



T.C
FIRAT ÜNİVERSİTESİ
TEKNOLOJİ FAKÜLTESİ
YAZILIM MÜHENDİSLİĞİ BÖLÜMÜ

AĞ DİNLEME ARAÇLARI

DANIŞMAN

Doç. Dr. Resul DAŞ

HAZIRAYAN

Mazlum BAYDAR-180541701

Sinan AŞKIN-180541702

ELAĞIĞ-2019

İÇİNDEKİLER

1.GİRİŞ	1
2.AĞ DİNLEME ARAÇLARI	2
2.1 Nagios Network Analyzer	2
2.2 Cacti	3
2.3 Zabbix	4
2.4 Ntop	5
2.5 Icinga	6
2.6 Observium	7
2.7 Wireshark	8
2.8 Nmap	9
2.9 OpenNMS	10
2.10 Bandwidth Monitor	11
2.11 Capsa Free Network Analyzer	12
2.12 Microsoft MessageAnalyzer	13
2.13 NetworkMiner	14
2.14 Advanced IP Scanner.....	15
2.15 Zenoss Core	16
2.16 Telerik Fiddler	17
2.17 MiTeC Network Scanner	18
2.18 Pandora FMS.....	19
2.19 Windump	20
2.20 Tcptrack	20
2.21 PRTG Network Monitor	21
2.22 Angry IP Scanner	22
2.23 SolarWinds NPM	23
2.24 WirelessNetView	24
2.25 NetFlow Traffic Analyzer.....	25
2.26 Xirrus Wi-Fi Inspector	26
2.27 Ngrep	27
2.28 Tcpdump	28

2.29 Ettercap	29
2.30 NetStumbler	30
2.31 P0F	31
2.32 KisMAC	32
2.33 Dsniff	33
2.34 InSSIDer	34
2.35 EtherApe	35
3.Table 1:Comparison of Network Listening Tools	36
4.SONUÇ	38
5.KAYNAKÇA	39

1.GİRİŞ

Ağ dinleme araçları ağdan geçen tüm veri paketlerini yakalayıp izlemeye yarar.Bir ağ izleyicisi HTTP, HTTPS, SNMP ,FTP, SMTP, POP3, IMAP, DNS, SSH, TELNET, SSL, TCP , ICMP, SIP, UDP ve Medya Akışı gibi protokollerle çalışır. Bunlardan bahsetmek gerekirse bazı ağ dinleme araçları şunlardır ; nagios,cacti,zabbix,ntop,icnga,observium community,wireshark,nmap,traceroute NG, Bandwidth Monitor vb. gibi birçok ağ dinleme araçları mevcuttur.Bu araçlardan kullanım alanları ve özelliklerine göre sınıflandırılacağı gibi bu araçların bir kısmı ücretsiz olarak kullanıma sunulurken bir kısmı da ücretli olarak piyasada mevcuttur.

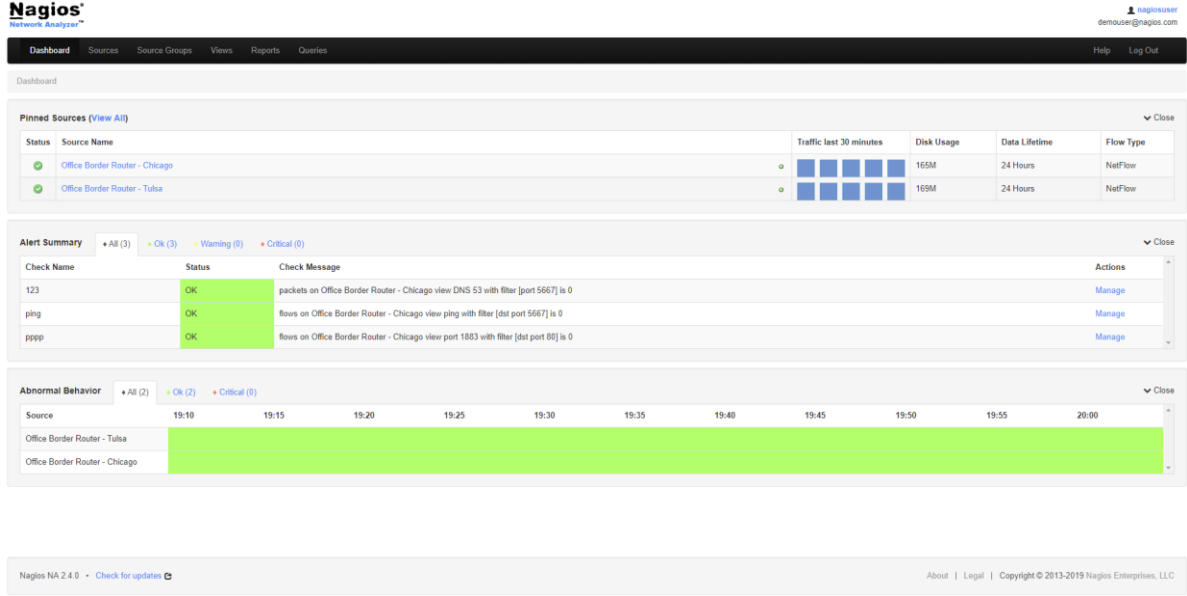
Ağ dinleme araçlarını amacı doğrultusunda kullanım şekilleri güvenlik veya saldırı amaçlı olabilir. Güvenlik amaçlı kullanım olarak yöneticilerin tipik olarak ağ servislerinin kullanılabilirliğini, ağ ara yüzlerinin işlevselliğini, kritik donanım sistemlerinin durumunu, CPU, belleği veya ağdaki sunucular ve cihazlar için diğer istatistikleri izleyebilir ve network penetrasyon testlerini örnek olarak verebilir.

Network penetrasyon testleri kurumları bilgisayar ağlarının siber saldırılara karşı ne derece güvende olduğunu belirler. Ağ sızma testlerinin başlıca adımları saldırganların kullandığı araç ve yöntemleri kullanarak gerçek bir saldırı esnasında sistemlerin ne tür bir dayanıklılık göstereceğini ortaya çıkaracak sızma girişimlerinde bulunmak ve elde edilen bulguları kuruma önerilecek tavsiyelerle birlikte raporlamaktır.

Diğer bir kullanım amacı ise siyah şapkalı hackerlar tarafından yapılan saldırılarda kullanılmak için ağ hakkında bilgi almak ve bunu para, zarar vermek, izinsiz ağ izlemek gibi saldırganın amacı doğrultusunda da kullanılabilir.

2.AĞ DİNLEME ARAÇLARI

2.1 Nagios Network Analyzer



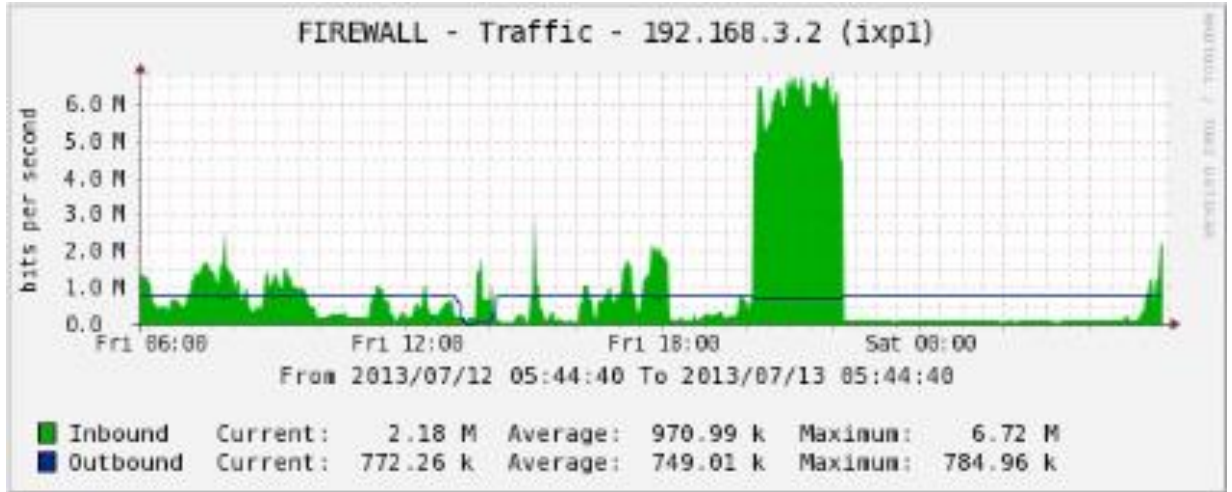
Nagios, Linux (ve Unix tüveri) platformlar üzerinde çalışabilen ve bir endüstri standardı halini almış olan GPL lisanslı ücretsiz bir sistem ve network monitoring yazılımıdır. Bir çok özelliği içerisinde barındıran Nagios'un temel özellikleri aşağıdaki gibidir.[1]

- Host bazında kaynak monitörleme (Disk, İşlemci, Memory)
- Servis bazında network monitörleme (SMTP, POP3, HTTP, NNTP, FTP, PING vs.)[2]
- Plugin desteği sayesinde kendi pluginlerinizi yazabilem esnekliği.
- “Parent” hosts özelliği ile network hiyerarşisi tanımlayabilme.[3]
- Belirli durum ve makineler için belirli kişilere uyarı mesajları gönderebilme. (E-mail, Pager, SMS vs.)
- Web Arayüzü'nden anlık durum görüntülemesi ve gelişmiş raporlar

2.2 Cacti

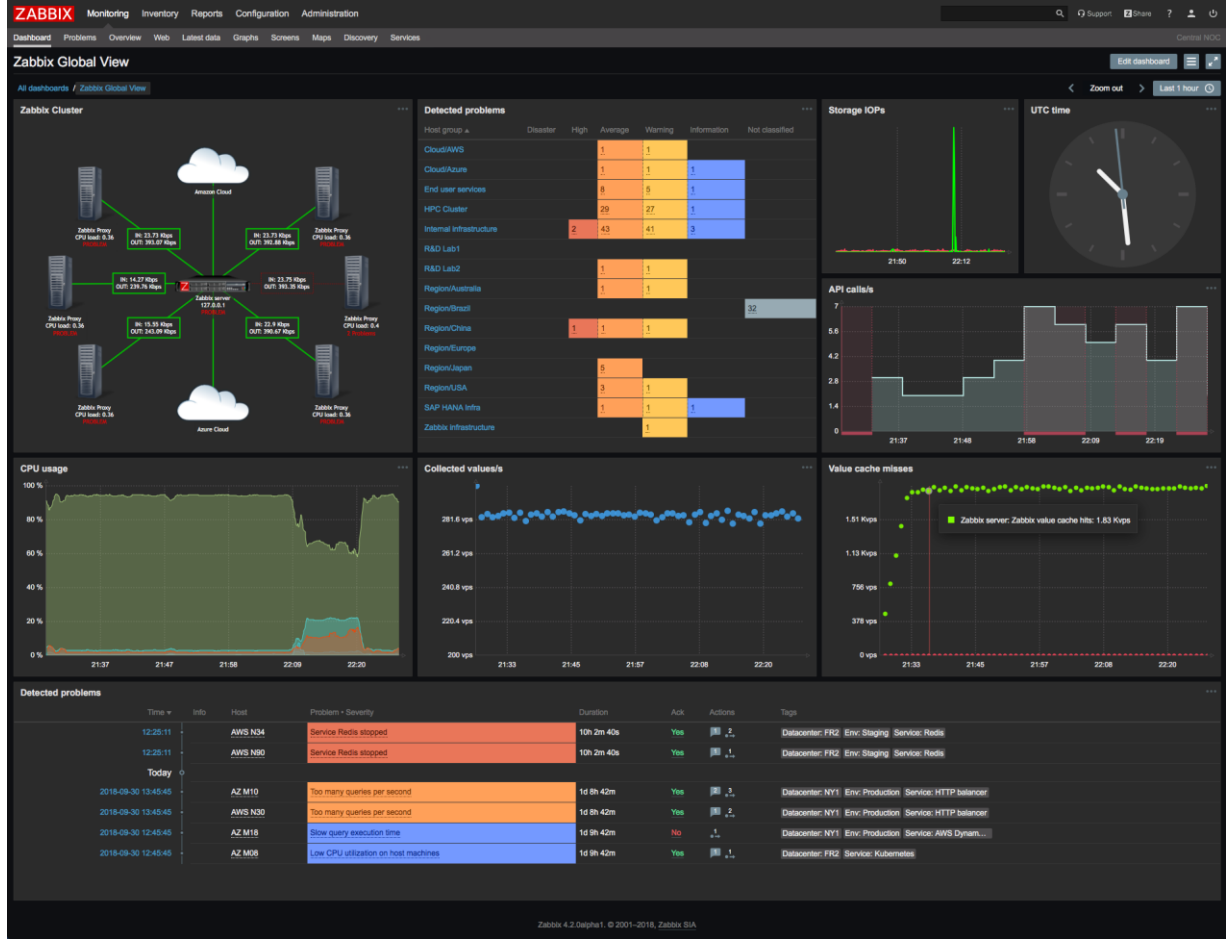


Item	ID	Data Input Method	Poller Interval	Active	Template Name	
SWITCH - CPU Usage - Nice	82	Get SNMP Data	5 Minutes	Yes	ucd/net - CPU Usage - Nice	
SWITCH - CPU Usage - System	83	Get SNMP Data	5 Minutes	Yes	ucd/net - CPU Usage - System	
SWITCH - CPU Usage - User	84	Get SNMP Data	5 Minutes	Yes	ucd/net - CPU Usage - User	
SWITCH - Load Average - 1 Minute	85	Get SNMP Data	5 Minutes	Yes	ucd/net - Load Average - 1 Minute	
SWITCH - Load Average - 15 Minute	86	Get SNMP Data	5 Minutes	Yes	ucd/net - Load Average - 15 Minute	
SWITCH - Load Average - 5 Minute	87	Get SNMP Data	5 Minutes	Yes	ucd/net - Load Average - 5 Minute	
SWITCH - Memory - Buffers	88	Get SNMP Data	5 Minutes	Yes	ucd/net - Memory - Buffers	
SWITCH - Memory - Cache	89	Get SNMP Data	5 Minutes	Yes	ucd/net - Memory - Cache	
SWITCH - Memory - Free	90	Get SNMP Data	5 Minutes	Yes	ucd/net - Memory - Free	
SWITCH - Traffic - FS726T Fast Eth	105	Get SNMP Data (Indexed)	5 Minutes	Yes	Interface - Traffic	
SWITCH - Traffic - FS726T Fast Eth	91	Get SNMP Data (Indexed)	5 Minutes	Yes	Interface - Traffic	
SWITCH - Traffic - FS726T Fast Eth	92	Get SNMP Data (Indexed)	5 Minutes	Yes	Interface - Traffic	
SWITCH - Traffic - FS726T Fast Eth	93	Get SNMP Data (Indexed)	5 Minutes	Yes	Interface - Traffic	
SWITCH - Traffic - FS726T Fast Eth	94	Get SNMP Data (Indexed)	5 Minutes	Yes	Interface - Traffic	
SWITCH - Traffic - FS726T Fast Eth	95	Get SNMP Data (Indexed)	5 Minutes	Yes	Interface - Traffic	
SWITCH - Traffic - FS726T Fast Eth	104	Get SNMP Data (Indexed)	5 Minutes	Yes	Interface - Traffic	
SWITCH - Traffic - FS726T Fast Eth	103	Get SNMP Data (Indexed)	5 Minutes	Yes	Interface - Traffic	
SWITCH - Traffic - FS726T Fast Eth	102	Get SNMP Data (Indexed)	5 Minutes	Yes	Interface - Traffic	
SWITCH - Traffic - FS726T Fast Eth	101	Get SNMP Data (Indexed)	5 Minutes	Yes	Interface - Traffic	
SWITCH - Traffic - FS726T Fast Eth	100	Get SNMP Data (Indexed)	5 Minutes	Yes	Interface - Traffic	
SWITCH - Traffic - FS726T Fast Eth	111	Get SNMP Data (Indexed)	5 Minutes	Yes	Interface - Traffic	
SWITCH - Traffic - FS726T Fast Eth	98	Get SNMP Data (Indexed)	5 Minutes	Yes	Interface - Traffic	
SWITCH - Traffic - FS726T Fast Eth	112	Get SNMP Data (Indexed)	5 Minutes	Yes	Interface - Traffic	
SWITCH - Traffic - FS726T Fast Eth	113	Get SNMP Data (Indexed)	5 Minutes	Yes	Interface - Traffic	
SWITCH - Traffic - FS726T Fast Eth	107	Get SNMP Data (Indexed)	5 Minutes	Yes	Interface - Traffic	
SWITCH - Traffic - FS726T Fast Eth	108	Get SNMP Data (Indexed)	5 Minutes	Yes	Interface - Traffic	
SWITCH - Traffic - FS726T Fast Eth	109	Get SNMP Data (Indexed)	5 Minutes	Yes	Interface - Traffic	
SWITCH - Traffic - FS726T Fast Eth	110	Get SNMP Data (Indexed)	5 Minutes	Yes	Interface - Traffic	
SWITCH - Traffic - FS726T Fast Eth	96	Get SNMP Data (Indexed)	5 Minutes	Yes	Interface - Traffic	
SWITCH - Traffic - FS726T Fast Eth	99	Get SNMP Data (Indexed)	5 Minutes	Yes	Interface - Traffic	



GNU\GPL lisansı ile dağıtılan cacti,SNMP(Simple Network Management Protocol) protokolünü kullanarak ağ trafiğini dinlemek istediğimiz cihazlardan aldığı snmp sorgularının cevabına göre RRDTool aracı ile grafikler oluşturularak sistem ve ağ cihazlarını izlememizi(monitoring)sağlar.SNMP protokolü sayesinde ağ trafiği,port trafiği,kullanıcı,sistem yükü,disk kapasitesi,bellek kullanımı gibi bilgileri kolay anlaşılır bir grafik ile ekrana sunar. Cacti Open Source bir yazılımdır ve bu nedenle Linux Unix türevi sistemler üzerinde çalışır.[4]

2.3 Zabbix



Zabbix, Alexei Vladishev tarafından geliştirilen ağlar ve uygulamalar için bir kurumsal açık kaynak izleme çözümüdür. Çeşitli ağ hizmetleri, sunucular ve diğer ağ donanımlarını izlemek ve durumunu takip etmek için tasarlanmıştır. Zabbix, veri depolamak için MySQL, PostgreSQL, SQLite ve IBM DB2 dahil olmak üzere birçok veritabanı sistemi için destek sunar. Zabbix arka ucu C ile yazılmıştır ve ön uç PHP ile yazılmıştır. [5]

- Ağ servislerinin (SMTP, POP3, HTTP vb) izlenmesi[6]
- Sistem kaynaklarının (işlemci yükü, disk kullanımı vb) izlenmesi
- Ağdan veri gönderebilen herhangi bir cihazın (ısı sensörü, alarm vb) izlenmesi[7]
- Ajanlı ya da ajansız çalışabilme
- Belirli eşik değerleri aşıldığında farklı kademelerde uyarı üretebilme
- Uyarıların e-posta, SMS ya da benzeri bir araçla iletilmesi
- Uyarı anında önceden tanımlanmış işlemlerin gerçekleştirilerek proaktif sorun çözümü
- Tüm alınan verilerin ve üretilen uyarıların kaydedilmesi ve geriye dönük grafiklerinin çizilebilmesi
- Android/iPhone ile takip edebilme
- Çok sayıda hazır şablon
- Şablon yapısı sayesinde özel servisler için yeni eklentiler yazılabilmesi

2.4 Ntop



Active Flows

Info	Application	L4 Proto	Client	Server	Duration	Breakdown	Throughput	Total Bytes
Info	DropBox	TCP	lucasmacbookpro.home...:55614	dl-client119.dropbox...:443	6 min, 32 sec	Client	66.28 Kbit ↓	4.27 MB
Info	IMAPS	TCP	lucasmacbookpro.home...:55527	jake.ntop.org:993	1 min, 12 sec	Server	75.52 Kbit ↓	4.12 MB
Info	DropBox	TCP	lucasmacbookpro.home...:55612	dl-client119.dropbox...:443	6 min, 32 sec	Client	207.68 Kbit ↑	4.78 MB
Info	DropBox	UDP	lucasmacbookpro.home...:17500	Broadcast:17500	4 min, 31 sec	Client	0 bps —	5.07 KB
Info	DropBox	UDP	imacluca.homenet.tel...:17500	192.168.1.255:17500	1 sec	Client	0 bps —	518 Bytes
Info	DropBox	TCP	lucasmacbookpro.home...:55613	dl-client119.dropbox...:443	6 min, 11 sec	Client	0 bps —	5.23 MB
Info	IMAPS	TCP	jake.ntop.org:993	lucasmacbookpro.home...:55515	4 sec	Client Server	0 bps	2.76 KB
Info	DropBox	TCP	snt-re4-8d.sjc.dropb...:80	lucasmacbookpro.home...:49299	1 sec	Client Server	0 bps —	1.51 KB
Info	Spotify	UDP	lucasmacbookpro.home...:57621	192.168.1.255:57621	1 sec	Client	0 bps —	86 Bytes
Info	Unknown	TCP	jake.ntop.org:993	lucasmacbookpro.home...:55508	1 sec	Client Server	0 bps	251 Bytes

Ntop, gerçek zamanlı olarak ağ kullanımını gösteren bir ağ trafik aracıdır. Bu araçla ilgili iyi şeylerden biri, ağ durumunu daha iyi anlamak için trafik bilgilerini yönetmek ve gezinmek için bir web tarayıcısı kullanabilmenizdir. Bir çok özelliği içerisinde barındıran Ntop temel özellikleri aşağıdaki gibidir.[8]

- Ağ trafiğini IP adresi, port, L7 protokolü, verim, Özerk Sistemler (AS'ler) dahil olmak üzere birçok kritere göre sıralar.
- Gerçek zamanlı ağ trafiğini ve etkin ana bilgisayarları göster.
- Verimlilik ve uygulama protokolleri dahil olmak üzere çeşitli ağ ölçümleri için uzun vadeli raporlar oluşturur.
- En iyi konuşanlar (gönderenler / alıcılar), en iyi AS'ler, en iyi L7 uygulamalarını barındırır.
- Canlı iş hacmini, ağ ve uygulama gecikmelerini, Gidiş-Dönüş Süresi (RTT), TCP istatistiklerini (yeniden iletimler, sıra dışı paketler, kayıp paket) ve iletilen bayt ve paketleri izleyin ve raporlamaya yarar.
- Deep Packet Inspection (DPI) teknolojisinden yararlanarak nDPI'den yararlanarak uygulama protokollerini (Facebook, YouTube, BitTorrent, vb.) keşfetmeye olanak sağlar.
- Google ve HTTP Kara Listesi tarafından sağlanan karakterizasyon hizmetlerinden yararlanarak HTTP trafiğini karakterize etmeyi sağlar.
- HTML5 / AJAX ağ trafiği istatistiklerini üretir.[9]
- IPv4 ve IPv6 için tam destek sağlar.
- SNMP cihazlarının SNMP v1 / v2c desteği ve sürekli izlenmesini sağlar.

2.5 Icinga

The screenshot displays the Icinga web interface. At the top, there are status bars for various host states: 24 UP, 0/6/0 DOWN, 0/0/0 UNREACHABLE, 0 PENDING, 6/30 TOTAL; 35 OK, 0/0/0 WARNING, 0/4/6 CRITICAL, 0/0/0 UNKNOWN, 0 PENDING, 10/45 TOTAL. The Icinga logo is also present. Below the status bars, there's a 'Current Network Status' section with a 'Last Updated' timestamp and a 'Commands for checked services' dropdown. The main part of the interface is a table titled 'Service Status Details For All Hosts'. The table has columns for Host, Service, Status, Last Check, Duration, Attempt, and Status Information. The table lists various services for different hosts, including MySQL, PING, HTTP, MailQ, and Humidity, all showing 'OK' status. The interface also includes a sidebar with navigation links for General, Status, Problems, System, Reporting, and Configuration.

Host	Service	Status	Last Check	Duration	Attempt	Status Information
c1-db1	MySQL	OK	09-04-2013 21:30:50	143d 4h 48m 24s	1/5	MySQL: OK, SQLquery OK - Query took 18.058 sec
	PING	OK	09-15-2013 03:18:08	1d 13h 38m 15s	1/5	PING: OK, Packet loss = 21.336: RTA = 0.052
c1-db2	MySQL	OK	09-15-2013 03:18:18	1d 13h 39m 55s	1/5	MySQL: OK, SQLquery OK - Query took 14.849 sec
	PING	OK	09-15-2013 03:18:28	1d 13h 39m 32s	1/5	PING: OK, Packet loss = 0.631: RTA = 0.044
c1-fw	PING	OK	09-15-2013 03:18:38	1d 13h 26m 27s	1/5	PING: OK, Packet loss = 18.477: RTA = 0.055
c1-http	HTTP	OK	09-15-2013 03:18:48	12d 13h 50m 15s	1/5	HTTP: OK, HTTP OK HTTP/1.0 200 OK - 3270 bytes in 0.075 seconds
	PING	OK	09-15-2013 03:18:58	1d 13h 40m 0s	1/5	PING: OK, Packet loss = 14.882: RTA = 0.052
c1-mail1	MailQ	OK	09-15-2013 03:19:08	1d 13h 38m 19s	1/5	MailQ: OK, mailq reports 5.815 mails in the queue
	PING	OK	06-14-2013 21:38:32	138d 7h 49m 19s	1/5	PING: OK, Packet loss = 1.332: RTA = 0.039
c1-mail2	MailQ	OK	06-14-2013 21:38:32	143d 17h 55m 41s	1/5	MailQ: OK, mailq reports 6.188 mails in the queue
	PING	OK	09-15-2013 03:19:18	1d 13h 37m 41s	1/5	PING: OK, Packet loss = 0.016: RTA = 0.026
c1-nagios	PING	OK	09-02-2013 01:08:53	13d 2h 11m 12s	1/5	PING: OK, Packet loss = 2.792: RTA = 0.048
c1-router	PING	OK	09-15-2013 03:19:28	1d 13h 25m 37s	1/5	PING: OK, Packet loss = 0.668: RTA = 0.055
c1-switch	PING	OK	08-09-2013 08:38:23	138d 5h 8m 3s	1/5	PING: OK, Packet loss = 0.061: RTA = 0.024
c1-tt1	Humidity	OK	06-14-2013 21:38:32	138d 9h 8m 10s	1/5	Humidity: OK, OK (h=10.224 %)
	PING	OK	06-14-2013 21:38:32	142d 15h 24m 21s	1/5	PING: OK, Packet loss = 0: RTA = 0.444

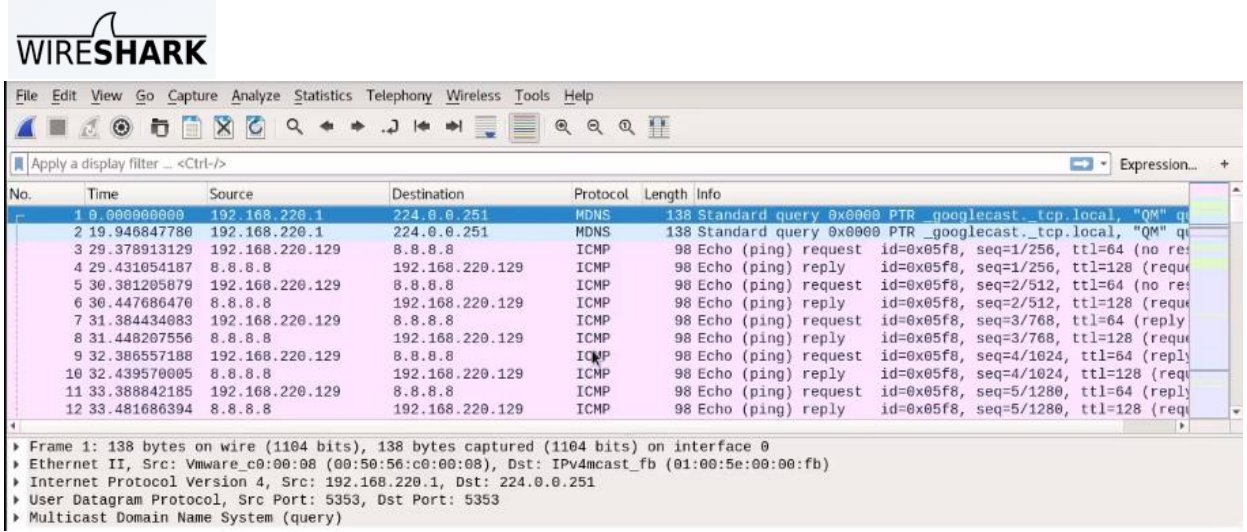
Icinga ,ağa bağılı sunucuların ve hizmetlerin sağılığını denetlemek için kullanılan esnek ve güçlü bir açık kaynak izleme sistemidir. İşlem yükünü ve çalışma süresini, bir depolama aygıtındaki boş disk alanı, bir önbellekleme hizmetinde bellek tüketimi vb. kaynakları izlemek için kullanılabilir. Düzgün bir şekilde kurulduktan sonra, Icinga size bildirimler, duruş zamanlaması ve performans verisinin uzun vadeli depolanmasının yanı sıra çok sayıda ana makinenin ve hizmetin durumuyla ilgili genel bir bakış verebilir. [10]

2.6 Observium



Observium, Network yapınız dâhilinde bulunan cihazlardan SNMP ile aldığı verileri grafiksel bir ara yüzde sunmaktadır. Birçok markanın (Cisco, Windows, Linux, HP, Juniper, Dell, FreeBSD, F5, Brocade, Citrix, NetApp vb.) ürününe ait CPU, RAM, hafıza, port, trafik vb. verileri otomatik olarak tespit edip toplamaktadır. Observium popüler Linux dağıtımları olan Debian ve Ubuntu üzerine inşa edilmiştir. Temel gereksinimler Apache, fping, MySQL, Net-SNMP, RRDtool ve PHP'den oluşur.[11]

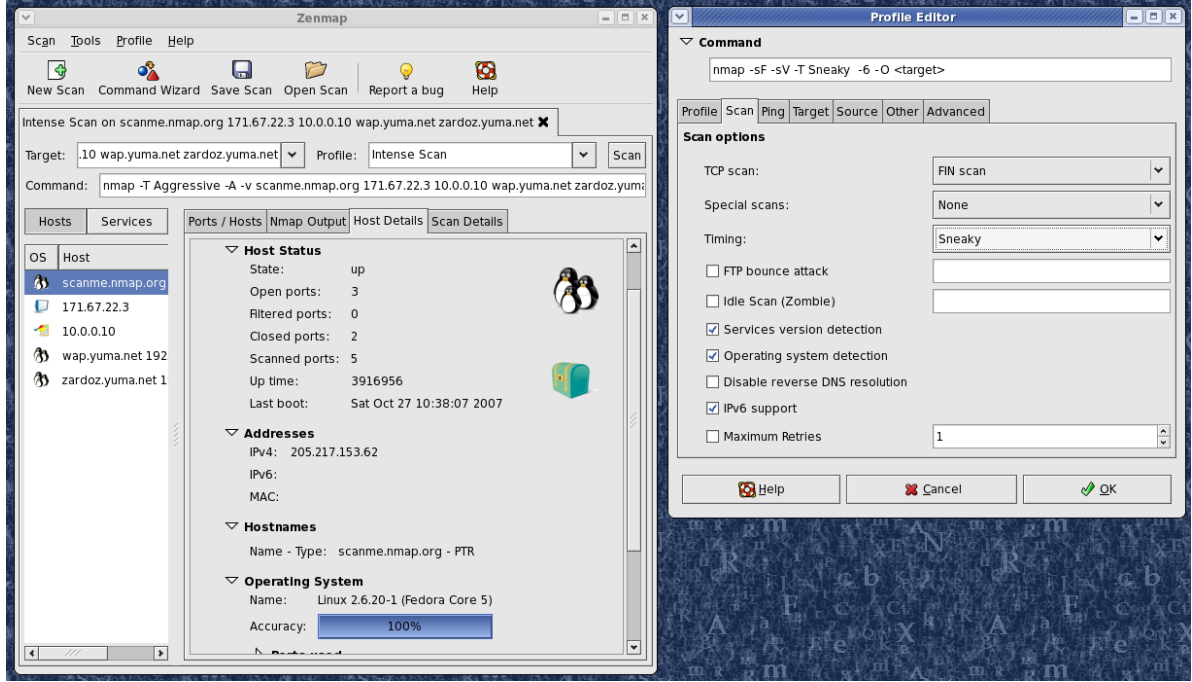
2.7 Wireshark



Wireshark, bir ağ veya ağ protokolünü analiz etmemize yardımcı olan ücretsiz bir araçtır. Wireshark'ın kendi sitesi üzerinden ücretsiz olarak indirebileceğimiz bu aracı kullanarak bir ağ trafiğini geçmişte yakalanan paketlerle birlikte detaylı olarak analiz etme şansına sahip olabiliriz. Unix, Linux, Windows ve MacOS işletim sistemlerinde çalışan Wireshark, komut satırı üzerinden kullanılabileceği gibi basit ve işlevsel kullanıcı ara yüzüde sunmaktadır. GTK+ ve bazı widget araç takımıyla güçlendirilen yazılım, veri paketlerini yakalamak için pcap'ı kullanır. Wireshark ve diğer tüm terminal tabanlı yazılımlar ve Tshark'da olduğu üzere yazılım GNU General Public License altında yayınlanmaktadır. Wireshark yazılımının kullanıcılarına sunduğu bazı temel ve öne çıkan özellikleri şunlardır:

- Kablolu veya kablosuz bağlantı üzerindeki ağ trafiğini ve önceden yakalanmış tüm veri paketlerini analiz etmek.[12]
- Gerçek zamanlı olarak aktarılan veri trafiğini kontrol etmek. Buna Ethernet, IEEE 802.11, point-to-point Protocol (PPP) gibi kapsamlı ağ türleri dahildir.
- Kullanıcı ara yüzü yardımıyla terminal veya komut satırını kullanmaya gerek kalmadan işlem yapabilmek ve yakalanmış veri paketlerini gözden geçirmek.
- Programsal olarak yakalanmış bir paketi düzenleme ve dönüştürme işlevlerini yerine getirmek.
- Belirlediğiniz herhangi bir filtre dahilinde ağ trafiğini filtrelemek ve yalnızca filtreye örtüşen sonuçları listelemek.
- Wireshark'ın harici modül desteği sayesinde çeşitli Plug-in'ler yardımıyla çeşitli protokoller için Wireshark'a geniş bir protokol desteği kazandırmak.
- Ağ üzerinden yapılan VoIP aramalarına dair çağrılarını saptayabilmek. [13]
- Linux ortamında kullandığınız taktirde raw USB trafiğini yakalamak

2.8 Nmap



Nmap, bilgisayar ağıları uzmanı Gordon Lyon tarafından geliştirilmiş bir güvenlik tarayıcısıdır. Taranan ağın haritasını çıkarabilir ve ağ makinalarında çalışan servislerin durumlarını, işletim sistemlerini, portların durumlarını gözlemleyebilir. [14] Kullanım alanı olarak;

- Ağ kurulumu yapıp hazırlık işlemleri sırasında gerekli ayarların test edilmesi,
- Ağ envanteri tutulması, haritalaması, bakımında ve yönetiminde,
- Ağdaki aktif ana bilgisayarları algılamasında,
- Ana bilgisayardaki açık bağlantı noktalarını algılamada,
- Yazılımı ve sürümü ilgili bağlantı noktasına algılamada,
- İşletim sistemini, donanım adresini ve yazılım sürümünü algılamada,
- Güvenlik açığını ve güvenlik açıklarını algılamada
- Bilinmeyen yeni sunucuları tanımlayarak, güvenlik denetimlerinin yapılmasında kullanabiliriz.

2.9 OpenNMS



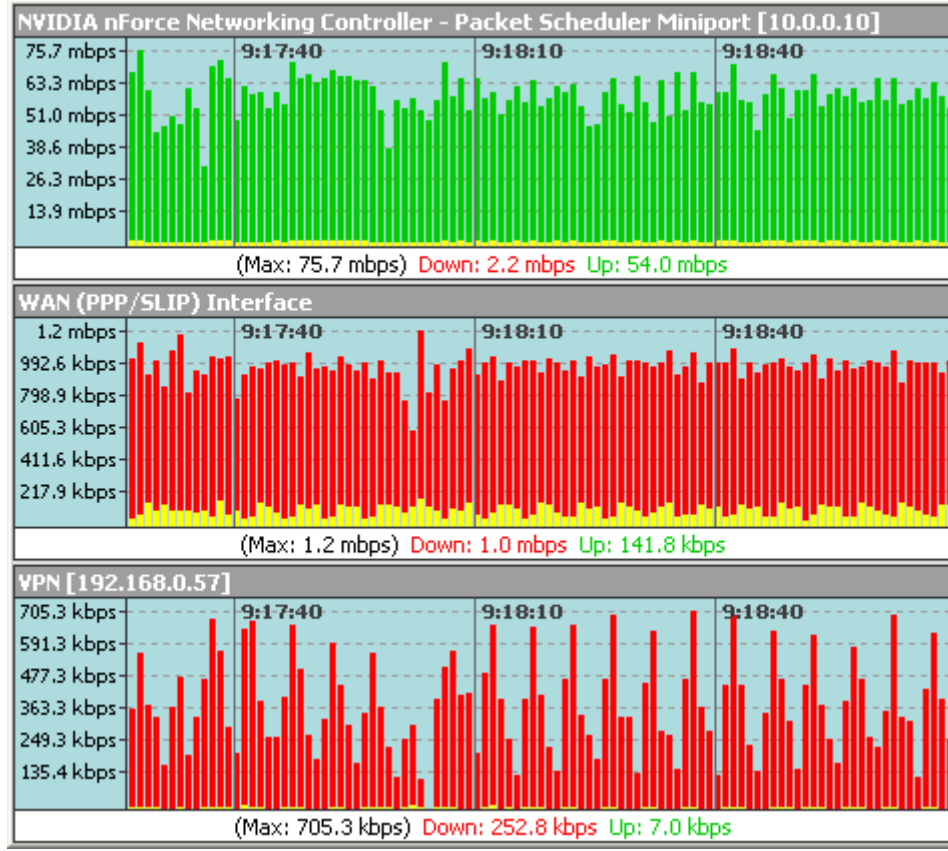
Nodes with Pending Problems	Availability Over the Past 24 Hours	Notifications																																	
modaniels.internal.opennms.com has 1 alarm (15 hours)	<table><thead><tr><th>Categories</th><th>Outages</th><th>Availability</th></tr></thead><tbody><tr><td>Network Interfaces</td><td>0 of 125</td><td>100.000%</td></tr><tr><td>Web Servers</td><td>0 of 51</td><td>100.000%</td></tr><tr><td>Email Servers</td><td>0 of 14</td><td>99.995%</td></tr><tr><td>DNS and DHCP Servers</td><td>0 of 9</td><td>100.000%</td></tr><tr><td>Database Servers</td><td>0 of 0</td><td>100.000%</td></tr><tr><td>JMX Servers</td><td>0 of 0</td><td>100.000%</td></tr><tr><td>Software Update</td><td>3 of 22</td><td>86.609%</td></tr><tr><td>Other Servers</td><td>0 of 71</td><td>100.000%</td></tr><tr><td>Total</td><td>Outages</td><td>Availability</td></tr><tr><td>Overall Service Availability</td><td>6 of 339</td><td>98.612%</td></tr></tbody></table>	Categories	Outages	Availability	Network Interfaces	0 of 125	100.000%	Web Servers	0 of 51	100.000%	Email Servers	0 of 14	99.995%	DNS and DHCP Servers	0 of 9	100.000%	Database Servers	0 of 0	100.000%	JMX Servers	0 of 0	100.000%	Software Update	3 of 22	86.609%	Other Servers	0 of 71	100.000%	Total	Outages	Availability	Overall Service Availability	6 of 339	98.612%	<p>You have 1 outstanding notice</p> <p>There are 1 outstanding notice</p> <p>On-Call Schedule</p>
Categories	Outages	Availability																																	
Network Interfaces	0 of 125	100.000%																																	
Web Servers	0 of 51	100.000%																																	
Email Servers	0 of 14	99.995%																																	
DNS and DHCP Servers	0 of 9	100.000%																																	
Database Servers	0 of 0	100.000%																																	
JMX Servers	0 of 0	100.000%																																	
Software Update	3 of 22	86.609%																																	
Other Servers	0 of 71	100.000%																																	
Total	Outages	Availability																																	
Overall Service Availability	6 of 339	98.612%																																	
mephesto.internal.opennms.com has 1 alarm (18 hours)		Resource Graphs																																	
two-rr-nc-2-la-ca has 2 alarms (18 hours)		<input type="text"/> <input type="button" value="Search"/>																																	
stanford.internal.opennms.com has 1 alarm (23 hours)		KSC Reports																																	
uglybob.internal.opennms.com has 1 alarm (2 days)		No KSC reports defined																																	
atlgate has 2 alarms (2 days)		<input type="text"/> <input type="button" value="Search"/>																																	
cartman.internal.opennms.com has 1 alarm (2 days)		Grafana Dashboards																																	
timmy.internal.opennms.com has 1 alarm (2 days)		<ul style="list-style-type: none">CPU/LoadDatabase ServersOpenNMSOverviewPerformance Dashboard																																	
Nodes with Outages																																			
mephesto.internal.opennms.com (18 hours)																																			
two-rr-nc-2-la-ca (18 hours)																																			
stanford.internal.opennms.com (23 hours)																																			
uglybob.internal.opennms.com (2 days)																																			
modaniels.internal.opennms.com (4 days)																																			

Özgür yazılım veya açık kaynak modeli altında geliştirilen, kurumsal düzeyde bir ağ izleme ve ağ yönetim platformudur. Tek bir sunucudan on binlerce cihazı yönetmek ve bir sunucu kümesi kullanarak sınırsız cihazları yönetmek için tasarlanmıştır. OpenNMS, ağ cihazlarını operatör müdahalesi olmadan otomatik olarak yapılandırmak ve yönetmek için bir keşif motoru içerir. Java ile yazılmış ve GNU Genel Kamu Lisansı altında yayınlanmıştır. [15]

Bir ağ platformu olarak, birkaç ana özellik kategorisi sunar:

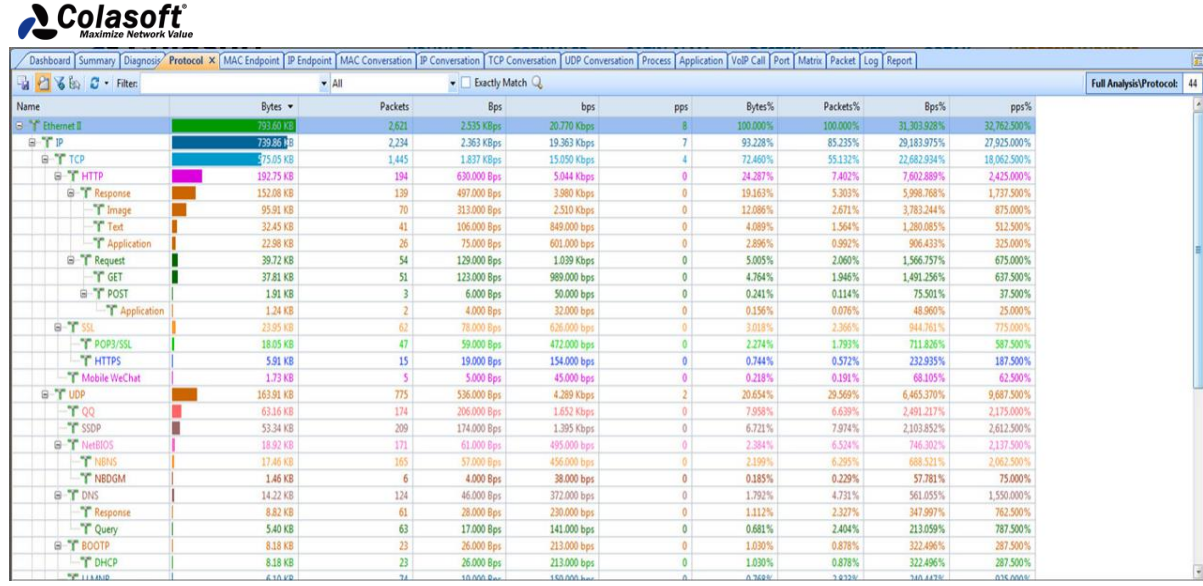
- Keşif - ağınızda hangi donanımın bulunduğunu bulma ve veri tabanına ekleme
- İzleme - ağa bağlı ekipmanın durumunu takip etmek
- Olaylar - bildirim alma, ilişkilendirme ve gönderme
- Veri Toplama - mevcut çeşitli veri noktalarının toplanması, depolanması ve raporlanması.

2.10 Bandwidth Monitor



Bandwidth Monitor programı, Windows bilgisayarlarda gerçekleşen ağ işlemlerini takip etmek için kullanabileceğimiz ücretsiz ölçüm araçları arasında yer almaktadır ve program sayesinde ne kadar verinin indirildiğini ya da internete gönderildiğini görebiliyorsunuz. Bu aracımız İnternet kullanımını sürekli ekranda göstermektedir. Ayrıca URL alma,E-posta bilgi servisi,Ping,Traceroute,UpnP NAT araçlarınınıda içinde barındırmaktadır.Bandwidth Monitor programı, programın içerisinde olan bitenleri kontrol etmek isterseniz varolan raporlama aracını da kullanabilir ve böylece tüm işlemleri daha sonra da kontrol edebilme imkanı sunmaktadır.[16]

2.11 Capsa Free Network Analyzer



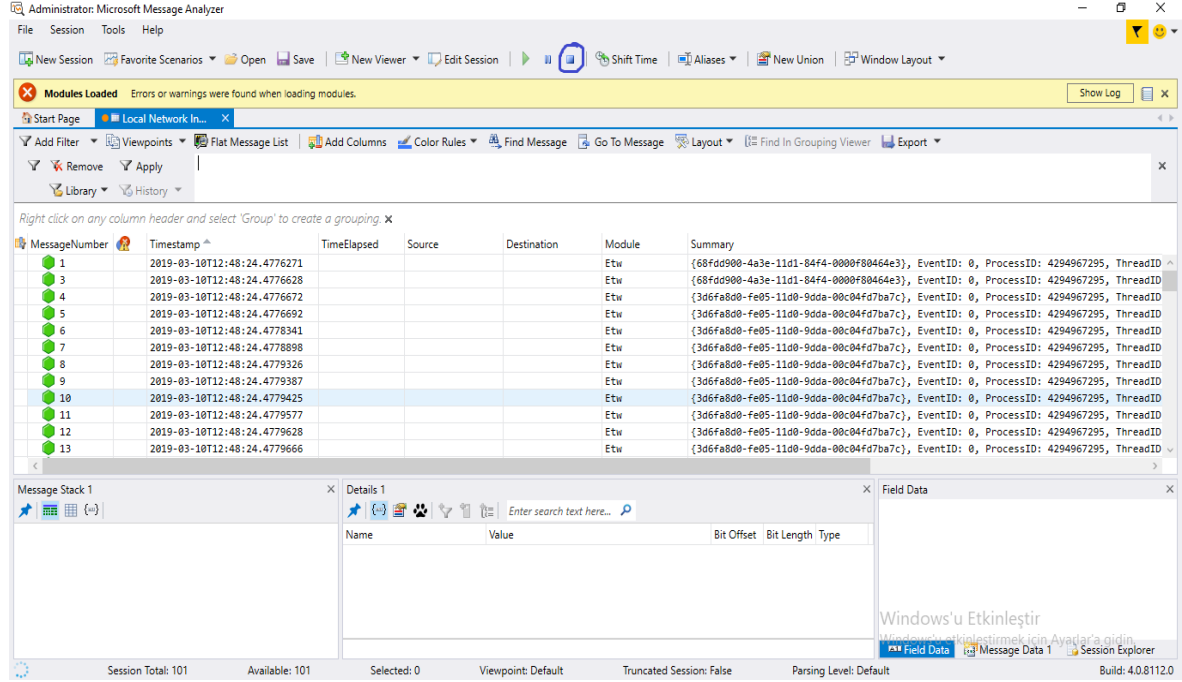
The image shows the Colasoft Capsa Free Network Analyzer interface. The top menu bar includes Dashboard, Summary, Diagnosis, Protocol, MAC Endpoint, IP Endpoint, MAC Conversation, IP Conversation, TCP Conversation, UDP Conversation, Process, Application, VoIP Call, Port, Matrix, Packet, Log, and Report. The main window displays a table of network traffic analysis results. The table has columns for Name, Bytes, Packets, Bps, pps, Bytes%, Packets%, Bps%, and pps%. The data is organized into a tree view on the left, showing various protocols and their sub-protocols. The table lists various network protocols and their associated traffic statistics, including Ethernet II, IP, TCP, HTTP, Response, Image, Text, Application, Request, GET, POST, SSL, POP3/SSL, HTTPS, Mobile WeChat, UDP, QQ, SSDP, mDNS, NBNS, NBNS, DNS, Response, Query, BOOTP, and DHCP.

Name	Bytes	Packets	Bps	pps	Bytes%	Packets%	Bps%	pps%
Ethernet II	791.60 KB	2,621	2,525 Kbps	20,770 Kpps	8	100.00%	100.00%	31,303.828%
IP	729.24 KB	2,234	2,363 Kbps	19,363 Kpps	7	92.22%	85.23%	29,183.975%
TCP	715.05 KB	1,445	1,877 Kbps	15,050 Kpps	4	72.46%	55.13%	22,682.894%
HTTP	192.75 KB	194	630.000 Bps	5,044 Kpps	0	24.28%	7.402%	7,602.889%
Response	152.08 KB	139	497.000 Bps	3,980 Kpps	0	19.16%	5.303%	5,998.768%
Image	95.91 KB	70	313.000 Bps	2,510 Kpps	0	12.08%	2.671%	3,783.244%
Text	32.45 KB	41	106.000 Bps	849.000 bps	0	4.08%	1.564%	1,280.085%
Application	22.98 KB	26	75.000 Bps	601.000 bps	0	2.89%	0.992%	906.433%
Request	39.72 KB	54	129.000 Bps	1,039 Kpps	0	5.00%	2.060%	1,566.757%
GET	37.81 KB	51	123.000 Bps	989.000 bps	0	4.76%	1.946%	1,491.256%
POST	1.91 KB	3	6.000 Bps	50.000 bps	0	0.24%	0.114%	75.501%
Application	1.24 KB	2	4.000 Bps	32.000 bps	0	0.15%	0.076%	48.960%
SSL	23.95 KB	62	78.000 Bps	626.000 bps	0	3.01%	2.366%	944.761%
POP3/SSL	18.05 KB	47	59.000 Bps	472.000 bps	0	2.27%	1.793%	711.826%
HTTPS	5.91 KB	15	19.000 Bps	154.000 bps	0	0.74%	0.572%	232.935%
Mobile WeChat	1.73 KB	5	5.000 Bps	45.000 bps	0	0.21%	0.191%	68.105%
UDP	163.91 KB	775	536.000 Bps	4,289 Kpps	2	20.65%	29.569%	6,465.370%
QQ	63.16 KB	174	206.000 Bps	1,652 Kpps	0	7.95%	6.639%	2,491.217%
SSDP	53.34 KB	209	174.000 Bps	1,395 Kpps	0	6.72%	7.974%	2,103.852%
mDNS	18.92 KB	171	61.000 Bps	495.000 bps	0	2.38%	6.524%	746.302%
NBNS	17.46 KB	165	57.000 Bps	456.000 bps	0	2.19%	6.295%	688.521%
NBNS	1.46 KB	6	4.000 Bps	38.000 bps	0	0.18%	0.229%	57.781%
DNS	14.22 KB	124	46.000 Bps	372.000 bps	0	1.79%	4.731%	561.055%
Response	8.82 KB	61	28.000 Bps	230.000 bps	0	1.11%	2.327%	347.997%
Query	5.40 KB	63	17.000 Bps	141.000 bps	0	0.68%	2.404%	213.059%
BOOTP	8.18 KB	23	26.000 Bps	213.000 bps	0	1.03%	0.878%	322.496%
DHCP	8.18 KB	23	26.000 Bps	213.000 bps	0	1.03%	0.878%	322.496%
LLDP	4.15 KB	74	16.000 Bps	130.000 bps	0	0.50%	1.812%	740.443%

Colasoft capsa free programı ağ trafiğini gözetleme ve inceleme uygulaması olarak çalışan ve ağ analizini kullanıcılara kolay halle getiren bir uygulamadır. Hata raporları, toplam trafik, paket büyüklüğü dağılımı, uzak ve yerel IP adreslerinin sayısı, veri bağlantısı, ağ, ulaşım ve sunum katmanları, DNS sorguları ve yanıtları, SMTP ve POP3 bağlantıları gibi detayları içeren özet raporları görüntüleyebilmemizi sağlar .Ve bu sayede ağda oluşan sorunları blmada ve güvenliğini sağlamada kullanıcılara kolaylık sağlamış oluyor. Yükleme işlemi oldukça yumuşaktır ve sarma işlemi, iki sekme üzerine kurulu, biri adaptör durumunun grafiksel bir gösterimini görüntülemenizi sağlarken diğeri paket dosyaları CAP, BFR , TRC0, PKT , 5VW, RAWPKT ve CSCPKT eklemenize yardımcı olur. Programı online kayıt olarak ücretsiz bir şekilde kullanıma sunuluyor ancak bu version bize sadece 50 node desteği sunabiliyor. Bu program bize aşağıdaki işlemleri yapmamıza olanak sağlıyor.

- DDoS ataklarını, worm aktivitelerini, ARP saldırılarını ve diğer şüpheli konularda tespit yapabiliyor. Ağ trafiği ve bant genişliğini gözleyebiliyor.300'den fazla protokolü desteklemektedir.[17]
- HTTP, E-posta, DNS, FTP, MSN ve Yahoo! Messenger trafiklerini inceleyebiliyor. Ağdaki tüm hostları detaylarıyla listeleyebilmektedir.
- Ağ sorunlarını otomatik olarak tespit ederek çözümler önermekteAğı görsel olarak göstermekte ve trafiği ortaya koymaktadır. Bu özelliklere ek olarak irili ufaklı pek çok başka yetenek de programda mevcut. Colasoft Capsa Free özellikle ufak çaptaki ağlarda çalışmalar yapmak isteyenler veya ağ trafiği yönetimini öğrenmek isteyen öğrenciler tarafından kolaylıkla kullanılabilir.[18]

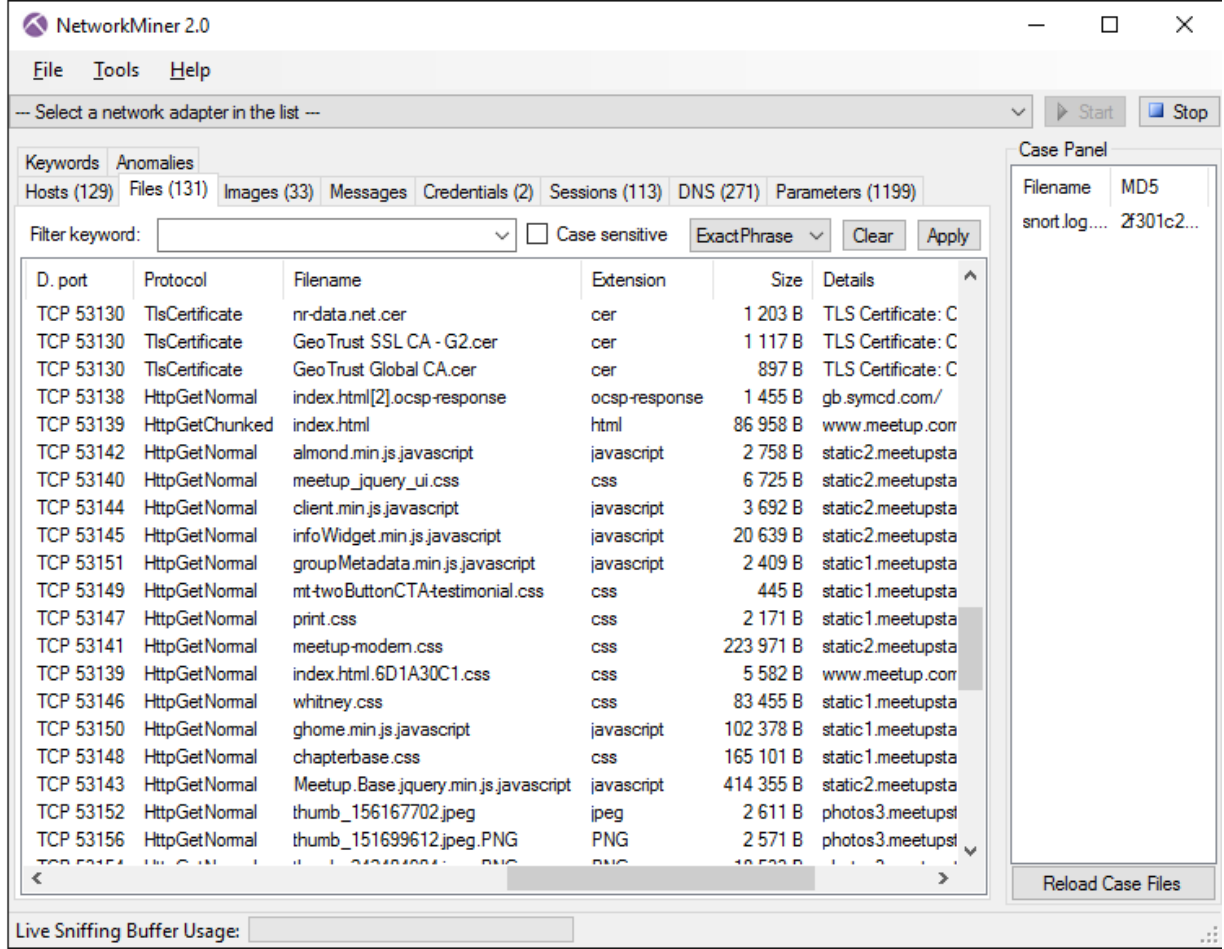
2.12 Microsoft Message Analyzer



Microsoft'un Network Monitor yazılımı istemci ve sunucularda ağ trafiğini izlememizi kolaylaştıran bir araçtır. İstemci ve sunucuların ağ trafiğini inceleyerek detaylı rapor çıkarabilmektedir.

Canlı olarak ağ kartının trafiğini dinleyen Message Analyzer'ı aynı ağdaki başka bir istemci ya da sunucuları izlemek için de kullanılabilir. Ağ trafiğini canlı olarak izlemek dışında farklı kaynaklardan alınmış ağ trafik izleme raporlarını (ETL dosyalarını) açma, Azure bulut yapınıza bağlanma, Olay günlüklerini analiz etme, powershell bağlantısı sağlama, sql server da yer alan tablolardaki bilgileri getirme gibi birçok işlevi de mevcuttur.[19]

2.13 NetworkMiner

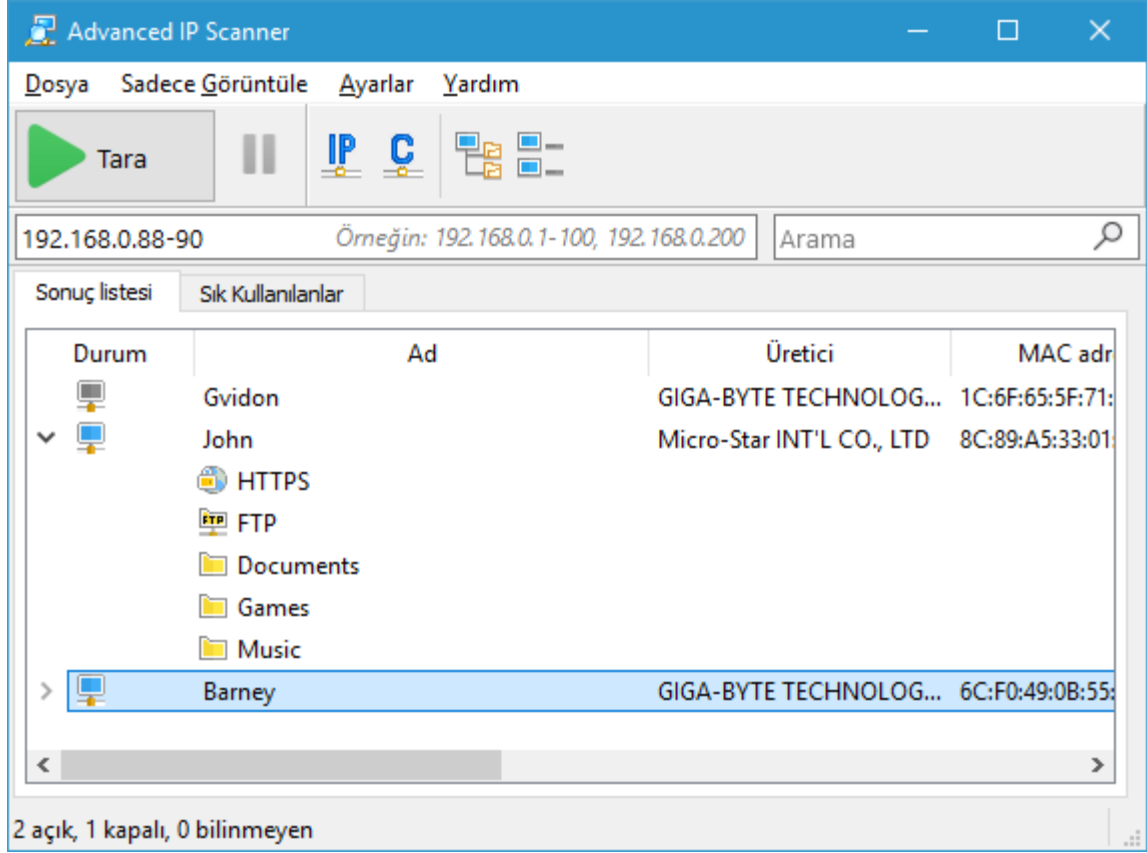


NetworkMiner, Windows için açık kaynaklı bir Ağ Adli Analiz Aracıdır (NFAT) (ayrıca Linux / Mac OS X / FreeBSD'de de çalışır). NetworkMiner, işletim sistemlerini, oturumları, ana bilgisayar adlarını, açık portları vb. Tespit etmek için ağ üzerinde trafik çekmeden pasif bir ağ dinleyicisi / paket yakalama aracı olarak kullanılabilir. NetworkMiner, çevrimdışı analiz için PCAP dosyalarını ayrıştırabilir ve iletilen dosyaları ve sertifikaları PCAP dosyalarından yeniden oluşturabilir / yeniden birleştirebilir.[20]

NetworkMiner, sezgisel bir kullanıcı ara yüzünde çıkarılan eserler sağlayarak gelişmiş Ağ Trafik Analizi (NTA) gerçekleştirmeyi kolaylaştırır. Verilerin sunulması sadece analizi kolaylaştırmakla kalmaz, aynı zamanda analist veya adli araştırmacı için de zaman kazandırır.

NetworkMiner, 2007'deki ilk sürümünden bu yana, olay müdahale ekipleri ve kanun uygulayıcıları arasında popüler bir araç haline geldi. NetworkMiner bugün tüm dünyadaki şirketler ve organizasyonlar tarafından kullanılmaktadır.

2.14 Advanced IP Scanner



Advanced IP Scanner sisteminiz üzerinde ayrıntılı bir IP taraması yapan ve IP numarasının hangi yerel ağda olduğunu inceleyerek sizi bilgilendiren ücretsiz ve başarılı bir yazılımdır.[21] Özellik olarak;

- Saniyeler içerisinde tüm ağı tarar
- Herhangi bir ağ aygıtını algılar
- Ağ paylaşımlarına kolay erişim sağlar
- MAC adresleri tespiti
- HTTP, HTTPS, FTP ve paylaşılan klasörleri bulur
- Ağ bilgisayarlarını uzaktan açma/kapatma
- Kolay ağ yönetimi için sık kullanılanlar listesi
- HTML veya CSV olarak dışa aktarma
- Kolay ve kullanıcı dostu ara yüz, özelliklerine sahiptir.

2.15 Zenoss Core

The screenshot displays the Zenoss Core web interface. The top navigation bar includes links for DASHBOARD, EVENTS, INFRASTRUCTURE, REPORTS, and ADVANCED. The user is logged in as 'gameday' and can click 'SIGN OUT'. Below the navigation bar, there's a sub-navigation bar with 'Event Console', 'History', 'Event Classes', and 'Event Manager'. The main content area shows a table of events with columns for Status, Severity, Device, Component, Event Class, Summary, First Seen, Last Seen, and Count. The table lists various events from different Amazon EC2 instances, mostly with a status of '0' (warning) and a severity of 'Warning'. One event is highlighted in blue, showing a status of '1' (error) and a severity of 'Error'. This event is for a MySQL component on a device 'ec2-184-72-248-3.compute-1.amazonaws.com'. A detailed view of this event is shown in a pop-up window, displaying the device name, component (MySQL), event class (/App/MySQL), status (0), start time (2010/07/19 23:51:34.000), stop time (2010/07/21 13:04:05.000), and count (426). The pop-up window also shows a 'prodState' of 1000 and a 'stateChange' of 2010/07/21 13:04:05.000.

Status	Severity	Device	Component	Event Class	Summary	First Seen	Last Seen	Count
0	Warning	ec2-184-73-113-182.compute-1.amazonaws.com		/Status/Ping	ip 184.7: 2010-07-20 16:34:46	2010-07-21 13:04:51	1231	
0	Warning	ec2-204-236-181-187.us-west-1.compute.amazonaws.com		/Status/Ping	ip 204.2: 2010-07-19 23:51:37	2010-07-21 13:02:51	1464	
0	Warning	ec2-184-72-2-67.us-west-1.compute.amazonaws.com		/Status/Ping	ip 184.7: 2010-07-19 23:51:37	2010-07-21 13:02:51	1464	
0	Warning	ec2-184-72-10-82.us-west-1.compute.amazonaws.com		/Status/Ping	ip 184.7: 2010-07-19 23:51:37	2010-07-21 13:02:51	1464	
0	Warning	ec2-72-44-61-32.compute-1.amazonaws.com		/Status/Ping	ip 72.44: 2010-07-19 20:50:40	2010-07-21 13:02:51	1464	
0	Warning	ec2-184-72-248-1.compute-1.amazonaws.com		/Status/Ping	ip 184.7: 2010-07-19 23:50:37	2010-07-21 13:02:51	1464	
0	Warning	ec2-184-72-248-3.compute-1.amazonaws.com		/Status/Ping	ip 184.7: 2010-07-19 23:50:37	2010-07-21 13:02:51	1464	
0	Warning	ec2-184-73-113-182.compute-1.amazonaws.com	http	/Status/IpService	IP Servit 2010-07-19 20:48:53	2010-07-20 16:35:01	64	
0	Warning	ec2-72-44-61-32.compute-1.amazonaws.com	http	/Status/IpService	IP Servit 2010-07-19 20:50:53	2010-07-19 20:50:53	1	
1	Error	ec2-184-72-248-3.compute-1.amazonaws.com	MySQL	/App/MySQL	Comma: 2010-07-19 23:51:34	2010-07-21 13:04:05	426	
0	Warning	ec2-184-73-113-182.compute-1.amazonaws.com	zer					
0	Warning	ec2-72-44-61-32.compute-1.amazonaws.com	zer					
0	Warning	ec2-184-73-113-182.compute-1.amazonaws.com	zer					
0	Warning	ec2-184-72-248-3.compute-1.amazonaws.com	zer					
0	Warning	ec2-204-236-181-187.us-west-1.compute.amazonaws.com	zer					
0	Warning	ec2-184-72-2-67.us-west-1.compute.amazonaws.com	zer					
0	Warning	ec2-184-72-10-82.us-west-1.compute.amazonaws.com	zer					
0	Warning	ec2-184-72-248-1.compute-1.amazonaws.com	zer					
0	Warning	ec2-184-73-113-182.compute-1.amazonaws.com	zer					
0	Warning	ec2-72-44-61-32.compute-1.amazonaws.com	zer					
0	Warning	ec2-184-73-113-182.compute-1.amazonaws.com	zer					
0	Warning	ec2-184-72-2-67.us-west-1.compute.amazonaws.com	api					
0	Warning	ec2-204-236-181-187.us-west-1.compute.amazonaws.com	zer					
0	Warning	ec2-184-72-248-1.compute-1.amazonaws.com	zer					
0	Warning	ec2-184-72-2-67.us-west-1.compute.amazonaws.com	zer					

Command timed out on device ec2-184-72-248-3.compute-1.amazonaws.com:

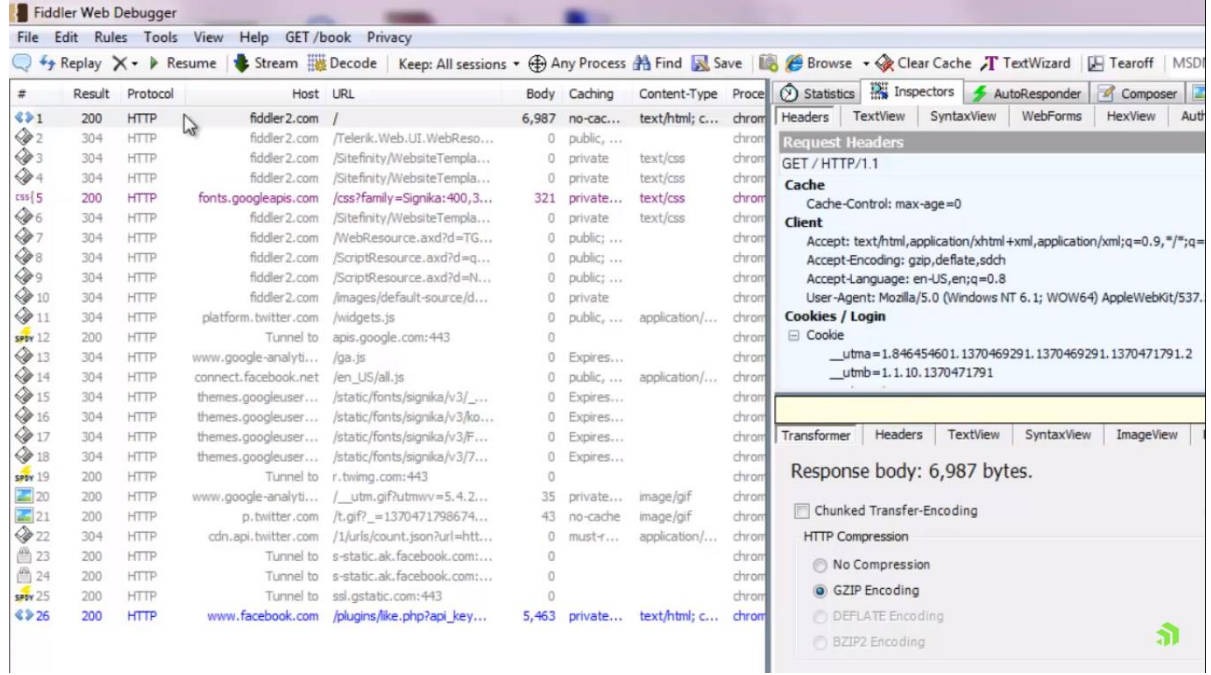
Device: ec2-184-72-248-3.compute-1.amazonaws.com
Component: MySQL
Event Class: /App/MySQL
Status: 0
Start Time: 2010/07/19 23:51:34.000
Stop Time: 2010/07/21 13:04:05.000
Count: 426

Hide details

prodState: 1000
stateChange: 2010/07/21 13:04:05.000

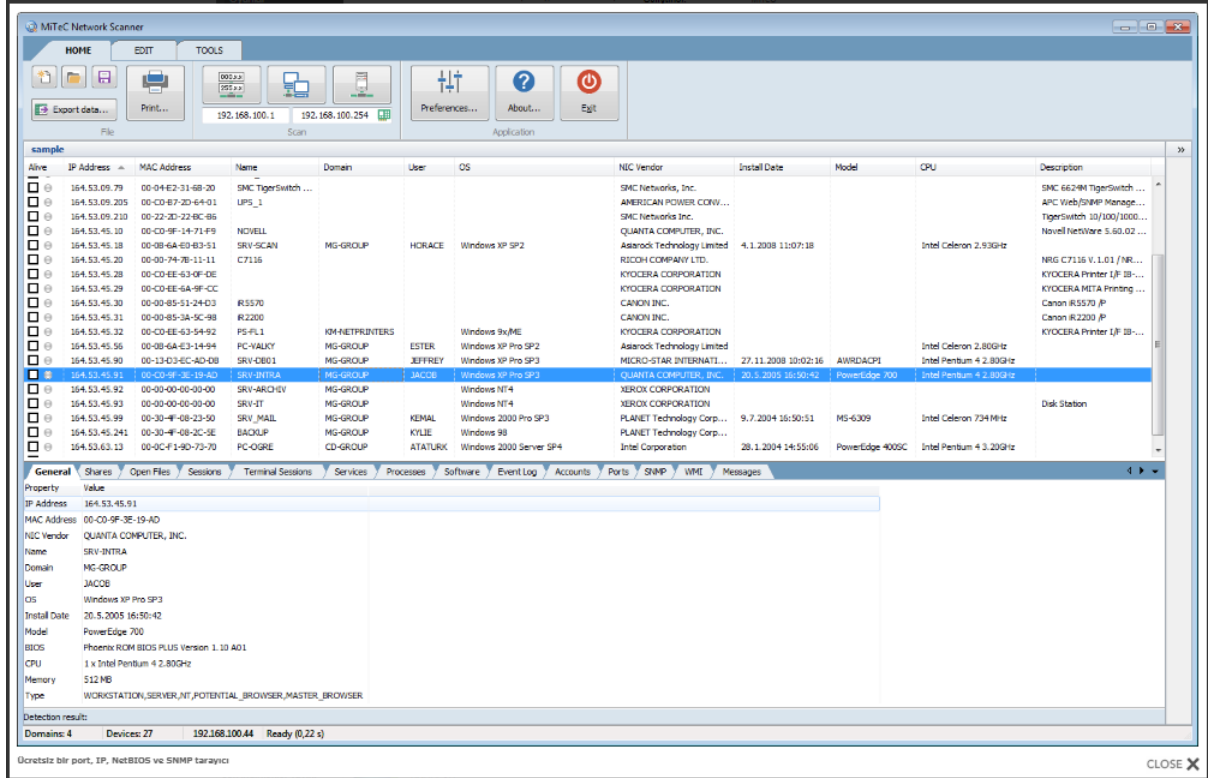
Zenoss core açık kaynaklı bir ağ dinleme aracıdır. Çekirdek, ağ cihazlarının ve ağ servislerinin kullanılabilirliğini izler ve Microsoft Windows dahil ana bilgisayar kaynak işletim sistemlerinde kullanılır. Servis Dynamics ve ZaaS izleme yeteneklerinden yoksun olan bu ağ dinleme aracı kullanıcı hesaplarını sınırlar. Ağ dinlemenin yanında sistemin performansını ve yapılandırmayı web ara yüzünde kullanıcıya sunar.[22]

2.16 Telerik Fiddler



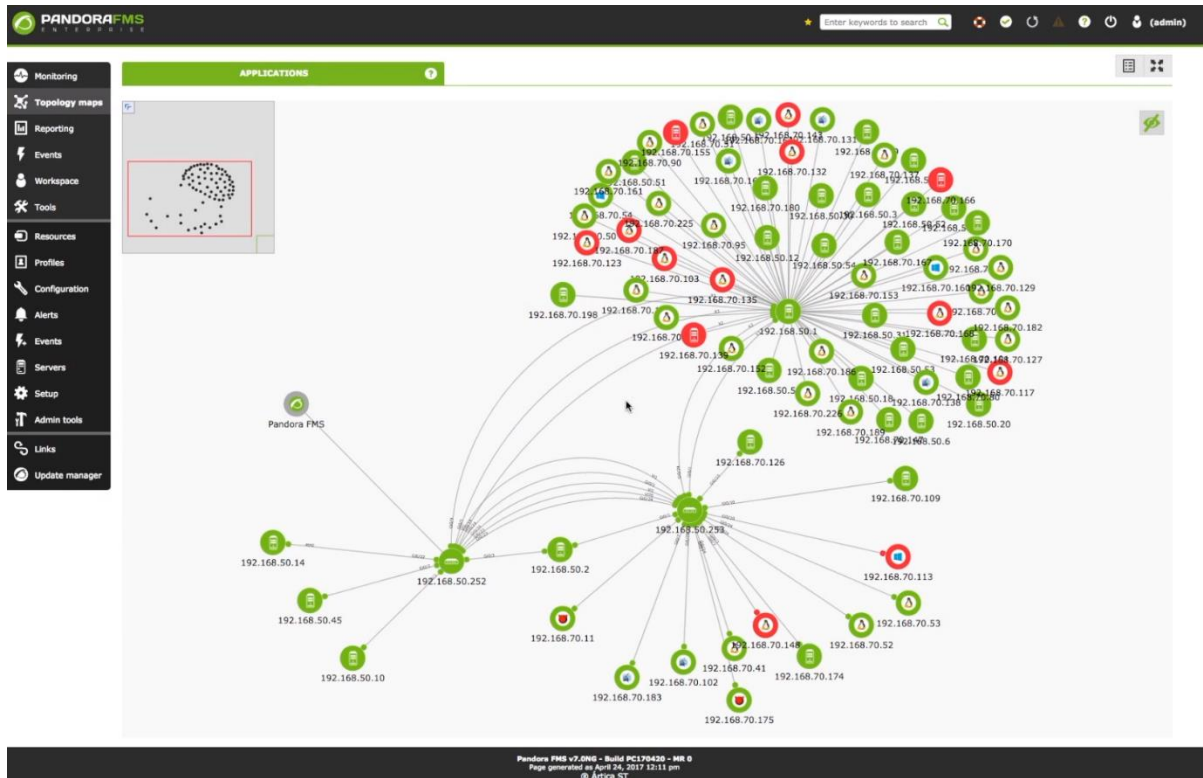
Fiddler, bilgisayar ve internet arasındaki tüm web trafiğini takip eden ve detaylı bir şekilde analiz yapmamızı sağlayan ücretsiz bir http debugging (Hata Ayıklama) programıdır. Bu program, http trafiğini incelememize, kırılma noktalarını ayarlamamıza ve bilgisayarımıza gelen veriler ve çıkan veriler üzerinde oynamalar yapmamıza olanak sağlar. Fiddler'in çok daha basit bir kullanımı vardır. Explorer, Google Chrome, Apple Safari, Mozilla Firefox, Opera vs. tüm browserlarda çalışır. Ayrıca Windows Phone, iPod/iPad, gibi cihazlarda da kullanılabilir. Yapısal olarak JScript.NET kodlama alt sistemini içermektedir. [23]

2.17 MiTeC Network Scanner



Birçok gelişmiş özelliğe sahip çok iş parçacıklı bir bağlantı noktası ICMP, NetBIOS, Port, IP, ActiveDirectory ve SNMP tarayıcısıdır. ağ cihazlarını ve özelliklerini taramak ve raporlamak için çeşitli yollar sunan taşınabilir ve ücretsiz bir araç olan MiTeC programda ping taraması gerçekleştirir, açılan TCP ve UDP portlarını, kaynak paylaşımlarını ve hizmetleri tarar. Ayrıca MiTeC ağ tarayıcısı active directory'yi otomatik olarak tarayabilir. Kendi başına tarama işlemi fazla zaman almaz. Uygulama MAC adresi, isim, etki alanı, kullanıcı, işletim sistemi, CPU ve açıklama gibi diğer yararlı detayların her IP adresini gösterir.[24]

2.18 Pandora FMS



Pandora FMS, büyük network ortamları için hazır araçlar içeren performans ve kullanılabilirlik izleme sistemi yazılımıdır. Yerel izleme maddeleri kullanır. Linux Ajanlar, Windows, AIX, HP-UX, Solaris ve BSD sistemlerde işletim sistemlerin de çalışır. Uzak ağ izleme (SNMP v3, TCP çekler, uzak WMI prob ...) protokollerini destekler.[25]

Yüksek derecede ölçeklenebilir, tamamen web tabanlı ve multitenant arabirimi (tek sunucu ile 2000'e kadar düğüm desteği). Çok esnek ACL sistemi ve grafik raporları ve kullanıcı-tanımlı kontrol ekranları ile kullanımı çok kolaydır.

- Pandora FMS, yönlendiricinizi / anahtarını SNMP üzerinden sorgulayarak veya yönlendiricinizin gönderdiği Netflow istatistiklerini işleyerek ağınızın bant genişliğini ölçebilir.[26]
- Pandora FMS, ile bir cihazı birkaç tıklamayla yapılandırabilir ve bant genişliği ara yüzünü, durumunu, yük ortalamasını, depolama alanını, bellek kullanımını ve diğer birçok şeyi izleyebilirsiniz.

2.19 Windump

```
reading from file winpractice.txt, link-type EN10MB (Ethernet)
16:49:48.486263 IP 172.20.42.32.1171 > cisco.csn.edu.80: S 3052711201:3052711201(0) win 65535 <m
ss 1460,nop,nop,sackOK>
16:49:48.584168 IP 172.20.42.32.1172 > cisco.csn.edu.80: S 3052783489:3052783489(0) win 65535 <m
ss 1460,nop,nop,sackOK>

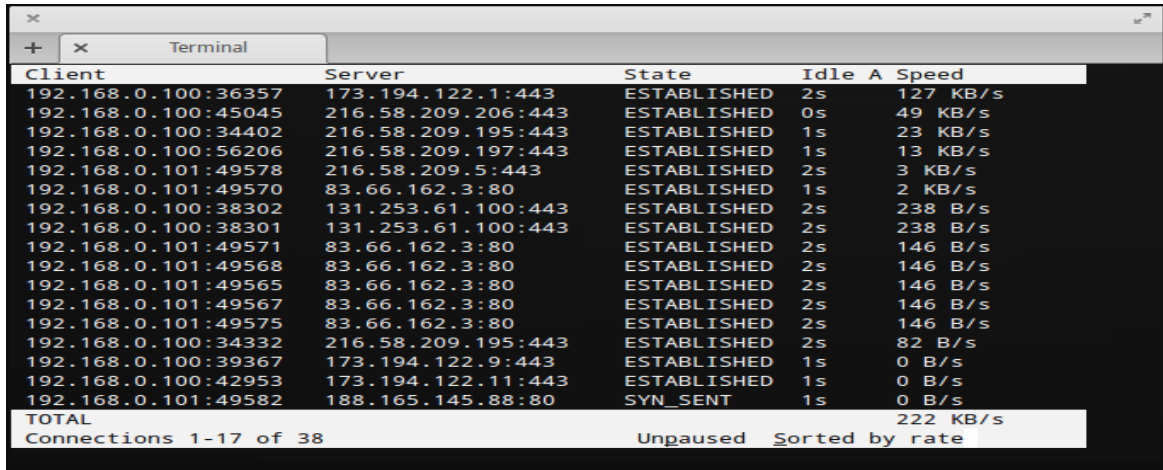
C:\Users\Owner\Documents\School\Fall2016>windump.exe -r winpractice.txt tcp[13]==16
reading from file winpractice.txt, link-type EN10MB (Ethernet)
16:49:46.066361 IP 172.20.42.32.1093 > 172.20.42.63.139: . ack 3763894567 win 64817
16:49:48.486555 IP 172.20.42.32.1171 > cisco.csn.edu.80: . ack 99587050 win 65535
16:49:48.584412 IP 172.20.42.32.1172 > cisco.csn.edu.80: . ack 99647816 win 65535
16:49:48.761387 IP 172.20.42.32.1171 > cisco.csn.edu.80: . ack 1039 win 64497
16:49:48.761438 IP 172.20.42.32.1172 > cisco.csn.edu.80: . ack 564 win 64972
16:49:49.062374 IP 172.20.42.32.1171 > cisco.csn.edu.80: . ack 1602 win 65394
16:49:49.062435 IP 172.20.42.32.1172 > cisco.csn.edu.80: . ack 1127 win 64409

C:\Users\Owner\Documents\School\Fall2016>windump.exe -r winpractice.txt tcp[13]==16 and less 300
reading from file winpractice.txt, link-type EN10MB (Ethernet)
16:49:46.066361 IP
```

Windump ,Tcpdump’ın altında çalışan, işlevselliği ve performansı test etmeyi sağlayan windows tabanlı bir araçtır. Windump programı protokol ve ağ güvenliğinin analizini yapan windows ve Unix işletim sistemlerinde çalışan paket yakalama, dosya çıktılarını analiz etme ve şifreli ağ trafiğini deşifre etmeye yarar. Windump’ın aşağıda bazı özellikleri yer almaktadır.[27]

- Ağ bağdaştırıcılarının listesini alma imkanı sağlar.
- Unix ‘deki gibi kesin standartları tanımlı olmadığı için windows ta adaptör adlarını kullanmak zordur bunun için bunların her birinin açıklamasını yapar.

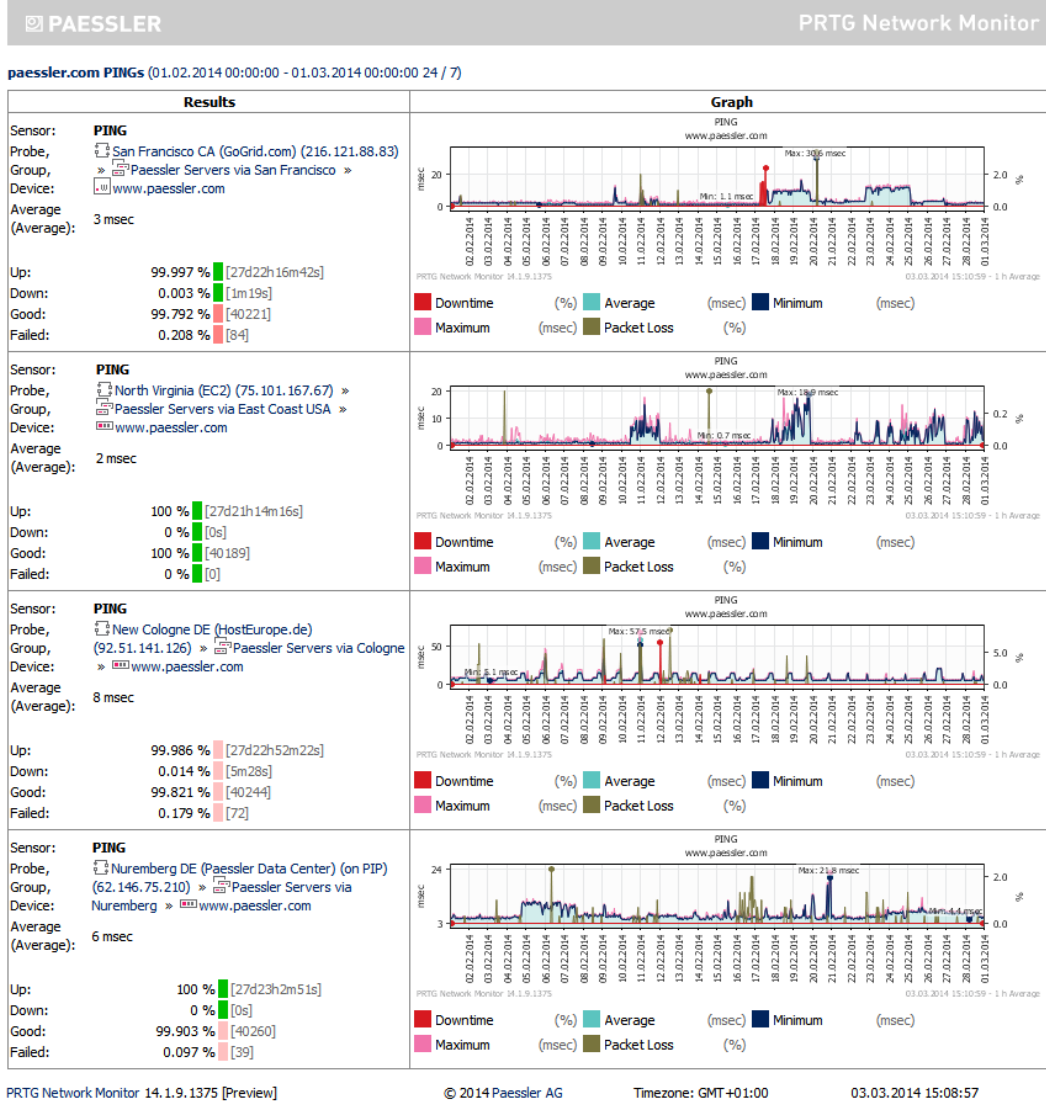
2.20 Tcptrack



Client	Server	State	Idle	A	Speed
192.168.0.100:36357	173.194.122.1:443	ESTABLISHED	2s		127 KB/s
192.168.0.100:45045	216.58.209.206:443	ESTABLISHED	0s		49 KB/s
192.168.0.100:34402	216.58.209.195:443	ESTABLISHED	1s		23 KB/s
192.168.0.100:56206	216.58.209.197:443	ESTABLISHED	1s		13 KB/s
192.168.0.101:49578	216.58.209.5:443	ESTABLISHED	2s		3 KB/s
192.168.0.101:49570	83.66.162.3:80	ESTABLISHED	1s		2 KB/s
192.168.0.100:38302	131.253.61.100:443	ESTABLISHED	2s		238 B/s
192.168.0.100:38301	131.253.61.100:443	ESTABLISHED	2s		238 B/s
192.168.0.101:49571	83.66.162.3:80	ESTABLISHED	2s		146 B/s
192.168.0.101:49568	83.66.162.3:80	ESTABLISHED	2s		146 B/s
192.168.0.101:49565	83.66.162.3:80	ESTABLISHED	2s		146 B/s
192.168.0.101:49567	83.66.162.3:80	ESTABLISHED	2s		146 B/s
192.168.0.101:49575	83.66.162.3:80	ESTABLISHED	2s		146 B/s
192.168.0.100:34332	216.58.209.195:443	ESTABLISHED	2s		82 B/s
192.168.0.100:39367	173.194.122.9:443	ESTABLISHED	1s		0 B/s
192.168.0.100:42953	173.194.122.11:443	ESTABLISHED	1s		0 B/s
192.168.0.101:49582	188.165.145.88:80	SYN_SENT	1s		0 B/s
TOTAL					222 KB/s
Connections 1-17 of 38					
Unpaused Sorted by rate					

Linux sistemlerde kablolu yada kablosuz ağ arabirimlerine ait TCP bağlantılarının trafiğini izlemek için kullanılan bir paket dinleyicisidir. Belirli bir ağ arabirimindeki bağlantıları pasif olarak izler, durumlarını izler ve bunları Unix 'top' komutuna benzer bir şekilde listeler. Kaynak ve hedef adreslerini, bağlantı noktalarını, bağlantı durumunu, boşa kalma süresini ve bant genişliği kullanımını gösterir. Filtre ifadesi, tcptrack'in göreceği TCP bağlantılarının özelliklerini filtreleyebilen standart bir pcap filtre ifadesidir.[28]

2.21 PRTG Network Monitor

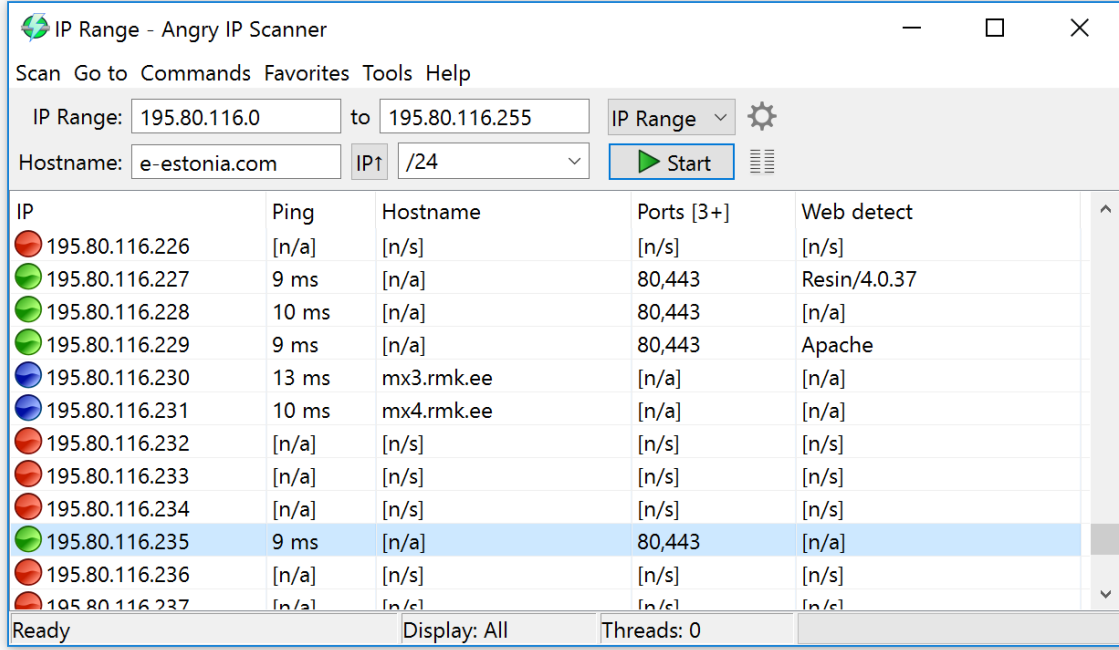


PRTG (Paessler Router Traffic Grapher - Paessler Yönlendirici Trafiği Grafikleyicisi), Windows işletim sistemi üzerinde ağ yöneticileri için hazırlanmış bir gözlemleme (monitoring) yazılımıdır. PRTG temel olarak ağ cihazlarının bant genişliği kullanımını gözlemlemek için kullanılsa da bellek, CPU (Central Processing Unit - Merkezi İşlemci Birimi) değerlerini gözlemlemek için de kullanılabilir. [29]

PRTG'de sık kullanılan sistem, ağ servis ve protokollerini gözlemlemek için (Ping, SMTP (Simple Mail Transfer Protocol - Basit Posta İletim Protokolü), FTP (File Transfer Protocol - Dosya İletim Protokolü) vb.) için 115'ten fazla sensör bulunmaktadır.

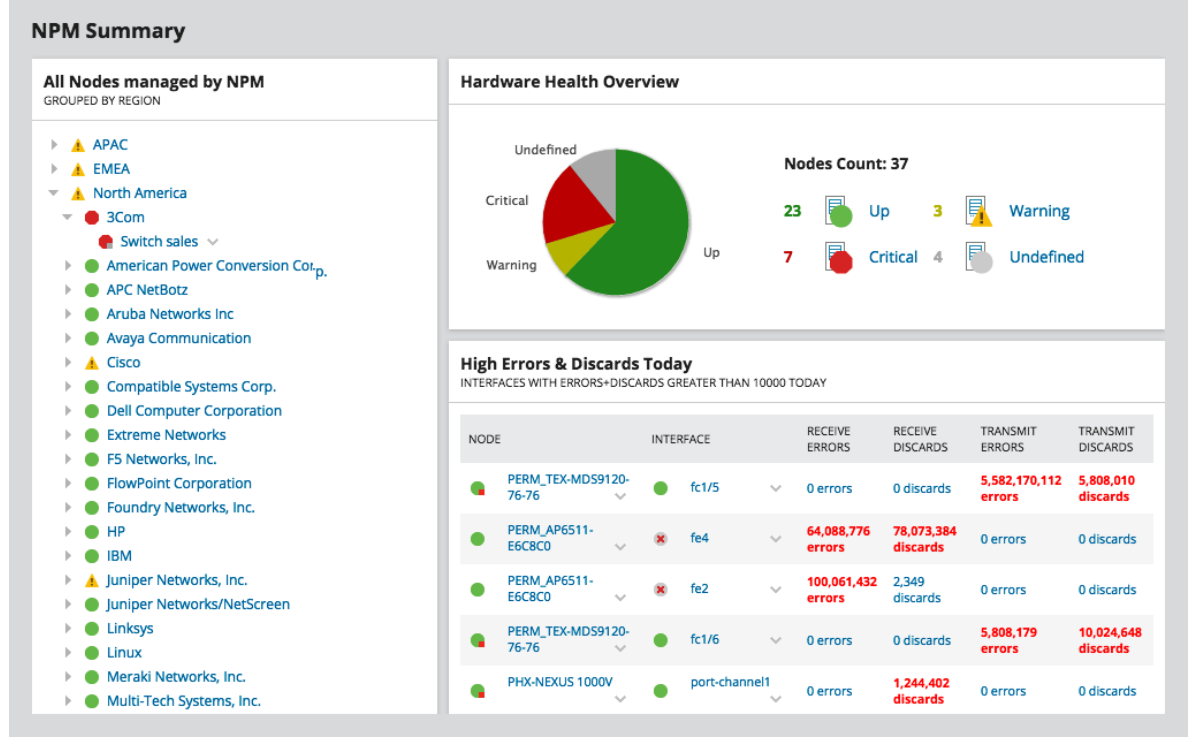
PRTG'de sistemde meydana gelebilecek herhangi bir alarm durumunda kullanıcı e-posta, kısa mesaj, çağrı ya da diğer yöntemlerle uyarılabilir. İstenen zaman aralıklarındaki kayıtlar, sistemin düştüğü zamanlar programın veri tabanına kaydedilerek kullanıcıya sistem hakkında genel bir bakış açısı sağlamaya yardımcı olur. PRTG'nin 9. sürümünden itibaren IPv6 (İnternet Protocol version 6 - İnternet Protokolü versiyon 6) cihazlar da gözlemlenebilmektedir.[30]

2.22 Angry IP Scanner



- Angry IP Scanner çok hızlı bir IP adresi ve port tarayıcıdır.[31]
- Herhangi bir aralıktaki IP adreslerini ve portlarını tarayabilir. Araç olarak ufak kolay kurulumla sahiptir. Herhangi bir kurulum gerektirmeden, serbestçe kopyalanabilir ve herhangi bir yerde kullanılabilir.
- Angry IP Scanner, her IP adresine ping gönderir, daha sonra isteğe bağlı olarak ana bilgisayar adını çözümler, MAC adresini belirler, portları tarar, vb. Her ana bilgisayar hakkında toplanan veri miktarı eklentilerle genişletilebilir.[32]
- Ayrıca NetBIOS bilgileri (bilgisayar adı, çalışma grubu adı ve şu anda Windows kullanıcısına giriş yapmış), favori IP adresi aralıkları, web sunucusu algılama, özelleştirilebilir açıcılar, vb. Gibi ek özelliklere sahiptir.
- Tarama sonuçları CSV, TXT, XML veya IP-Port liste dosyalarına kaydedilebilir. Eklentiler yardımıyla, Angry IP Scanner taranan IP'ler hakkında her türlü bilgiyi toplayabilir.

2.23 SolarWinds NPM



Ağımızda SNMP,WMI,ICMP özelliği açık olan switch ,router gibi tüm cihazların yanıt verme zamanını, kullanılabilirliğini, donanımsal durumlarını ve çalışma zamanlarını görüntüler. Dinamik ağ haritası sayesinde performans istatistiklerini gerçek zamanlı görüntüleme imkanı sunar. Ağ altyapısında problem oluşturmadan önce, ağı tarar, sorunları tespit edip tanımlar. Router, switch, wireless access point, sunucu ve SNMP özelliği açık olan herhangi bir cihaz için gerçek zamanlı, network performans istatistiklerini görüntüler ve analiz eder.

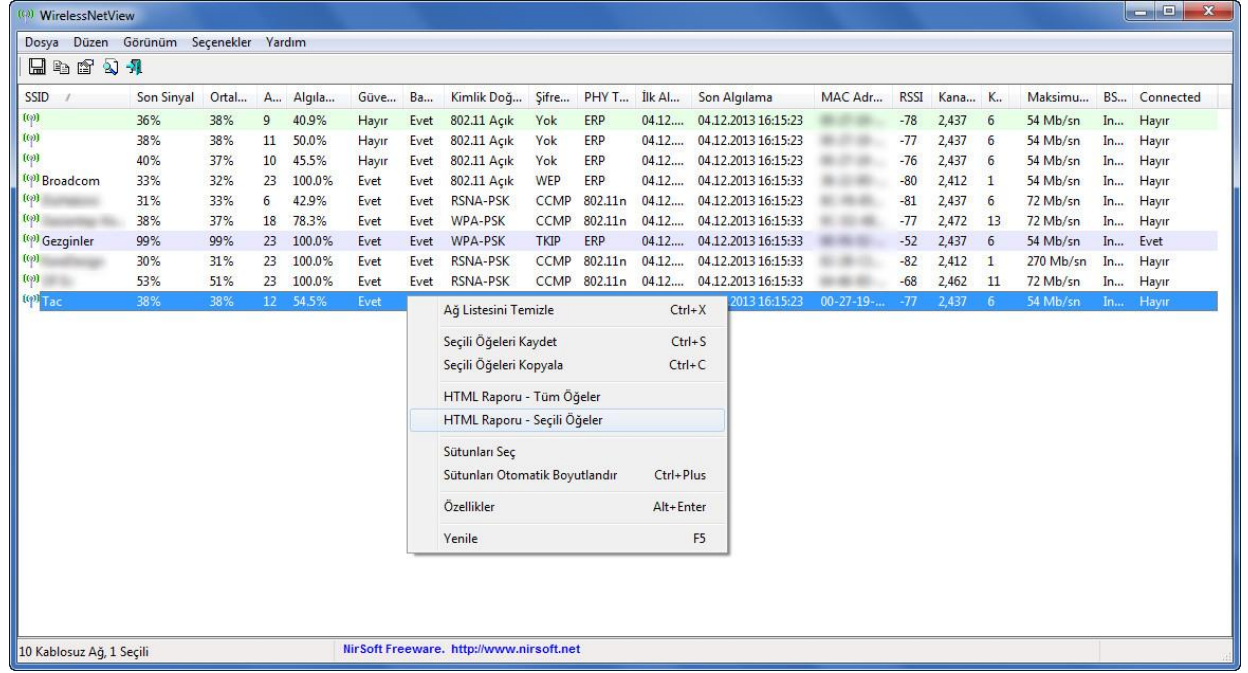
Teknik Özellikleri;

- Ağ kullanılabilirliği ve performans görüntüleme[33]
- Otomatik ağ keşfetme
- Akıllı ağ uyarma
- Ağdaki her türlü cihaza destek Multi-Vendor cihaz desteği
- Hızlı ve pratik ağ konumlandırma

Genel Özellikleri;

- VMware sunucularının performanslarını vCenterdan alır, takip eder ve görüntüler.
- Sanallaştırılmış Cisco Nexus 1000V switchleri görüntüler.
- Cisco Unified Computing System (UCS) bileşenlerinin yönetimini kolaylaştırır.
- Sisteminiz ve cihazlarınız ile ilgili IT hizmetlerinin durumunu hızlı bir şekilde görüntüler.
- Geliştirilmiş alarm sistemine sahiptir.
- Yeni cihazları görüntülemek için size hatırlatmalarda bulunur.
- Geniş ve kurumsal network yapıları için FoE (failover engine), multiple polling engine ve ek web sunucu ölçeklendirmesi yapılabilir.
- NCM, SAM, NTA, IP SLA, IPAM modülleri ile entegre çalışır.
- LUCID (Logical, Usable, Customizable, Interactive, Drill-down) web arayüzüne sahiptir.

2.24 WirelessNetView

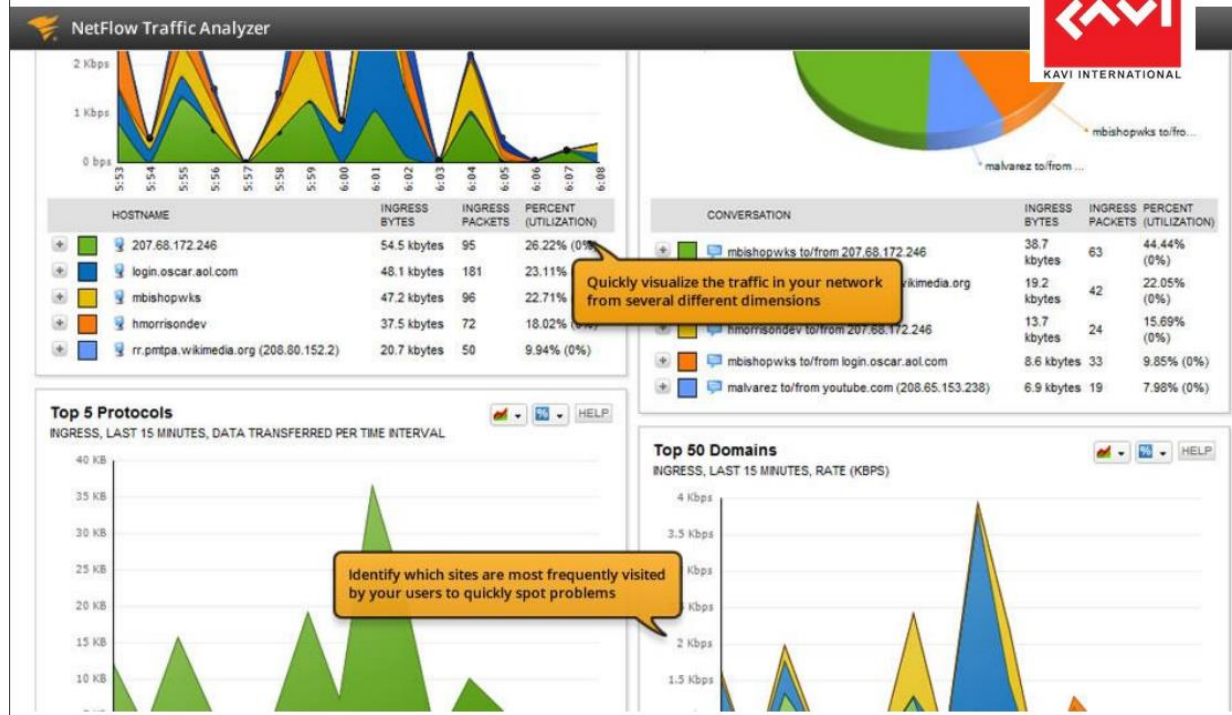


WirelessNetView, küçük boyutlu, arkaplanında çalışan ve kablosuz ağ bağlantılarını takip edip, listelemenize yardımcı olan bir programdır.

WirelessNetView ile ilgili bağlantı noktası hakkında; sinyal şiddeti, şifreleme biçimi, hızı, frekans bandı, kullandığı kanalı, MAC adresi, cihaz üreticisi, ilk ve son görüntülenme zamanı gibi birçok detaylı bilgiyi elde erişim sağlar.[34]

Programı çalıştırdığınızda kablosuz bağlantıları listelemeye başlar ve bu bağlantıları 10'ar dakikalık aralıklarla yeniler.

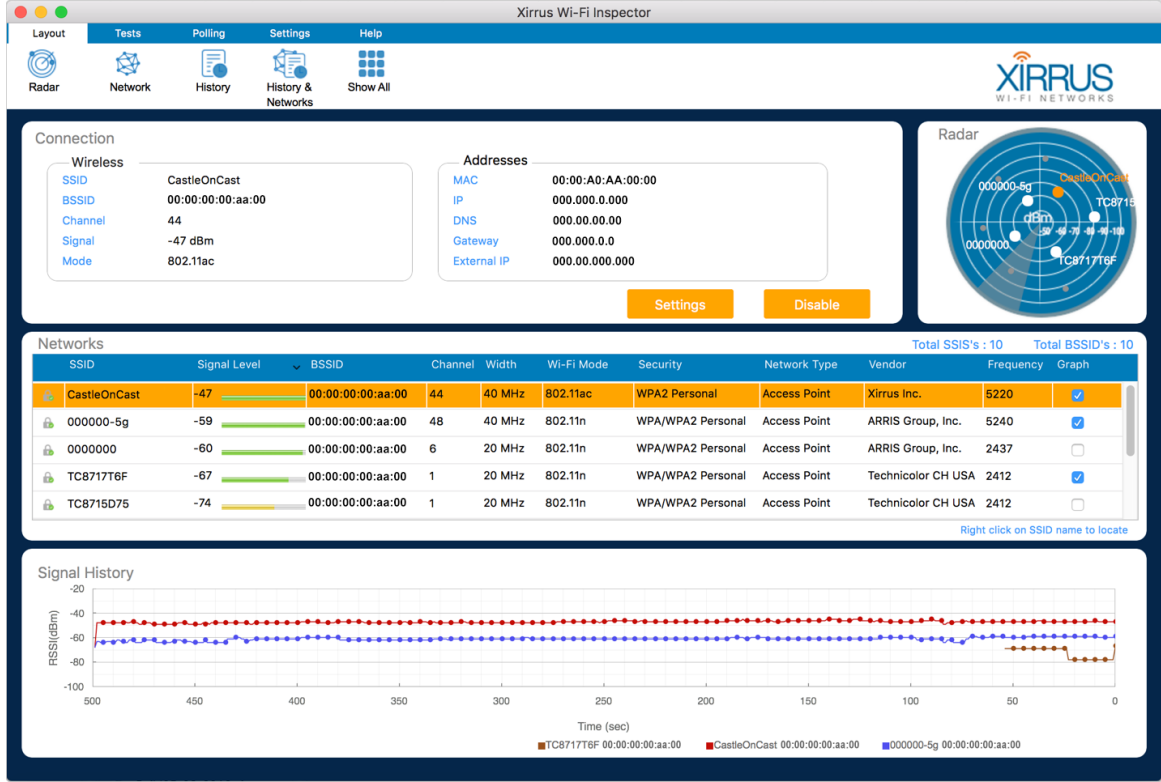
2.25 NetFlow Traffic Analyzer



Cisco tarafından geliştirilen ve IP trafik bilgisini toplayan bir network protokolüdür. Network altyapısında meydana gelen trafiği analiz eder ve anlık olarak izler. NetFlow protokolü aktif olan router ve switch gibi ağ cihazlarında tüm arayüzlerinden IP trafik bilgisini toplayabilirsiniz. Ayrıca NetFlow kayıtları tutup tekrardan bilgilerinizi görüntülemeye yarar. Netflow Traffic Analyzer (NTA), ağındaki sürekli akan trafikten verileri yakalar ve istatistikler sayesinde kontrol etmenizi sağlar. Bu verileri belirli sayılara çevirerek grafik ve tablolara dönüştürür. Daha kurumsal bir ağ yapısı meydana getirmiş olur. Aşağıda da teknik özellikleri yer almaktadır.

- Ağ Analiz Paneli [35]
- Ağdaki Her Türlü Cihaza Destek! Multi-Vendor Cihaz Desteği
- Uygulama Bazlı Bant Genişliği Kullanımı
- Eşik Değeri ile Bant Genişliği Alarm Sistemi
- Hızlı ve Pratik Ağ Konumlandırması

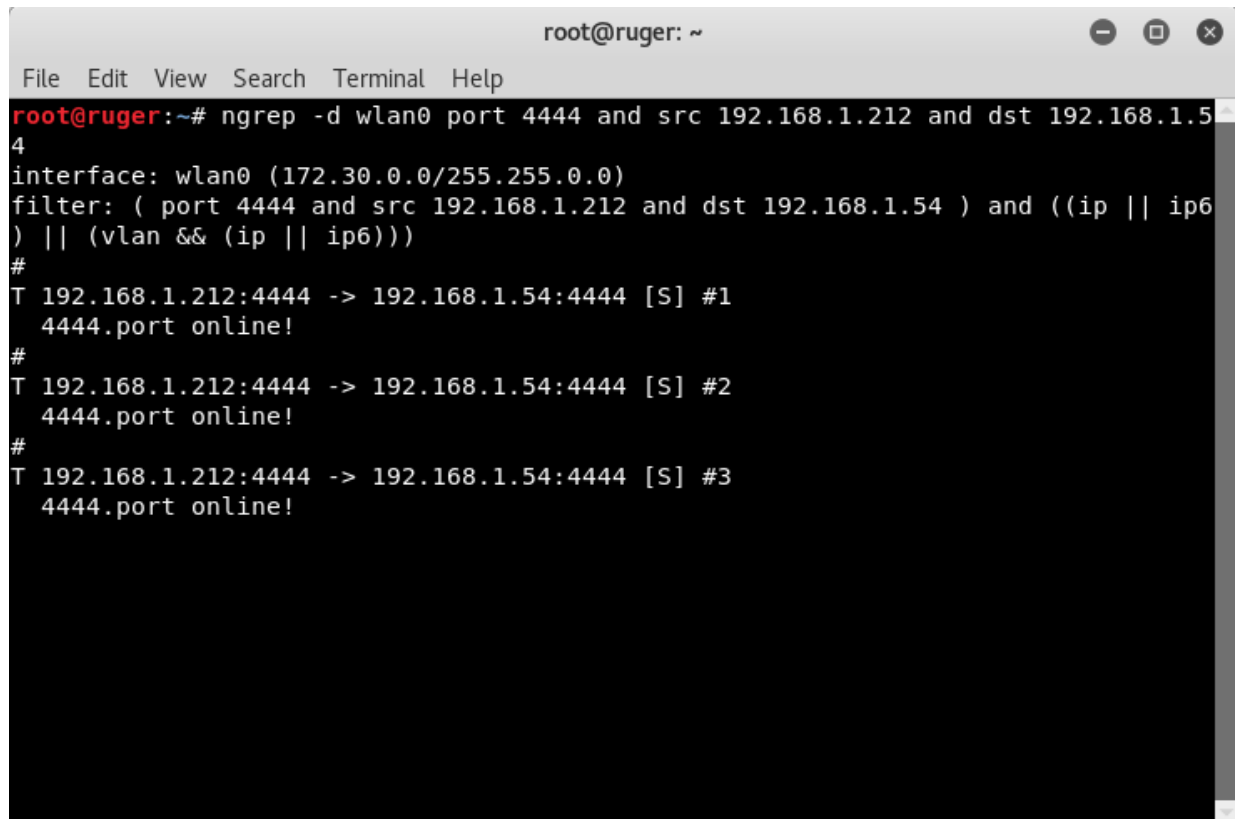
2.26 Xirrus Wi-Fi Inspector



Xirrus Wi-Fi Inspector kullanıcılara çevrelerindeki WiFi ağlar ile ilgili olarak detaylı bilgiler verebilen bir kablosuz ağ izleme programıdır. Xirrus Wi-Fi Inspector temel olarak kablosuz ağ adaptörünüzü kullanarak etrafınızdaki ağları tarar ve analiz ederek bu ağlar hakkında bilgi vermektedir. Radar şeklinde bir görünüm sunan Xirrus Wi-Fi Inspector etrafınızdaki kablosuz ağların adlarını ve sizden uzaklıklarını listeleyebilmektedir. Xirrus Wi-Fi Inspector ile bu ağların hangilerinin ne kadar yüksek sinyal kalitesi sağladığını da gerçek zamanlı olarak takip etmeye imkan sağlar.[36]

Xirrus Wi-Fi Inspector ile bağlı olduğunuz kablosuz ağlar için internet hızı ölçme işlemini gerçekleştirebilirsiniz. Xirrus Wi-Fi Inspector size internet güvenliğinizi sağlama konusunda da yardımcı olabilmektedir. Xirrus Wi-Fi Inspector ile kablosuz ağınıza izinsiz şekilde dağıtan kaçak erişim noktalarını tespit edebilmektedir.[37]

2.27 Ngrep



```
root@ruger: ~
File Edit View Search Terminal Help
root@ruger:~# ngrep -d wlan0 port 4444 and src 192.168.1.212 and dst 192.168.1.54
4
interface: wlan0 (172.30.0.0/255.255.0.0)
filter: ( port 4444 and src 192.168.1.212 and dst 192.168.1.54 ) and ((ip || ip6) || (vlan && (ip || ip6)))
#
T 192.168.1.212:4444 -> 192.168.1.54:4444 [S] #1
4444.port online!
#
T 192.168.1.212:4444 -> 192.168.1.54:4444 [S] #2
4444.port online!
#
T 192.168.1.212:4444 -> 192.168.1.54:4444 [S] #3
4444.port online!
```

Grep'in network trafiği üzerinde iş yapan versiyonu olan ngrep, özellikle sorun çözme, anormallik tespiti vs. gibi konularda kullanılan araçtır. Özellikle HTTP, SMTP, FTP gibi plain-text her türlü ağ trafiğini izlemek, analiz etmek ve içerisinde string/pattern aramak gibi işlere olanak sağlayan ngrep ile örnek olarak bir ağ uygulamasındaki problem, sunucu – istemci arasındaki ilgili trafiği analiz ederek tespit edilebilir ki bu şekilde problemi ilgili uygulamanın hata bildirimlerinden ya da log dosyaları üzerinden tespit etmek yerine daha alt bir katmanda yakalamanıza olanak sağlar.[38]

Ngrep, IP, TCP, UDP, ICMP, IGMP protokollerini tanıyabiliyor ve BPF destekliyor. Bu nedenle spesifik olarak hedef, kaynak, protokol ve port seçilebilmesine olanak sağlıyor. Ayrıca filtrelenen bu network trafiğinde data paketleri içerisinde aynı grep'te olduğu gibi string ya da regular expression patternleri arayabiliyorsunuz.[39]

Ngrep, promiscuous mode'da çalışabildiğinden dolayı, hedefi dinlediği interface olmayan paketleri analiz edebilmektedir. Başka bir deyişle firewall vs. gibi merkezi bir noktadan geçen trafik, ilgili paketlerin hedefi firewall'un kendisi olmasa bile dinlenebilmekte ve analiz edilebilmektedir. Bu şekilde örneğin networkünüzde bulunan bir zombie bilgisayarı (misal irc trafiğini dinleyerek) saptamanız mümkün olabilir. Öte yandan ngrep trafiği sonradan incelemek için bir pcap dump dosyasına kaydedebilir, daha önceden kaydedilmiş bir pcap dump dosyasını okuyabilip ve replay edebilir.

2.28 Tcpdump

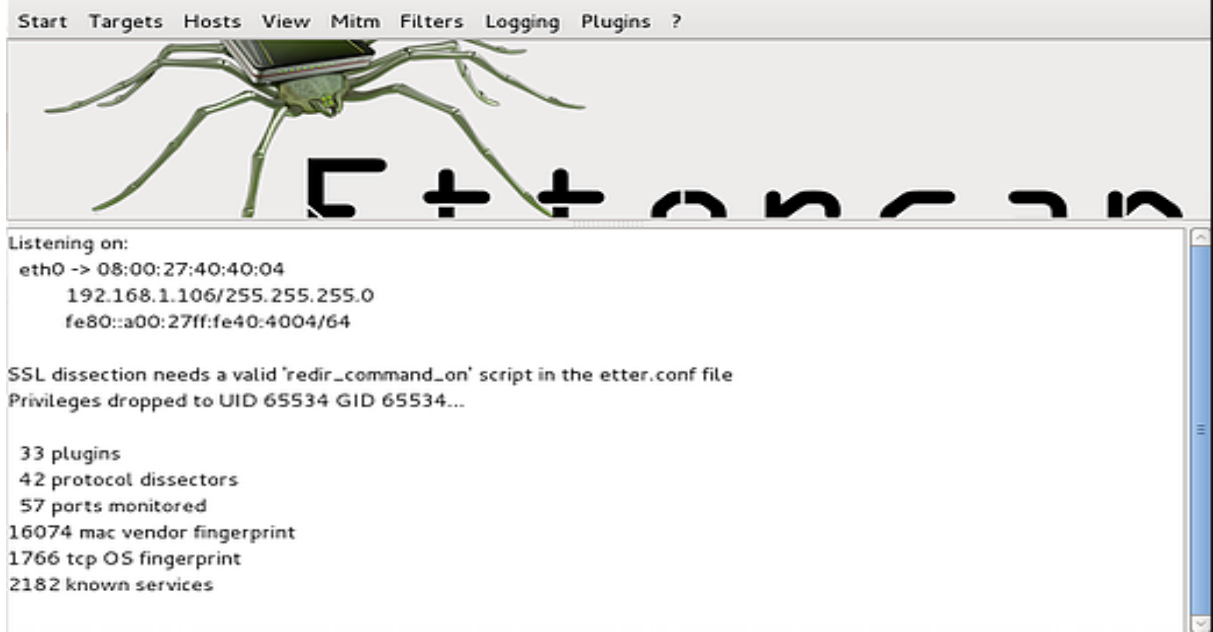
TCPDUMP(8)	System Manager's Manual	TCPDUMP(8)
NAME		
tcpdump - dump traffic on a network		
SYNOPSIS		
tcpdump [-AbdDefhHIJKLlnNOpqRStuUvX#] [-B <u>buffer_size</u>] [-c <u>count</u>] [-C <u>file_size</u>] [-G <u>rotate_seconds</u>] [-F <u>file</u>] [-i <u>interface</u>] [-j <u>tstamp_type</u>] [-m <u>module</u>] [-M <u>secret</u>] [--number] [-Q <u>in out inout</u>] [-r <u>file</u>] [-V <u>file</u>] [-s <u>snaplen</u>] [-T <u>type</u>] [-w <u>file</u>] [-W <u>filecount</u>] [-E <u>spi@ipaddr algo:secret,...</u>] [-y <u>datalinktype</u>] [-z <u>postrotate-command</u>] [-Z <u>user</u>] [--time-stamp-precision= <u>tstamp_precision</u>] [--immediate-mode] [--version] [<u>expression</u>]		
DESCRIPTION		
<u>Tcpdump</u> prints out a description of the contents of packets on a network interface that match the boolean <u>expression</u> ; the description is preceded by a time stamp, printed, by default, as hours, minutes, seconds, and fractions of a second since mid-night. It can also be run with the -w flag, which causes it to save the packet data to a file for later analysis, and/or with the -r flag, which causes it to read from a saved packet file rather than to read packets from a network interface (please note <u>tcpdump</u> is protected via an enforcing <u>apparmor</u> (7) profile in Ubuntu which limits the files <u>tcpdump</u> may access). It can also be run with the -V flag, which causes it to read a list of saved packet files. In all cases, only packets that match <u>expression</u> will be processed by <u>tcpdump</u> .		

Tcpdump, Linux işletim sistemine sahip bilgisayarlarda komut satırında çalışan bir paket analizcisi programıdır. Kullanıcıya bağlı bulunduğu bir ağ üzerinden iletilen veya alınan TCP/IP paketlerini veya diğer paketleri yakalama ve gözlemleme olanağı sunar. BSD lisansı altında dağıtılan Tcpdump ücretsiz bir yazılımdır.[40]

Tcpdump, paket yakalamak için “libpcap” kütüphanesini kullanır. Tcpdump'ın Windows için olanı WinDump olarak adlandırılır ve libpcap'in Windows'a port edilmiş hali olan WinPcap kullanır.

Tcpdump klasik Linux/UNIX araçları gibi komut satırından çalışır ve tüm özelliklerini parametre olarak alır. Parametresiz çalıştırıldığında sistemde bulunduğu ilk aktif ağ arabirimini dinlemeye alır(root izni varsa*). Tcpdump'ın çeşitli amaçlarla kullanılacak onlarca parametreleri vardır.

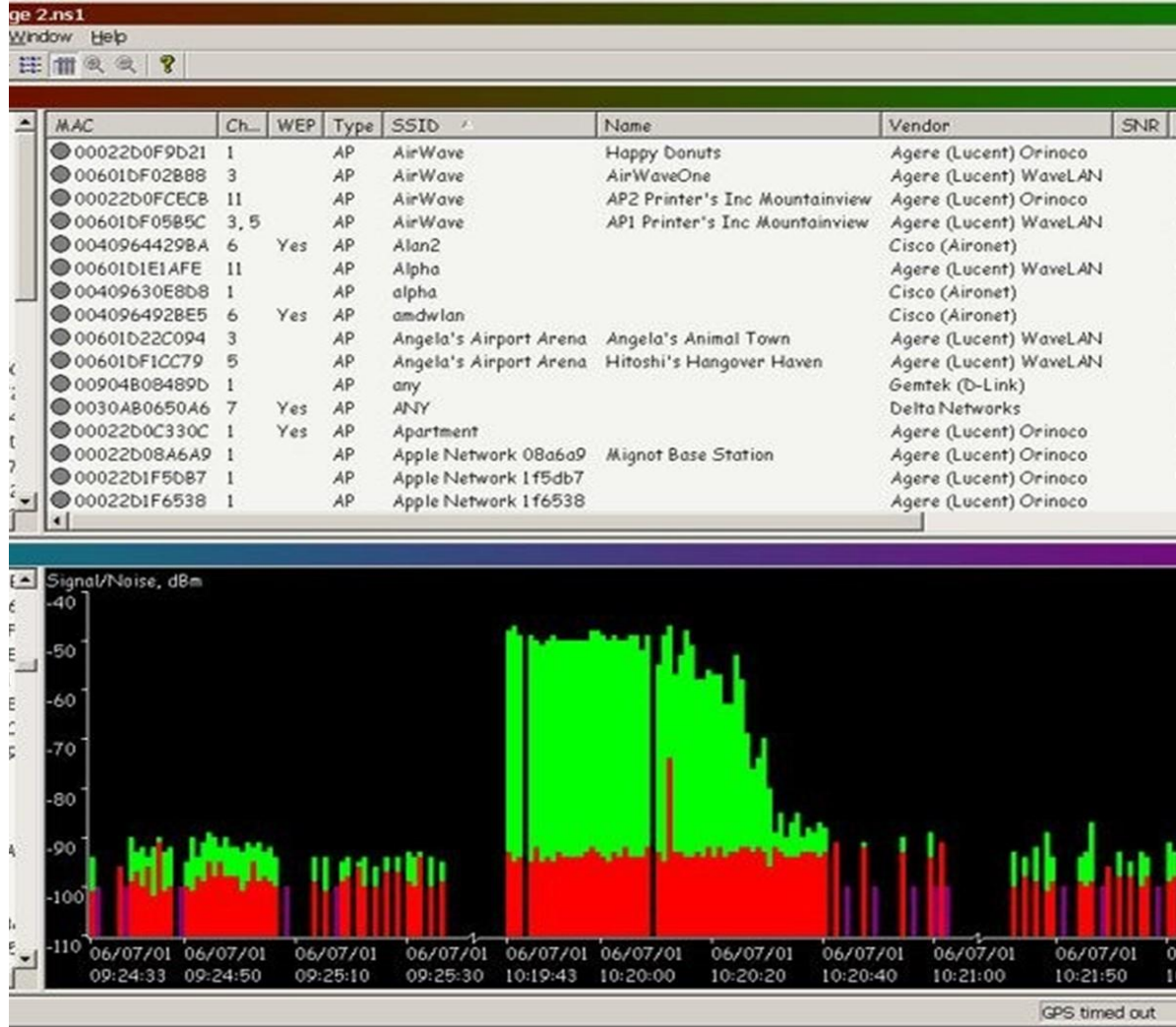
2.29 Ettercap



Ettercap , LAN üzerindeki ortadaki adam saldırıları için ücretsiz ve açık kaynaklı bir ağ güvenlik aracıdır .[41] Bilgisayar ağ protokolü analizi ve güvenlik denetimi için kullanılabilir . Unix benzeri işletim sistemleri de dahil olmak üzere Linux , Mac OS X , BSD, Solaris ve Microsoft Windows bir çok işletim sistemleri üzerinde çalışabilir .Bir ağ kesimi üzerindeki trafiği yakalayabilen, şifreleri yakalayabilen ve birçok ortak protokole karşı aktif dinlemeyi engelleme yeteneğine sahiptir . Aşağıda da bazı özellikleri yer almaktadır;

- IP tabanlı: paketler IP kaynağına ve hedefine göre filtrelendir.
- MAC tabanlı: paketler bir ağ geçidi üzerinden bağlantıları koklamak için yararlı olan MAC adresine göre filtrelendir .
- ARP tabanlı: iki ana bilgisayar (tam çift yönlü) arasında geçişli bir LAN'da koklamak için ARP poisoning kullanır .
- PublicARP tabanlı: kurban bir konaktan diğer tüm konakçılara (yarı çift yönlü) geçişli bir LAN'da koklamak için ARP poisoning kullanır.
- Ek olarak, aşağıdaki özellikleri de sunar:
- Yerleşik bir bağlantıya karakter enjeksiyonu: canlı bağlantıyı koruyarak karakterler bir sunucuya (emülasyon komutları) veya bir müşteriye (cevaplar taklit edilebilir) enjekte edilebilir .
- HTTPS desteği: bağlantı güvenli bir proxy aracılığıyla yapılsa bile , HTTP SSL güvenli verilerinin aranması .
- Bir GRE tüneli üzerinden uzak trafik: uzak bir Cisco yönlendiricisinden bir GRE tüneli üzerinden uzak trafiğin koklanması ve buna ortada bir adam saldırısı yapılması.
- Eklenti desteği: Ettercap API'sini kullanarak özel eklentiler oluşturma.
- Parola koleksiyoncuları: TELNET , FTP , POP , IMAP , rlogin , SSH1 , ICQ , SMB , MySQL , HTTP , NNTP , X11 , Napster , IRC , RIP , BGP , SOCKS 5 , IMAP 4 , VNC , LDAP , NFS , SNMP , MSN , YMSG dir.
- Paket filtreleme / bırakma: TCP veya UDP yükünde belirli bir dize (veya onaltılık sıra) arayan ve bunu özel bir dize / dizi ile değiştiren veya tüm paketi bırakan bir filtre ayarlama .
- OS parmak izi : kurban ev sahibinin işletim sistemini ve ağ adaptörünü belirler.
- Bir bağlantıyı kes: bağlantı listesinden tercih edilen bağlantıların kesilmesi.
- LAN'ın pasif taranması : LAN üzerindeki ana bilgisayarlar, açık portları , mevcut servislerin sürüm numaraları , ana bilgisayarın türü (ağ geçidi , yönlendirici veya basit PC) ve atlama sayısında tahmini mesafeler hakkında bilgi alınması .

2.30 NetStumbler



NetStumbler, wireless noktalarını (kablosuz internet bağlantı noktalarını) tespit eden, sinyal gücünü belirleyen ve analizini ayrıntılı bir şekilde görsel arayüzüne aktaran network yazılımlarından biridir. Bunları yapmakla yetinmeyip; bağlantı kopmalarını, sinyal gücü zayıflamalarını, gps aracılığı ile yerlerini belirlemeyi, sinyal kalitesini ve mesafesini MAC, SSID, Ad, Satıcı, Hız, Tür, Şifreleme, IP Adresi, Alt Ağ gibi pek çok işi kolaylıkla yapmaktadır. Böylelikle internete bağlanırken size sağlayacağı yararları görebiliyorsunuz.[42]

- 802.11b, 802.11a ve 802.11g ile çalışabilmektedir.
- NetStumbler Wardriving için de kullanılabilir . Wardriving, hareket eden bir araçtan Wi-Fi şebekeleri arıyor. GPS yetenekleri ile NetStumbler Wardriving için gerçekten iyi bir araçtır.
- Kapsama alanında anons yapan tüm aktif cihazları bularak bunları raporlar.[43]
- NetStumbler'i pasif keşif aracı olarak kullanabiliriz.

2.31 P0F

```
p0frep: p0f v2 log analyzer by <lcamtuf@coredump.cx>
Usage: ./p0frep logfile.txt sortby [ 'ipmask' 'sysmask' ]

    logfile.txt      - input file
    sortby           - 'system' or 'addr'; sort order
    ipmask           - IP mask, e.g. 195.117.3. (can be '')
    sysmask          - system name mask, e.g. 'Windows'

Typical usage might be:

To get your local systems in 10.0 subnet sorted by OS name:
    p0frep log.txt system 10.0.

To get all AIX boxes sorted by IP:
    p0frep log.txt addr '' AIX

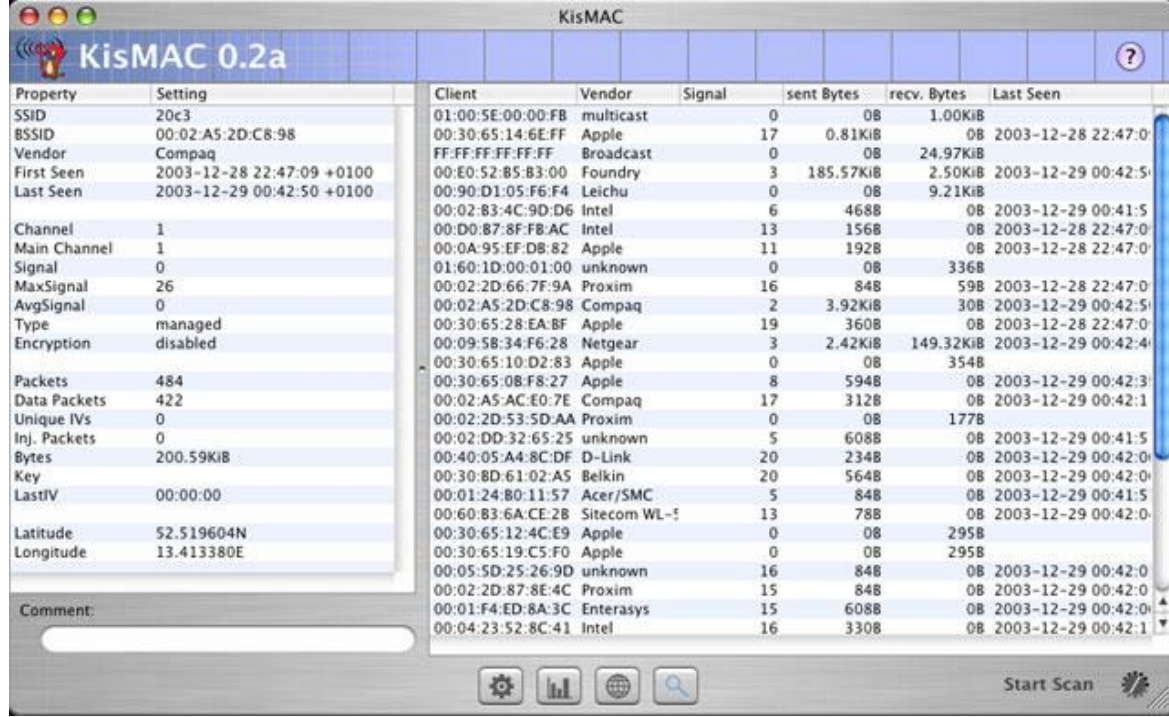
...and so on.
```

P0F pasif bir TCP / IP yığın parmak izi aracıdır. P0F, ağ trafiğinin çalıştığı kutuya veya üzerinde çalıştığı aracı paylaşan ve ağ trafiğini gönderen makinelerde çalışan sistemi tanımlamayı deneyebilir. P0F ayrıca uzak sistemin diğer yönlerini analiz etmede yardımcı olabilir.[44]

P0F'nin bazı özellikleri;

- Ağ trafiğini pasif olarak inceleyerek, p0f, algılayıcı makinenin ağ arabirimine veya algılayıcı makinenin dinleyebileceği fiziksel bir alt ağa TCP paketleri gönderen uzak makinelerde işletim sistemlerini belirlemeye çalışabilir.
- Sürüm 3'ten bu yana p0f, uygulama düzeyinde HTTP mesajlarını inceleyerek uzak sistemin özelliklerini de tespit edebilir.
- P0F ayrıca güvenlik duvarının varlığını kontrol edebilir.
- Uzak bir sisteme olan mesafeyi tahmin edebilir ve çalışma süresini hesaplayabilir.
- Uzaktaki sistemin ağa bağlanma yöntemini de tahmin eder (DSL, OC3, vb.).

2.32 KisMAC



Ücretsiz ve açık kaynaklı programdır, çevredeki WiFi ağları hakkında önemli bilgiler toplamanıza yardımcı olur. KisMAC WiFi tarayıcı uygulaması SSID'leri algılayabilir, giriş yapmış istemcileri gösterebilir, WiFi haritalarını çizmenize olanak tanır ve daha fazla özellikleri sağlayabilir.[45]

KisMac gibi bir WiFi tarayıcı uygulamaları, etrafınızdaki gizli, gizlenmiş ve kapalı olanlar da dahil olmak üzere her tür WiFi ağını bulmanızı sağlar. WiFi ağının adını, MAC adresini, WiFi şifrelemesini, kanalı ve sinyal seviyesini kontrol eder.[46] Başlıca Özellikleri Şunlardır;

- Gizli / gizlenmiş / kapalı SSID'leri algılar ve gösterir
- Ağda oturum açan kullanıcıları listeler (MAC Adresi, IP adresi, sinyal gücü)
- Kablosuz ağların mükemmel haritalanması
- Şebeke kapsama alanı haritasını çizebilir
- PCAP ithalat ve ihracat
- 802.11b / g frekansını destekler
- Şifreli ağlara karşı farklı saldırılar yapabilir
- Kimlik doğrulama saldırıları yapabilir
- Uygulamanın AppleScript özellikli olduğu kabul eder
- Kismet drone yakalamalarını destekler

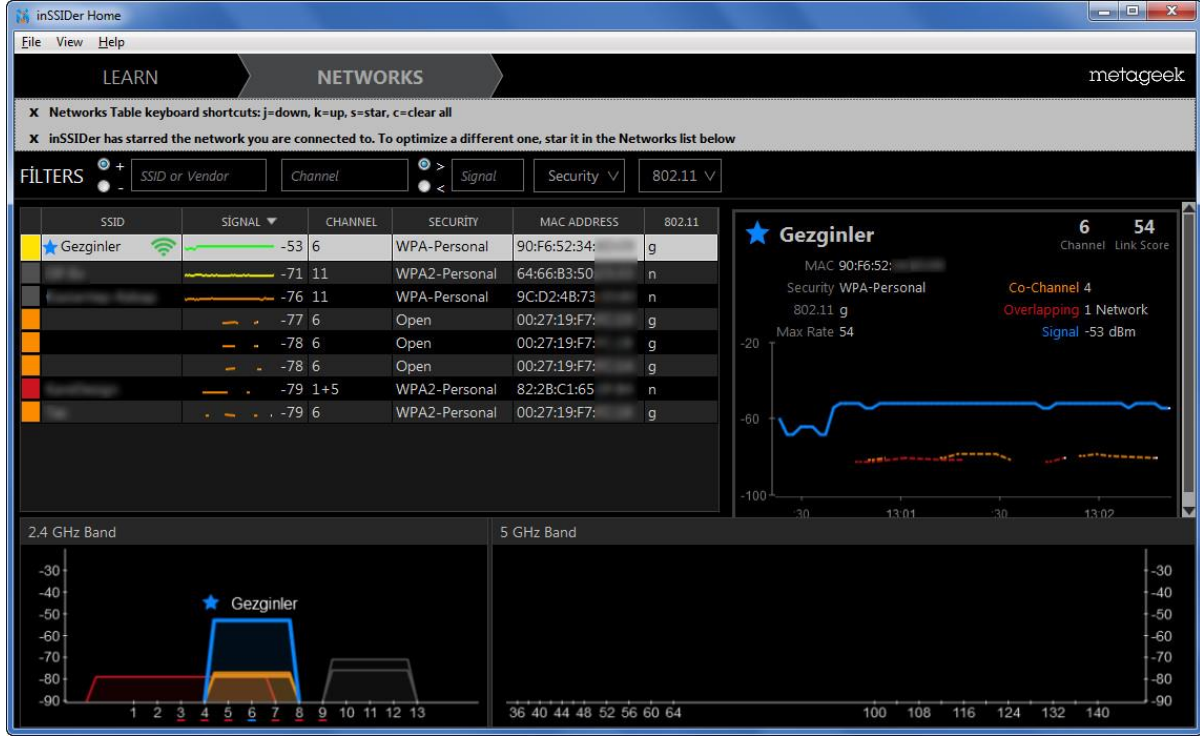
2.33 Dsniff

```
Session Edit View Bookmarks Settings Help
[root@c1ec ~]$ dsniff
dsniff: listening on eth0
-----
01/11/07 21:51:57 tcp 10-1-227-207.int.sds.uw.edu.pl.2142 -> pop3.wp.pl.110 (pop)
USER malapumka
PASS awruk16h
-----
01/11/07 21:51:57 tcp 10-1-250-140.int.sds.uw.edu.pl.2142 -> pop3.wp.pl.110 (pop)
USER malapumka
PASS awruk16h
-----
01/11/07 21:52:24 tcp 10-1-250-140.int.sds.uw.edu.pl.2146 -> 10-1-227-207.int.sds.uw.edu.pl.21 (ftp)
USER kasluta
PASS kasial234
```

Ham paketlere bir ağ arayüzünden (ağ koklama olarak da bilinir) erişme yeteneği, sistem ve ağ yöneticileri için uzun zamandır önemli bir araç olmuştur. Hata ayıklama amacıyla, tam olarak neyin iletildiğini görmek için ağ trafiğine kablo seviyesine bakmak genellikle yararlıdır. Dsniff, adından da anlaşılacağı gibi, bir ağ dinleyicisidir - ancak farklı bir türün sınanması için tasarlanmıştır. Hacker Dug Song tarafından yazılan dsniff, birçok farklı uygulama protokolünü ayırtmak ve kullanıcı adları ve şifreler, ziyaret edilen web sayfaları, e-posta içeriği ve daha fazlası gibi ilginç bilgileri çıkarmak için kod içeren bir yardımcı program paketidir. [47] Ek olarak, anahtarlamalı ağların normal davranışını yenmek ve aynı ağ segmentindeki diğer ana bilgisayarlardan ağ trafiğinin görünür olmasına neden olmak için kullanılabilir,

Bu yetenekler tek başına ilgi çekmek için yeterli, ancak en son sürümünde SSH ve HTTPS protokollerine ortadaki saldırıları başlatan yeni programlar içeriyor. Şifreli olmayan trafiğin görüntülenmesine ve etkileşimli SSH oturumları devralma ihtimaline bile izin ver. Bu yeni yetenekler güvenlik topluluğunda bir miktar karışıklığa neden oldu, ancak bu belge etik veya teknik bir tartışma değildir.

2.34 InSSIDer



InSSIDer, bağlı olduğunuz ya da çevrenizdeki WiFi ağları hakkında birçok bilgiye ulaşmanızı sağlayan bir programdır.[48] Programın kolay arayüzüyle kablosuz bağlantılar hakkında SSID (adı), BSSID, kanalı, sinyal seviyesi, ağ biçimi, güvenlik protokolü, maksimum bağlantı hızı, gibi çeşitli bilgileri görüntüleyebilirsiniz. Grafikselsel arayüzünde sinyal gücü ve durumuna ait geçmiş verileri de görüntüleyebilirsiniz.

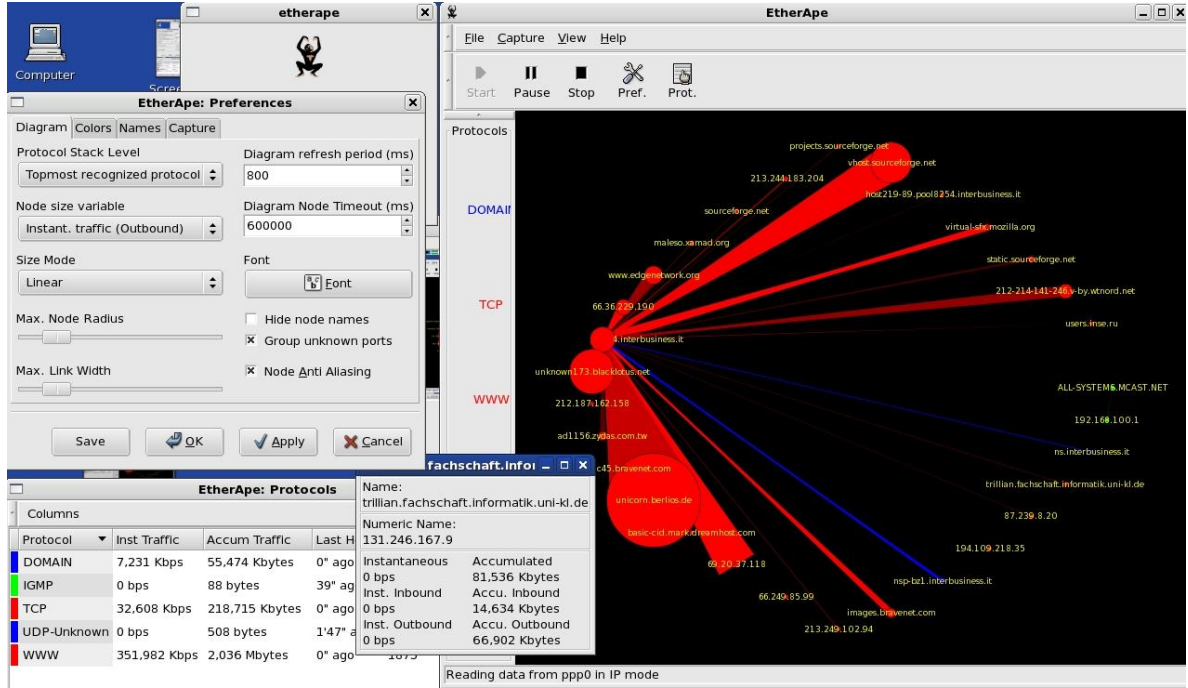
Tam olarak ağınızın sinyal gücüne etki eden olumsuz koşulları tespit edebilen ve bu konuda sizi bilgilendiren program, böylece uğraşmadan ağınızdaki yavaşlıkları görmeye olanak tanıyor.

Sizin ağınızın yanında, diğer ağların da genel bilgilerini, güvenlik sistemlerini ve adreslerini görüntüleyebilen program, kullandığınız bağlantı noktalarının da güçlerini karşılaştırmanızı ve görüntülemenizi sağlıyor.

Wireless dağıtıcılar genellikle birbirlerine yakın frekans aralıkları kullandıklarında, bağlantı kanalları üzerinde karışıklıklar meydana gelir ve bu nedenle bağlantı hızında büyük problemlerle karşılaşılır. Eğer ağınızda bu tip bir sorun varsa InSSIDer sayesinde sorunu kolayca tespit edebilirsiniz.

Uzun vadeli gözlem yapma imkanı sayesinde, ağınızın hızı üzerinde etki eden koşulları zamana yayılmış bir grafik ile gözleme şansınız da var. Tespit edilen ağların GPS üzerinden konumlarını bildirebilen program, daha sonra bu bilgilerin KML dosyaları olarak paylaşımalarına da imkan vermektedir.

2.35 EtherApe



EtherApe ağ monitörü, ağınızın veri trafiğini izlemek için orta seviye bir seçenektir. Açık kaynaklı bir ağ monitörü olarak, EtherApe dinamik bir grafik ara yüz sunar; IP ve TCP modlarını içerir; Ethernet, FDDI, PPP ve slip cihazlarını destekler; trafiği filtreler; ve bir tcpdump dosyasından gelen trafiği okur ve ağı canlı olarak izler.[49]

Ağ trafiği, grafiksel bir ara yüz kullanarak görüntülenir. Her düğüm belirli bir ana bilgisayarını temsil eder. Bağlantılar, ana bilgisayarlara bağlantıları temsil eder. Düğümler ve bağlantılar, ağdaki çeşitli trafik türlerini oluşturan farklı protokolleri temsil etmek için renk kodu kullanır. Bireysel düğümler ve bağlantı noktaları, ağ trafiğindeki artış ve azalışlarla birlikte büyür ve küçülür. [50] Başlıca özelliklerine bakacak olursak şöyledir;

- İsteğe bağlı ad c-ares kütüphanesini kullanarak çözme,
- Farklı işlemlerde paket yakalama ve görüntüleme çalışması,
- Renk kodlu düğüm ve en çok kullanılan protokoller için bağlantılar,
- Ethernet, WLAN, VLAN ve diğer birçok medya ve kapsülleme tipindeki trafiği yönetir,
- Bir dosyadan veya gerçek bir ağdan gelen trafiği okuyabilir,
- IPv4'ü ve IPv6'yı destekler,
- Düğüm istatistiklerinin XML dışı aktarımı,
- Trafik kendi ağında, uçtan uca (IP) veya porttan porta (TCP) görülebilir,
- Veri görünümü bir ağ filtresi kullanılarak değiştirilebilir gibi özelliklere sahiptir.

3.Table 1: Comparison of Network Listening Tools

Referene Numbes	Tool	Type	Operating System	Latest Version	Key Features
[1,2,3]	Nagios Network Analyzer	Free/Commercial	Windows, Linux, Wmware	Nagios Network Analyzer 4.4.3 (15 January 2019)	Network Monitoring, Define a network hierarchy
[4]	Cacti	Free	Unix,GNU/Linux	Cacti 1.2.3 (30 March 2019)	Network Monitoring,Traffic Monitoring, RRDTool
[5,6,7]	Zabbix	Free	CentOs, Oracle Linux,Ubuntu,Debian,SUSE Linux Enterprise Server,Raspbian	Zabbix 4.2.0 (29 Mar 2019)	Monitoring network services(SMTP, POP3, HTTP)
[8,9]	Ntop	Free	Windows, GNU Linux.Unix, MacOSX	Ntop 3.9 (16 April 2014)	Network Analysis
[10]	Icinga	Free	Windows, Debian, RHEL, Ubuntu, Fedora, SLES, OpenSUSE	Icinga 2.10.4 (19 March 2019)	Internet Usage Monitoring, Server Monitoring, Web Traffic Reporting
[11]	Observium	Free/Commercial	Windows,Linux,Ubuntu,Debian,RHEL, CentOS7	Observium 19.3.9774 (14 March 2019)	Bandwidth,SLA,Uptime,Server Monitoring,NetworkDiagnosis,Network Resource Management
[12,13]	Wireshark	Free	Windows, MacOSX, Linux, Unix,	Wireshark 3.0.1 (8 April 2019)	GUI Support
[14]	Nmap	Free	Windows,Linux, MacOS, FreeBSD, OpenBSD, NetBSD	Nmap 7.70 (20 March 2019)	Port Scan,Network Map Decal,Host discovery,Service discovery,Nmap scripts
[15]	OpenNMS	Free	Windows,YUM/RPM,APT/Debian, MacOSX	OpenNMS Horizon 23.0.4 (21 March 2019)	Network Monitoring,Network management,
[16]	Bandwidth Monitor	Free	Windows	Bandwidth Monitor 3.4(2017)	Follow network operations, Internet usage
[17,18]	Capsa Free Network Analyzer	Free/Commercial	Windows, Mac OS X	Capsa Free Network Analyzer 7.8.0 (25 April 2018)	Network Analysis, Detecting attacks, Review mail traffic
[19]	Microsoft MessageAnalyzer	Free	Windows,Windows Server	MicrosoftMessageAnalyzer 1.4, (28 December 2016)	Network traffic monitoring,Analyzing event logs
[20]	NetworkMiner	Free/Commercial	Windows, MacOSX, FreeBSD, Linux	NetworkMiner 2.4 (10 January 2019)	Network Analysis, PCAP
[21]	Advanced IP Scanner	Free	Windows	Advanced IP Scanner 2.5.3850(29 March 2019)	IP Scanner, Remote Computer Power Off
[22]	Zenoss Core	Free/Commercial	Windows, Linux, VMware, Unix	Zenoss Core 6.2 (13 June 2018)	Network Monitoring, Network listening,
[23]	Telerik Fiddler	Free/Commercial	Windows, Linux,MacOS	Telerik Fiddler 4.6 (22 August 2017)	Web traffic tracking, Http debugging, Http traffic review
[24]	MiTeC Network Scanner	Free	Windows	MiTeC Network Scanner 5.3.0 (05 February 2019)	Network Monitoring, ActiveDirectory
[25,26]	Pandora FMS	Free/Commercial	Windows,MacOS,WMware,OpenSUSE, Debian,RHEL,Android,Linux	Pandora FMS 7.0 (28 March 2019)	Remote network monitoring, Statistical information collection, Multiple network monitoring
[27]	Windump	Free	Windows, Linux	Windump 3.9.5 (06 December 2006)	Packet capture, Network analysis, encrypted network traffic decoding
[28]	Tcptrack	Free	Linux, Unix	Tcptrack 1.4.2 (5 August 2017)	Tcp traffic monitoring,
[29,30]	PRTG Network Monitor	Free/Commercial	Windows,Windows Server	PRTG Network Monitor 19.1.49(28 March 2019)	Hierarchical management of devices and sensors, Alarms, Warning And Unusual Alerts
[31,32]	Angry IP Scanner	Free	Windows, Mac OS X,Linux,Ubuntu	Angry IP Scanner 3.5.5 (09.12.2016)	Port Scan, Web Server Detection
[33]	SolarWinds NPM	Free	Windows	SolarWinds NPM 12.4 (4 December 2018)	Network Performance Monitor, Network Monitoring
[34]	WirelessNetView	Free	Windows	WirelessNetView 1.75 (03 December 2017)	Provides Detailed Information About Wifi Port
[35]	NetFlow Traffic Analyzer	Free	Windows	NetFlow Traffic Analyzer 4.5(4 December 2018)	Traffic monitoring, Network Analyzer
[36,37]	Xirrus Wi-Fi Inspector	Free	Windows,Mac OS X	Xirrus Wi-Fi Inspector 2.0 (5 October 2016)	Gives detailed information about wireless networks
[38,39]	Ngrep	Free	FreeBSD,NetBSD,Open BSD,MacOS X Linux,Solaris,Illumos	Ngrep 1.45 (28 November 2006)	Monitor Network Traffic, Network Analysis,Captures the Problem in a Lower Layer, BPF support,Pcap Library and GNU Regex Library

[40]	Tcpdump	Free	Windows, Linux	Tcpdump 4.9.1 (23 July 2017)	Is a package analysis program,
[41]	Ettercap	Free	Windows, Linux, Mac OS X, BSD and Solaris	Ettercap 0.8.2-Ferri (14 March 2015)	Detecting Man in the Middle Attacks
[42,43]	NetStumbler	Free	Windows	NetStumbler 0.4.0 (18 April 2017)	Passive Reconnaissance Vehicle, Detecting wireless ports
[44]	P0f	Free	Linux, Windows, Macintosh	P0f 3.09b(18 April 2016)	TCP/IP stack fingerprint, API Access and Nat Support
[45,46]	KisMAC	Free	Mac OS X	KisMAC 0.3.4 (Alpha 4)/Sep, 2015	Penetration Test, GUI Support
[47]	Dsniff	Free	Unix Like	Dsniff 2.3 (17 November 2000)	Package Analysis
[48]	InSSIDer	Free/Commercial	Windows, Mac OS X, and Android	inSSIDer Office Beta 4.4.2.7(July 16)	WiFi Troubleshooting, GUI Support, and Optimization
[49,50]	EtherApe	Free	Linux, Unix-like	EtherApe 0.9.16 (14 January 2018)	Ethernet, FDDI, ISDN, Token Ring, PPP, SLIP, WLAN Device Support

4.SONUÇ

Eskiden bilgiyi korumak için fiziksel çözümler yeter iken günümüze baktığımızda bu çözümler yetersiz kalmaktadır. Teknolojinin gün geçtikçe gelişmesiyle bilgiler dijital ortamda daha fazla depolanmaya başlanmıştır. Buda fiziksel çözümlerin yanında siber çözümlerde gerek duyulmaya başlanmıştır. Buna paralel olarak kişi, kurum ve kuruluşlar açısından bilgi sistemleri güvenliğinin öneminde büyük ölçüde artan bir süreç yaşanmaktadır ve buna eş olarak dijital ortamlar birçok zafiyet barındırmaktadır.

Kişi, kurum ve kuruluşlara ait olan bilgiler siber saldırganlar tarafından ele geçirildiği takdir de bilgi sahipleri tarafından maddi ve manevi açıdan kayba uğrar ve bu kayıp durumunda büyük çaplı zararlarla birlikte can ve mal kaybı da doğurabilir. Bu gibi durumlarda saldırganlar dijital ortamda depolanan bilgiye ulaşmak için kurumun ağına sızması, ağı dinlemesi, ağdan geçen paketleri analiz etmesi ve bunları anlamlandırması gerekmekte bu sayede oradan bilgiyi elde edebilir. Tam bu noktada yukardaki bahsetmiş olduğumuz 35 farklı ağ dinleme araçları devreye girmektedir.

Bu 35 araç her biri ağı dinlese de her birinin kendine has özellikleri mevcuttur. Yukarıda da bahsettiğimiz araçlar farklı işletim sistemleri olsun, çalışma prensipleri olsun, bilgiye ulaşma şekilleri olsun ve ağ da uygulanan korunma tedbirlerini geçme şekilleri olsun, kullanım amaçları olsun, ücretli veya ücretsiz olsun bunlara yukarda detaylı bir şekilde yer vermiş bulunmaktayız. Saldırganlar bu araçları kullanarak bilgiyi elde edebildikleri gibi bir siber güvenlik uzmanı da aynı araçları da kullanarak saldırganın kullanmış olduğu yöntemlerle ağı güvenlik açıklarını kapatabilir ve bilgi sistemleri güvenliği konusunda önem arz eden sağlam güvenlik politikaları, kişisel veya kurumsal olarak ihtiyaç duyulan temel güvenlik stratejileri ortaya koyabilmiş olur.

5.KAYNAKÇA

1. <https://www.syslogs.org/nagios-kurulumu-ve-yapilandirmasi/>
2. <https://ozguryazilim.com.tr/sistem-yonetimi/sunucu-teknolojileri/sistem-yonetim-araclari/zabbix/>
3. <http://www.look2linux.com/linux/icinga-network-monitoring/>
4. <http://www.observium.org/>
5. <https://www.cacti.net/documentation.php>
6. <https://www.cacti.net/downloads/docs/contrib/Cacti-El-Kitab.pdf>
7. <http://www.cozumpark.com/cacti-sistem-ve-ag-cihazlari-izleme-yazilimi/>
8. https://www.howtoforge.com/network_monitoring_with_ntop
9. <https://www.ntop.org/products/traffic-analysis/ntop/>
10. <https://nmap.org/>
11. <http://www.bwmonitor.com/>
12. <https://www.advanced-ip-scanner.com/tr/>
13. <http://www.yazilimmutfagi.com/index.php/2011/10/21/web-debugging-hata-ayiklama-fiddler-aracinin-kullanimi/>
14. <http://pandorafms.org/>
15. <https://wmaraci.com/nedir/wireshark>
16. <https://www.tamindir.com/windows/colasoft-capsa-free/>
17. <http://colasoft-capsa-free-7-80.allapp.biz/>
18. <https://www.netresec.com/?page=Networkminer>
19. http://wiki.zenoss.org/Main_Page
20. <https://searchitoperations.techtarget.com/definition/Zenoss>
21. https://www.afterdawn.com/software/network/misc_net_tools/mitec_network_scanner.cfm
22. <http://www.download82.com/download/windows/mitec-network-scanner/>
23. <https://www.softpedia.com/get/Network-Tools/Network-IP-Scanner/MiTeC-Network-Scanner.shtml>
24. <https://angryip.org/about/>
25. <https://www.winpcap.org/windump/docs/default.htm>
26. <https://searchitchannel.techtarget.com/tip/The-Windows-TCPdump-WinDump>
27. <https://lifeoverlinux.com/tcptrack-araci-ile-network-baglantilarini-dinlemek/>
28. <https://directory.fsf.org/wiki/Tcptrack>
29. <https://www.riverbed.com/gb/products/xirrus/inspector.html>
30. <http://bidb.itu.edu.tr/sevir-defteri/blog/2013/09/06/tcpdump-kullan%C4%B1m%C4%B1>
31. <https://www.winpcap.org/windump/docs/default.htm>
32. <https://searchitchannel.techtarget.com/tip/The-Windows-TCPdump-WinDump>
33. <https://lifeoverlinux.com/tcptrack-araci-ile-network-baglantilarini-dinlemek/>
34. <https://directory.fsf.org/wiki/Tcptrack>
35. <https://www.paessler.com/manuals/prtg/introduction>
36. https://www.slideshare.net/kavicomtr/solarwinds-orion-npm-ve-nta?from_action=save
37. <https://inssider.tr.softonic.com/>
38. <https://en.wikipedia.org/wiki/EtherApe>
39. <https://www.syslogs.org/ngrep-network-grep-ile-ag-trafiginin-incelenmesi/>
40. <https://en.wikipedia.org/wiki/Ngrep>
41. [https://en.wikipedia.org/wiki/Ettercap_\(software\)](https://en.wikipedia.org/wiki/Ettercap_(software))
42. <https://en.wikipedia.org/wiki/P0f>
43. <http://www.ouah.org/dsniffintr.html>