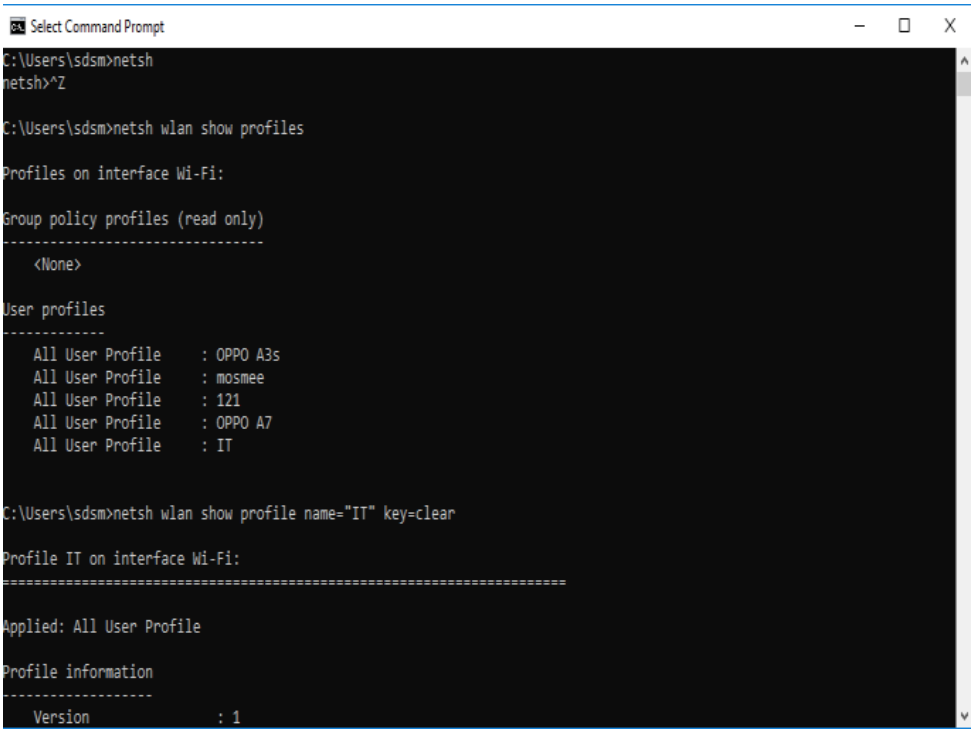
Untuk menyerang mesin tertentu, langkah pertama adalah Reconnaissance. Ini berarti pengamatan tentang korban. Itu bisa aktif atau pasif. Dalam tipe aktif penyerang terlibat dengan sistem yang ditargetkan untuk mengumpulkan informasi tentang kerentanan. Dalam tipe pasif penyerang untuk mendapatkan informasi tentang sistem yang ditargetkan tanpa secara aktif terlibat dengan sistem. Perintahnya terutama ipconfig, netstat, netsh, dan snort.



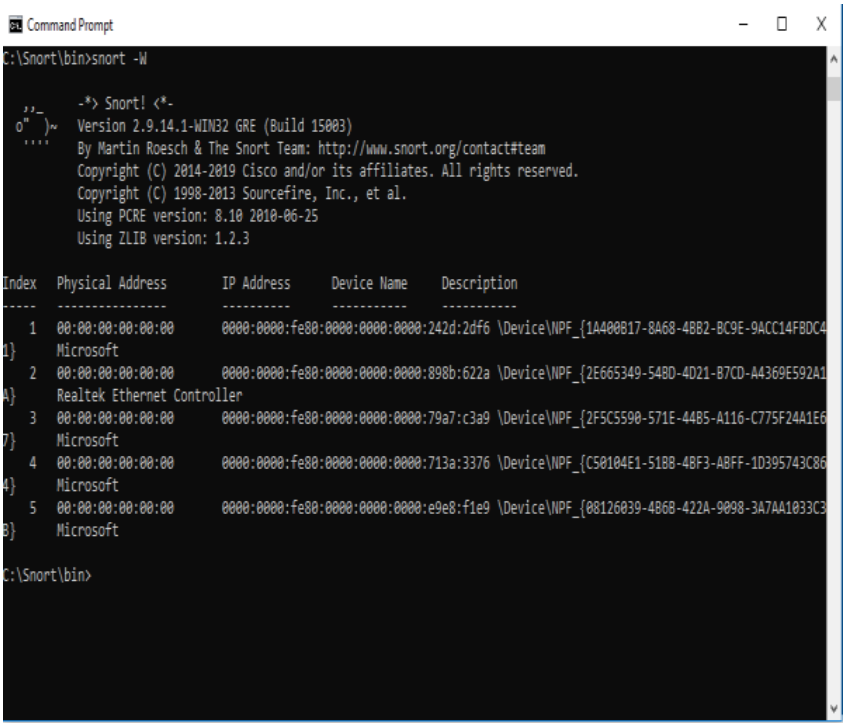
Gambar 1. menunjukkan perintah ipconfig yang digunakan untuk pengintaian.



Gambar 2. menunjukkan perintah netstat yang digunakan untuk informasi rinci tentang sistem dan juga dengan komputer lain yang terhubung melalui jaringan



Gambar 3. menunjukkan perintah netsh yang digunakan untuk menampilkan atau mengubah konfigurasi jaringan computer yang sedang berjalan.



Gambar 4. menunjukkan perintah snort. Snort digunakan untuk membaca paket IP, mencatat paket IP dan juga digunakan sebagai Intrusion Prevention System.

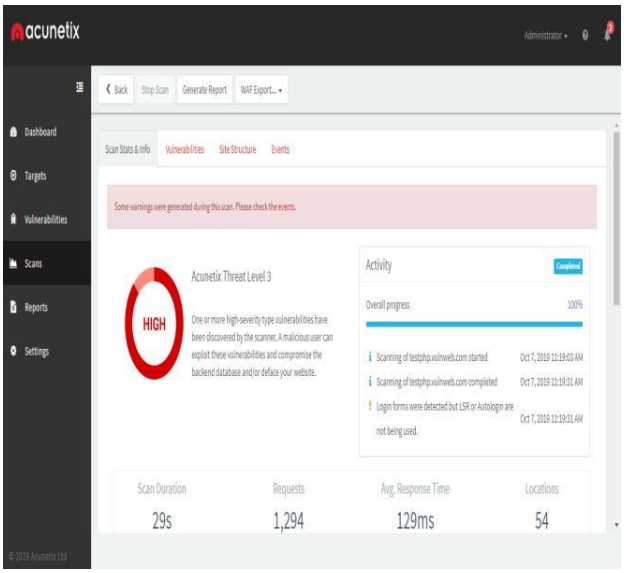
Untuk mencegah pengintaian aktif, sistem pencegahan intrusi bersama dengan firewall digunakan. Kombinasi ini membantu mendeteksi jenis serangan ini. Dalam pengintaian pasif

tidak ada komunikasi langsung dengan klien. Itu hanya mengumpulkan informasi tanpa sepengetahuan klien.

4. Hasil

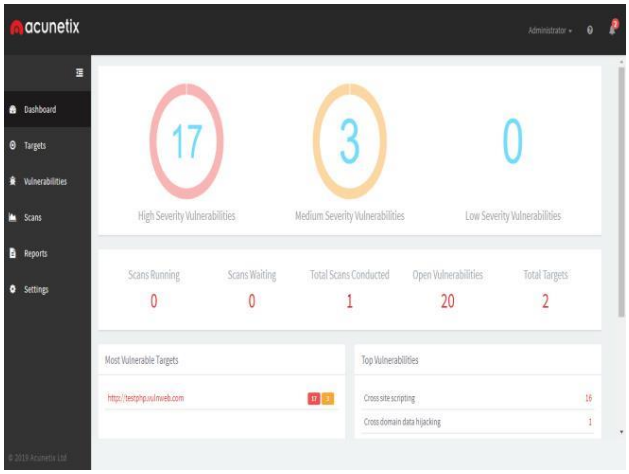
Pemindaian jaringan digunakan untuk mengumpulkan informasi dari sistem komputer. Hal ini terutama digunakan untuk evaluasi keamanan, pemeliharaan sistem, dan juga melakukan serangan oleh penyusup. Ini mengevaluasi sistem penyaringan host target juga antara pengguna dan host yang ditargetkan. Ini memindai port serta kerentanan sistem komputasi.

Dalam makalah ini, kami menggunakan Acunetix sebagai alat pemindaian yang rentan. Ini digunakan untuk memindai aplikasi web. Alat ini tersedia di Windows, sistem operasi Linux serta layanan online. Gbr.5 menunjukkan jendela pemindaian alat acunetix.

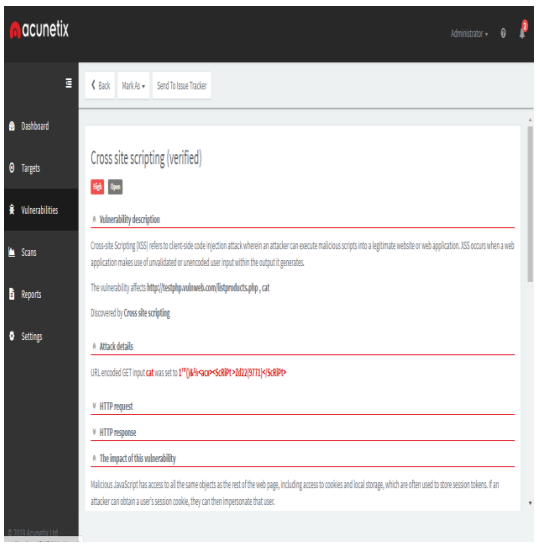


Gambar 5. Kemajuan Pemindaian

Gambar. 6 menunjukkan laporan kerentanan. Dalam pemindaian ini, kami menggunakan situs web sampel untuk menguji data. Di dalamnya, kami menemukan total 20 kerentanan di mana 17 ditemukan kerentanan tingkat tinggi dan 3 kerentanan sedang.



Gambar 6. laporan kerentanan



Gambar 7. Laporan satu kerentanan

Intrusion Prevention System (IPS) adalah perangkat lunak atau perangkat untuk mendeteksi atau mencegah ancaman berbahaya. Itu terus mengamati jaringan Anda, mencari kemungkinan aktivitas jahat dan mengumpulkan informasi mereka. IPS langsung berada di belakang firewall dan jalur komunikasi antara sumber dan tujuan. Ini menganalisis lalu lintas dan mengambil tindakan pada semua arus lalu lintas yang masuk ke jaringan. Ini juga disebut sistem pencegahan deteksi intrusi.

Itu mengirim alarm ke administrator, menjatuhkan paket jahat, memblokir lalu lintas, dan juga mengatur ulang koneksi. Sistem Pencegahan Intrusi ditemukan dalam empat cara berbeda.

1. Berbasis jaringan: Ini digunakan untuk melindungi jaringan komputer kita. Ia membaca semua paket yang masuk dan menemukan pola yang mencurigakan dan memberi tahu administrator. Ini mendeteksi aktivitas mencurigakan seperti serangan penolakan layanan, pemindaian port, dll.
2. Nirkabel: Yang melindungi jaringan nirkabel. Ini memonitor kinerja jaringan dan juga menemukan jalur akses dengan konfigurasinya.
3. Perilaku jaringan: Ini menganalisis dan memantau sistem jaringan dan menghasilkan peringatan.
5. Berbasis host: Muncul sebagai perangkat lunak yang diinstal untuk melindungi satu komputer. Misalnya snort, Suricata, malware defender.

Komparasi

Tabel 1. Alat keamanan dan tujuannya

Command /Tool	Purpose
Ipconfig	reconnaissance
Netstat	reconnaissance
Netsh	reconnaissance
Snort	Packet sniffer
Acunetix	Web scanning

Tabel I menunjukkan alat-alat sehubungan dengan tujuan mereka yang digunakan dalam penelitian ini. Dapat diamati bahwa semua perintah seperti ipconfig, netstat netsh bertindak sebagai pengintaian. Itu berarti alat pengumpulan informasi. Perintah seperti snort digunakan sebagai packet sniffer. Ini juga digunakan sebagai sistem pencegahan intrusi. Alat seperti Acunetix berfungsi sebagai pemindaian web.

5. Kesimpulan

Sekarang keamanan sehari di jaringan adalah Masalah utama. Di pasar banyak alat keamanan tersedia untuk melindungi data tetapi tetap saja, data yang dikirimkan melalui jaringan tidak aman. Dalam makalah ini bagian III dan IV memberikan rincian perintah dan alat keamanan yang menyediakan pemindaian dan pengintaian sistem. Bagian V memberikan rincian sistem pencegahan intrusi untuk memahami risiko, serangan, dan pertanggungjawaban jaringan

REFERENSI

[1] X Dr. Yogesh Kumar Sharma, "Deep and machine Learning Approaches for Anomaly-Based Intrusion Detection of Imbalanced Network Traffic", IOSR Journal of Engineering (IOSR JEN),ISSN (E):2250-3021, ISSN (P):2278-8719, PP 63-67

[2] Himani Sharma, Er. Meenakshi, Dr. Sandeep Kaur Bhatia (2017)," A COMPARATIVE ANALYSIS AND AWARENESS SURVEY OF PHISHING DETECTION TOOLS", 2nd IEEE International Conference on Recent Trends in Electronics Information & Communication Technology (RTEICT).

[3] Pallavi Asrodia, Hemlata Patel (2012)," Analysis of Various Packet Sniffing Tools for Network Monitoring and Analysis", ISSN No. (Online): 2277-2626, International Journal of Electrical, Electronicsand Computer Engineering, ISSN No. (Online): 2277-2626.

[4] Inderjit Kaur, Harkarandeep Kaur, Er. Gurjot Singh (2014), "Analysing Various Packet Sniffing Tools", International Journal of Electrical Electronics & Computer Science Engineering Volume 1, Issue 5 (October 2014), ISSN: 2348 2273.

[5] Sunita Saini and Dr. Yogesh Kumar Sharma, "A research study of wireless network security: A Case study", International Journal of Advanced Research in Computer Science and Software Engineering, volume 6 issue 3, March 2016,ISSN 2277 128X.

******