

Daftar Isi

1.1	Pendahuluan.....	1
1.2	Rumusan Masalah.....	3
1.3	Batasan Masalah	3
1.4	Tujuan Penelitian.....	4
1.5	Manfaat Penelitian.....	4
1.6	Metode Penelitian	4
1.7	Sistematika Penulisan	5
2.1	Penelitian Terdahulu.....	6
2.2	Landasan Teori.....	12
2.2.1	<i>Domain Name System (DNS)</i>	12
2.2.2	<i>DNS Tunneling</i>	14
2.2.3	Komponen DNS tunnel	15
2.2.4	Encoding.....	15
2.2.5	Tools DNS tunnel	16
2.2.6	DNS Sinkhole	16
2.2.7	Elasticsearch.....	18
2.2.8	Packetbeat.....	19
2.2.9	Watcher.....	20
2.2.10	Kibana.....	20
3.1	Studi Literatur.....	22
3.2	Perancangan dan Topologi.....	22
3.3	Simulasi dan Pengumpulan Log	22
3.4	Deteksi dan Analisis	24
3.5	Laporan	25
4.1	Studi Literatur.....	26
4.2	Perancangan dan Topologi.....	26
4.3	Simulasi Tanpa DNS Tunneling.....	30
4.4	Simulasi dengan Iodine.....	31
4.5	Simulasi dengan Dnscat2.....	38
4.6	Simulasi dengan <i>malware DNSExfiltrator</i>	43

4.7	Memblokir DNS <i>Tunnel</i> dengan DNS Sinkhole.....	49
4.8	Analisis Kualitas Jaringan.....	51
4.9	Ringkasan Bab	57
5.1	Kesimpulan	58
5.2	Saran	58



Daftar Tabel

Tabel 2.1 Literatur Review.....	9
Tabel 4.1 Daftar Alamat IP.....	27
Tabel 4.2 Sampel <i>jitter</i> pada komputer yang melakukan DNS <i>tunneling</i>	52
Tabel 4.3 Hasil perhitungan uji t berpasangan dengan sampel <i>jitter</i>	52
Tabel 4.4 Sampel <i>packet loss</i> UDP pada komputer yang melakukan DNS <i>tunneling</i>	53
Tabel 4.5 Hasil perhitungan uji t berpasangan dengan sampel <i>packet loss</i> UDP.....	54
Tabel 4.6 Sampel <i>jitter</i> pada komputer yang tidak melakukan DNS <i>tunneling</i>	54
Tabel 4.7 Hasil uji T berpasangan dengan sampel <i>jitter</i>	55
Tabel 4.8 Sampel <i>packet loss</i> UDP pada komputer yang tidak melakukan DNS <i>tunneling</i>	56
Tabel 4.9 Hasil uji T berpasangan dengan sampel <i>packet loss</i> UDP.....	56



Daftar Gambar

Gambar 1.1 Daftar Malware yang menggunakan DNS <i>tunneling</i>	1
Gambar 2.1 Proses <i>request</i> DNS dari <i>client</i> hingga mendapat jawaban dari DNS <i>server</i> ..	13
Gambar 2.2 Proses <i>request</i> sebuah nama <i>domain</i> oleh <i>client</i> ke DNS <i>server</i> tanpa <i>sinkhole</i>	17
Gambar 2.3 Proses <i>request</i> sebuah nama <i>domain</i> oleh <i>client</i> ke DNS <i>server</i> dengan <i>sinkhole</i>	18
Gambar 2.4 Contoh <i>capture</i> DNS dengan Packetbeat	20
Gambar 2.5 Contoh tampilan <i>dashboard kibana</i>	21
Gambar 3.3.1 Alur metodologi penelitian.....	22
Gambar 3.3.2 Alur simulasi deteksi DNS <i>tunneling</i>	23
Gambar 3.3.3 Alur pendeteksian DNS <i>tunneling</i>	24
Gambar 4.1 Topologi simulasi DNS <i>tunneling</i>	27
Gambar 4.2 <i>unique hostname</i> pada trafik DNS normal.....	30
Gambar 4.3 Pembuatan <i>sub domain t1.sanisa.xyz</i> dan <i>pointing</i> ke <i>authoritative name</i> <i>server t1ns.sanisa.xyz</i>	31
Gambar 4.4 <i>Pointing authoritative name server</i> ke alamat IP <i>server</i>	32
Gambar 4.5 Pengecekan konfigurasi <i>sub domain</i> untuk Iodine	32
Gambar 4.6 Menjalankan DNS <i>tunnel server</i> Iodine	33
Gambar 4.7 Proses dial DNS <i>tunnel server</i>	34
Gambar 4.8 <i>Network interface</i> dan alamat IP yang didapat dari DNS <i>tunnel</i>	34
Gambar 4.9 Mengecek koneksi ke DNS <i>tunnel server</i> dengan perintah <i>ping</i>	34
Gambar 4.10 SSH <i>tunnel</i> di dalam DNS <i>tunnel</i>	35
Gambar 4.11 Pengaturan SOCKS <i>Proxy</i>	35
Gambar 4.12 Pengecekan DNS <i>tunnel</i> dengan situs <i>whatismyip.com</i>	36
Gambar 4.13 Lonjakan <i>unique hostname</i> ketika proses <i>tunneling</i> menggunakan <i>Iodine</i> pada domain <i>sanisa.xyz</i>	36
Gambar 4.14 <i>Email</i> notifikasi kepada administrator bahwa telah terjadi <i>suspect</i> DNS <i>Tunneling</i>	37
Gambar 4.15 <i>Capture</i> DNS <i>traffic</i> dengan <i>wireshark</i>	37
Gambar 4.16 Salah satu <i>request</i> dan <i>response</i> DNS <i>tunneling</i> dari IP <i>client</i>	37
Gambar 4.17 Pembuatan subdomain <i>t3.sanisa.xyz</i>	38

Gambar 4.18 <i>Pointing authoritative name server</i> ke alamat IP	39
Gambar 4.19 Menjalankan DNS tunnel server <i>dnscat2</i>	39
Gambar 4.20 Proses <i>dialing</i> ke server DNS tunnel <i>dnscat2</i>	40
Gambar 4.21 <i>Dnscat2</i> telah terhubung ke <i>client</i> dan dapat melakukan <i>command and control</i>	41
Gambar 4.22 Lonjakan <i>unique hostname</i> ketika proses <i>tunneling</i> dengan <i>dnscat2</i> pada <i>domain sanisa.xyz</i>	41
Gambar 4.23 <i>Email</i> notifikasi kepada Administrator jaringan	42
Gambar 4.24 <i>Capture packet dnscat2</i> menggunakan Wireshark	42
Gambar 4.25 Proses <i>request</i> dan <i>response dnscat2</i>	42
Gambar 4.26 <i>Malware DNSExfiltrator</i> saat pengecekan di <i>virustotal.com</i>	43
Gambar 4.27 Pembuatan subdomain <i>t4.sanisa.xyz</i>	44
Gambar 4.28 <i>Pointing authoritative name server t4ns.sanisa.xyz</i> ke alamat IP 45.64.96.244	44
Gambar 4.29 Menjalankan malware <i>DNSExfiltrator</i> sisi <i>server</i>	45
Gambar 4.30 Menjalankan <i>DNSExfiltrator client</i>	45
Gambar 4.31 Proses penerimaan data oleh <i>server</i>	46
Gambar 4.32 <i>File data.pdf</i> yang diterima oleh <i>server</i>	46
Gambar 4.33 Lonjakan <i>unique hostname</i> ketika proses <i>tunneling</i> dengan <i>malware</i> <i>DNSExfiltrator</i> pada <i>domain sanisa.xyz</i>	47
Gambar 4.34 <i>Email</i> notifikasi kepada Administrator Jaringan	47
Gambar 4.35 <i>Sniffing trafik</i> DNS menggunakan <i>wireshark</i>	48
Gambar 4.36 <i>Query</i> DNS hasil <i>filtering</i> pada <i>wireshark</i>	48
Gambar 4.37 Membuat <i>zone</i> untuk DNS sinkhole	49
Gambar 4.38 <i>Zone file sanisa.xyz</i> pada DNS Sinkhole	49
Gambar 4.39 Proses DNS <i>tunneling</i> yang gagal setelah domain <i>sanisa.xyz</i> diblokir dengan DNS <i>Sinkhole</i>	50
Gambar 4.40 <i>Capture traffic</i> DNS ketika nama domain <i>sanisa.xyz</i> diblokir	50
Gambar 4.41 <i>Query response</i> dari nama domain <i>sanisa.xyz</i>	50

Glosarium

DNS	- Domain Name System
UDP	- User Datagram Protocol
TCP	- Transmission Control Protocol
IP	- Internet Protocol
SSH	- Secure Shell
SOCKS	- Socket Secure
NS	- Name Server
MX	- Mail Exchange
PTR	- Pointer
VPS	- Virtual Private Server
BIND	- Berkeley Internet Name Domain
VOIP	- Voice over Internet Protocol
IDS	- Intrusion Detection System
IPS	- Intrusion Prevention System

