JUDUL BESAR:

IMPLEMENTASI INTERNET PUBLIK DI PUSAT KEGIATAN BELAJAR MASYARAKAT LANGGENG IKHLAS

SUB JUDUL:

ANALISIS KEAMANAN MIKHMON MENGGUNAKAN METODE *PENETRATION TESTING*

SKRIPSI

WAHYU ADI PAMUNGKAS 1907422001

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

DEPOK

2023

ANALISIS KEAMANAN MIKHMON MENGGUNAKAN METODE *PENETRATION TESTING*

SKRIPSI

Dibuat Untuk Melengkapi Syarat-Syarat yang Diperlukan Untuk Memperoleh Diploma Empat Politeknik

WAHYU ADI PAMUNGKAS 1907422001

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

DEPOK

2023

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini:

Nama : Wahyu Adi Pamungkas

NIM : 1907422001

Jurusan/ProgramStudi : Teknik Informatika dan Komputer / Teknik Multimedia dan Jaringan

Judul skripsi : Analisis Keamanan Mikhmon Menggunakan Metode *Penetration Testing*

Menyatakan dengan sebenarnya bahwa skripsi ini benar-benar merupakan hasil karya saya sendiri, bebas dari peniruan terhadap karya dari orang lain. Kutipan pendapat dan tulisan orang lain ditunjuk sesuai dengan cara-cara penulisan karya ilmiah yang berlaku. Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa dalam skripsi ini terkandung cirri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Depok, 21 Agustus 2023

Yang membuat pernyataan

(Wahyu Adi Pamungkas)

NIM 1907422001

LEMBAR PENGESAHAN

Skripsi diajukan oleh :

Nama : Wahyu Adi Pamungkas

NIM : 1907422001

Program Studi : Teknik Multimedia dan Jaringan

Judul Skripsi : Analisis Keamanan Mikhmon Menggunakan Metode *Penetration Testing*

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Jumat, Tanggal 28, Bulan Juli, Tahun 2023 dan dinyatakan **LULUS**.

Disahkan oleh

Pembimbing I : Defiana Arnaldy, S.Tp., M.Si. ( )

Penguji I : Ayu Rosyida Zain, S.ST., M.T. ( )

Penguji II : Indra Hermawan, S.Kom., M.Kom. ( )

Penguji III : Maria Agustin, S.Kom., M.Kom. ( )

Mengetahui :
Jurusan Teknik Informatika dan Komputer
Ketua

Dr. Anita Hidayati, S.Kom.,M.Kom.
NIP. 197908032003122003

KATA PENGANTAR

Puji syukur saya panjatkan kepada Tuhan Yang Maha Esa, karena atas berkat dan rahmat-Nya, penulis dapat menyelesaikan Laporan Skripsi ini. Penulisan Laporan Skripsi ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Diploma Empat Politeknik. Penulis menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, sangatlah sulit bagi penulis untuk menyelesaikan Laporan Skripsi. Oleh karena itu, penulis mengucapkan terima kasih kepada.

a. Defiana Arnaldy, S.Tp., M.Si. selaku dosen pembimbing yang telah menyediakan waktu, tenaga dan pikiran untuk membimbing penulis dalam menyusun Laporan Skripsi ini;
b. Pusat Kegiatan Belajar Masyarakat Langgeng Ikhlas yang telah mengizinkan untuk dilaksanakannya penelitian ini;
c. Orang tua yang telah memberikan dukungan moral dan materi untuk penulis sampai bisa menyelesaikan Laporan Skripsi ini;
d. Nafikiri yang telah memberi hujatan kepada penulis sehingga membuat penulis semakin semangat untuk menyelesaikan Skripsi ini;
e. Nadea dan Haickal yang telah mendukung, menyemangati, dan mendengarkan keluh kesah penulis selama mengerjakan Skripsi;
f. Teman-teman CCIT SEC 8 yang telah memberi semangat dan solidaritas dalam pengerjaan Skripsi ini;
g. Mantan Gebetan yang telah menolak perasaan penulis sehingga membuat penulis untuk terpacu semakin semangat menyelesaikan Skripsi ini;

Akhir kata, penulis berharap Tuhan Yang Maha Esa membalas segala kebaikan semua pihak yang telah membantu penulis. Semoga Laporan Skripsi ini membawa manfaat bagi pembaca dan pengembangan ilmu pengetahuan.

Bogor, 12 Juli 2023

Penulis

ABSTRAK

Semakin meningkatnya serangan dalam dunia internet didukung pula dengan data yang dirilis oleh BSSN (Badan Siber Sandi Negara) dalam hasil laporan tahunan 2021 HONEYNET PROJECT BSSN – IHP, bahwa sepanjang tahun 2021 telah terjadi serangan siber sebanyak 266.741.784 kali di dunia. Belum adanya analisis keamanan yang dilakukan pada mikhmon dijaringan yang telah diimplementasikan menjadi masalah yang akan diangkat dalam penelitian ini. Penelitian ini bertujuan untuk melakukan analisis keamanan Mikhmon yang telah diimplementasikan di jaringan internet PKBM (Pusat Kegiatan Belajar Masyarakat) Langgeng Ikhlas menggunakan metode penetration testing. Sebelum melakukan penetration testing dilakukan sebuah vulnerability assesment menggunakan tools vulnerability scanner yang berfungsi untuk mencari celah kerentanan dalam jaringan di PKBM Langgeng Ikhlas dan selanjutnya dilakukan penetration testing untuk mensimulasikan penyerangan seperti SQL injection dan dictionary attack terhadap jaringan tersebut. Hasil dari analisis kerentanan terhadap mikhmon didapatkan kerentanan terbanyak pada tingkatan high sebanyak 1 oleh nessus, medium sebanyak 8 oleh acunetix, low sebanyak 7 oleh acunetix dan information sebanyak 24 oleh nessus. Hasil dari pengujian serangan terhadap mikhmon menggunakan teknik sql injection tidak ditemukan celah kerentanan dan menggunakan teknik dictionary attack dapat ditemukan username dan password yang dapat digunakan untuk masuk kedalam mikhmon.

Kata kunci: *penetration testing, vulnerability assesment, vulnerability scanner, SQL injection, dan dictionary attack*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi pada saat ini sangatlah pesat. Dalam beberapa tahun terakhir banyak sekali inovasi teknologi dibidang informasi khususnya internet yang mempermudah kita untuk saling berkomunikasi dari belahan dunia manapun. Dengan mudahnya komunikasi kepada siapapun, kapanpun, dan dimanapun sangat berdampak positif pada perkembangan dalam dunia bisnis, Pendidikan, entertain, dan lainnya. Dilansir dari republika.co.id, berdasarkan survei terbaru jumlah pengguna internet di Indonesia berjumlah 210.026.769 dari total jumlah penduduk Indonesia tahun 2021 272.682.600 jiwa. Dibalik dari semakin banyaknya pengguna internet di dunia khususnya di negara Indonesia, semakin banyak pula kejahatan di dunia internet. Hal tersebut didukung dengan laporan tahunan 2021 HONEYNET PROJECT BSSN – IHP yang dikeluarkan oleh BSSN (Badan Siber Sandi Negara) bahwa sepanjang tahun 2021 telah terjadi serangan siber sebanyak 266.741.784 kali di dunia dan diantaranya sebanyak 32.091.240 kali menyasar ke negara Indonesia.

Jaringan komputer menjadi bagian penting dalam infrastruktur bagi sebuah organisasi atau perusahaan. Oleh karena itu, keamanan jaringan pada saat ini menjadi hal yang sangat penting dan krusial. Karena dewasa ini banyak sekali ancaman terhadap jaringan yang selalu mengintai. Banyak sekali organisasi atau perusahaan yang belum menjadikan keamanan jaringan sebagai prioritas. Ancaman terhadap keamanan jaringan semakin berkembang pesat dan kompleks, diantaranya adalah *virus, malware, sniffing, bruteforce* dan serangan siber lainnya yang dapat mengakibatkan ancaman kebocoran data atau bahkan hal yang lebih buruk dari itu.

Diperlukan sebuah analisis keamanan yang menyeluruh untuk mengidentifikasi celah kerentanan atau keamanan dalam jaringan.

Penetration testing merupakan salah satu metode yang digunakan untuk mengevaluasi keamanan jaringan. Metode ini dilakukan dengan cara melakukan serangan langsung terhadap sistem dimana serangan tersebut merupakan simulasi serangan yang sama dengan apa yang dilakukan oleh *hacker*. Metode ini meliputi langkah-langkah pengumpulan informasi, pemindaian kerentanan, dan penyerangan terhadap sistem. Ada beberapa alasan mengapa perlu dilakukannya *penetration testing* dalam sebuah jaringan adalah untuk mengidentifikasi kerentanan dan kelemahan dalam sebuah jaringan. Dengan menemukan dan memperbaiki kerentanan yang ditemukan dapat mengurangi risiko dan melindungi data sensitif dari serangan siber yang sewaktu-waktu dapat terjadi dan menyebabkan kebocoran data atau bahkan merusak infrastruktur jaringan tersebut.

Dalam penelitian ini dilakukan sebuah analisis keamanan terhadap Mikhmon pada jaringan yang telah diimplementasikan di PKBM (Pusat Kegiatan Belajar Masyarakat) Langgeng Ikhlas dengan menggunakan metode *penetration testing*. Mikhmon merupakan sebuah server manajemen yang terhubung langsung ke perangkat mikrotik dan berfungsi untuk mencetak kode *voucher* dan selanjutnya kode *voucher* tersebut akan digunakan sebagai kode atau username dan password untuk masuk kedalam hotspot di jaringan internet PKBM (Pusat Kegiatan Belajar Masyarakat).

1.2 Rumusan Masalah

Dari latar belakang dapat disimpulkan terdapat beberapa masalah sebagai berikut?

a. Bagaimana cara menemukan celah kerentanan atau kelemahan pada Mikhmon di jaringan internet PKBM Langgeng Ikhlas?
b. Bagaimana cara melakukan uji kerentanan yang ditemukan pada Mikhmon?
c. Bagaimana hasil analisis pengujian keamanan Mikhmon?

1.3 Batasan Masalah

Terdapat batasan masalah yang bertujuan agar pembahasan menjadi lebih mengerucut dan efisien. Adapun batasan masalah dapat dijelaskan sebagai berikut:

a. Analisis keamanan mikhmon dilakukan pada dalam jaringan atau lokal.

b. *Tools* yang digunakan dalam penelitian ini adalah Accunetix, Nmap, Nessus, Burpsuite dan Sqlmap.
c. Teknik serangan yang digunakan adalah *Sql Injection* dan *Dictionary attack.*

1.4 Tujuan dan Manfaat

Adapun tujuan dan manfaat dari dilakukannya penelitian ini adalah sebagai berikut:

1.4.1 Tujuan

Adapun tujuan dari dilakukannya penelitian ini adalah untuk mengetahui celah kerentanan pada Mikhmon di jaringan internet PKBM (Pusat Kegiatan Belajar Masyarakat) Langgeng Ikhlas dengan melakukan *vulnerability scanning* lalu selanjutnya dilakukan *penetration testing* dan dibuat sebuah rekomendasi apabila terdapat kerentanan pada sistem tersebut.

1.4.2 Manfaat

Adapun manfaat dari dilakukannya penelitian ini adalah untuk mengetahui seberapa aman dan mengetahui apa saja celah kerentanan pada mikhmon serta membantu meningkatkan kualitas keamanan Mikhmon berdasarkan informasi celah kerentanan yang ditemukan melalui proses *penetration testing* terhadap mihkmon di jaringan internet PKBM (Pusat Kegiatan Belajar Masyarakat) Langgeng Ikhlas.

1.5 Sistematika Penulisan

Sistematika penulisan dalam penyusunan proposal ini adalah sebagai berikut:

a. BAB 1 PENDAHULUAN

   Berisi latar belakang penelitian, perumusan masalah, batasan masalah, tujuan dan manfaat serta sistematika penulisan.

b. BAB II TINJAUAN PUSTAKA

   Berisi uraian pembahasan mengenai teori yang mendukung dan membantu peneletian.

c. BAB III METODOLOGI PENELITIAN

Berisi metode pembahasan metode penelitian, tahapan penelitian, objek penelitian, teknik pengumpulan data dan jadwal penelitian.

d. BAB IV PEMBAHASAN

Berisi pembahasan proses serta hasil kegiatan selama penelitian yang dilakukan sesuai dengan tahapan dan metode yang telah ditentukan sebelumnya.

e. BAB V KESIMPULAN DAN SARAN

Berisi kesimpulan dan saran dari penelitian yang telah dilaksanakan

BAB V
KESIMPULAN

5.1 Kesimpulan

Hasil analisis kerentanan menggunakan metode *penetration testing* dengan target mikhmon mendapatkan beberapa kesimpulan diantaranya adalah:

a. Celah kerentanan dan kelemahan pada mikhmon dapat ditemukan dengan cara melakukan *vulnerability scanning* menggunakan nessus dan acunetix. Dimana hasil kerentanan dari kedua *tools* tersebut memberikan hasil berupa informasi pengkategorian tingkat level celah kerentanan mikhmon dimulai dari timgkat *critical, high, medium, low* hingga *informational*. Informasi lain hasil *vulnerability* scanning menggunakan nessus dan acunetix juga berupa informasi penjelasan dari setiap kerentanan yang ditemukan beserta rekomendasi yang dapat dilakukan untuk memperbaiki kerentanan yang ditemukan tersebut.
b. Berdasarkan data kerentanan yang didapatkan maka ditentukan untuk melakukan uji kerentanan mikhmon dengan melakukan simulasi serangan menggunakan teknik *sql injection* dan *dictionary attack* menggunakan burpsuite dan sqlmap.
c. Hasil dari pengujian keamanan dengan melakukan *vulnerability scanning* menggunakan nessus dan acunetix terhadap perangkat mikrotik didapatkan hasil ditemukan celah kerentanan dengan kategori *level critical* sebanyak 2 kerentanan, *high* sebanyak 2 kerentanan, *medium* sebanyak 4 kerentanan dan *low* sebanyak 6 kerentanan. Serta ditemukan celah kerentanan pada mikhmon menggunakan nessus dan acunetix dengan kategori *level high* sebanyak 1 kerentanan, *medium* sebanyak 13 kerentanan dan *low* sebanyak 7 kerentanan. Adapun simulasi serangan terhadap mikhmon menggunakan teknik *sql injection* dan *dictionary attack* mendapatkan hasil bahwa pengujian eksploitasi *sql injection* pada mikhmon yang dilakukan menggunakan burpsuite dan sqlmap mendapatkan hasil tidak ditemukan bahwa mikhmon dapat dieksploitasi menggunakan teknik *sql injection*.

Selain itu, pengujian eksploitasi *dictionary attack* pada mikhmon yang dilakukan menggunakan burpsuite dengan dua skenario berbeda dimana skenario pertama *username* dan *password* tidak diketahui berhasil menebak *username* dan *password* yang dapat digunakan untuk masuk kedalam mikhmon sedangkan hasil skenario kedua *username* diketahui dan *password* tidak diketahui berhasil menemukan *password* yang dapat digunakan untuk masuk kedalam mikhmon.

5.2 Saran

Berdasarkan penelitian yang telah dilakukan terdapat saran yang dapat diterapkan dan dikembangkan pada penelitian yang akan datang selanjutnya yaitu dengan menggunakan teknik serangan dan penggunaan *tools penetration testing* yang berbeda supaya mendapatkan hasil dan cakupan *penetration testing* dari aspek yang lebih luas.

DAFTAR PUSTAKA

Abdul Kholiq, D. K. (2019). ANALISIS KEAMANAN WIRELESS LOCAL AREA NETWORK (WLAN) DENGAN . *Jurnal Ilmiah Fakultas Teknik LIMIT'S*.

Achmady, S. (2017). Analysis DictionaryAttack dan Modifikasi Password Cracking Serta Strategi Antisipasi. *JURNAL SAINS RISET*, No.1.

Amarudin, F. U. (2018). DESAIN KEAMANAN JARINGAN PADA MIKROTIK ROUTER OS . *Jurnal TEKNOINFO*, No.2.

BSSN. (2021). *2021 HONEYNET PROJECT BSSN - IHP*. Jakarta : Badan SIber Sandi Negara.

Dalila, A. H. (2022). ANALISIS KEAMANAN PADA WEBSITE PT. ANEKA TIRTA TALENTA MENGGUNAKAN METODE PENETRATION TESTING.

Defiana Arnaldy, A. R. (2019). Implementation and Analysis of Penetration . *IC2IE*.

Djibran, M. N. (2022). Analisis Uji Sistem Keamanan Jaringan Web dan Database .

Feri Wibowo, H. A. (2019). Uji Vulnerability pada Website Jurnal Ilmiah Universitas Muhammadiyah Purwokerto Menggunakan OpenVAS dan Acunetix WVS. *Jurnal Informatika*.

Hermawa, R. (2021). TEKNIK UJI PENETRASI WEB SERVER MENGGUNAKAN SQL . *STRING (Satuan Tulisan Riset dan Inovasi Teknologi)* , No.2.

Hermawan, R. (2021). TEKNIKUJI PENETRASI WEB SERVER MENGGUNAKAN SQL INJECTIONDENGAN SQLMAP DI KALILINUX.

Husna, M. A. (2021). Implementasi Sistem Monitoring Jaringan dan Server Menggunakan Zabbix. *Jurnal Riset Komputer*.

Johanna. (2022, oktober). *Apa itu Penetration Testing? Manfaat, Tahapan dan Cara Kerjanya*. Retrieved from dewaweb.com: https://www.dewaweb.com/blog/pengertian-penetration-testing/

Juardi, D. (2017). Kajian Vulnerability Keamanan Jaringan Internet . *SYNTAX Jurnal Informatika*.

Juardi, D. (2018). Kajian Vulnerability Keamanan Jaringan Internet Menggunakan Nessus. *SYNTAX Jurnal Informatika*.

Muhammad Ivan Susanto, A. H. (2019). Sistem Proteksi Jaringan Wlan Terhadap Serangan Wireless Hacking. *JREC*.

Muhyidin, Y. (2022). Perbandingan Tingkat Keamanan Website Menggunakan Nmap Dan Nikto. *Jurnal Teknologika*, No.1.

Mulyadi. (2018, januari 2). *Bagaimana Melakukan "Penetration Test"?* Retrieved from Kompasiana.com: https://www.kompasiana.com/moengil/5a4ae2655e13736b135dd7e3/bagaimana-melakukan-penetration-testing

Mustofa, T. A. (2019). PERANCANGAN DAN IMPLEMENTASI SISTEM MONITORING JARINGAN WI-FI MENGGUNAKAN MIKHMON ONLINE DI WISMA MUSLIM KLITREN GONDOKUSUMAN YOGYAKARTA. *Jurnal JARKOM*, No.2.

Penetration Testing Execution Standard (PTES). (2022, november 21). Retrieved from www.geeksforgeeks.org: https://www.geeksforgeeks.org/penetration-testing-execution-standard-ptes/

Pengertian LAN, MAN, WAN dan Perbedaannya. (2022, maret 14). Retrieved from Kompas.com: https://tekno.kompas.com/read/2022/03/14/17290067/pengertian-lan-man-wan-dan-perbedaannya

Perdana, A. R. (2019). IMPLEMENTASI DAN ANALISIS TEKNIK PENETRASI MENGGUNAKAN METODE MAN-IN-THE-MIDDLE ATTACK. *IEEE*.

Pradana, D. (2020, juli 5). *WiFi Pentesting dengan aircrack-ng*. Retrieved from denypradana.com: https://www.denypradana.com/2020/07/05/wifi-pentesting-dengan-aircrack-ng/

Prasetyo, A. (2019). Pengertian Flowchart Beserta Fungsi dan .

Reivaldi Kesuma Kagi, M. F. (2020). DESAIN DAN IMPLEMENTASI PADA WIFI PUSTIKOM FREE ACCESSDI PUSAT TEKNOLOGI INFORMASI DAN KOMUNIKASI UNIVERSITAS NEGERI JAKARTA MENGGUNAKAN MIKROTIK DAN WIRESHARK UNTUK ANALISIS TERHADAP SERANGAN PACKET SNIFFING DAN NETCUT. *Jurnal Pinter*.

Santoso, R. M. (2022). ANALISIS JARINGAN VPN PROTOKOL SSTP PADA VIDEO .

Satria, D. (2018). Network Security Assessment Using Internal Network. *INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION*.

DAFTAR RIWAYAT HIDUP

Wahyu Adi Pamungkas, Lahir di Bogor, 09 Agustus 2001. Sudah menempuh Pendidikan Sekolah Dasar SD Negeri Bedahan 01 Cibinong (2007-2013), Sekolah Menengah Pertama SMP Citra Nusa (2013-2016), Sekolah Menengah Atas SMK Negeri 01 Cibinong Jurusan Teknik Komputer dan Jaringan (2016-2019), Pendidikan professi CEP-CCIT Fakultas Teknik Universitas Indoenesia (2019-2021) konsentrasi Network Administrator Professional dan Perguruan Tinggi Politeknik Negeri Jakarta Jurusan Teknik Informatika dan Komputer program studi Teknik Multimedia dan Jaringan konsentrasi Sistem Keamanan Informasi.

LAMPIRAN 1-Data hasil *Vulnerability scanning* dengan acunetix

Acunetix by Invicti

Comprehensive Report

MEDIUM

Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Scan Detail

Target	http://192.168.20.29
Scan Type	Full Scan
Start Time	Jul 8, 2023, 12:03:38 PM GMT+7
Scan Duration	21 minutes
Requests	40491
Average Response Time	1ms
Maximum Response Time	29707ms

0	8	7	15
High	Medium	Low	Informational

Severity	Vulnerabilities	Instances
High	0	0
Medium	8	8
Low	7	7
Informational	11	15
Total	26	30

Informational

	Instances
Content Security Policy (CSP) not implemented	1
Content Security Policy Misconfiguration	5
Content type is not specified	1
Others	8

Low Severity

	Instances
Clickjacking: CSP frame-ancestors missing	1
Clickjacking: X-Frame-Options header	1
Cookies with missing, inconsistent or contradictory properties	1
Others	4

Impacts

Severity Filter: High Medium Low Informational

SEVERITY		IMPACT
Medium	1	Apache server-info enabled
Medium	1	Apache server-status enabled
Medium	1	Application error messages
Medium	1	Directory listings
Medium	1	Test CGI script leaking environment variables
Medium	1	Unencrypted connection
Medium	1	User credentials are sent in clear text
Medium	1	Vulnerable JavaScript libraries
Low	1	Clickjacking: CSP frame-ancestors missing
Low	1	Clickjacking: X-Frame-Options header
Low	1	Cookies with missing, inconsistent or contradictory properties
Low	1	Cookies without HttpOnly flag set
Low	1	Possible sensitive directories
Low	1	Possible sensitive files
Low	1	TRACE method is enabled
Informational	1	Content Security Policy (CSP) not implemented

LAMPIRAN 2-Data hasil *Vulnerability scanning* dengan nessus

nessus

Report generated by Nessus™

mikhmon

Sat, 08 Jul 2023 11:51:08 SE Asia Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

- 192.168.20.29

Vulnerabilities by Host

Collapse All | Expand All

192.168.20.29

0	1	5	0	25
CRITICAL	HIGH	MEDIUM	LOW	INFO

Show

nessus

Report generated by Nessus™

mikrotik

Sat, 08 Jul 2023 11:46:45 SE Asia Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

- 192.168.20.1

Vulnerabilities by Host

Collapse All | Expand All

192.168.20.1

2	4	3	4	25
CRITICAL	HIGH	MEDIUM	LOW	INFO