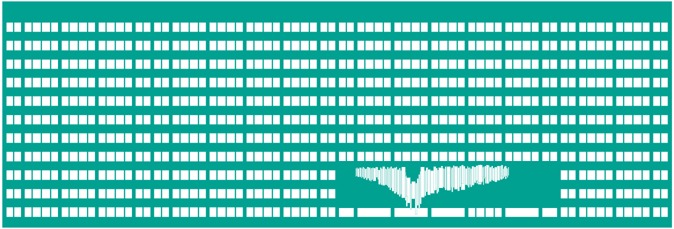
VŠB TECHNICKÁ
UNIVERZITA
OSTRAVA

VSB TECHNICAL
UNIVERSITY
OF OSTRAVA



www.vsb.cz

Fundamentals of the Security in Communications

Monitoring, Scanning and Analysis of the Network Traffic from a Security Point of View. Google Hacking and Traffic Scanners.

Filip Řezáč

VSB – Technical University of Ostrava

filip.rezac@vsb.cz

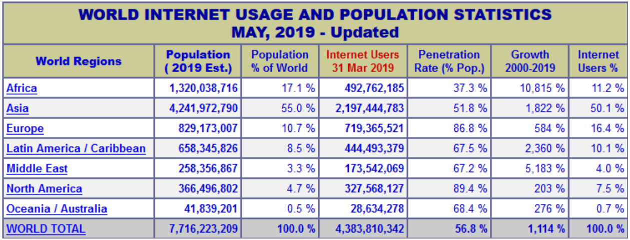
July 13, 2021

VSB TECHNICAL UNIVERSITY OF OSTRAVA | FACULTY OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE

Introduction 1/6

Growth of Internet Users

- The number of Internet users is growing.



WORLD INTERNET USAGE AND POPULATION STATISTICS
MAY, 2019 - Updated

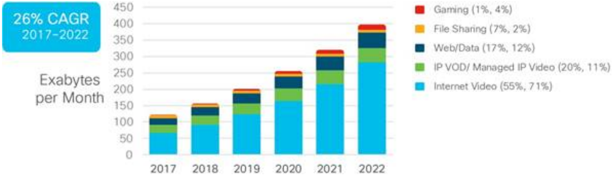
World Regions	Population (2019 Est.)	Population % of World	Internet Users 31 Mar 2019	Penetration Rate (% Pop.)	Growth 2000-2019	Internet Users %
Africa	1,320,038,716	17.1 %	492,762,185	37.3 %	10,815 %	11.2 %
Asia	4,241,972,790	55.0 %	2,197,444,783	51.8 %	1,822 %	50.1 %
Europe	829,173,007	10.7 %	719,365,521	86.8 %	584 %	16.4 %
Latin America / Caribbean	658,345,826	8.5 %	444,493,379	67.5 %	2,360 %	10.1 %
Middle East	258,356,867	3.3 %	173,542,069	67.2 %	5,183 %	4.0 %
North America	366,496,802	4.7 %	327,568,127	89.4 %	203 %	7.5 %
Oceania / Australia	41,839,201	0.5 %	28,634,278	68.4 %	276 %	0.7 %
WORLD TOTAL	7,716,223,209	100.0 %	4,383,810,342	56.8 %	1,114 %	100.0 %

Introduction 2/6

Growth of Internet Users

- Internet traffic has increased dramatically.

Year	Global Internet Traffic
1992	100 GB per day
1997	100 GB per hour
2002	100 GB per second
2007	2 000 GB per second
2017	46 600 GB per second
2022	150 700 GB per second



* Figures (n) refer to 2017, 2022 traffic share

Source: Cisco VNI Global IP Traffic Forecast, 2017-2022

Introduction 3/6

Stand-alone applications can now utilize networking

- Cooperative editing: Google Docs, Abiword, ACE, MS SharePoint Workspace
- Browser-based software/gaming: Chrome OS, Google Wave, Google Stadia
- Game consoles/Smart TV's: Microsoft XBOX, Sony Playstation, Smart TV

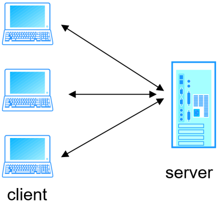
Network Applications

- Online games, shopping, banking, stock trading, network storage, clouding, P2P applications, M2M communications, IoT
- VOD, EOD, VoIP, IPTV, Live Streaming

Introduction 4/6

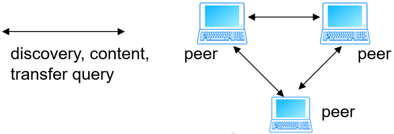
Client-Server

- Traditional structure



Peer-to-Peer (P2P)

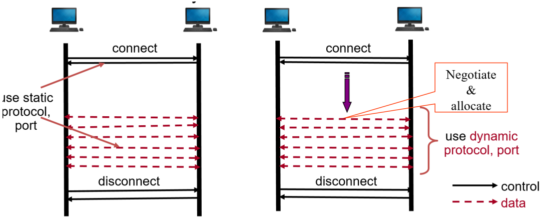
- New concept between file sharing and trasfering
- Generates high volume of traffic



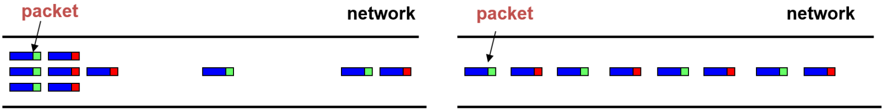
Introduction 5/6

Types of Traffic

- Static sessions vs. Dynamic sessions

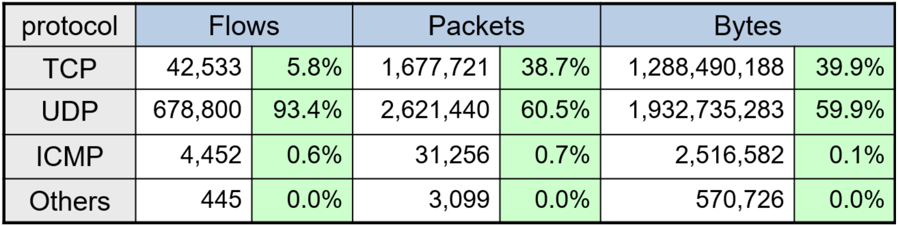


- Bursty data transfer vs. Streaming data transfer



Introduction 6/6

Internet Protocol Distribution



protocol	Flows		Packets		Bytes	
TCP	42,533	5.8%	1,677,721	38.7%	1,288,490,188	39.9%
UDP	678,800	93.4%	2,621,440	60.5%	1,932,735,283	59.9%
ICMP	4,452	0.6%	31,256	0.7%	2,516,582	0.1%
Others	445	0.0%	3,099	0.0%	570,726	0.0%

Transport Protocol Distribution

- The amount of UDP flows is increasing by P2P, gaming and multimedia streaming apps

Motivation 1/2

Needs of Service Providers

- Understand the behavior of their networks
- Provide fast, high-quality, reliable service to satisfy customers and thus reduce churn rate
- Plan for network deployment and expansion
- SLA monitoring, Network security
- Increase Revenue!

Needs of Customers

- Want to get their money's worth
- Fast, reliable, high-quality, secure, virus-free Internet access

Motivation 2/2

Application Areas

- Network Problem Determination and Analysis
- Traffic Report Generation
- Intrusion & Hacking Attack (e.g., DoS, DDoS) Detection
- Service Level Monitoring (SLM)
- Network Planning
- Usage-based Billing
- Customer Relationship Management (CRM)
- Marketing

Issues in Traffic Monitoring

Choices

- Single-point vs. Multi-point monitoring - Number of probing or test packet generation point.
- In-service vs. Out-of-service monitoring - Whether monitoring should be executed during service or not.
- Continuous vs. On-demand monitoring - Monitoring executes continuously or by on-demand.
- Packet vs. Flow-based monitoring - Collect packets or flows from network devices.
- One-way vs. Bi-directional monitoring - Monitor forward path only / forward and return path

Trade-offs

- Network bandwidth
- Processing overhead
- Accuracy
- Cost

Problems

Capturing Packets

- High-speed networks $(Mbps \rightarrow Gbps \rightarrow Tbps)$
- High-volume traffic
- Streaming media (Windows Media, Real Media, Quicktime)
- Service Level Monitoring (SLM)
- P2P traffic
- Network Security Attacks

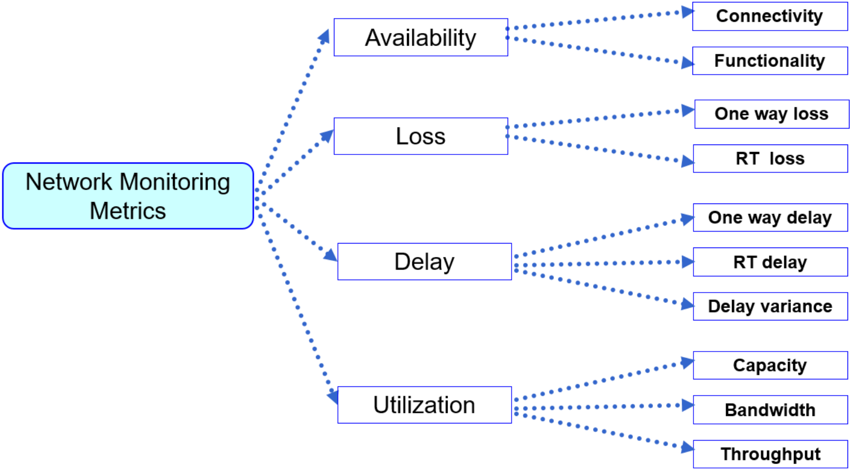
Flow Generation and Storage

- What packet information needs to be save to perform various analysis?
- How to minimize storage requirements?

Analysis

- How to analyze and generate data quickly?
- What kind of info needs to be generated? → Depends on applications.

Network Monitoring Metrics 1/5



Network Monitoring Metrics 2/5

Availability

- The percentage of a specified time interval during which the system was available for normal use.
- What is supposed to be available? (Service, Host, Network).
- Availabilities are usually reported as a single monthly figure.
- One can test availability by sending suitable packets and observing the answering packets (latency, packet loss).

Network Monitoring Metrics 3/5

Packet Loss

- The fraction of packets lost in transit from a host to another during a specified time interval.
- Internet packet transport works on a best-effort basis, i.e., a router may drop them depending on its current conditions.
- A moderate level of packet loss is not in itself tolerable.
- Metrics - One way loss, Round Trip (RT) loss.

Network Monitoring Metrics 4/5

Delay (Latency)

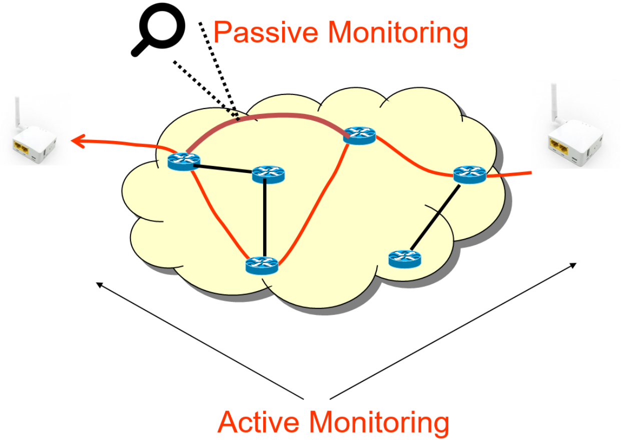
- The time taken for a packet to travel from a host to another.
- Round Trip Time (RTT) - forward transport delay + server delay + backward transport delay.
- Forward transport delay is often not the same as backward transport delay (may use different paths).
- For streaming applications, high delay or delay variation (jitter) can cause degradation on user-perceived QoS.
- Metrics - One way delay, Round Trip Time, Delay variance (Jitter).

Network Monitoring Metrics 5/5

Throughput

- The rate at which data is sent through the network, usually expressed in bytes/sec, packets/sec, or flows/sec.
- Be careful in choosing the interval; a long interval will average out short-term bursts in the data rate.
- Link Utilization over a specified interval is simply the throughput for the link expressed as a percentage of the access rate.
- Metrics - Link Capacity (Mbps, Gbps), Throughput, Utilization

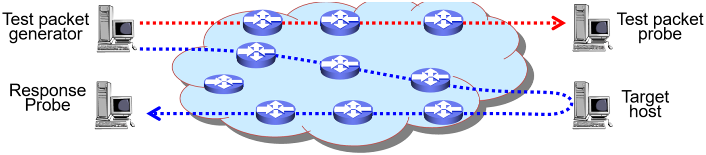
Traffic Monitoring Approaches 1/4



Traffic Monitoring Approaches 2/4

Active Monitoring

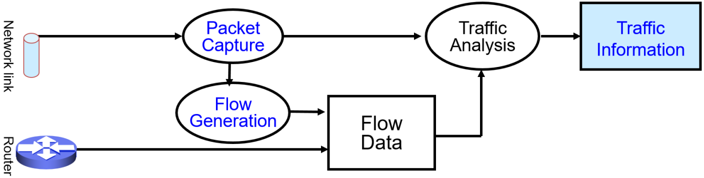
- Performed by sending test (probe) traffic into network.
  - Generate test packets periodically or on-demand.
  - Measure performance of test packets or responses.
  - Take the statistics.
- Impose extra traffic on network and distort its behavior in the process.
- Test packet can be blocked by firewall or processed at low priority by routers.
- Mainly used to monitor network performance



Traffic Monitoring Approaches 3/4

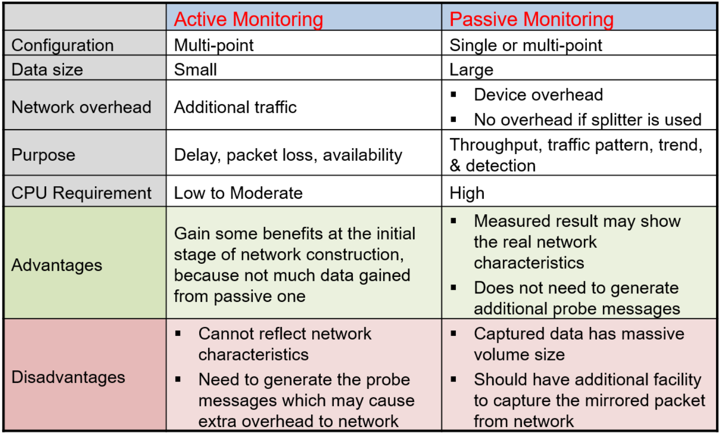
Passive Monitoring

- Carried out by observing network traffic.
  - Collect packets from a link or network flow from a router.
  - Perform analysis on captured packets for various purposes.
- Network device performance degrades by mirroring or flow export.
- Used to perform various traffic usage/characterization analysis or intrusion detection.



Traffic Monitoring Approaches 4/4

Comparison of Two Monitoring Approaches



	Active Monitoring	Passive Monitoring
Configuration	Multi-point	Single or multi-point
Data size	Small	Large
Network overhead	Additional traffic	▪ Device overhead ▪ No overhead if splitter is used
Purpose	Delay, packet loss, availability	Throughput, traffic pattern, trend, & detection
CPU Requirement	Low to Moderate	High
Advantages	Gain some benefits at the initial stage of network construction, because not much data gained from passive one	▪ Measured result may show the real network characteristics ▪ Does not need to generate additional probe messages
Disadvantages	▪ Cannot reflect network characteristics ▪ Need to generate the probe messages which may cause extra overhead to network	▪ Captured data has massive volume size ▪ Should have additional facility to capture the mirrored packet from network

Active Monitoring Techniques

ICMP-based Method

- Diagnose network problems.
- Availability / Round-trip delay / Round-trip packet loss.

TCP-based Method

- One-way bandwidth / Round trip bandwidth.
- Bulk transfer rate.

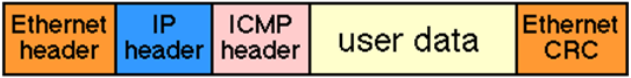
UDP-based Method

- One-way packet loss / Round trip bandwidth.

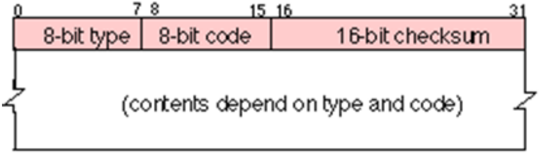
ICMP-based Method 1/5

Active Monitoring - ICMP

- Internet Control Message Protocol (ICMP), RFC 792.
- The purpose of ICMP messages is to provide feedback about problems in the IP network environment.
- Delivered in IP packets.



- ICMP message format.
  - 4 byte of ICMP header and optional message.



ICMP-based Method 2/5

ICMP Functions

- To announce network errors.
  - If a network, host, port is unreachable, ICMP Destination Unreachable Message is sent to the source host.
- To announce network congestion.
  - When a router runs out of buffer queue space, ICMP Source Quench Message is sent to the source host.
- To assist troubleshooting .
  - ICMP Echo Message is sent to a host to test if it is alive - used by ping.
- To announce timeouts.
  - If a packet's TTL field drops to zero, ICMP Time Exceeded Message is sent to the source host - used by traceroute.

ICMP-based Method 3/5

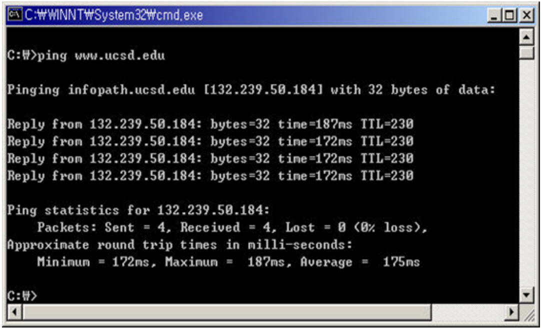
ICMP Drawbacks

- ICMP messages may be blocked (i.e., dropped) by firewall and processed at low priority by router.
- ICMP has also received bad press by being used in many denial of service (DoS) attacks and because of the number of sites generating monitoring traffic.
- As a consequence some ISPs disable ICMP even though this potentially causes poor performance and does not comply with RFC1009 (Internet Gateway Requirements).
- In spite of these limitations, ICMP is still most widely used in active network measurements.

ICMP-based Method 4/5

Ping

- A simple application that runs on a host, typically supplied as part of the host's operating system.
- Uses ICMP ECHO_REQUEST and ECHO_RESPONSE packets.
- Provides round-trip time and packet loss.
- For average measurement, run ping at regular intervals so as to measure the site's latency and packet loss.



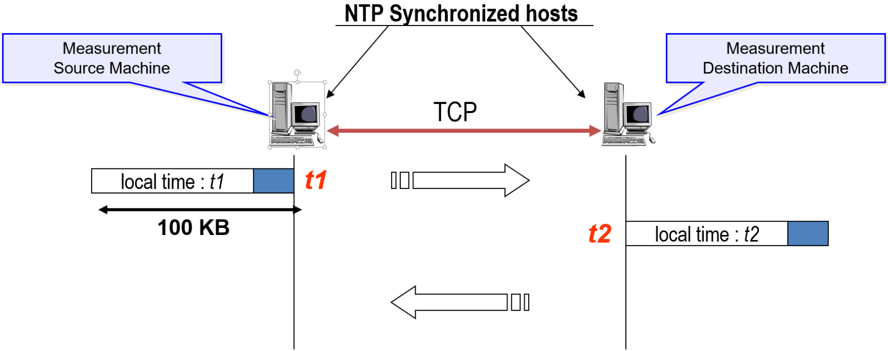
```
C:₩>ping www.ucsd.edu

Pinging infopath.ucsd.edu [132.239.50.184] with 32 bytes of data:

Reply from 132.239.50.184: bytes=32 time=187ms TTL=230
Reply from 132.239.50.184: bytes=32 time=172ms TTL=230
Reply from 132.239.50.184: bytes=32 time=172ms TTL=230
Reply from 132.239.50.184: bytes=32 time=172ms TTL=230

Ping statistics for 132.239.50.184:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 172ms, Maximum =  187ms, Average =  175ms

C:₩>
```

ICMP-based Method 5/5

Traceroute

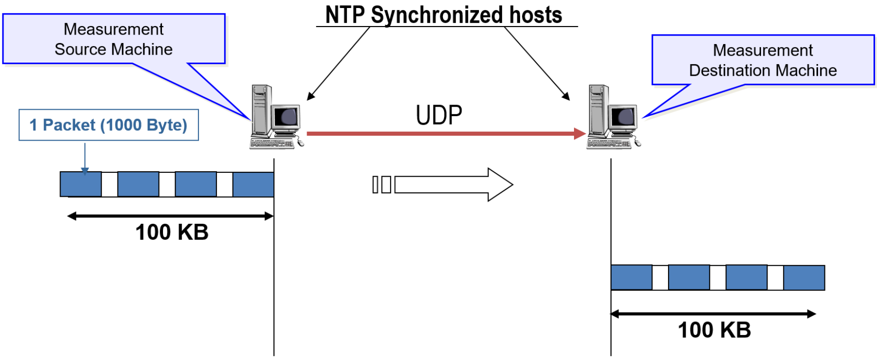
- Produces a hop-by-hop listing for each router along the path to the target host.
- For each hop, it prints the round-trip time for the router.
- Algorithm: uses ICMP and TTL field in the IP header.
  - Send an ICMP packet with TTL=1.
  - First router sends back ICMP TIME_EXCEEDED.
  - Then send ICMP packet with TTL=2 and hear back from the second router.
  - Continue till the destination is reached or TTL expires (default max TTL=30).
- It shows you only the forward path
  - The reverse path is seldom the same.
  - To trace the reverse path one must run traceroute on the remote host (reverse traceroute server, Looking Glass Server).

TCP-based Method



$$\text{Throughput (Mbps)} = \frac{10^5 \times 8}{t2(\mu s) - t1(\mu s)}$$

UDP-based Method

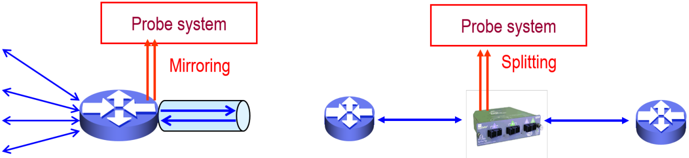


$$\text{One way Loss} = 100 - \frac{\text{Received Packet Counts}}{\text{Sent Packet Counts}} \times 100\ (\%)$$

Packet Capturing 1/2

Packet Capturing

- Packets can be captured using Port Mirroring or Network Splitter (Tap).

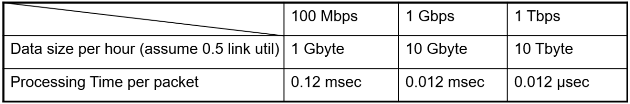


	Port Mirroring	Network Splitter
How it works	- Copies all packets passing on a port to another port	- Splits the signal and sends a signal to original path and another to probe
Advantage	- No extra hardware required	- No processing overhead on router/switch
Disadvantage	- Processing overhead on router/switch	- Splitter hardware required

Packet Capturing 2/2

Difficulties in packet capturing

- Massive amount of data
  - How much packet data is generated from 100 Mbps network in an hour?
    $\rightarrow Portspeed \times InOut \times LinkUtilization \times sec/hour =$
    $throughput100Mbps \times 2 \times 0.5 \times 3600 = 360Gbps$
    $\rightarrow Throughput/avg.packetlength \times bytesofpacketdata =$
    $datasize360Gbps/(1500 \times 8) \times 30 = 1Gbyte$
- Processing of high-speed packets
  - Processing time for 100 Mbps network
    $\rightarrow Portspeed \times InOut \times LinkUtilization/averagepacketlength =$
    $8333packets/sec => 0.12msec/packet$

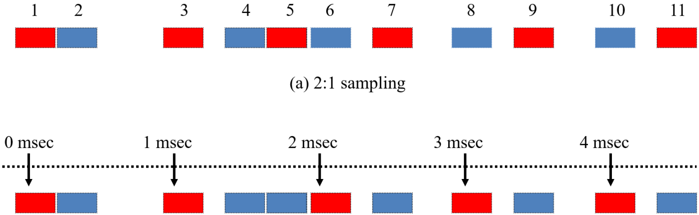


	100 Mbps	1 Gbps	1 Tbps
Data size per hour (assume 0.5 link util)	1 Gbyte	10 Gbyte	10 Tbyte
Processing Time per packet	0.12 msec	0.012 msec	0.012 µsec

Sampling

Why we need sampling?

- If the rate is too high to capture all packets reliably, there is no alternative but to sample the packets.
- Sampling algorithms: every Nth packet or fixed time interval.



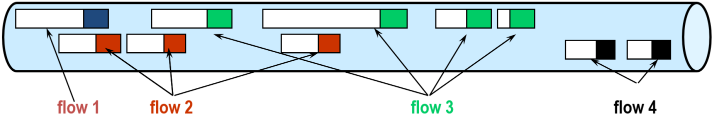
(a) 2:1 sampling

(b) 1 msec sampling

Flow Generation

Flow

- Flow is a collection of packets with the same SRC and DST IP address, SRC and DST port number, protocol number.
- Flow data can be collected from routers directly, or standalone flow generator having packet capturing capability.
- Popular flow formats: NetFlow, sFlow, IPFIX
- Issues in flow generation:
  - What information should be included in a flow data?
  - How to generate flow data from raw packet information efficiently?
  - How to save bulk flow data into DB or binary file in a collector?
  - How long should the data be preserved?



Google Hacking 1/10

When we searching in Google:

- We are not actually searching the web - just the index of the web.
- Indexing is done in google with a software called Spiders.
- Spider collects every links in a particular webpage and the webpages where the links lead to and it goes on and on...
- Once after spidering, there created a big chunk of data which is the index.
- Once the search term is entered, google checks in the index for several criteria and shows the results.
- How many times the search keywords are used.
- Whether it is present in title and the URL.
- Does the page have synonyms and good PR.

Google Hacking 2/10

What is Google Hacking?

- Is not about hacking Google itself.
- Is all about tips and tricks how to get more information from a Google search.
- Is used to search and locate security vulnerabilities on poorly constructed web applications on the Internet.
- Is used by hackers to get the sensitive information about the passwords and so by the easy way.
- Helps us to highly customize the search results.

Google Hacking 3/10

Google search operators

- Two types:
  - Basic operators
  - Advanced operators

Google Hacking 4/10

Basic Operators (symbols)

- "" Double quotes: Exact phrases
- - Minus: Exludes the keyword or values
- + Add : includes the keyword or values
- . Dot: Single character wildcard
- .. Num range: Creates a number range b/w 2
- * Asterisk: Place holder to any unknown term
- ˜ Tilde: Synonyms of the keyword
- ... and more available.

Google Hacking 5/10

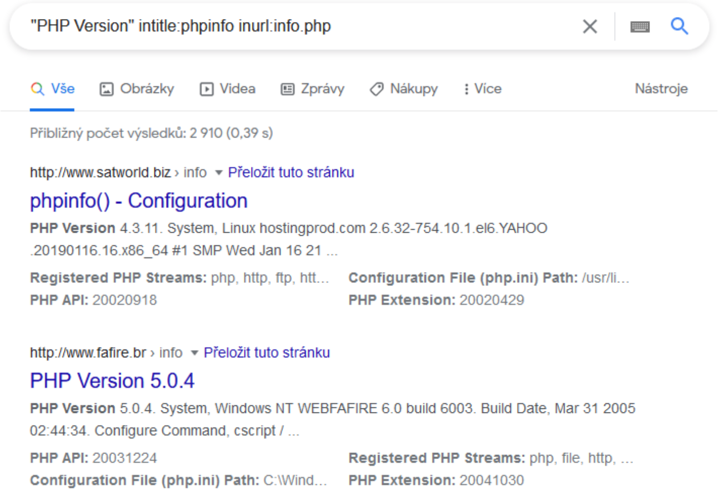
Advanced operators (or keywords)

- Define - shows the definition of the word
- Related - shows related websites
- Similar - shows similar websites
- Cache - shows the cache of a webpage
- Info - shows the information about a web address
- Filetype - finds specific format in the web
- Inurl - searches the keyword in the URL
- Intitle - searches the keyword in the title
- Site: searches in the particular wesite
- The best use of adv. operators are utilized when multiple operator are combined.
- Example: security analytic intitle:"cv" filetype:pdf

Google Hacking 6/10

Unauthenticated programs

- "PHP Version" intitle:phpinfo inurl:info.php



Přibližný počet výsledků: 2 910 (0,39 s)

http://www.satworld.biz › info ▾ Přeložit tuto stránku

phpinfo() - Configuration

PHP Version 4.3.11. System, Linux hostingprod.com 2.6.32-754.10.1.el6.YAHOO .20190116.16.x86_64 #1 SMP Wed Jan 16 21 ...

Registered PHP Streams: php, http, ftp, htt... **Configuration File (php.ini) Path:** /usr/li...
PHP API: 20020918 **PHP Extension:** 20020429

http://www.fafire.br › info ▾ Přeložit tuto stránku

PHP Version 5.0.4

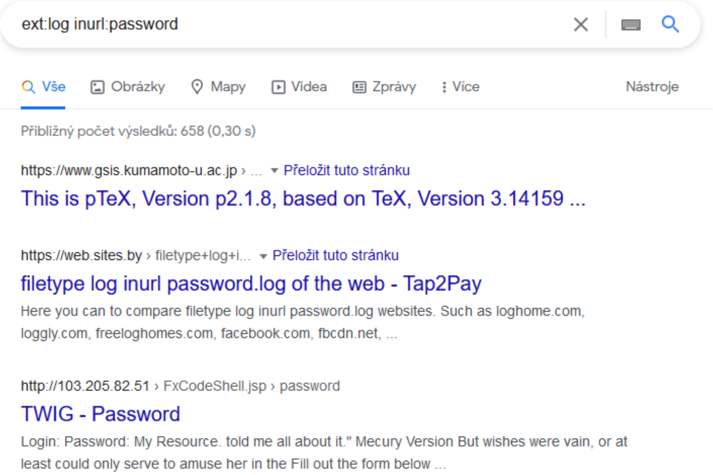
PHP Version 5.0.4. System, Windows NT WEBFAFIRE 6.0 build 6003. Build Date, Mar 31 2005 02:44:34. Configure Command, cscript / ...

PHP API: 20031224 **Registered PHP Streams:** php, file, http, ...
Configuration File (php.ini) Path: C:\Wind... **PHP Extension:** 20041030

Google Hacking 7/10

Clear texts and passwords

- ext:log inurl:password



ext:log inurl:password

Přibližný počet výsledků: 658 (0,30 s)

https://www.gsis.kumamoto-u.ac.jp › ... ▾ Přeložit tuto stránku

This is pTeX, Version p2.1.8, based on TeX, Version 3.14159 ...

https://web.sites.by › filetype+log+i... ▾ Přeložit tuto stránku

filetype log inurl password.log of the web - Tap2Pay

Here you can to compare filetype log inurl password.log websites. Such as loghome.com, loggly.com, freeloghomes.com, facebook.com, fbcdn.net, ...

http://103.205.82.51 › FxCodeShell.jsp › password

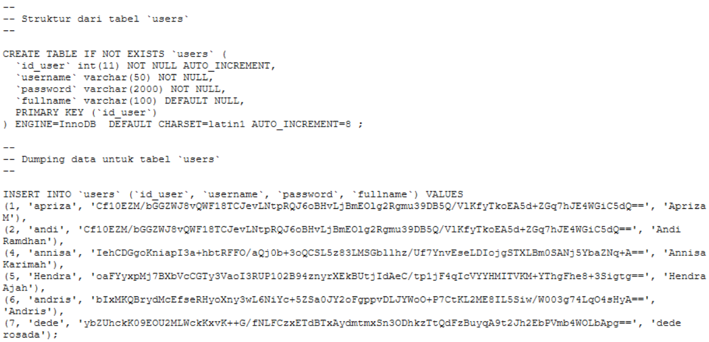
TWIG - Password

Login: Password: My Resource. told me all about it." Mecury Version But wishes were vain, or at least could only serve to amuse her in the Fill out the form below ...

Google Hacking 8/10

Hashed passwords in dump files

- "create table" "insert into" "pass|passwd|password" (ext:sql | ext:dump | ext:dmp)



```
--
-- Struktur dari tabel `users`
--

CREATE TABLE IF NOT EXISTS `users` (
  `id_user` int(11) NOT NULL AUTO_INCREMENT,
  `username` varchar(50) NOT NULL,
  `password` varchar(2000) NOT NULL,
  `fullname` varchar(100) DEFAULT NULL,
  PRIMARY KEY (`id_user`)
) ENGINE=InnoDB  DEFAULT CHARSET=latin1 AUTO_INCREMENT=8 ;

--
-- Dumping data untuk tabel `users`
--

INSERT INTO `users` (`id_user`, `username`, `password`, `fullname`) VALUES
(1, 'apriza', 'Cf10EZM/bGGZWJ8vQWF18TCJevLNtpRQJ6oBHvLjBmEOlg2Rgmu39DB5Q/VlKfyTkoEA5d+ZGq7hJE4WGiC5dQ==', 'Apriza
M'),
(2, 'andi', 'Cf10EZM/bGGZWJ8vQWF18TCJevLNtpRQJ6oBHvLjBmEOlg2Rgmu39DB5Q/VlKfyTkoEA5d+ZGq7hJE4WGiC5dQ==', 'Andi
Ramdhan'),
(4, 'annisa', 'IehCDGgoKniapI3a+hbtRFFO/aQj0b+3oQCSL5z83LMSGbllhz/Uf7YnvEseLDIojgSTXLBm0SANj5YbaZNq+A==', 'Annisa
Karimah'),
(5, 'Hendra', 'oaFYyxpMj7BXbVcCGTy3VaoI3RUP102B94znyrXEkBUtjIdAeC/tp1jF4qIcVYYHMITVKM+YThgFhe8+3Sigtg==', 'Hendra
Ajah'),
(6, 'andris', 'bIxMKQBrydMcEfseRHyoXny3wL6NiYc+5ZSa0JY2oFgppvDLJYWoO+P7CtKL2ME8IL5Siw/W003g74LqO4sHyA==',
'Andris'),
(7, 'dede', 'ybZUhckK09EOU2MLWckKxvK++G/fNLFCzxETdBTxAydmtmxSn3ODhkzTtQdFzBuyqA9t2Jh2EbPVmb4WOLbApg==', 'dede
rosada');
```

Google Hacking 9/10

Live web cameras

- **inurl:/view.shtml** Mostly security cameras, car parks, colleges, etc..
- **inurl:/view/index.shtml** Mostly security cameras, airports, car parks, back gardens, traffic cams, etc...
- **inurl:viewerframe?mode=** Network cameras, mostly private webcams, etc..
- **inurl:"viewerframe?mode=motion"** Web cams

Google Hacking 10/10

Robots.txt

- The robots.txt file contains "rules" about where web spiders are allowed (and NOT allowed) to look in a website's directory structure. Without over-complicating things, this means, that the robots.txt file gives a miniroadmap of what is somewhat public and private on the website. It contains interesting stuff.

Thank you for your attention

Filip Řezáč

VSB – Technical University of Ostrava

filip.rezac@vsb.cz

July 13, 2021