ANALISIS KINERJA PADA *TOOLS INTRUSION PREVENTION SYSTEM* DALAM MENANGANI KERENTANAN SISTEM KEAMANAN JARINGAN

SKRIPSI

Devita Ariandi
1803421024

PROGRAM STUDI BROADBAND MULTIMEDIA
JURUSAN TEKNIK ELEKTRO
POLITEKNIK NEGERI JAKARTA
2023

ANALISIS KINERJA PADA *TOOLS INTRUSION PREVENTION SYSTEM* DALAM MENANGANI KERENTANAN SISTEM KEAMANAN JARINGAN

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Terapan

Devita Ariandi

1803421024

PROGRAM STUDI BROADBAND MULTIMEDIA

JURUSAN TEKNIK ELEKTRO

POLITEKNIK NEGERI JAKARTA

2023

HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya saya sendiri dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama	**:**	**Devita Ariandi**
NIM	**:**	**1803421024**
Tanda Tangan	**:**	
Tanggal	**:**	**18 Januari 2023**

LEMBAR PENGESAHAN
SKRIPSI

Skripsi diajukan oleh:

Nama	:	Devita Ariandi
NIM	:	1803421024
Program Studi	:	Brodband Multimedia
Judul Tugas Akhir	:	Analisis Kinerja pada *Tools Intrusion Prevention System* dalam Menangani Kerentanan Sistem Keamanan Jaringan

Telah diuji oleh tim penguji dalam Sidang Tugas Akhir pada 20 Januari 2023 dan dinyatakan **LULUS**.

Pembimbing : Dandun Widhiantoro, A.Md., M.T. ( )
NIP. 197011251995031001

Depok,.....

Disahkan oleh
Ketua Jurusan Teknik Elektro

Rika Novita Wardhani, S.T., M.T.
NIP. 197011142008122001

KATA PENGANTAR

Puji syukur saya panjatkan kepada Tuhan Yang Maha Esa, karena atas berkat dan rahmat-Nya, penulis dapat menyelesaikan Skripsi ini. Penulisan Skripsi yang berjudul "Analisis Kinerja pada *Tools* Intrusion Prevention System dalam Menangani Kerentanan Sistem Keamanan Jaringan" dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana Terapan Politeknik.

Penulis menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan skripsi ini, sangatlah sulit bagi penulis untuk menyelesaikan skripsi ini. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Dandun Widhiantoro, A.Md., M.T., selaku dosen pembimbing yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan penulis dalam penyusunan skripsi ini;
2. Orang tua dan keluarga penulis yang telah memberikan bantuan dukungan material dan moral; dan
3. Sahabat yang telah banyak membantu penulis dalam menyelesaikan skripsi ini.

Akhir kata penulis berharap Tuhan Yang Maha Esa berkenan membalas segala kebaikkan semua pihak yang telah membantu. Semoga Skripsi ini membawa manfaat bagi pengembangan ilmu.

Depok, 18 Januari 2023

Penulis

Analisis Kinerja pada *Tools Intrusion Prevention System* dalam Menangani Kerentanan Sistem Keamanan Jaringan

Abstrak

Saat ini banyak kegiatan yang dilakukan dengan menggunakan sistem digital, sehingga penggunaan jaringan sudah menjadi kebutuhan pokok, yang menyebabkan tingkat keamanan jaringan perlu lebih diperhatikan. Pada umumnya dalam melindungi jaringan, organisasi atau pengguna akan menggunakan firewall sebagai lapisan pertama dalam sistem keamanan jaringan. Namun firewall memiliki kekurangan, yaitu tidak dapat mendeteksi isi dari paket data. Untuk mengatasi kekurangan tersebut dapat dibuat sistem pencegahan intrusi (IPS) dengan cara mengkombinasikan kerja sistem firewall dengan sistem pendeteksian intrusi (IDS). Snort dan Suricata adalah IDS bersifat sumber tebuka dan banyak komunitas yang melakukan pengembangan dari sisi pembuatan aturan maupun dari sisi algoritma IDS. Saat ini kedua IDS tersebut dapat dijadikan IPS serta bekerja secara multithread. Untuk mengetahui kinerja dari Snort dan Suricata, dilakukan pengujian dengan mengkombinasikan Snort/Suricata pada IPTables sebagai firewall yang dipasang secara inline untuk melindungi web server. Pada pengujian dengan menggunakan framework Pytbull, Snort lebih unggul dengan persentase mendeteksi penuh sebesar 13,79%, mendeteksi sebagian sebesar 58,62%, dan tidak mendeteksi sebesar 27,59%. Pengujian kedua dilakukan serangan DDoS dan Snort dapat memblokir serangan lebih banyak dibandingkan Suricata, yaitu dengan rata-rata persentase jumlah paket data yang lolos pada serangan Ping Flood 0,62%, TCP SYN Flood 0,58%, TCP SYN Flood dengan 500 byte 0,52%, TCP SYN Flood dengan 1000 byte 0,44%. Sehingga performa pada Snort dapat dikatakan lebih unggul dibandingkan Suricata.

Kata kunci: *Firewall*, IDS, IPS, Snort, Suricata

Performance Analysis on Intrusion Prevention System Tools in Handling Network Security System Vulnerabilities

Abstract

Currently, many activities are carried out using digital systems, so that the use of the network has become a basic requirement, which causes the level of network security to pay more attention. In general, in protecting networks, organizations or users will use a firewall as the first layer in a network security system. But the firewall has a drawback, which is unable to detect the contents of the data packet. To overcome these deficiencies, an intrusion prevention system (IPS) can be made by combining the work of a firewall system with an intrusion detection system (IDS). Snort and Suricata are open source IDS and many communities are developing both from the rule-making side and from the IDS algorithm side. Currently the two IDS can be used as IPS and work in multithread. To find out the performance of Snort and Suricata, a test was carried out by combining Snort/Suricata on IPTables as a firewall that was installed inline to protect the web server. In testing using the Pytbull framework, Snort is superior with a full detection percentage of 13.79%, partial detection of 58.62%, and no detection of 27.59%. The second test was carried out by DDoS attacks and Snort was able to block more attacks than Suricata, namely with an average percentage of data packets that passed the Ping Flood attack of 0.62%, TCP SYN Flood 0.58%, TCP SYN Flood with 500 bytes 0 .52%, TCP SYN Flood with 1000 bytes 0.44%. So the performance on Snort can be said to be superior to Suricata.

Keywords: *Firewall*, IDS, IPS, Snort, Suricata

DAFTAR ISI

HALAMAN PERNYATAAN ORISINALITAS iii
LEMBAR PENGESAHAN SKRIPSI iv
KATA PENGANTAR v
DAFTAR ISI viii
DAFTAR GAMBAR xi
DAFTAR TABEL xii
DAFTAR LAMPIRAN xiii
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Perumusan Masalah 2
1.3 Tujuan 2
1.4 Luaran 3
BAB II TINJAUAN PUSTAKA 4
2.1 Keamanan Informasi 4
2.2 Jaringan 5
2.3 *Firewall* 6
2.4 *Intrusion Detection System* (*IDS*) dan *Intrusion Prevention System* (*IPS*) 7
2.4.1 *Intrusion Detection System* (*IDS*) 7
2.4.2 *Intrusion Prevention System* (*IPS*) 8
2.4.3 Topologi *IDS/IPS* 8
2.4.4 *Pembuatan Rule IDS/IPS* 9
2.5 *Tools IDS/IPS* 10
2.5.1 Snort 10
2.5.2 Suricata 13
2.6 Web Server 13

2.7 *Framework Pytbull* 13
2.8 *Tools* 15
2.8.1 *Hping3* 15
2.8.2 *Nmap* 17
BAB III PERENCANAAN DAN REALISASI 18
3.1 Rancangan Sistem 18
3.1.1 Deskripsi Sistem 18
3.1.2 Cara Kerja Sistem 18
3.1.3 Spesifikasi Sistem 19
3.1.4 Rancangan Jaringan 20
3.1.5 Rancangan Halaman Web 21
3.2 Realisasi Sistem 22
3.3 Skenario Pengujian Pengujian 31
3.3.1 Skenario Pengujian Sistem Deteksi Menggunakan *Framework Pytbull* 32
3.3.2 Skenario Pengujian Sistem Pencegahan dalam Melindungi Web server dari Serangan *DDoS* 32
BAB IV PEMBAHASAN 33
4.1 Pengujian Sistem Deteksi Menggunakan *Framework* Pytbull 33
4.1.1 Deskripsi Pengujian 33
4.1.2 Prosedur Pengujian 33
4.1.3 Data Hasil Pengujian 35
4.1.4 Analisis Data 36
4.2 Pengujian Sistem Pencegahan dalam Melindungi Web server dari Serangan DDoS 37
4.2.1 Deskripsi Pengujian 37
4.2.2 Prosedur Pengujian 37

4.2.3 Data Hasil Pengujian 39
4.2.4 Analisis Data 42
4.3 Hasil Pengujian Secara Keseluruhan 44
BAB V SIMPULAN 46
DAFTAR PUSTAKA 47

DAFTAR GAMBAR

Gambar 2. 1 Cara Kerja *Firewall* 6
Gambar 2. 2 Topologi Jaringan IDS dan *IPS* 9
Gambar 2. 3 *Rule* pada *Tools IDS/IPS* 9
Gambar 2. 4 Kondisi *Log* File pada Kasus *Full*, *Partial*, dan *No Detection* 15
Gambar 3. 1 Tahapan Kerja Sistem *IPS* 18
Gambar 3. 2 Topologi Fisik Jaringan Internal dan Eksternal 21
Gambar 3. 3 Rancangan Halaman Web 22
Gambar 3. 4 Alur Pembuatan Sistem *IPS* 23
Gambar 3. 5 Konfigurasi Alamat *IP* pada Router 24
Gambar 3. 6 Konfigurasi *IP* pada *PC* 25
Gambar 3. 7 Konfigurasi *Static Route* pada modem router TP-Link 26
Gambar 3. 8 Konfigurasi Tabel *Filter* 26
Gambar 3. 9 Konfigurasi Tabel *NAT* 26
Gambar 3. 10 Hasil Tes *Ping* Antar Perangkat 27
Gambar 3. 11 Halaman Web 28
Gambar 3. 12 Instalasi Snort 29
Gambar 3. 13 Konfigurasi *HOME_NET* dan *EXTERNAL_NET* 29
Gambar 3. 14 Konfigurasi *Include File Rules* Pada Snort 30
Gambar 4. 1 Hasil Pendeteksian Snort dan Suricata Menggunakan *Framework Pytbull* 35
Gambar 4. 2 Persentase Akurasi Pendeteksian Snort dan Suricata 36
Gambar 4. 3 Data Hasil Pengujian dan Persentase Paket Data yang Tidak Terblokir pada Pengujian 1 40
Gambar 4. 4 Data Hasil Pengujian dan Persentase Paket Data yang Tidak Terblokir pada Pengujian 2 41
Gambar 4. 5 Data Hasil Pengujian dan Persentase Paket Data yang Tidak Terblokir pada Pengujian 3 41
Gambar 4. 6 Data Hasil Pengujian dan Persentase Paket Data yang Tidak Terblokir pada Pengujian 4 42
Gambar 4. 7 Rata-Rata Persentase Paket Data yang Tidak Terblokir oleh Snort dan Suricata 42

DAFTAR TABEL

Tabel 2. 1 Tabel perbandingan fitur dan perfoma Snort2 dengan Snort3 11
Tabel 3. 1 Spesikasi Perangkat Keras 19
Tabel 3. 3 Spesifikasi Perangkat Lunak 20
Tabel 3. 4 Pengalamatan *IP* Perangkat 21
Tabel 3. 5 Perancangan Tabel *user_table* 22
Tabel 4. 1 Hasil Pendeteksian Snort dan Suricata 35
Tabel 4. 2 Hasil Pengujian Secara Keseluruhan 44

DAFTAR LAMPIRAN

L-1 Lampiran Pengujian 1

L-2 Lampiran Pengujian 2

BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada situs beritasatu.com yang dipublikasikan oleh Whisnu Bagus Prasetyo pada tanggal 17 Maret 2021 pukul 22:06 WIB, Kepala Badan Siber dan Sandi Negara (BSSN), Letjen TNI (Purn) Hinsa Siburian mengatakan bahwa “Ancaman dan risiko serangan siber naik seiring banyaknya pengguna internet dan aktivitas digital masyarakat". Hal ini terbukti dengan banyaknya kasus serangan siber seperti kebocoran data yang terjadi selama pandemi *covid-19* yang pada saat itu diterapkan sistem *lockdown* di beberapa kota, sehingga masyarakat lebih banyak beraktivitas secara daring.

Salah satu upaya dalam mengatasi serangan siber adalah melakukan perlindungan terhadap jaringan internal. Dalam melindungi sebuah jaringan, biasanya dapat digunakan *firewall* yang memiliki fungsi mengatur lalu lintas jaringan dengan cara melakukan autentikasi terhadap akses.(Ramadhani & Muzzakir, 2017) Namun, kekurangannya adalah *firewall* hanya dapat bekerja berdasarkan aturan yang telah dibuat oleh administrator. Dengan demikian, jika terdapat serangan terbaru yang tidak diketahui oleh administrator maka serangan tersebut akan tetap diteruskan oleh *firewall*.

Adanya teknologi *IPS* (*Intrusion Prevention System*), yaitu penggabungan fungsi *IDS* (*Intrusion Detection System*) dengan fungsi *firewall*, dapat membantu kinerja *firewall* menjadi dinamis.(Waltermire & Scarfone, 2011) Sehingga *firewall* dapat memberikan akses pada trafik berdasarkan hasil pendeteksian isi dari paket data. Snort dan Suricata adalah *tools IDS/IPS* yang akan diujicoba dalam penelitian ini. Pada masing-masing situs resmi dari kedua *tools* tersebut, yaitu snort.org dan suricata.io, menyatakan bahwa Snort maupun Suricata adalah *IDS/IPS* yang bersifat *open source* dan memiliki kemampuan *multithread*. Sehingga *tools* dapat mendeteksi maupun memblokir paket data yang bersifat berbahaya secara *parallel*, akibatnya kerja *tools* dapat bekerja dengan efisien. Hal inilah yang menjadi latar belakang dari topik yang diangkat untuk menganalisa kinerja *tools IPS* dalam menangani kerentanan sistem keamanan jaringan.

1.2 Perumusan Masalah

Perumusan masalah yang disusun untuk melakukan pengujian kinerja *tools IPS* dalam menangani kerentanan sistem keamanan jaringan, adalah:

1) Bagaimana membangun sistem *IDS/IPS* menggunakan Snort dan Suricata?
2) Bagaimana pengujian dan analisa antara Snort dan Suricata?
3) Bagaimana perbandingan performansi kinerja antara Snort dan Suricata?

Berdasarkan perumusan masalah yang dibuat, terdapat batasan masalah untuk membatasi ruang lingkup pengujian kinerja *tools IPS* dalam menangani kerentanan sistem keamanan jaringan, adalah:

1) *Tools IPS* yang diuji adalah Snort 3.1.49 dan Suricata 6.0.9 dengan menggunakan aturan (*rule*) yang sudah tersedia dari masing – masing *tools IPS*.
2) Metode *IDS* yang digunakan adalah *Knowledge-based*.
3) Menggunakan *IPTables* sebagai *firewall* untuk menahan serangan.
4) Objek yang dilindungi adalah web server yang menggunakan *OS* linux Ubuntu desktop 20.04 dan halaman web berupa *login* dan *signup*.
5) Pengujian terfokus pada penyerangan terhadap jaringan berupa serangan *DDoS*.

1.3 Tujuan

Adapun tujuan yang ingin dicapai dalam penyusunan skripsi ini adalah:

1) Mengetahui cara membangun sistem *IDS/IPS* menggunakan Snort dan Suricata.
2) Mengetahui hasil pengujian dan analisa antara Snort dan Suricata.
3) Mengetahui hasil perbandingan performansi kinerja antara Snort dan Suricata.

1.4 Luaran

Luaran yang didapatkan dari pembuatan skripsi ini adalah publikasi dalam bentuk artikel ilmiah mengenai analisis kinerja *tools IPS* yaitu Snort dengan Suricata.

BAB V
SIMPULAN

Berdasarkan analisis data hasil pengujian dalam menguji performa kinerja Snort dan Suricata dalam mengatasi kerentanan sistem keamanan jaringan. Dapat disimpulkan sebagai berikut:

1. Dalam melakukan pengujian akurasi sistem deteksi yang diuji menggunakan *framework Pytbull*, snort lebih unggul dibanding suricata dalam mendeteksi serangan-serangan yang dilancarkan oleh *Pytbull*.
2. Lalu pada pengujian berikutnya, yaitu menguji sistem pencegahan dalam menangani serangan *DDoS*. Snort memiliki jumlah paket data yang lolos lebih sedikt dibanding suricata.
3. Dari hasil kedua pengujian tersebut, dapat disimpulkan bahwa Snort memiliki performa yang lebih unggul dibandingkan Suricata.

DAFTAR PUSTAKA

Agustini, S., & Mudzakir, A. (2019). Rancang Bangun Jaringan Komputer Dengan Bandwidth Management Menggunakan Teknik Brust Limit Dan Firewall Sebagai Pengaman Jaringan. *Network Engineering Research Operation*, *4*(3), 189–195. https://nero.trunojoyo.ac.id/index.php/nero/article/view/138

Alrajeh, N. A., Khan, S., & Shams, B. (2013). Intrusion detection systems in wireless sensor networks: A review. *International Journal of Distributed Sensor Networks*, *2013*. https://doi.org/10.1155/2013/167575

Aminanto, M. E & Gian, N. L. (2013). Menangani Serangan Intrusi Menggunakan IDS dan IPS. Diakses pada 18 Februari 2022, dari https://keamanan-informasi.stei.itb.ac.id/2013/10/30/menangani-serangan-intrusi-menggunakan-ids-dan-ips/

Anggraeni, E. Y. & Irviani, R. (2017). Pengantar Sistem Informasi. 1 penyunt. Yogyakarta: Andi.https://books.google.co.id/books/about/Pengantar_Sistem_Informasi.html?hl=id&id=8VNLDwAAQBAJ&redir_esc=y

International Standard Organization. (2011). *INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Application security — . 2011*. https://www.iso.org/obp/ui/#!iso:std:44378:en

International Standard Organization. (2018). INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Information security management systems — Overview and. *ACM Workshop on Formal Methods in Security Engineering.Washington, DC, USA*, *34*(19), 45–55. https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip

KBBI. (2016). Kamus Besar Bahasa Indonesia (KBBI). https://kbbi.kemdikbud.go.id/entri/keamanan.

Khamphakdee, N., Benjamas, N., & Saiyod, S. (2015). Improving intrusion detection system based on snort rules for network probe attacks detection with association rules technique of data mining. *Journal of ICT Research and Applications*, *8*(3), 234–250. https://doi.org/10.5614/itbj.ict.res.appl.2015.8.3.4

Purba, W. W., & Efendi, R. (2021). Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT. *Aiti*, *17*(2), 143–158. https://doi.org/10.24246/aiti.v17i2.143-158

Salamadian. (2020). Pengertian LAN, MAN, WAN Serta Fungsi & Kelebihan Kekurangan. https://www.dataglobal.co.id/pengertian-lan-man-wan-beserta-fungsi-kelebihan-kekurangannya/

Sutarti, Pancaro, A. P., & Saputra, F. I. (2018). Implementasi IDS (Intrusion

Detection System) Pada Sistem Keamanan Jaringan SMAN 1 Cikeusal. *Jurnal PROSISKO*, *5*(1), 1–8.

Vasconcelos, G., Miani, R. S., Guizilini, V. C., & Souza, J. R. (2019). Evaluation of DoS attacks on commercial Wi-Fi-based UAVs. *International Journal of Communication Networks and Information Security*, *11*(1), 212–223.

Wagito. (2005). Jaringan Komputer: Teori dan Implentasi Berbasis Linux. Yogyakarta: Gava Media. https://openlibrary.telkomuniversity.ac.id/pustaka/21479/jaringan-komputer-teori-dan-implementasi-berbasis-linux.html

DAFTAR RIWAYAT HIDUP PENULIS

Devita Ariandi lahir di Jakarta tanggal 6 Desember 2000, anak ke-4 dari empat bersaudara. Lulus dari SDN 05 Paseban pada tahun 2012, SMPN 2 Jakarta pada tahun 2015, SMAN 20 Jakarta pada tahun 2018, dan saat ini menempuh Pendidikan Diploma IV di Politeknik Negeri Jakarta, Jurusan Teknik Elektro, Program Studi Broadband Multimedia.

1. Serangan yang dapat dideteksi oleh Snort

#	Description	Module	Port	Payload fmt	Result
1	001e2710555613a82e94156d3ed9c289	clientSideAttacks		wget	no
2	004e74d54dcf79c641d5cf8a615488a0	clientSideAttacks		wget	no
3	0106fb569e87e02fc88d496064abdf19	clientSideAttacks		wget	partial
4	Simple LFI	testRules	80/tcp	socket	partial
5	LFI using NULL byte	testRules	80/tcp	socket	partial
6	Full SYN Scan	testRules		command	partial
7	Full Connect() Scan	testRules		command	full
8	SQL Injection	testRules	80/tcp	socket	no
9	Netcat Reverse Shell	testRules	22/tcp	socket	partial
10	Nikto Scan	testRules		command	partial
11	Ping of death	fragmentedPackets		scapy	partial
12	Nestea Attack 1/3	fragmentedPackets		scapy	partial
13	Nestea Attack 2/3	fragmentedPackets		scapy	no
14	Nestea Attack 3/3	fragmentedPackets		scapy	partial
15	Bruteforce against FTP with ncrack	bruteForce		command	partial
16	Nmap decoy test (6th position)	evasionTechniques		command	full
17	Nmap decoy test (7th position)	evasionTechniques		command	full
18	Hex encoding	evasionTechniques	80/tcp	socket	partial
19	Nmap scan with fragmentation	evasionTechniques		command	partial
20	Javascript Obfuscation	evasionTechniques	80/tcp	socket	partial
21	SHELLCODE ** sparc setuid 0	shellCodes	21/tcp	socket	partial
22	SHELLCODE x86 setgid	shellCodes	21/tcp	socket	partial
23	SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0	shellCodes	21/tcp	socket	partial
24	OVERFLOW attempt	shellCodes	21/tcp	socket	no
25	SHELLCODE x86 setuid 0	shellCodes	21/tcp	socket	partial
26	win32_bind_dllinject - EXITFUNC=seh DLL=c:\ LPORT=4444 Size=312 Encoder=PexFnstenvSub	shellCodes	21/tcp	socket	partial
27	win32_bind_dllinject - EXITFUNC=seh DLL=c:\ LPORT=4444 Size=312 Encoder=Pex	shellCodes	21/tcp	socket	partial
28	win32_bind - EXITFUNC=seh LPORT=4444 Size=709 Encoder=PexAlphaNum	shellCodes	21/tcp	socket	no
29	Rothenburg Shellcode	shellCodes	21/tcp	socket	partial

2. Serangan yang dapat dideteksi oleh Suricata

#	Description	Module	Port	Payload fmt	Result
1	001e2710555613a82e94156d3ed9c289	clientSideAttacks		wget	Partial
2	004e74d54dcf79c641d5cf8a615488a0	clientSideAttacks		wget	no
3	0106fb569e87e02fc88d496064abdf19	clientSideAttacks		wget	no
4	Simple LFI	testRules	80/tcp	socket	no
5	LFI using NULL byte	testRules	80/tcp	socket	no
6	Full SYN Scan	testRules		command	Partial
7	Full Connect() Scan	testRules		command	Partial
8	SQL Injection	testRules	80/tcp	socket	full
9	Netcat Reverse Shell	testRules	22/tcp	socket	no
10	Nikto Scan	testRules		command	full
11	Ping of death	fragmentedPackets		scapy	no
12	Nestea Attack 1/3	fragmentedPackets		scapy	partial
13	Nestea Attack 2/3	fragmentedPackets		scapy	no
14	Nestea Attack 3/3	fragmentedPackets		scapy	no
15	Bruteforce against FTP with ncrack	bruteForce		command	full
16	Nmap decoy test (6th position)	evasionTechniques		command	full
17	Nmap decoy test (7th position)	evasionTechniques		command	full
18	Hex encoding	evasionTechniques	80/tcp	socket	no
19	Nmap scan with fragmentation	evasionTechniques		command	Partial
20	Javascript Obfuscation	evasionTechniques	80/tcp	socket	Partial
21	SHELLCODE ** sparc setuid 0	shellCodes	21/tcp	socket	Partial
22	SHELLCODE x86 setgid	shellCodes	21/tcp	socket	no
23	SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0	shellCodes	21/tcp	socket	no
24	OVERFLOW attempt	shellCodes	21/tcp	socket	no
25	SHELLCODE x86 setuid 0	shellCodes	21/tcp	socket	Partial
26	win32_bind_dllinject - EXITFUNC=seh DLL=c:\ LPORT=4444 Size=312 Encoder=PexFnstenvSub	shellCodes	21/tcp	socket	Partial
27	win32_bind_dllinject - EXITFUNC=seh DLL=c:\ LPORT=4444 Size=312 Encoder=Pex	shellCodes	21/tcp	socket	no
28	win32_bind - EXITFUNC=seh LPORT=4444 Size=709 Encoder=PexAlphaNum	shellCodes	21/tcp	socket	no
29	Rothenburg Shellcode	shellCodes	21/tcp	socket	Partial

Dokumentasi pengujian
Snort

5	0106fb569e87e02fc88d496064abdf19	clientSideAttacks		wget	

- **Start:** 2023-01-12 06:56:56.306774
- **End:** 2023-01-12 06:57:00.507456
- **Sig match:** 1:17668:1

Alerts:

```
01/12-06:56:58.010527 [**] [112:1:1] "(arp_spoof) unicast ARP request" [**] [Priority: 3] {ARP}  ->
```

51	Simple LFI	testRules	80/tcp	socket	

- **Start:** 2023-01-12 06:59:54.964124
- **End:** 2023-01-12 06:59:54.966366
- **Sig match:** 1:1122:8

Payload:

```
GET /index.php?page=../../../etc/passwd HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.7.5) Gecko/20041202 Firefox/1.0
```

Alerts:

```
01/12-06:59:55.007721 [**] [1:1122:16] "SERVER-WEBAPP /etc/passwd file access attempt" [**]
[Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.0.123:47236 -> 172.20.0.2:80
```

52	LFI using NULL byte	testRules	80/tcp	socket	

- **Start:** 2023-01-12 06:59:59.365360
- **End:** 2023-01-12 06:59:59.375113
- **Sig match:** 1:1122:8

Payload:

```
GET /index.php?page=../../../etc/passwd%00 HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.7.5) Gecko/20041202 Firefox/1.0
```

Alerts:

```
01/12-06:59:59.415964 [**] [1:1122:16] "SERVER-WEBAPP /etc/passwd file access attempt" [**]
[Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.0.123:32908 -> 172.20.0.2:80
```

	53	Full SYN Scan	testRules		command

- **Start:** 2023-01-12 07:00:03.793797
- **End:** 2023-01-12 07:00:30.697111
- **Sig match:** 122:1:1

Payload:

```
/usr/bin/sudo /usr/bin/nmap -sS -p- 172.20.0.2
```

Alerts:

```
01/12-07:00:03.941866 [**] [116:434:1] "(icmp4) ICMP ping Nmap" [**] [Priority: 3] {ICMP} 192.168.0.123
-> 172.20.0.2
01/12-07:00:03.941866 [**] [1:384:8] "PROTOCOL-ICMP PING" [**] [Classification: Misc activity]
[Priority: 3] {ICMP} 192.168.0.123 -> 172.20.0.2
01/12-07:00:03.942112 [**] [1:453:8] "PROTOCOL-ICMP Timestamp Request" [**] [Classification: Misc
activity] [Priority: 3] {ICMP} 192.168.0.123 -> 172.20.0.2
01/12-07:00:04.063663 [**] [122:1:1] "(port_scan) TCP portscan" [**] [Priority: 3] {TCP}
172.20.0.2:3306 -> 192.168.0.123:64695
01/12-07:00:07.706561 [**] [112:1:1] "(arp_spoof) unicast ARP request" [**] [Priority: 3] {ARP}  ->
01/12-07:00:07.707984 [**] [112:1:1] "(arp_spoof) unicast ARP request" [**] [Priority: 3] {ARP}  ->
01/12-07:00:18.394356 [**] [1:1420:19] "PROTOCOL-SNMP trap tcp" [**] [Classification: Attempted
Information Leak] [Priority: 2] {TCP} 192.168.0.123:64695 -> 172.20.0.2:162
01/12-07:00:20.296291 [**] [1:1420:19] "PROTOCOL-SNMP trap tcp" [**] [Classification: Attempted
Information Leak] [Priority: 2] {TCP} 192.168.0.123:64697 -> 172.20.0.2:162
```

	54	Full Connect() Scan	testRules		command

- **Start:** 2023-01-12 07:00:35.293927
- **End:** 2023-01-12 07:05:51.092113
- **Sig match:** 122:1:1

Payload:

```
/usr/bin/nmap -sT -p- 172.20.0.2
```

Alerts:

```
01/12-07:00:35.421938 [**] [116:434:1] "(icmp4) ICMP ping Nmap" [**] [Priority: 3] {ICMP} 192.168.0.123
-> 172.20.0.2
01/12-07:00:35.421938 [**] [1:384:8] "PROTOCOL-ICMP PING" [**] [Classification: Misc activity]
[Priority: 3] {ICMP} 192.168.0.123 -> 172.20.0.2
01/12-07:00:35.422459 [**] [1:453:8] "PROTOCOL-ICMP Timestamp Request" [**] [Classification: Misc
activity] [Priority: 3] {ICMP} 192.168.0.123 -> 172.20.0.2
01/12-07:00:45.332704 [**] [1:1420:19] "PROTOCOL-SNMP trap tcp" [**] [Classification: Attempted
Information Leak] [Priority: 2] {TCP} 192.168.0.123:45698 -> 172.20.0.2:162
01/12-07:00:50.203665 [**] [112:1:1] "(arp_spoof) unicast ARP request" [**] [Priority: 3] {ARP}  ->
01/12-07:00:54.554574 [**] [112:1:1] "(arp_spoof) unicast ARP request" [**] [Priority: 3] {ARP}  ->
01/12-07:00:58.902554 [**] [112:1:1] "(arp_spoof) unicast ARP request" [**] [Priority: 3] {ARP}  ->
01/12-07:01:08.592725 [**] [1:1418:19] "PROTOCOL-SNMP request tcp" [**] [Classification: Attempted
Information Leak] [Priority: 2] {TCP} 192.168.0.123:41582 -> 172.20.0.2:161
01/12-07:01:14.075891 [**] [122:1:1] "(port_scan) TCP portscan" [**] [Priority: 3] {TCP}
```

56	Netcat Reverse Shell	testRules	22/tcp	socket	

- **Start:** 2023-01-12 07:05:59.950975
- **End:** 2023-01-12 07:05:59.961117
- **Sig match:** 1:1324:10

Payload:

```
/bin/sh
```

Alerts:

```
01/12-07:06:00.002657 [**] [1:1324:12] "INDICATOR-SHELLCODE ssh CRC32 overflow /bin/sh" [**]
[Classification: Executable code was detected] [Priority: 1] {TCP} 192.168.0.123:53266 -> 172.20.0.2:22
```

57	Nikto Scan	testRules		command	

- **Start:** 2023-01-12 07:06:04.410263
- **End:** 2023-01-12 07:06:06.712020
- **Sig match:** (?i)nikto

Payload:

```
/usr/bin/sudo /usr/bin/nikto -config /etc/nikto.conf -h 172.20.0.2 -Plugins cgi
```

Alerts:

```
01/12-07:06:04.784422 [**] [1:1242:24] "SERVER-IIS ISAPI .ida access" [**] [Classification: Access to a
potentially vulnerable web application] [Priority: 2] {TCP} 192.168.0.123:50594 -> 172.20.0.2:80
01/12-07:06:04.840914 [**] [1:987:32] "FILE-IDENTIFY .htr access file download request" [**]
[Classification: Misc activity] [Priority: 3] {TCP} 192.168.0.123:50594 -> 172.20.0.2:80
01/12-07:06:04.849010 [**] [1:1071:15] "SERVER-WEBAPP .htpasswd access attempt" [**] [Classification:
Web Application Attack] [Priority: 1] {TCP} 192.168.0.123:50594 -> 172.20.0.2:80
01/12-07:06:05.017675 [**] [1:1245:24] "SERVER-IIS ISAPI .idq access" [**] [Classification: Access to a
potentially vulnerable web application] [Priority: 2] {TCP} 192.168.0.123:50594 -> 172.20.0.2:80
01/12-07:06:05.143522 [**] [1:1129:16] "SERVER-WEBAPP .htaccess access" [**] [Classification: Attempted
Information Leak] [Priority: 2] {TCP} 192.168.0.123:50594 -> 172.20.0.2:80
01/12-07:06:05.232264 [**] [1:1131:14] "SERVER-WEBAPP .wwwacl access" [**] [Classification: Attempted
Information Leak] [Priority: 2] {TCP} 192.168.0.123:50594 -> 172.20.0.2:80
01/12-07:06:05.480762 [**] [1:1129:16] "SERVER-WEBAPP .htaccess access" [**] [Classification: Attempted
Information Leak] [Priority: 2] {TCP} 192.168.0.123:37258 -> 172.20.0.2:80
```

61	Ping of death	fragmentedPackets		scapy	

- **Start:** 2023-01-12 07:06:24.809582
- **End:** 2023-01-12 07:06:24.883906
- **Sig match:** 123:

Payload:

```
send(fragment(IP(dst="172.20.0.2")/ICMP()/("X"*60000)), verbose=0)
```

Alerts:

```
01/12-07:06:24.923935 [**] [1:384:8] "PROTOCOL-ICMP PING" [**] [Classification: Misc activity]
[Priority: 3] {ICMP} 192.168.0.123 -> 172.20.0.2
```

62	Nestea Attack 1/3	fragmentedPackets		scapy	

- **Start:** 2023-01-12 07:06:29.239384
- **End:** 2023-01-12 07:06:29.288049
- **Sig match:** 123:

Payload:

```
send(IP(dst="172.20.0.2", id=42, flags="MF")/UDP()/("X"*10), verbose=0)
```

Alerts:

```
01/12-07:06:27.609385 [**] [112:1:1] "(arp_spoof) unicast ARP request" [**] [Priority: 3] {ARP}  ->
```

64	Nestea Attack 3/3	fragmentedPackets		scapy	

- **Start:** 2023-01-12 07:06:39.154331
- **End:** 2023-01-12 07:06:39.192189
- **Sig match:** 123:

Payload:

```
send(IP(dst="172.20.0.2", id=42, flags="MF")/UDP()/("X"*224), verbose=0)
```

Alerts:

```
01/12-07:06:39.869254 [**] [116:444:1] "(ipv4) IPv4 option set" [**] [Priority: 3] {IP} 172.20.0.1 ->
224.0.0.251
01/12-07:06:40.246561 [**] [116:444:1] "(ipv4) IPv4 option set" [**] [Priority: 3] {IP} 172.20.0.2 ->
224.0.0.22
```

65	Bruteforce against FTP with ncrack	bruteForce		command	

- **Start:** 2023-01-12 07:06:43.570859
- **End:** 2023-01-12 07:07:04.587460
- **Sig match:** (?i)brute

Payload:

```
/usr/bin/ncrack -f -U data/ncrack-users.txt -P data/ncrack-passwords.txt 172.20.0.2:21
```

Alerts:

```
01/12-07:06:46.516980 [**] [1:491:15] "PROTOCOL-FTP Bad login" [**] [Classification: Potentially Bad
Traffic] [Priority: 2] {TCP} 172.20.0.2:21 -> 192.168.0.123:48032
01/12-07:06:49.494168 [**] [1:491:15] "PROTOCOL-FTP Bad login" [**] [Classification: Potentially Bad
Traffic] [Priority: 2] {TCP} 172.20.0.2:21 -> 192.168.0.123:48032
01/12-07:06:52.867877 [**] [1:491:15] "PROTOCOL-FTP Bad login" [**] [Classification: Potentially Bad
Traffic] [Priority: 2] {TCP} 172.20.0.2:21 -> 192.168.0.123:48032
01/12-07:06:55.667018 [**] [1:491:15] "PROTOCOL-FTP Bad login" [**] [Classification: Potentially Bad
Traffic] [Priority: 2] {TCP} 172.20.0.2:21 -> 192.168.0.123:51390
01/12-07:06:55.671749 [**] [1:491:15] "PROTOCOL-FTP Bad login" [**] [Classification: Potentially Bad
Traffic] [Priority: 2] {TCP} 172.20.0.2:21 -> 192.168.0.123:51418
01/12-07:06:55.673683 [**] [1:491:15] "PROTOCOL-FTP Bad login" [**] [Classification: Potentially Bad
Traffic] [Priority: 2] {TCP} 172.20.0.2:21 -> 192.168.0.123:51440
01/12-07:06:55.675540 [**] [1:491:15] "PROTOCOL-FTP Bad login" [**] [Classification: Potentially Bad
Traffic] [Priority: 2] {TCP} 172.20.0.2:21 -> 192.168.0.123:51336
```

66	Nmap decoy test (6th position)	evasionTechniques		command	

- **Start:** 2023-01-12 07:07:08.988631
- **End:** 2023-01-12 07:07:35.380312
- **Sig match:** 192.168.0.123

Payload:

```
/usr/bin/sudo /usr/bin/nmap -sS -A -D
192.168.100.1,192.168.100.2,192.168.100.3,192.168.100.4,192.168.100.5,ME 172.20.0.2
```

Alerts:

```
01/12-07:07:09.552725 [**] [116:434:1] "(icmp4) ICMP ping Nmap" [**] [Priority: 3] {ICMP} 192.168.100.2
-> 172.20.0.2
01/12-07:07:09.552725 [**] [1:384:8] "PROTOCOL-ICMP PING" [**] [Classification: Misc activity]
[Priority: 3] {ICMP} 192.168.100.2 -> 172.20.0.2
01/12-07:07:09.552899 [**] [116:434:1] "(icmp4) ICMP ping Nmap" [**] [Priority: 3] {ICMP} 192.168.100.3
-> 172.20.0.2
01/12-07:07:09.552899 [**] [1:384:8] "PROTOCOL-ICMP PING" [**] [Classification: Misc activity]
[Priority: 3] {ICMP} 192.168.100.3 -> 172.20.0.2
01/12-07:07:09.553018 [**] [116:434:1] "(icmp4) ICMP ping Nmap" [**] [Priority: 3] {ICMP} 192.168.100.4
-> 172.20.0.2
01/12-07:07:09.553018 [**] [1:384:8] "PROTOCOL-ICMP PING" [**] [Classification: Misc activity]
[Priority: 3] {ICMP} 192.168.100.4 -> 172.20.0.2
01/12-07:07:09.553409 [**] [116:434:1] "(icmp4) ICMP ping Nmap" [**] [Priority: 3] {ICMP} 192.168.100.5
-> 172.20.0.2
```

69	Nmap scan with fragmentation	evasionTechniques		command	

- **Start:** 2023-01-12 07:15:17.452030
- **End:** 2023-01-12 07:15:41.196434
- **Sig match:** 122:2:1

Payload:

```
/usr/bin/sudo /usr/bin/nmap -PN -sS -A -f 172.20.0.2
```

Alerts:

```
01/12-07:15:19.305735 [**] [1:1421:19] "PROTOCOL-SNMP AgentX/tcp request" [**] [Classification:
Attempted Information Leak] [Priority: 2] {TCP} 192.168.0.123:46983 -> 172.20.0.2:705
01/12-07:15:19.306403 [**] [1:1418:19] "PROTOCOL-SNMP request tcp" [**] [Classification: Attempted
Information Leak] [Priority: 2] {TCP} 192.168.0.123:46983 -> 172.20.0.2:161
01/12-07:15:29.304167 [**] [112:1:1] "(arp_spoof) unicast ARP request" [**] [Priority: 3] {ARP}  ->
01/12-07:15:31.702501 [**] [1:365:11] "PROTOCOL-ICMP PING undefined code" [**] [Classification: Misc
activity] [Priority: 3] {ICMP} 192.168.0.123 -> 172.20.0.2
01/12-07:15:31.726909 [**] [1:384:8] "PROTOCOL-ICMP PING" [**] [Classification: Misc activity]
[Priority: 3] {ICMP} 192.168.0.123 -> 172.20.0.2
01/12-07:15:31.753264 [**] [1:1390:17] "INDICATOR-SHELLCODE x86 inc ebx NOOP" [**] [Classification:
Executable code was detected] [Priority: 1] {UDP} 192.168.0.123:59581 -> 172.20.0.2:31959
01/12-07:15:31.753264 [**] [122:19:1] "(port_scan) UDP portsweep" [**] [Priority: 3] {UDP}
192.168.0.123:59581 -> 172.20.0.2:31959
01/12-07:15:31.827019 [**] [116:401:1] "(tcp) Nmap XMAS attack detected" [**] [Priority: 3] {TCP}
```

80	Javascript Obfuscation	evasionTechniques	80/tcp	socket	

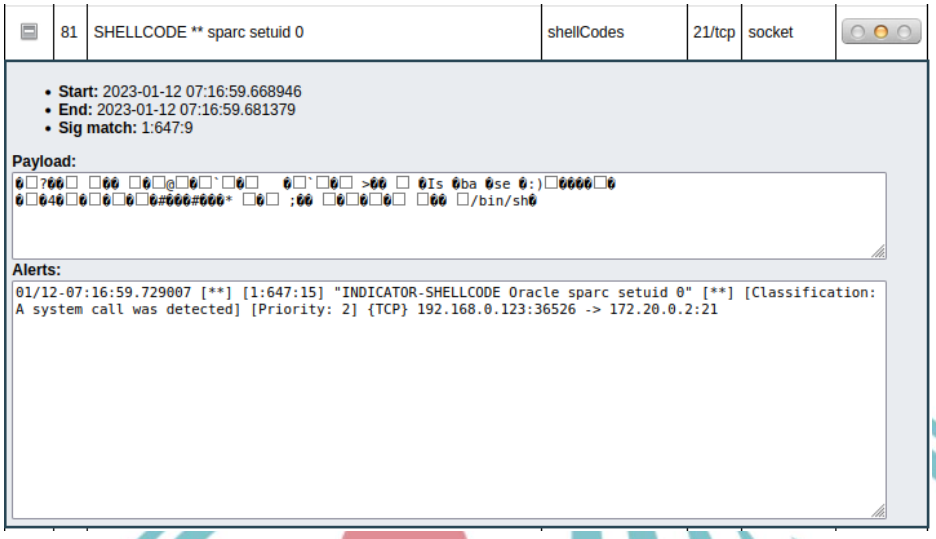
- **Start:** 2023-01-12 07:16:55.124702
- **End:** 2023-01-12 07:16:55.133547
- **Sig match:** 1:2009714:6

Payload:

```
GET /index.php?page=%sCscript%3Ealert%28%29%3C%2Fscript%3E HTTP/1.1
Host: 127.0.0.1
```

Alerts:

```
01/12-07:16:55.181559 [**] [119:212:1] "(http_inspect) unrecognized type of percent encoding in URI"
[**] [Priority: 3] {TCP} 192.168.0.123:50342 -> 172.20.0.2:80
```



81	SHELLCODE ** sparc setuid 0	shellCodes	21/tcp	socket

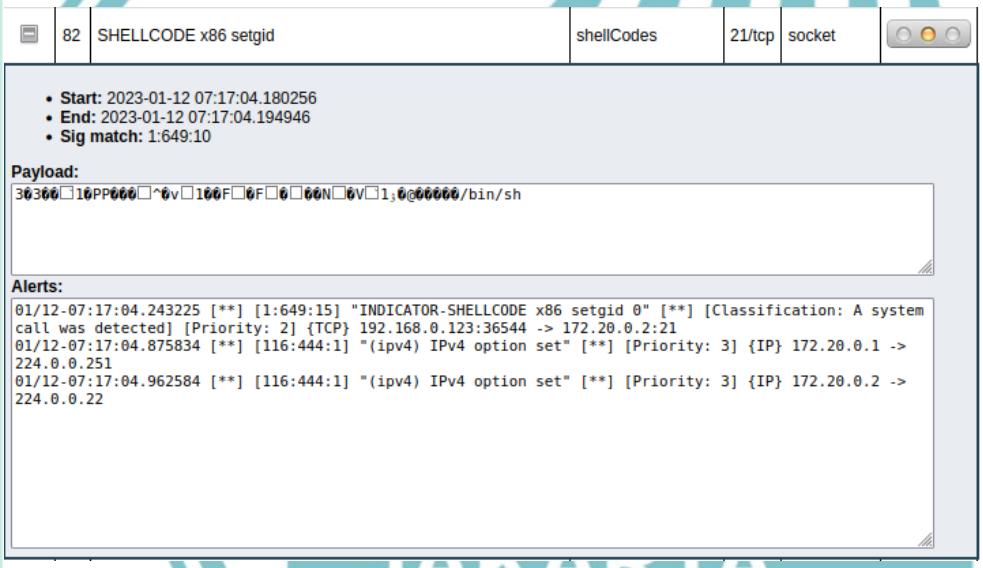
- **Start:** 2023-01-12 07:16:59.668946
- **End:** 2023-01-12 07:16:59.681379
- **Sig match:** 1:647:9

Payload:

```
[illegible] >[illegible] [illegible]Is [illegible]ba [illegible]se [illegible]:)[illegible]
[illegible]#[illegible]* [illegible] ;[illegible] [illegible] [illegible]/bin/sh[illegible]
```

Alerts:

```
01/12-07:16:59.729007 [**] [1:647:15] "INDICATOR-SHELLCODE Oracle sparc setuid 0" [**] [Classification:
A system call was detected] [Priority: 2] {TCP} 192.168.0.123:36526 -> 172.20.0.2:21
```



82	SHELLCODE x86 setgid	shellCodes	21/tcp	socket

- **Start:** 2023-01-12 07:17:04.180256
- **End:** 2023-01-12 07:17:04.194946
- **Sig match:** 1:649:10

Payload:

```
3[illegible]3[illegible]1[illegible]PP[illegible]^[illegible]v[illegible]1[illegible]F[illegible]F[illegible][illegible]N[illegible]V[illegible]1;[illegible]@[illegible]/bin/sh
```

Alerts:

```
01/12-07:17:04.243225 [**] [1:649:15] "INDICATOR-SHELLCODE x86 setgid 0" [**] [Classification: A system
call was detected] [Priority: 2] {TCP} 192.168.0.123:36544 -> 172.20.0.2:21
01/12-07:17:04.875834 [**] [116:444:1] "(ipv4) IPv4 option set" [**] [Priority: 3] {IP} 172.20.0.1 ->
224.0.0.251
01/12-07:17:04.962584 [**] [116:444:1] "(ipv4) IPv4 option set" [**] [Priority: 3] {IP} 172.20.0.2 ->
224.0.0.22
```

84	SHELLCODE x86 setgid 0 && SHELLCODE x86 setuid 0	shellCodes	21/tcp	socket	

- **Start:** 2023-01-12 07:17:13.166400
- **End:** 2023-01-12 07:17:13.172283
- **Sig match:** 1:650:10

Payload:

```
3@3@@□11□ɔ¡@PP@@@□^@v□1@@F□@F□@□@@N□@V□1¡@@@@@@/bin/sh
```

Alerts:

```
01/12-07:17:13.222247 [**] [1:650:15] "INDICATOR-SHELLCODE x86 setuid 0" [**] [Classification: A system
call was detected] [Priority: 2] {TCP} 192.168.0.123:46992 -> 172.20.0.2:21
01/12-07:17:13.222247 [**] [1:649:15] "INDICATOR-SHELLCODE x86 setgid 0" [**] [Classification: A system
call was detected] [Priority: 2] {TCP} 192.168.0.123:46992 -> 172.20.0.2:21
```

86	SHELLCODE x86 setuid 0	shellCodes	21/tcp	socket	

- **Start:** 2023-01-12 07:17:22.193611
- **End:** 2023-01-12 07:17:22.202266
- **Sig match:** 1:650:10

Payload:

```
3@3@@□1□ɔ¡@□^@v□1@@F□@F□@□@@N□@V□1¡@@@@@/bin/sh
```

Alerts:

```
01/12-07:17:22.250475 [**] [1:650:15] "INDICATOR-SHELLCODE x86 setuid 0" [**] [Classification: A system
call was detected] [Priority: 2] {TCP} 192.168.0.123:40750 -> 172.20.0.2:21
```

87	win32_bind_dllinject - EXITFUNC=seh DLL=c:\ LPORT=4444 Size=312 Encoder=PexFnstenvSub	shellCodes	21/tcp	socket	

- **Start:** 2023-01-12 07:17:26.678234
- **End:** 2023-01-12 07:17:26.684016
- **Sig match:** 1:17322:1

Payload:

```
)B@@@@t$@[@s□@@&□@@@@@j@&□@@s@@?J2@?c*        @#n@^@\@?|6@_@$@?□@@Z□@~@溺TR□C{+□E_@-
@@2cc?|2@_@@@@L@@@?'@i@□@@@{M@@&H@□r  @@M@?}
        @@M@@N@@@T=@n@'□@@pE□Q@1@@&@@@&@@@@@@@@@2o@@@@/@@üA@@oH□Aцy%@@}@ɔw@U=@@A9S□@□G@K□@}@"0□
@@@p@□B}@@C@@@F@@vV@@v@ɐ@ɐouE@&□@=@|@@q@ₓuA}@□E@@@C@=@n@6□@=@|@@&□@@uA}@>@n@"□@K@□
```

Alerts:

```
01/12-07:17:26.731490 [**] [1:1378:24] "PROTOCOL-FTP wu-ftp bad file completion attempt" [**]
[Classification: Misc Attack] [Priority: 2] {TCP} 192.168.0.123:53850 -> 172.20.0.2:21
```

88	win32_bind_dllinject - EXITFUNC=seh DLL=c:\ LPORT=4444 Size=312 Encoder=Pex	shellCodes		21/tcp	socket

- **Start:** 2023-01-12 07:17:31.137178
- **End:** 2023-01-12 07:17:31.143445
- **Sig match:** 1:17344:1

Payload:

```
+B[illegible]^0v□[illegible]□!5[illegible]S`[illegible]Y[illegible]p0p#0[illegible]o[illegible]0□h[illegible]□□□F[illegible]O×A[illegible]:[illegible]8[illegible]<[illegible]¥S![illegible]□[illegible]o[illegible]Sh[illegible]<[illegible]v[illegible]h[illegible]4
□□u□#[illegible])h[illegible]9□5[illegible]Gl[illegible]pn[illegible]n[illegible]pl[illegible]$]m[illegible]y[illegible]□-[illegible]b□w4[illegible] c[illegible]r[illegible]w5s[illegible]w5U[illegible]o[illegible]G[illegible]□[illegible]□[illegible]|G[illegible]□[illegible]GVY[illegible]:[illegible](□[illegible]□
[illegible]Ej[illegible]wnn[illegible]Wd□,[illegible]j8[illegible]@[illegible]pl[illegible]□l□"1[illegible]rs[illegible]□ \□[illegible]□[illegible]@"[illegible]F[illegible]'e[illegible]7e□[illegible][[illegible]$¥f[illegible]u5[illegible]Q[illegible]'b□[illegible]Sf[illegible]□"□[illegible] "[illegible]b
□w%[illegible]:[illegible]□5[illegible]wf[illegible]□"-b□w1[illegible]
```

Alerts:

```
01/12-07:17:32.182498 [**] [112:1:1] "(arp_spoof) unicast ARP request" [**] [Priority: 3] {ARP}  ->
01/12-07:17:32.184115 [**] [112:1:1] "(arp_spoof) unicast ARP request" [**] [Priority: 3] {ARP}  ->
```

92	Rothenburg Shellcode	shellCodes		21/tcp	socket

- **Start:** 2023-01-12 07:17:49.393545
- **End:** 2023-01-12 07:17:49.401771
- **Sig match:** 1:17322:1

Payload:

```
)B[illegible]t$[illegible][illegible]s□[illegible]&□[illegible]j[illegible]&□[illegible]s[illegible]@?J2[illegible]?c*  [illegible]#n[illegible]^[illegible]\[illegible]?|6[illegible]_[illegible]$[illegible]?□[illegible]Z□[illegible]~[illegible]溺TR□C{+□E_[illegible]-
[illegible]2cc?|2[illegible] @[illegible]L[illegible]?'[illegible]i[illegible]□[illegible]{M@[illegible]&H[illegible]□r [illegible]M[illegible]?}
[illegible]M[illegible]N[illegible]T=[illegible]n[illegible]'□[illegible]pE□Q[illegible]1[illegible]&[illegible]&[illegible]2o[illegible]/[illegible]üA[illegible]oH□Aцy%[illegible])[illegible]ɔw[illegible]U=[illegible]A9S□[illegible]G[illegible]K□[illegible])[illegible]"0□
[illegible]p[illegible]□B}[illegible]C[illegible]F[illegible]vV[illegible]v[illegible]ɐ[illegible]ɐouE[illegible]&□[illegible]=[illegible]|[illegible]q[illegible]ɯuA}[illegible]□E[illegible]C[illegible]=[illegible]n[illegible]6□[illegible]=[illegible]|[illegible]&□[illegible]uA}[illegible]>[illegible]n[illegible]"□[illegible]K[illegible]□
```

Alerts:

```
01/12-07:17:49.450678 [**] [1:1378:24] "PROTOCOL-FTP wu-ftp bad file completion attempt" [**]
[Classification: Misc Attack] [Priority: 2] {TCP} 192.168.0.123:56098 -> 172.20.0.2:21
```

- **Suricata**

1	001e2710555613a82e94156d3ed9c289	clientSideAttacks		wget

- **Start:** 2023-01-12 00:39:09.240307
- **End:** 2023-01-12 00:39:13.306541
- **Sig match:** 1:16664:1

Alerts:

```
01/12/2023-00:39:09.485580  [**] [1:2210059:1] SURICATA STREAM pkt seen on wrong thread [**]
[Classification: (null)] [Priority: 3] {TCP} 172.25.0.2:49243 -> 192.42.177.30:53
01/12/2023-00:39:09.612072  [**] [1:2210059:1] SURICATA STREAM pkt seen on wrong thread [**]
[Classification: (null)] [Priority: 3] {TCP} 172.25.0.2:58671 -> 199.7.83.42:53
01/12/2023-00:39:09.612159  [**] [1:2210059:1] SURICATA STREAM pkt seen on wrong thread [**]
[Classification: (null)] [Priority: 3] {TCP} 172.25.0.2:44903 -> 199.7.83.42:53
01/12/2023-00:39:09.795593  [**] [1:2210059:1] SURICATA STREAM pkt seen on wrong thread [**]
[Classification: (null)] [Priority: 3] {TCP} 172.25.0.2:40253 -> 192.82.134.30:53
01/12/2023-00:39:09.973870  [**] [1:2210059:1] SURICATA STREAM pkt seen on wrong thread [**]
[Classification: (null)] [Priority: 3] {TCP} 172.25.0.2:43377 -> 192.82.134.30:53
01/12/2023-00:39:10.011591  [**] [1:2210059:1] SURICATA STREAM pkt seen on wrong thread [**]
[Classification: (null)] [Priority: 3] {TCP} 172.25.0.2:57459 -> 192.82.134.30:53
01/12/2023-00:39:10.237224  [**] [1:2210059:1] SURICATA STREAM pkt seen on wrong thread [**]
[Classification: (null)] [Priority: 3] {TCP} 172.25.0.2:50043 -> 192.42.177.30:53
```

	53	Full SYN Scan	testRules		command

- **Start:** 2023-01-12 00:42:48.756048
- **End:** 2023-01-12 00:43:12.545468
- **Sig match:** 122:1:1

Payload:

```
/usr/bin/sudo /usr/bin/nmap -sS -p- 172.20.0.2
```

Alerts:

```
01/12/2023-00:42:48.981747  [**] [1:2010937:3] ET SCAN Suspicious inbound to mySQL port 3306 [**]
[Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.0.123:45712 -> 172.20.0.2:3306
01/12/2023-00:42:50.492250  [**] [1:2210059:1] SURICATA STREAM pkt seen on wrong thread [**]
[Classification: (null)] [Priority: 3] {TCP} 172.25.0.2:56800 -> 185.125.190.48:80
01/12/2023-00:42:55.074012  [**] [1:2002910:6] ET SCAN Potential VNC Scan 5800-5820 [**]
[Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.0.123:45712 -> 172.20.0.2:5809
01/12/2023-00:42:58.884965  [**] [1:2002911:6] ET SCAN Potential VNC Scan 5900-5920 [**]
[Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.0.123:45712 -> 172.20.0.2:5904
01/12/2023-00:43:01.027993  [**] [1:2010935:3] ET SCAN Suspicious inbound to MSSQL port 1433 [**]
[Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.0.123:45712 -> 172.20.0.2:1433
01/12/2023-00:43:03.177843  [**] [1:2010939:3] ET SCAN Suspicious inbound to PostgreSQL port 5432 [**]
[Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.0.123:45712 -> 172.20.0.2:5432
01/12/2023-00:43:09.141388  [**] [1:2010936:3] ET SCAN Suspicious inbound to Oracle SQL port 1521 [**]
[Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.0.123:45712 -> 172.20.0.2:1521
```

	54	Full Connect() Scan	testRules		command

- **Start:** 2023-01-12 00:43:17.182685
- **End:** 2023-01-12 00:47:10.625177
- **Sig match:** 122:1:1

Payload:

```
/usr/bin/nmap -sT -p- 172.20.0.2
```

Alerts:

```
01/12/2023-00:43:18.329734  [**] [1:2010937:3] ET SCAN Suspicious inbound to mySQL port 3306 [**]
[Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.0.123:48656 -> 172.20.0.2:3306
01/12/2023-00:43:27.431809  [**] [1:2010938:3] ET SCAN Suspicious inbound to mSQL port 4333 [**]
[Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.0.123:46356 -> 172.20.0.2:4333
01/12/2023-00:43:48.693691  [**] [1:2010936:3] ET SCAN Suspicious inbound to Oracle SQL port 1521 [**]
[Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.0.123:52562 -> 172.20.0.2:1521
01/12/2023-00:44:03.945845  [**] [1:2210059:1] SURICATA STREAM pkt seen on wrong thread [**]
[Classification: (null)] [Priority: 3] {TCP} 172.25.0.2:47069 -> 199.7.83.42:53
01/12/2023-00:44:03.945696  [**] [1:2210059:1] SURICATA STREAM pkt seen on wrong thread [**]
[Classification: (null)] [Priority: 3] {TCP} 172.25.0.2:37401 -> 199.7.83.42:53
01/12/2023-00:44:04.730641  [**] [1:2210059:1] SURICATA STREAM pkt seen on wrong thread [**]
[Classification: (null)] [Priority: 3] {TCP} 172.25.0.2:33855 -> 192.36.148.17:53
01/12/2023-00:45:13.723731  [**] [1:2010935:3] ET SCAN Suspicious inbound to MSSQL port 1433 [**]
[Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.0.123:49310 -> 172.20.0.2:1433
```

	55	SQL Injection	testRules	80/tcp	socket

- **Start:** 2023-01-12 00:47:15.245233
- **End:** 2023-01-12 00:47:15.253021
- **Sig match:** (?i)UNION

Payload:

```
GET /form.php?q=1+UNION+SELECT+VERSION%28%29 HTTP/1.1
Host: 127.0.0.1
```

Alerts:

```
01/12/2023-00:47:15.312257  [**] [1:2006446:14] ET WEB_SERVER Possible SQL Injection Attempt UNION
SELECT [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.0.123:60908 ->
172.20.0.2:80
01/12/2023-00:47:15.312257  [**] [1:2011037:6] ET WEB_SERVER Possible Attempt to Get SQL Server Version
in URI using SELECT VERSION [**] [Classification: Web Application Attack] [Priority: 1] {TCP}
192.168.0.123:60908 -> 172.20.0.2:80
```

	57	Nikto Scan	testRules		command

- **Start:** 2023-01-12 00:47:24.775893
- **End:** 2023-01-12 00:47:26.672104
- **Sig match:** (?i)nikto

Payload:

```
/usr/bin/sudo /usr/bin/nikto -config /etc/nikto.conf -h 172.20.0.2 -Plugins cgi
```

Alerts:

```
01/12/2023-00:47:25.150288  [**] [1:2002677:14] ET SCAN Nikto Web App Scan in Progress [**]
[Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.0.123:60914 -> 172.20.0.2:80
01/12/2023-00:47:25.450678  [**] [1:2101071:8] GPL WEB_SERVER .htpasswd access [**] [Classification:
Web Application Attack] [Priority: 1] {TCP} 192.168.0.123:60914 -> 172.20.0.2:80
01/12/2023-00:47:25.941816  [**] [1:2101129:9] GPL WEB_SERVER .htaccess access [**] [Classification:
Attempted Information Leak] [Priority: 2] {TCP} 192.168.0.123:54032 -> 172.20.0.2:80
01/12/2023-00:47:26.024399  [**] [1:2100987:17] GPL EXPLOIT .htr access [**] [Classification: access to
a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.0.123:54032 -> 172.20.0.2:80
01/12/2023-00:47:26.096494  [**] [1:2101129:9] GPL WEB_SERVER .htaccess access [**] [Classification:
Attempted Information Leak] [Priority: 2] {TCP} 192.168.0.123:54032 -> 172.20.0.2:80
01/12/2023-00:47:26.218010  [**] [1:2101245:13] GPL EXPLOIT ISAPI .idq access [**] [Classification:
access to a potentially vulnerable web application] [Priority: 2] {TCP} 192.168.0.123:54032 ->
172.20.0.2:80
01/12/2023-00:47:26.453716  [**] [1:2101242:14] GPL EXPLOIT ISAPI .ida access [**] [Classification:
```

	62	Nestea Attack 1/3	fragmentedPackets		scapy

- **Start:** 2023-01-12 00:47:52.757936
- **End:** 2023-01-12 00:47:52.808333
- **Sig match:** 123:

Payload:

```
send(IP(dst="172.20.0.2", id=42, flags="MF")/UDP()/("X"*10), verbose=0)
```

Alerts:

```
01/12/2023-00:47:50.484427  [**] [1:2210059:1] SURICATA STREAM pkt seen on wrong thread [**]
[Classification: (null)] [Priority: 3] {TCP} 172.25.0.2:35776 -> 35.232.111.17:80
```

	65	Bruteforce against FTP with ncrack	bruteForce		command

- **Start:** 2023-01-12 00:48:06.729761
- **End:** 2023-01-12 00:48:27.746285
- **Sig match:** (?i)brute

Payload:

```
/usr/bin/ncrack -f -U data/ncrack-users.txt -P data/ncrack-passwords.txt 172.20.0.2:21
```

Alerts:

```
01/12/2023-00:48:16.261411  [**] [1:2010642:3] ET SCAN Multiple FTP Root Login Attempts from Single
Source - Possible Brute Force Attempt [**] [Classification: Attempted Information Leak] [Priority: 2]
{TCP} 192.168.0.123:40016 -> 172.20.0.2:21
01/12/2023-00:48:18.869005  [**] [1:2002383:12] ET SCAN Potential FTP Brute-Force attempt response [**]
[Classification: Unsuccessful User Privilege Gain] [Priority: 1] {TCP} 172.20.0.2:21 ->
192.168.0.123:39966
01/12/2023-00:48:18.882147  [**] [1:2002383:12] ET SCAN Potential FTP Brute-Force attempt response [**]
[Classification: Unsuccessful User Privilege Gain] [Priority: 1] {TCP} 172.20.0.2:21 ->
192.168.0.123:39950
01/12/2023-00:48:18.887172  [**] [1:2010642:3] ET SCAN Multiple FTP Root Login Attempts from Single
Source - Possible Brute Force Attempt [**] [Classification: Attempted Information Leak] [Priority: 2]
{TCP} 192.168.0.123:39950 -> 172.20.0.2:21
01/12/2023-00:48:22.086983  [**] [1:2002383:12] ET SCAN Potential FTP Brute-Force attempt response [**]
[Classification: Unsuccessful User Privilege Gain] [Priority: 1] {TCP} 172.20.0.2:21 ->
```

	66	Nmap decoy test (6th position)	evasionTechniques		command

- **Start:** 2023-01-12 00:48:32.358630
- **End:** 2023-01-12 00:56:40.353582
- **Sig match:** 192.168.0.123

Payload:

```
/usr/bin/sudo /usr/bin/nmap -sS -A -D
192.168.100.1,192.168.100.2,192.168.100.3,192.168.100.4,192.168.100.5,ME 172.20.0.2
```

Alerts:

```
01/12/2023-00:48:33.508131  [**] [1:2010937:3] ET SCAN Suspicious inbound to mySQL port 3306 [**]
[Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.100.3:61864 -> 172.20.0.2:3306
01/12/2023-00:48:33.508241  [**] [1:2010937:3] ET SCAN Suspicious inbound to mySQL port 3306 [**]
[Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.100.4:61864 -> 172.20.0.2:3306
01/12/2023-00:48:33.508434  [**] [1:2010937:3] ET SCAN Suspicious inbound to mySQL port 3306 [**]
[Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.100.5:61864 -> 172.20.0.2:3306
01/12/2023-00:48:33.508007  [**] [1:2010937:3] ET SCAN Suspicious inbound to mySQL port 3306 [**]
[Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.100.2:61864 -> 172.20.0.2:3306
01/12/2023-00:48:33.508588  [**] [1:2010937:3] ET SCAN Suspicious inbound to mySQL port 3306 [**]
[Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.0.123:61864 -> 172.20.0.2:3306
01/12/2023-00:48:33.666315  [**] [1:2010939:3] ET SCAN Suspicious inbound to PostgreSQL port 5432 [**]
[Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.100.2:61864 -> 172.20.0.2:5432
01/12/2023-00:48:33.666505  [**] [1:2010939:3] ET SCAN Suspicious inbound to PostgreSQL port 5432 [**]
[Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.100.3:61864 -> 172.20.0.2:5432
```

	67	Nmap decoy test (7th position)	evasionTechniques		command

- **Start:** 2023-01-12 00:56:45.208956
- **End:** 2023-01-12 00:58:49.372642
- **Sig match:** 192.168.0.123

Payload:

```
/usr/bin/sudo /usr/bin/nmap -sS -A -D
192.168.100.1,192.168.100.2,192.168.100.3,192.168.100.4,192.168.100.5,192.168.100.6,ME 172.20.0.2
```

Alerts:

```
01/12/2023-00:56:45.884033  [**] [1:2010937:3] ET SCAN Suspicious inbound to mySQL port 3306 [**]
[Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.100.2:56193 -> 172.20.0.2:3306
01/12/2023-00:56:45.884201  [**] [1:2010937:3] ET SCAN Suspicious inbound to mySQL port 3306 [**]
[Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.100.3:56193 -> 172.20.0.2:3306
01/12/2023-00:56:45.884362  [**] [1:2010937:3] ET SCAN Suspicious inbound to mySQL port 3306 [**]
[Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.100.4:56193 -> 172.20.0.2:3306
01/12/2023-00:56:45.884686  [**] [1:2010937:3] ET SCAN Suspicious inbound to mySQL port 3306 [**]
[Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.100.6:56193 -> 172.20.0.2:3306
01/12/2023-00:56:45.884852  [**] [1:2010937:3] ET SCAN Suspicious inbound to mySQL port 3306 [**]
[Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.0.123:56193 -> 172.20.0.2:3306
01/12/2023-00:56:45.884527  [**] [1:2010937:3] ET SCAN Suspicious inbound to mySQL port 3306 [**]
[Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.100.5:56193 -> 172.20.0.2:3306
01/12/2023-00:56:45.946908  [**] [1:2010936:3] ET SCAN Suspicious inbound to Oracle SQL port 1521 [**]
[Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.100.2:56193 -> 172.20.0.2:1521
```

69	Nmap scan with fragmentation	evasionTechniques		command	

- **Start:** 2023-01-12 00:58:58.715299
- **End:** 2023-01-12 00:59:21.829874
- **Sig match:** 122:2:1

Payload:

```
/usr/bin/sudo /usr/bin/nmap -PN -sS -A -f 172.20.0.2
```

Alerts:

```
01/12/2023-00:58:58.209165  [**] [1:2230002:1] SURICATA TLS invalid record type [**] [Classification:
Generic Protocol Command Decode] [Priority: 3] {TCP} 172.20.0.2:21 -> 192.168.0.123:37238
01/12/2023-00:58:58.209165  [**] [1:2230010:1] SURICATA TLS invalid record/traffic [**]
[Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 172.20.0.2:21 ->
192.168.0.123:37238
01/12/2023-00:58:59.978404  [**] [1:2010937:3] ET SCAN Suspicious inbound to mySQL port 3306 [**]
[Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.0.123:35615 -> 172.20.0.2:3306
01/12/2023-00:59:00.131694  [**] [1:2002911:6] ET SCAN Potential VNC Scan 5900-5920 [**]
[Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.0.123:35615 -> 172.20.0.2:5901
01/12/2023-00:59:00.156258  [**] [1:2010939:3] ET SCAN Suspicious inbound to PostgreSQL port 5432 [**]
[Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.0.123:35615 -> 172.20.0.2:5432
01/12/2023-00:59:00.176967  [**] [1:2010935:3] ET SCAN Suspicious inbound to MSSQL port 1433 [**]
[Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.0.123:35615 -> 172.20.0.2:1433
01/12/2023-00:59:00.194595  [**] [1:2010936:3] ET SCAN Suspicious inbound to Oracle SQL port 1521 [**]
```

80	Javascript Obfuscation	evasionTechniques	80/tcp	socket	

- **Start:** 2023-01-12 01:00:33.631309
- **End:** 2023-01-12 01:00:33.643349
- **Sig match:** 1:2009714:6

Payload:

```
GET /index.php?page=%sCscript%3Ealert%28%29%3C%2Fscript%3E HTTP/1.1
Host: 127.0.0.1
```

Alerts:

```
01/12/2023-01:00:33.697719  [**] [1:2009714:8] ET WEB_SERVER Script tag in URI Possible Cross Site
Scripting Attempt [**] [Classification: Web Application Attack] [Priority: 1] {TCP} 192.168.0.123:53704
-> 172.20.0.2:80
```

81	SHELLCODE ** sparc setuid 0	shellCodes	21/tcp	socket	

- **Start:** 2023-01-12 01:00:38.714115
- **End:** 2023-01-12 01:00:38.724187
- **Sig match:** 1:647:9

Payload:

```
[illegible]
[illegible]/bin/sh[illegible]
```

Alerts:

```
01/12/2023-01:00:36.606907  [**] [1:2230002:1] SURICATA TLS invalid record type [**] [Classification:
Generic Protocol Command Decode] [Priority: 3] {TCP} 172.20.0.2:21 -> 192.168.0.123:32882
01/12/2023-01:00:36.606907  [**] [1:2230010:1] SURICATA TLS invalid record/traffic [**]
[Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 172.20.0.2:21 ->
192.168.0.123:32882
01/12/2023-01:00:38.778546  [**] [1:2100647:7] GPL SHELLCODE sparc setuid 0 [**] [Classification: A
system call was detected] [Priority: 2] {TCP} 192.168.0.123:54020 -> 172.20.0.2:21
```

86	SHELLCODE x86 setuid 0	shellCodes	21/tcp	socket

- **Start:** 2023-01-12 01:01:02.433765
- **End:** 2023-01-12 01:01:02.437838
- **Sig match:** 1:650:10

Payload:

```
3@3@@□1□ɔ¡@□^@v□1@@F□@F□@□@@N□@V□1¡@@@@@@/bin/sh
```

Alerts:

```
01/12/2023-01:01:03.469403  [**] [1:2230002:1] SURICATA TLS invalid record type [**] [Classification:
Generic Protocol Command Decode] [Priority: 3] {TCP} 172.20.0.2:21 -> 192.168.0.123:32898
01/12/2023-01:01:03.469403  [**] [1:2230010:1] SURICATA TLS invalid record/traffic [**]
[Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 172.20.0.2:21 ->
192.168.0.123:32898
```

87	win32_bind_dllinject - EXITFUNC=seh DLL=c:\ LPORT=4444 Size=312 Encoder=PexFnstenvSub	shellCodes	21/tcp	socket

- **Start:** 2023-01-12 01:01:07.234096
- **End:** 2023-01-12 01:01:07.237790
- **Sig match:** 1:17322:1

Payload:

```
)B@@@@ts@[@s□@@&□@@@@@j@&□@@s@@?J2@?c*        @#n@^@\@?|6@_@$@?□@@Z□@~@溺TR□C{+□E_@-
@@2cc?|2@ @@@@L@@@?'@i@□@@@{M@@&H@□r  @@M@?}
        @@M@@N@@@T=@n@'□@@pE□Q@1@@&@@@&@@@@@@@@@@2o@@@@/@@üA@@oH□Aщy%@@}@ɔw@U=@@A9S□@□G@K□@}@"O□
@@@p@□B}@@C@@@F@@vV@@v@ɔ@@ouE@&□@=@|@@q@ɴuA}@□E@@@C@=@n@6□@=@|@@&□@@uA}@>@n@"□@K@□
```

Alerts:

```
01/12/2023-01:01:07.293054  [**] [1:2009247:3] ET SHELLCODE Rothenburg Shellcode [**] [Classification:
Executable code was detected] [Priority: 1] {TCP} 192.168.0.123:60400 -> 172.20.0.2:21
```

92	Rothenburg Shellcode	shellCodes	21/tcp	socket

- **Start:** 2023-01-12 01:01:30.719946
- **End:** 2023-01-12 01:01:30.730162
- **Sig match:** 1:17322:1

Payload:

```
)B@@@@ts@[@s□@@&□@@@@@j@&□@@s@@?J2@?c*        @#n@^@\@?|6@_@$@?□@@Z□@~@溺TR□C{+□E_@-
@@2cc?|2@ @@@@L@@@?'@i@□@@@{M@@&H@□r  @@M@?}
        @@M@@N@@@T=@n@'□@@pE□Q@1@@&@@@&@@@@@@@@@@2o@@@@/@@üA@@oH□Aщy%@@}@ɔw@U=@@A9S□@□G@K□@}@"O□
@@@p@□B}@@C@@@F@@vV@@v@ɔ@@ouE@&□@=@|@@q@ɴuA}@□E@@@C@=@n@6□@=@|@@&□@@uA}@>@n@"□@K@□
```

Alerts:

```
01/12/2023-01:01:30.785670  [**] [1:2009247:3] ET SHELLCODE Rothenburg Shellcode [**] [Classification:
Executable code was detected] [Priority: 1] {TCP} 192.168.0.123:55330 -> 172.20.0.2:21
```

Snort

Ping Flood

```
-------------------------------------------------
Packet Statistics
-------------------------------------------------
daq
                received: 213861
                analyzed: 213861
                   allow: 8187
                   block: 205674
                    idle: 226
                rx_bytes: 6270942
-------------------------------------------------
```

SYN Flood 0 byte

```
-------------------------------------------------
Packet Statistics
-------------------------------------------------
daq
                received: 254047
                analyzed: 254047
                   allow: 2033
                   block: 252014
                    idle: 121
                rx_bytes: 10235770
-------------------------------------------------
```

SYN Flood 500 byte

```
-------------------------------------------------
Packet Statistics
-------------------------------------------------
daq
                received: 267489
                analyzed: 267489
                   allow: 8595
                   block: 258894
                    idle: 46
                rx_bytes: 141822113
-------------------------------------------------
```

SYN Flood 1000 byte

```
-------------------------------------------------
Packet Statistics
-------------------------------------------------
daq
                received: 279529
                analyzed: 279529
                   allow: 2819
                   block: 276710
                    idle: 53
                rx_bytes: 289038375
-------------------------------------------------
```

Suricata

Ping Flood

```
security@security-GK35:/etc/suricata$ sudo suricata -c /etc/suricata/suricata.yaml -q 0 -l /var/log/suricata
13/1/2023 -- 23:14:19 - <Notice> - This is Suricata version 6.0.9 RELEASE running in SYSTEM mode
13/1/2023 -- 23:14:20 - <Notice> - all 6 packet processing threads, 4 management threads initialized, engine started.
^C13/1/2023 -- 23:21:14 - <Notice> - Signal Received.  Stopping engine.
13/1/2023 -- 23:21:18 - <Notice> - (RX-NFQ#0) Treated: Pkts 304581, Bytes 8899827, Errors 0
13/1/2023 -- 23:21:18 - <Notice> - (RX-NFQ#0) Verdict: Accepted 115061, Dropped 189520, Replaced 0
```

SYN Flood 0 byte

```
security@security-GK35:/etc/suricata$ sudo suricata -c /etc/suricata/suricata.yaml -q 0 -l /var/log/suricata
14/1/2023 -- 00:04:09 - <Notice> - This is Suricata version 6.0.9 RELEASE running in SYSTEM mode
14/1/2023 -- 00:04:09 - <Notice> - all 6 packet processing threads, 4 management threads initialized, engine started.
^C14/1/2023 -- 00:09:40 - <Notice> - Signal Received.  Stopping engine.
14/1/2023 -- 00:09:45 - <Notice> - (RX-NFQ#0) Treated: Pkts 294066, Bytes 12012469, Errors 0
14/1/2023 -- 00:09:45 - <Notice> - (RX-NFQ#0) Verdict: Accepted 69707, Dropped 224359, Replaced 0
```

SYN Flood 500 byte

```
security@security-GK35:/etc/suricata$ sudo suricata -c /etc/suricata/suricata.yaml -q 0 -l /var/log/suricata
14/1/2023 -- 01:06:18 - <Notice> - This is Suricata version 6.0.9 RELEASE running in SYSTEM mode
14/1/2023 -- 01:06:18 - <Notice> - all 6 packet processing threads, 4 management threads initialized, engine started.
^C14/1/2023 -- 01:11:32 - <Notice> - Signal Received.  Stopping engine.
14/1/2023 -- 01:11:37 - <Notice> - (RX-NFQ#0) Treated: Pkts 265568, Bytes 142903139, Errors 0
14/1/2023 -- 01:11:37 - <Notice> - (RX-NFQ#0) Verdict: Accepted 62102, Dropped 203466, Replaced 0
```

SYN Flood 1000 byte

```
security@security-GK35:/etc/suricata$ sudo suricata -c /etc/suricata/suricata.yaml -q 0 -l /var/log/suricata
14/1/2023 -- 01:17:00 - <Notice> - This is Suricata version 6.0.9 RELEASE running in SYSTEM mode
14/1/2023 -- 01:17:00 - <Notice> - all 6 packet processing threads, 4 management threads initialized, engine started.
^C14/1/2023 -- 01:21:50 - <Notice> - Signal Received.  Stopping engine.
14/1/2023 -- 01:21:55 - <Notice> - (RX-NFQ#0) Treated: Pkts 274110, Bytes 283720266, Errors 0
14/1/2023 -- 01:21:55 - <Notice> - (RX-NFQ#0) Verdict: Accepted 64432, Dropped 209677, Replaced 0
```