School of Computer Science

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
DEHRADUN, UTTARAKHAND

PHYSICAL AND IT SECURITY LAB

Lab File
(2023-2024)

for

3rd Semester

Submitted To:
Dr Gopal Rawat
Assistant Professor-SS
School of Computer Science

Submitted By:
Akshat Negi
Btech CSF [3rd Semester]
500106533
Batch 2

TABLE OF CONTENTS

8. EXPERIMENT 8:

Network Scanning Tool - NMAP

9. EXPERIMENT 9:

Network Traffic Sniffing – Wireshark

10. EXPERIMENT 10:

Nessus Essentials for Vulnerability Scanning

LAB EXPERIMENT – 1

LOGS TABLE FOR WINDOWS

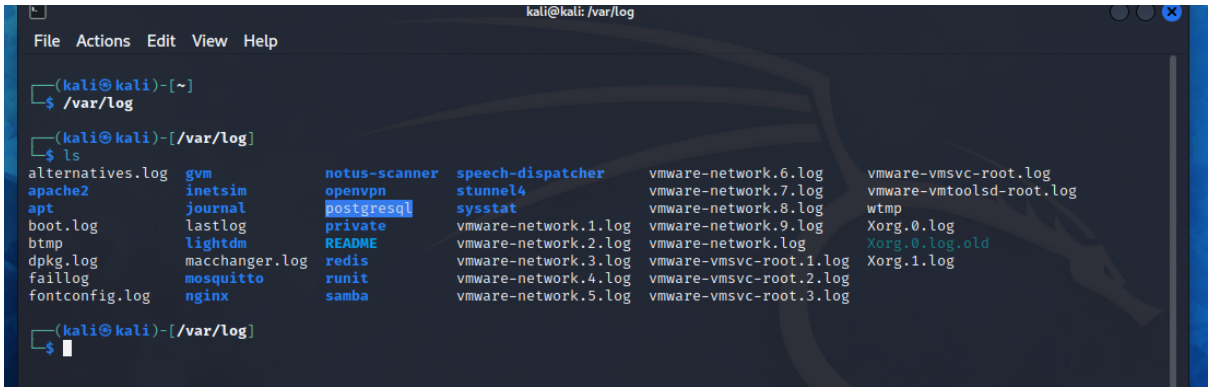
Windows Log	Source	Event ID	General Info	Mitigation Steps
Critical	**Kernel-Power**	**41**	The system has rebooted without cleanly shutting down first. This error could be caused if the system stopped responding, crashed, or lost power unexpectedly.	Basically, to get rid of this type of error is by outdated drivers installed on your devices, so kindly update the audio drivers if still didn't receive any fix, then you can go for all drivers updating process.
Critical	**WinREAgent**	**4502**	This problem occurs when a MicrosoftDNS container is created before a full replication of the application partition.	A supported hotfix is now available from Microsoft, but it is only intended to correct the problem. Only apply it to systems that are experiencing this specific problem. You do not have to restart your computer after you apply this hotfix.
Error	**BugCheck**	**1001**	This type of error usually occurs when third party antivirus software conflicts with windows security.	To resolve this type of event error you need to disable your third-party antivirus installed and even the firewall applications if you are not using antivirus software.
Error	**Service Control Manager**	**7024**	This issue is when the component that raises this event is not installed on your local computer or the installation is corrupted.	To resolve this kind of issues kindly install or repair the component on the local computer.
Error	**DistributedCOM**	**10010**	The server {A463FCB9-6B1C-4E0D-A80B-A2CA7999E25D} did not register with DCOM within the required timeout.	Some steps by which you can fix it are: - 1. Tweak Component Services 2. Enable Function Discovery Resource Publication service 3. Reset DCOM permissions 4. Use SFC Scan 5. Install the latest Windows update 6. Reset your PC
Error	**WindowsUpdateClient**	**20**	Installation Failure: Windows failed to install the following update with error 0x80073D02: 9NMPJ99VJBWV-Microsoft.YourPhone.	If updates are available but are not automatically downloaded then restart the system which can fix these issues.
Error	**Service Control Manager**	**7000**	The Steam Client Service failed to start due to the following error: The service did not respond to the start or control request in a timely fashion.	To fix this error you have to manually give a start to the SteamClient service in services pannel from the START menu.
Error	**NDIS**	**10317**	Miniport Microsoft Wi-Fi Direct Virtual Adapter #2, {1848adcf-46a9-4b89-8ee6-dbcd71e49c54}, had event Fatal error: The miniport has failed a power transition to operational power	This frequently occurs when the mobile broadband device was turned off and is restarting. If you are using router then I suggest you to reset the router and check if the issue persist otherwise reinstall the network drivers.

Error	**Service Control Manager**	**7023**	The NVIDIA LocalSystem Container service terminated with the following error: A generic command executable returned a result that indicates failure.	This is the service failed issue that can be resolved when you just have to restart the service from services from Start Menu.
Error	**volmgr**	**162**	Dump file generation succeeded. {Some files of the Windows 11 are corrupted}	This can be fixed by troubleshooting or repair of Windows 11 by a USB bootable pen drive.

LOGS IN LINUX

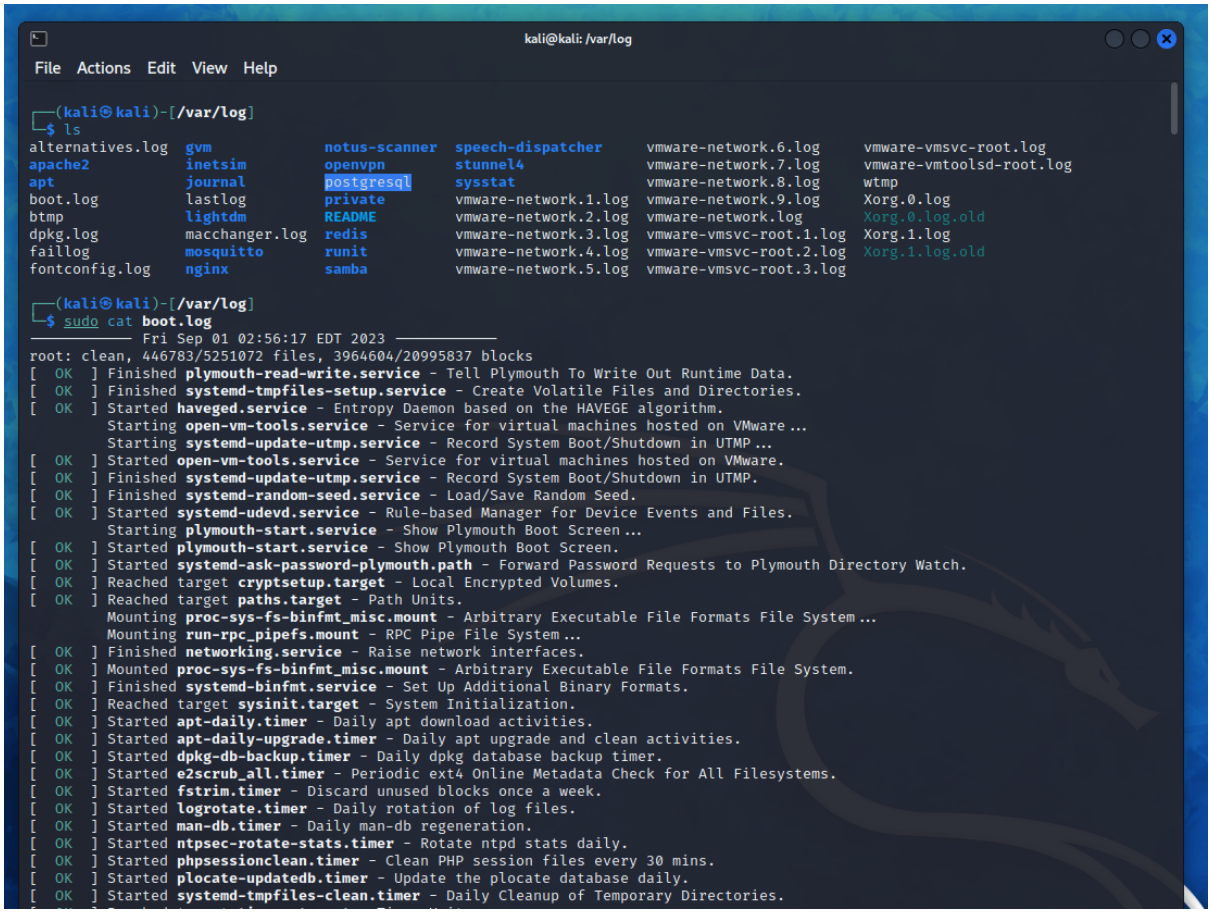
STEP 1: Use the command /var/log

STEP 2: Use the command ls to list the logs for the OS.

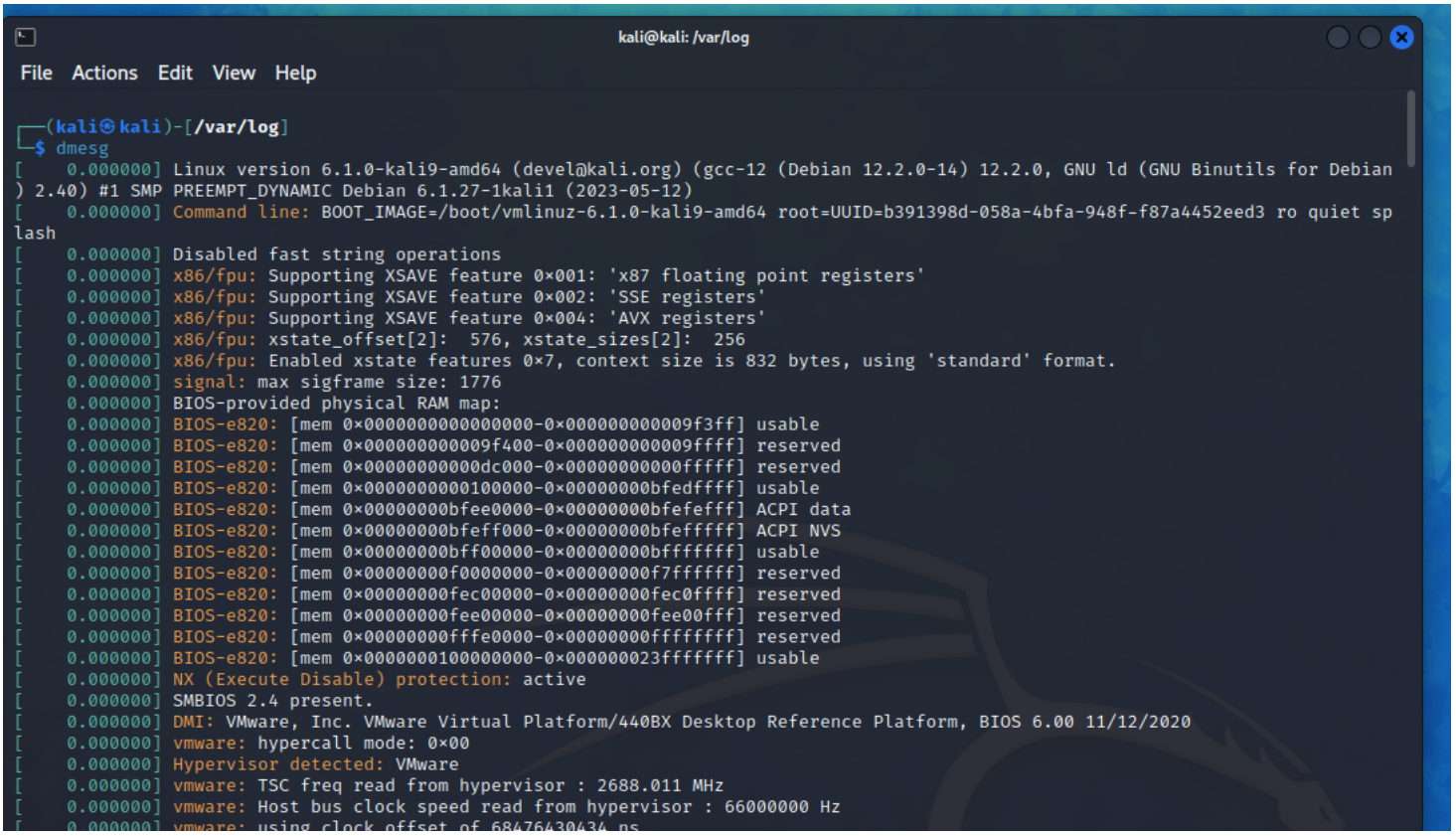


STEP 3: Use the command line 'tail boot.log' for few information of the log file to be displayed.

Step 4: Use the command line ‘cat boot.log’ for all the information of the individual log file to be displayed.



STEP 5: Use the command line ‘dmesg’ shows entire log file contents.



INTRODUCTION

Logging is a crucial aspect of managing and troubleshooting computer systems, applications, and networks. Different levels and categories of logs help you track events, errors, and activities. Here's an overview of important commands and log details for various levels and categories of logs, primarily focusing on Unix/Linux systems:

Logging Levels:

DEBUG: Detailed information, typically used for debugging purposes.

INFO: General information about the system or application.

WARNING: Indicates potential issues or anomalies that should be monitored.

ERROR: Denotes errors that need attention but don't cause system failure.

CRITICAL: Severe errors that may lead to system failure.

LOG CATEGORIES

System Logs:

Command: dmesg - Display kernel ring buffer.

Log File: /var/log/syslog (Ubuntu) or /var/log/messages (Red Hat).

Description: Contains kernel and system-related messages.

Authentication Logs:

Command: ***auth.log*** (Ubuntu) or secure (Red Hat).

Log File: /var/log/auth.log (Ubuntu) or /var/log/secure (Red Hat).

Description: Records authentication-related events like login attempts.

Application Logs:

Command: Varies by application (e.g., Apache, Nginx, MySQL).

Log Files: Typically, in /var/log or specified in application configuration.

Description: Contains information about specific applications' activities.

System Performance Logs:

Command: vmstat, iostat, top, sar.

Log Files: Typically, not stored as logs but generated on-demand.

Description: Provides system performance metrics like CPU, memory, and disk usage.

Security Logs:

Command: auditd (Audit daemon).

Log File: /var/log/audit/audit.log.

Description: Records security-related events for auditing purposes.

Common Log Commands:

View Log Contents:

cat, less, more, tail, head.

Example: tail -f /var/log/syslog (real-time log updates).

Search for Specific Entries:

grep, egrep.

Example: grep "ERROR" /var/log/application.log.

Rotate and Archive Logs:

logrotate.

Configuration files located in /etc/logrotate.conf and /etc/logrotate.d/.

Monitor Logs in Real-Time:

tail -f, journalctl -f.

Clear Log Files (Be cautious):

echo > /var/log/file.log (Truncates the file).

truncate -s 0 /var/log/file.log (Zeroes the file).

Analyze Log Files:

Tools like awk, sed, and log analysis software (e.g., ELK Stack).

Log Format:

Logs typically follow a common format, which may include the following information:

Timestamp: When the event occurred.

Hostname: The name of the system generating the log.

Application/Process Name: The source of the log entry.

Log Level: The severity level (e.g., INFO, ERROR).

Message: A description of the event or error.

Remember to consult documentation and specific log sources for more details and customization options. Proper log management is essential for system troubleshooting, security analysis, and performance optimization.

LAB EXPERIMENT – 2

EMAIL HEADER ANALYSIS

S.NO.	SENDER'S DOMAIN	EMAIL PROTOCOL	DATE/TIME SENT	TIME ZONE	GEOLOCATION
1.	.ru	ESMPTS	06 Sep 2023, Wed 17:06:10	UTC+03:00	UN
2.	.org	SMPTS	22 Mar 2023, Wed 07:51:50	CDT-05:00	UN
3.	.com	SMTP	09 Jul 2023, 05:07:01	GMT +5:30	US
4.	.com	LSMTP	09 Aug 2023, 09:47:58	GMT +5:30	US
5.	.com	ESMPTS	18 Apr 2021, 05:22:09	GMT +5:30	France

BONUS

There are three methods of EMAIL AUTHENTICATION:

- SPF (Sender Policy Framework) : It allows email senders to stipulate the IP addresses allowed to send mail for a specific domain. SPF helps to harden your DNS servers and limit those who use your domain to send emails.

- DKIM (DomainKeys Identified Mail) : It offers an encryption key and digital signature that confirms an email is authentic and not faked or modified.

- DMARC (Domain-based Message Authentication, Reporting, and Conformance): It offers directions on what the receiver should do if a message from a domain fails the authorization test. The email receiver can reject or junk such an email. Unlike SPF and DKIM that can be employed as stand-alone methods, DMARC depends on SPF or DKIM to offer authentication.

ONLY **SPF** IS PASS IN EMAIL AUTHENTICATION

```
        N1xSVSwYfmvdYYIZG8XVfzzrX0Y567QSsqaQJrtxFqvoHsBxjIMqhgoHGH1zKpOXcUj3
        FmKpjkk93e4g4mlzBXOEZej/tue230rcDbewzdHgECn3OgEG8I9tZvRVxvBl6nI5yWQ+
        alcQ==
ARC-Authentication-Results: i=1; mx.google.com;
       spf=pass (google.com: domain of nginx@cs.rin.ru designates 185.100.87.208 as permitted sender) smtp.mailfrom=nginx@cs.rin.ru
Return-Path: <nginx@cs.rin.ru>
Received: from cs.rin.ru (cs.rin.ru. [185.100.87.208])
        by mx.google.com with ESMTPS id a21-20020a656415000000b0041d10a62bfcsi5255218pgv.392.2022.08.31.08.01.03
        for <akshatnegiarchit272003@gmail.com>
        (version=TLS1_3 cipher=TLS_AES_256_GCM_SHA384 bits=256/256);
        Wed, 31 Aug 2022 08:01:03 -0700 (PDT)
Received-SPF: pass (google.com: domain of nginx@cs.rin.ru designates 185.100.87.208 as permitted sender) client-ip=185.100.87.208;
Authentication-Results: mx.google.com;
       spf=pass (google.com: domain of nginx@cs.rin.ru designates 185.100.87.208 as permitted sender) smtp.mailfrom=nginx@cs.rin.ru
Received: by cs.rin.ru (Postfix, from userid 992) id CA99230BF749; Wed, 31 Aug 2022 18:01:01 +0300 (EEST)
To: AkshatNegI27 <akshatnegiarchit272003@gmail.com>
Subject: New password activation
X-PHP-Originating-Script: 1000:functions_messenger.php
From: <noreply@cs.rin.ru>
Reply-To: <noreply@cs.rin.ru>
Sender: <noreply@cs.rin.ru>
```

In this **SPF**, **DKIM** & **DMARC** all three are passed fully Authenticated.

```
        CP4A==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@youtube.com header.s=20230601 header.b=KvTwqgt+;
       spf=pass (google.com: domain of 3oh3_zagle8c01-4r2ybb1767or.p1znxb.o1b.p14214n6v10tznvy.p1z@scoutcamp.bounces.google.com designates 209.85.220.69 as permitted
sender) smtp.mailfrom=3oH3_ZAgLE8c01-4r2yBB1767or.p1znxB.o1B.p14214n6v10tznvy.p1z@scoutcamp.bounces.google.com;
       dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=youtube.com
Return-Path: <3oH3_ZAgLE8c01-4r2yBB1767or.p1znxB.o1B.p14214n6v10tznvy.p1z@scoutcamp.bounces.google.com>
Received: from mail-sor-f69.google.com (mail-sor-f69.google.com. [209.85.220.69])
        by mx.google.com with SMTPS id bq13-20020a056638468d00b00437bf337353sor1179421jab.12.2023.09.11.13.50.40
        for <aky.boy.corporation@gmail.com>
        (Google Transport Security);
        Mon, 11 Sep 2023 13:50:40 -0700 (PDT)
Received-SPF: pass (google.com: domain of 3oh3_zagle8c01-4r2ybb1767or.p1znxb.o1b.p14214n6v10tznvy.p1z@scoutcamp.bounces.google.com designates 209.85.220.69 as
permitted sender) client-ip=209.85.220.69;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@youtube.com header.s=20230601 header.b=KvTwqgt+;
       spf=pass (google.com: domain of 3oh3_zagle8c01-4r2ybb1767or.p1znxb.o1b.p14214n6v10tznvy.p1z@scoutcamp.bounces.google.com designates 209.85.220.69 as permitted
sender) smtp.mailfrom=3oH3_ZAgLE8c01-4r2yBB1767or.p1znxB.o1B.p14214n6v10tznvy.p1z@scoutcamp.bounces.google.com;
       dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=youtube.com
```

EMAIL 1

GMAIL ORIGINAL HEADER VIEW

Original Message

Message ID	<7b8746bfc3a28f56647d1967e8af2a30@cs.rin.ru>
Created at:	Wed, Sep 6, 2023 at 7:36 PM (Delivered after 1 second)
From:	noreply@cs.rin.ru Using phpBB3
To:	AkshatNegI27 <akshatnegiarchit272003@gmail.com>
Subject:	New private message has arrived
SPF:	PASS with IP 2a06:1700:0:3a:43:5352:494e:1337 Learn more

Download Original

Copy to clipboard

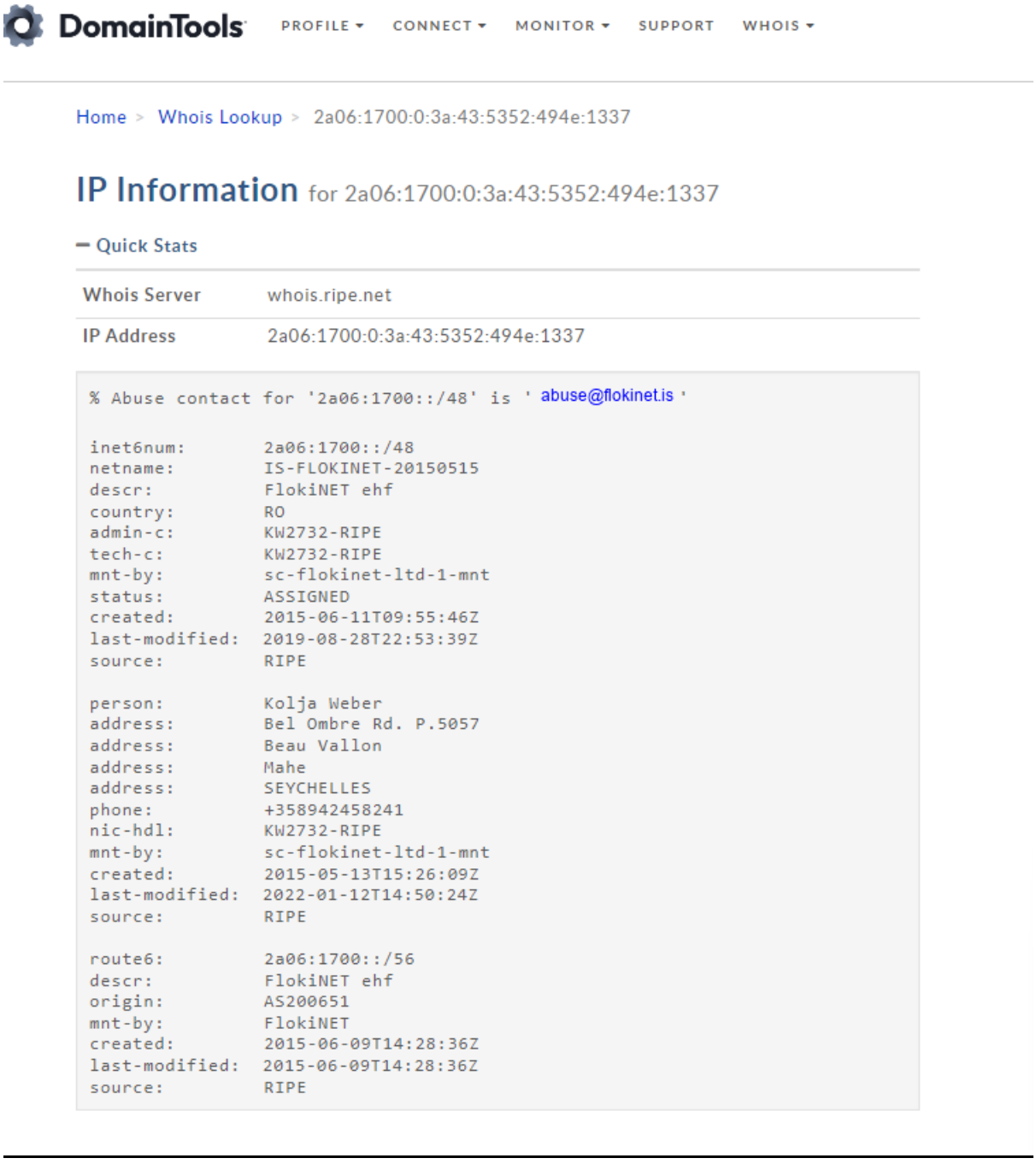
```
Delivered-To: akshatnegiarchit272003@gmail.com
Received: by 2002:a05:7022:3882:b0:6b:573e:d389 with SMTP id pm2csp697648dlb;
        Wed, 6 Sep 2023 07:06:12 -0700 (PDT)
X-Google-Smtp-Source:
AGHT+IFz0O+SpKDmHbY+yfdl0qk/BHj+MS9J+m7St54L/ccavGeGCN0Z5g1XVQ5Jph8TSfpKSw3k
X-Received: by 2002:a1f:c487:0:b0:48f:9778:2b9f with SMTP id u129-
20020a1fc487000000b0048f97782b9fmr2548015vkf.11.1694009171936;
        Wed, 06 Sep 2023 07:06:11 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1694009171; cv=none;
        d=google.com; s=arc-20160816;
        b=xHwRVWGzYAK76hEtq0S81ITD3Y74DFrNPp+a4EH8hRY1LbtbGuCdxmkn5Gz4wisEei
         pqfQUGDHsGt+oERNwu4vSs8I1Q99j923Vu83MhYtapHuyv66/XLpe3+j50DumROYX8Ug
         NYUWc4hx1IfeSz2zlEsEjb5zENkYBnHC6WgFiimTnI1PtQAbBX8awc4yW8Z8fRvW/63d
         SW0br/VmEpkXhtf5Uv8ea3f/iMA3j3zggsSPTTBC8iATFBh38Jpo2MREN9VnMZDn5CEm
         xPfvl1T6QRYEvgXrvG85A+E7ZHpWfzLIiZleDFQqgIgl0gAL6GqpPOCj4xVUTurbT4w8
         drsQ==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-
20160816;
        h=content-transfer-encoding:date:message-id:mime-version:sender
         :reply-to:from:subject:to;
        bh=1ztDCJsLu+B5+9+wXe8LWXnwsDxX1C6bviBuwmYBDX8=:
```

https://toolbox.googleapps.com/

MessageId	7b8746bfc3a28f56647d1967e8af2a30@cs.rin.ru
Created at:	9/6/2023, 7:36:10 PM GMT+5:30 (Delivered after 2 sec)
From:	<noreply@cs.rin.ru> Using phpBB3
To:	AkshatNegI27 <akshatnegiarchit272003@gmail.com>
Subject:	New private message has arrived
SPF:	**pass** with IP 2a06:1700:0:3a:43:5352:494e:1337 Learn more

#	Delay	From *		To *	Protocol	Time received
0	1 sec	cs.rin.ru	→ [Google]	mx.google.com	ESMTPS	9/6/2023, 7:36:11 PM GMT+5:30
1			→ [Google]	2002:a1f:c487:0:b0:48f:9778:2b9f	SMTP	9/6/2023, 7:36:11 PM GMT+5:30
2	1 sec		→ [Google]	2002:a05:7022:3882:b0:6b:573e:d389	SMTP	9/6/2023, 7:36:12 PM GMT+5:30

https://whois.domaintools.com/



DomainTools PROFILE CONNECT MONITOR SUPPORT WHOIS

Home > Whois Lookup > 2a06:1700:0:3a:43:5352:494e:1337

IP Information for 2a06:1700:0:3a:43:5352:494e:1337

− Quick Stats

Whois Server	whois.ripe.net
IP Address	2a06:1700:0:3a:43:5352:494e:1337

```
% Abuse contact for '2a06:1700::/48' is ' abuse@flokinet.is '

inet6num:       2a06:1700::/48
netname:        IS-FLOKINET-20150515
descr:          FlokiNET ehf
country:        RO
admin-c:        KW2732-RIPE
tech-c:         KW2732-RIPE
mnt-by:         sc-flokinet-ltd-1-mnt
status:         ASSIGNED
created:        2015-06-11T09:55:46Z
last-modified:  2019-08-28T22:53:39Z
source:         RIPE

person:         Kolja Weber
address:        Bel Ombre Rd. P.5057
address:        Beau Vallon
address:        Mahe
address:        SEYCHELLES
phone:          +358942458241
nic-hdl:        KW2732-RIPE
mnt-by:         sc-flokinet-ltd-1-mnt
created:        2015-05-13T15:26:09Z
last-modified:  2022-01-12T14:50:24Z
source:         RIPE

route6:         2a06:1700::/56
descr:          FlokiNET ehf
origin:         AS200651
mnt-by:         FlokiNET
created:        2015-06-09T14:28:36Z
last-modified:  2015-06-09T14:28:36Z
source:         RIPE
```

https://mxtoolbox.com/

Header Name	Header Value
Delivered-To	akshatnegiarchit272003@gmail.com
X-Google-Smtp-Source	AGHT+IFz0O+SpKDmHbY+yfdl0qk/BHj+MS9J+m7St54L/ccavGeGCN0Z5g1XVQ5Jph8TSfpKSw3k
X-Received	by 2002:a1f:c487:0:b0:48f:9778:2b9f with SMTP id u129-20020a1fc487000000b0048f97782b9fmr2548015vkf.11.1694009171936; Wed, 06 Sep 2023 07:06:11 -0700 (PDT)
ARC-Seal	i=1; a=rsa-sha256; t=1694009171; cv=none; d=google.com; s=arc-20160816; b=xHwRVWGzYAK76hEtq0S81ITD3Y74DFrNPp+a4EH8hRY1LbtbGuCdxmkn5Gz4wisEei pqfQUGDHsGt+oERNwu4vSs8hQ99j923Vu83MhYtapHuyv66/XLpe3+j50DumROYX8Ug NYUWc4hx1IfeSz2zlEsEjb5zENkYBnHC6WgFiimTnH1PtQAbBX8awc4yW8Z8fRvW/63d SW0br/VmEpkXhtf5Uv8ea3f/iMA3j3zggsSPTTBC8iATFBh38Jpo2MREN9VnMZDn5CEm xPfvl1T6QRYEvgXrvG85A+E7ZHpWfzLliZleDFQqglgl0gAL6GqpPOCj4xVUTurbT4w8 drsQ==
ARC-Message-Signature	i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816; h=content-transfer-encoding:date:message-id:mime-version:sender :reply-to:from:subject:to; bh=1ztDCJsLu+B5+9+wXe8LWXnwsDxX1C6byiBuwmYBDX8=; fh=nFaHerUKDMpYiFEnLlE6QoD8P/kUBTqNCTgRG+x/lqs=; b=j9SGOTbReaNSwMpgkxkdP6isGDRUrruzkFXrGenat8V1xysrUHmVKAklG7jWoU7bl1 gBfVfHA8UszoFkVh6VMvvDoBWiewaBVjAQc8bYYe/qe0fQTQGDKLSG8rt3i6Cqy/SWMc z5w+/mHC0OfWSFR+WYEJoa7498GJnHjK7FfzYLnZRempBLIAuRWAj0Q56vHlGeYqfrOU pgLJ4ceVb7XqtLXicAk1JlwHYyJlc1b/DXUnQRTlEBnJWJttUimZ3Nih3fkzPe1i4gu8 Xmoa3A38biAi3uVV7mVnYuuV2bOErhKeQFLxCDi9xx/rmJevSPM3vKtr7/X1KPqDJVXS 19qw==
ARC-Authentication-Results	i=1; mx.google.com; spf=pass (google.com: domain of php-fpm-csrin@cs.rin.ru designates 2a06:1700:0:3a:43:5352:494e:1337 as permitted sender) smtp.mailfrom=php-fpm-csrin@cs.rin.ru
Return-Path	<php-fpm-csrin@cs.rin.ru>
Received-SPF	pass (google.com: domain of php-fpm-csrin@cs.rin.ru designates 2a06:1700:0:3a:43:5352:494e:1337 as permitted sender) client-ip=2a06:1700:0:3a:43:5352:494e:1337;
Authentication-Results	mx.google.com; spf=pass (google.com: domain of php-fpm-csrin@cs.rin.ru designates 2a06:1700:0:3a:43:5352:494e:1337 as permitted sender) smtp.mailfrom=php-fpm-csrin@cs.rin.ru
To	AkshatNegI27 <akshatnegiarchit272003@gmail.com>
Subject	New private message has arrived
X-PHP-Originating-Script	1000:functions_messenger.php
From	<noreply@cs.rin.ru>
Reply-To	<noreply@cs.rin.ru>
Sender	<noreply@cs.rin.ru>
MIME-Version	1.0
Message-ID	<7b8746bfc3a28f56647d1967e8af2a30@cs.rin.ru>
Date	Wed, 06 Sep 2023 17:06:10 +0300
Content-Type	text/plain; charset=UTF-8

Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	userid	cs.rin.ru		9/6/2023 2:06:10 PM	
2	1 Second	cs.rin.ru 2a06:1700:0:3a:43:5352:494e:1337	mx.google.com	ESMTPS	9/6/2023 2:06:11 PM	✓
3	1 Second		2002:a05:7022:3882:b0:6b:573e:d389	SMTP	9/6/2023 2:06:12 PM	

EMAIL 2

GMAIL ORIGINAL HEADER VIEW

Original Message

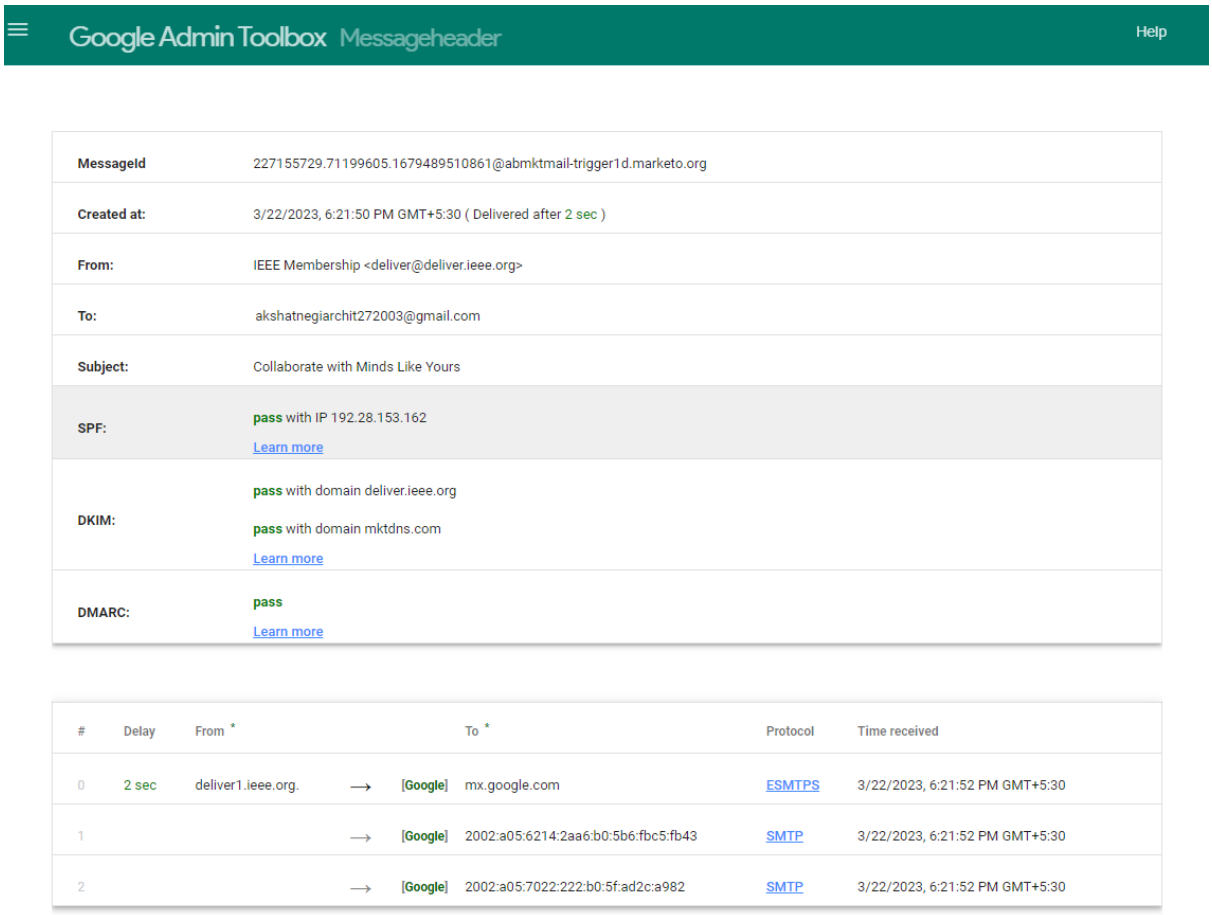
Message ID	<227155729.71199605.1679489510861@abmktmail-trigger1d.marketo.org>
Created at:	Wed, Mar 22, 2023 at 6:21 PM (Delivered after 2 seconds)
From:	IEEE Membership <deliver@deliver.ieee.org>
To:	akshatnegiarchit272003@gmail.com
Subject:	Collaborate with Minds Like Yours
SPF:	PASS with IP 192.28.153.162 Learn more
DKIM:	'PASS' with domain deliver.ieee.org Learn more
DMARC:	'PASS' Learn more

Download Original

Copy to clipboard

```
Delivered-To: akshatnegiarchit272003@gmail.com
Received: by 2002:a05:7022:222:b0:5f:ad2c:a982 with SMTP id 34csp3036212dll;
        Wed, 22 Mar 2023 05:51:52 -0700 (PDT)
X-Google-Smtp-Source: AK7set8fYaVY43t5niY377cwLMZtXzBiW4cfK1RxkVH7jsW8idmj2dwDex2IfbfKxv4oStL/hayb
X-Received: by 2002:a05:6214:2aa6:b0:5b6:fbc5:fb43 with SMTP id js6-
20020a0562142aa600b005b6fbc5fb43mr5022800qvb.30.1679489512126;
        Wed, 22 Mar 2023 05:51:52 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1679489512; cv=none;
        d=google.com; s=arc-20160816;
        b=onYx9u7CE2Z5oTHCClGPydohpIPEzXWbMU8qDn8vzAMSdU53cTQJuIrDk1qToe2jtu
         UwAoWUG+K/G39a4RFBfeJXe2QTciGcV+zxRan3NHa8AWW0SPcAhcO9YlTUhzZ15oLY7b
         gysz3CKIUcJOV7nl2IqeW4JRLzglpxG+L63MiyMGJ89plrqNHgm+8fw+iw1+rDB5tpkw
         bAgH2RYHxuHXMHwDKbu3T1rKlcceQHVPiUY633OM1k+7a7Byb4+71XI6wPFxXyDW/h6s
         GfEiK2iLaPM9f2xn6FtMxi5jrGmzu7hrz3fuCfxgS2lBpf525cVsTLh6JUksm7PfH/Y4
         UY1g==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=list-unsubscribe:mime-version:subject:message-id:to:reply-to:from
         :date:dkim-signature:dkim-signature;
        bh=GO1g4XKh9CgT0I5mvWTxrzWeDiqhSzSkn4eG/IEHC4g=;
        b=yEvfU7BzzGwSMJO+VSumnEXezLGbH+7MTEKSadJQ1tiqRGRa6Oy3FmFAi/2Z8YbNUI
```

https://toolbox.googleapps.com/



https://whois.domaintools.com/

DomainTools PROFILE CONNECT MONITOR SUPPORT Whois Lookup

Home > Whois Lookup > 192.28.153.162

IP Information for 192.28.153.162

Quick Stats

IP Location	United States San Mateo Marketo Inc.
ASN	AS15224 OMNITURE, US (registered Apr 05, 2000)
Resolve Host	deliver1.ieee.org
Whois Server	whois.arin.net
IP Address	192.28.153.162

```
NetRange:       192.28.144.0 - 192.28.191.255
CIDR:           192.28.144.0/20, 192.28.160.0/19
NetName:        MARKETO-CORE2
NetHandle:      NET-192-28-144-0-1
Parent:         NET192 (NET-192-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   MARKETO, Inc. (MARKE-120)
RegDate:        2014-02-27
Updated:        2014-03-06
Ref:            https://rdap.arin.net/registry/ip/192.28.144.0

OrgName:        MARKETO, Inc.
OrgId:          MARKE-120
Address:        901 MARINERS ISLAND BL
Address:        #200
City:           San Mateo
StateProv:      CA
PostalCode:     94404
Country:        US
RegDate:        2010-02-09
Updated:        2022-01-04
Ref:            https://rdap.arin.net/registry/entity/MARKE-120

OrgTechHandle: ASNE-ARIN
OrgTechName:   Adobe SaaS Network Engineering
OrgTechPhone:  +1-385-345-0000
OrgTechEmail:  global-delivops-team@adobe.com
OrgTechRef:    https://rdap.arin.net/registry/entity/ASNE-ARIN

OrgAbuseHandle: ABUSE2888-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-408-536-2800
```

https://mxtoolbox.com/

Headers Found

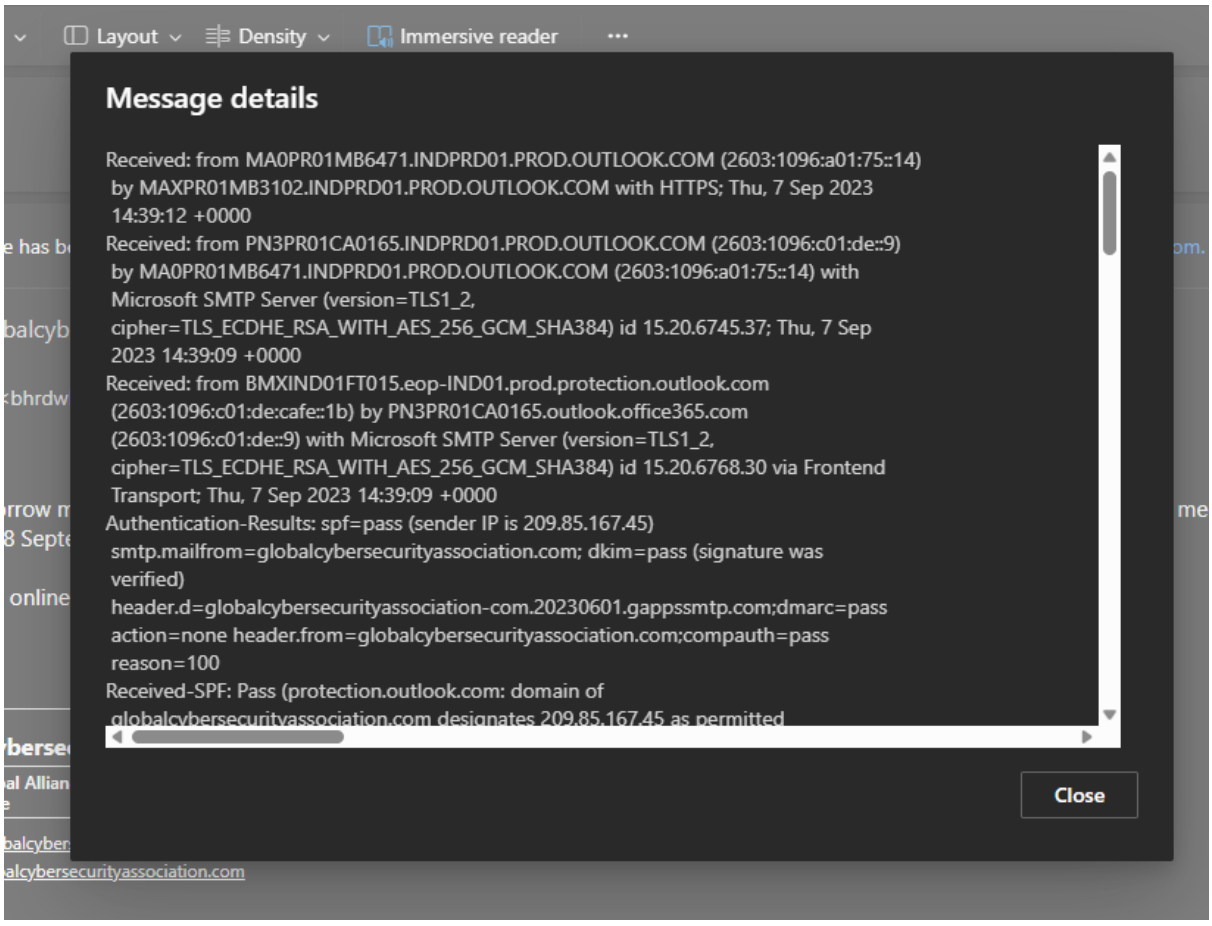
Header Name	Header Value
Delivered-To	akshatnegiarchit272003@gmail.com
X-Google-Smtp-Source	AK7set8fYaVY43t5niY377cwLMZtXzBiW4cfK1RxkVH7jsW8idmj2dwDex2IfbfKxv4oStL/hayb
X-Received	by 2002:a05:6214:2aa6:b0:5b6:fbc5:fb43 with SMTP id js6-20020a0562142aa600b005b6fbc5fb43mr5022800qvb.30.16794895 12126; Wed, 22 Mar 2023 05:51:52 -0700 (PDT)
ARC-Seal	i=1; a=rsa-sha256; t=1679489512; cv=none; d=google.com; s=arc-20160816; b=onYx9u7CE2Z5oTHCClGPydohpIPEzXWbMU8qDn8 vzAMSdU53cTQJulrDk1qToe2jtu UwAoWUG+K/G39a4RFBfeJXe2QTciGcV+zxRan3NHa8AWW0SPcAhcO9YITUhzZ15oLY7b gysz3C KIUcJOV7nl2lqeW4JRLzglpxG+L63MiyMGJ89plrqNHgm+8fw+iw1+rDB5tpkw bAgH2RYHxuHXMHwDKbu3T1rKlcceQHVPiUY633O M1k+7a7Byb4+71Xl6wPFxXyDW/h6s GfEiK2iLaPM9f2xn6FtMxi5jrGmzu7hrz3fuCfxgS2lBpf525cVsTLh6JUksm7PfH/Y4 UY1g==
ARC-Message-Signature	i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816; h=list-unsubscribe:mime-version:subject:message-id:to:re ply-to:from :date:dkim-signature:dkim-signature; bh=GO1g4XKh9CgT0l5mvWTxrzWeDiqhSzSkn4eG/IEHC4g=; b=yEvfU7BzzGwSM JO+VSumnEXezLGbH+7MTEKSadJQ1tiqRGRa6Oy3FmFAi/2Z8YbNUI d/1GNdJllFG6uzxQzptZWr8ZLpnly0jzirsvluPwF/D2imnBS45N6 WMiUUcIEOOkUMag zCXWycza0BN2A+V67tnnNBnsf1wrJHQ5w201cY8jplXoi9EK7cp1O6wuCJtsLCsESvAB U5Ty4FuxHRWN4lXv/w m2AwSObOTpDWthXJKqK6Ym+wwFeEuN/FwzWg8kkXaUGUxXlurU 4lpRpgCeA2cdg5houERzWKCOBmYjYCcvvMtMZ0uJBRGopy 90Y98PVWIlzX15oSFB5JBn wV0A==
ARC-Authentication-Results	i=1; mx.google.com; dkim=pass header.i=@deliver.ieee.org header.s=m1 header.b=MF6bNZv8; dkim=pass header.i=@mktdns.com header.s=m1 header.b=ZQ7hOyZ4; spf=pass (google.com: domain of 756-gph-899.0.30772.0.0.28936.9.50340944-1@deliver.iee e.org designates 192.28.153.162 as permitted sender) smtp.mailfrom=756-GPH-899.0.30772.0.0.28936.9.50340944-1@deliver.ie ee.org; dmarc=pass (p=QUARANTINE sp=QUARANTINE dis=NONE) header.from=deliver.ieee.org
Return-Path	<756-GPH-899.0.30772.0.0.28936.9.50340944-1@deliver.ieee.org>
Received-SPF	pass (google.com: domain of 756-gph-899.0.30772.0.0.28936.9.50340944-1@deliver.ieee.org designates 192.28.153.162 as per mitted sender) client-ip=192.28.153.162;
Authentication-Results	mx.google.com; dkim=pass header.i=@deliver.ieee.org header.s=m1 header.b=MF6bNZv8; dkim=pass header.i=@mktdns.com hea der.s=m1 header.b=ZQ7hOyZ4; spf=pass (google.com: domain of 756-gph-899.0.30772.0.0.28936.9.50340944-1@deliver.ieee.or g designates 192.28.153.162 as permitted sender) smtp.mailfrom=756-GPH-899.0.30772.0.0.28936.9.50340944-1@deliver.ieee. org; dmarc=pass (p=QUARANTINE sp=QUARANTINE dis=NONE) header.from=deliver.ieee.org
X-MSFBL	duTRVtLn4l13U2xs5AC1hVTM3SSmEjfHWMmu55vJUsE=eyJ1IjoiNzU2LUdQSC0 4OTk6MDoyNjE4MDo2MjU0NzowOjI4OTM2Ojk6M zA3NzI6NTAzNDA5NDQtMSIsImc iOiJiZy1hYmQtNzA1IiwiYiI6ImR2cC0xOTItMjgtMTUzLTE1MCIsInliOiJha3N oYXRuZWdpYXJjaGl0Mj cyMDAzQGdtYWlsLmNvbSJ9
DKIM-Signature	v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed; t=1679489510; s=m1; d=deliver.ieee.org; i=@deliver.ieee.org; h=Content-Type:MI ME-Version:Subject:To:From:Date; bh=GO1g4XKh9CgT0l5mvWTxrzWeDiqhSzSkn4eG/IEHC4g=; b=MF6bNZv86pRcwfUqMglbLRfS nvLXoO6uRTR13UFvlGhaW+G9aEU/k8iLaCF1DHln i1wHN3RHQmm750/Et6/0u2H1swGZAaKVs5Z0ftYRz0MNWSLuxY7ZCJmZ01Ta Olyrq9d AcZ3wWlAHLz+5YEH+g7SR8BiajTFoNFgTo5hWgpE=
Date	Wed, 22 Mar 2023 07:51:50 -0500 (CDT)
From	IEEE Membership <deliver@deliver.ieee.org>
Reply-To	no-reply@deliver.ieee.org

Date	Wed, 22 Mar 2023 07:51:50 -0500 (CDT)
From	IEEE Membership <deliver@deliver.ieee.org>
Reply-To	no-reply@deliver.ieee.org
To	akshatnegiarchit272003@gmail.com
Message-ID	<227155729.71199605.1679489510861@abmktmail-trigger1d.marketo.org>
Subject	Collaborate with Minds Like Yours
MIME-Version	1.0
Content-Type	multipart/alternative; boundary="----=_Part_71199604_607877396.1679489510860"
X-Binding	bg-abd-705
X-MarketoID	756-GPH-899:0:26180:62547:0:28936:9:30772:50340944-1
X-Mailfrom	756-GPH-899.0.30772.0.0.28936.9.50340944-1@deliver.ieee.org
List-Unsubscribe	<mailto:KBREUT3XLJVFERDPMJMVO4CVLJIGGUDOK5VTKVLVIVLGY5KHGZXHMS2MGF2GCMCZKRZVCPI=.30772.28936.9@unsu b-ab.mktomail.com>
X-MktArchive	false
X-MSYS-API	{"options":{"open_tracking":false,"click_tracking":false}}
X-MktMailDKIM	true

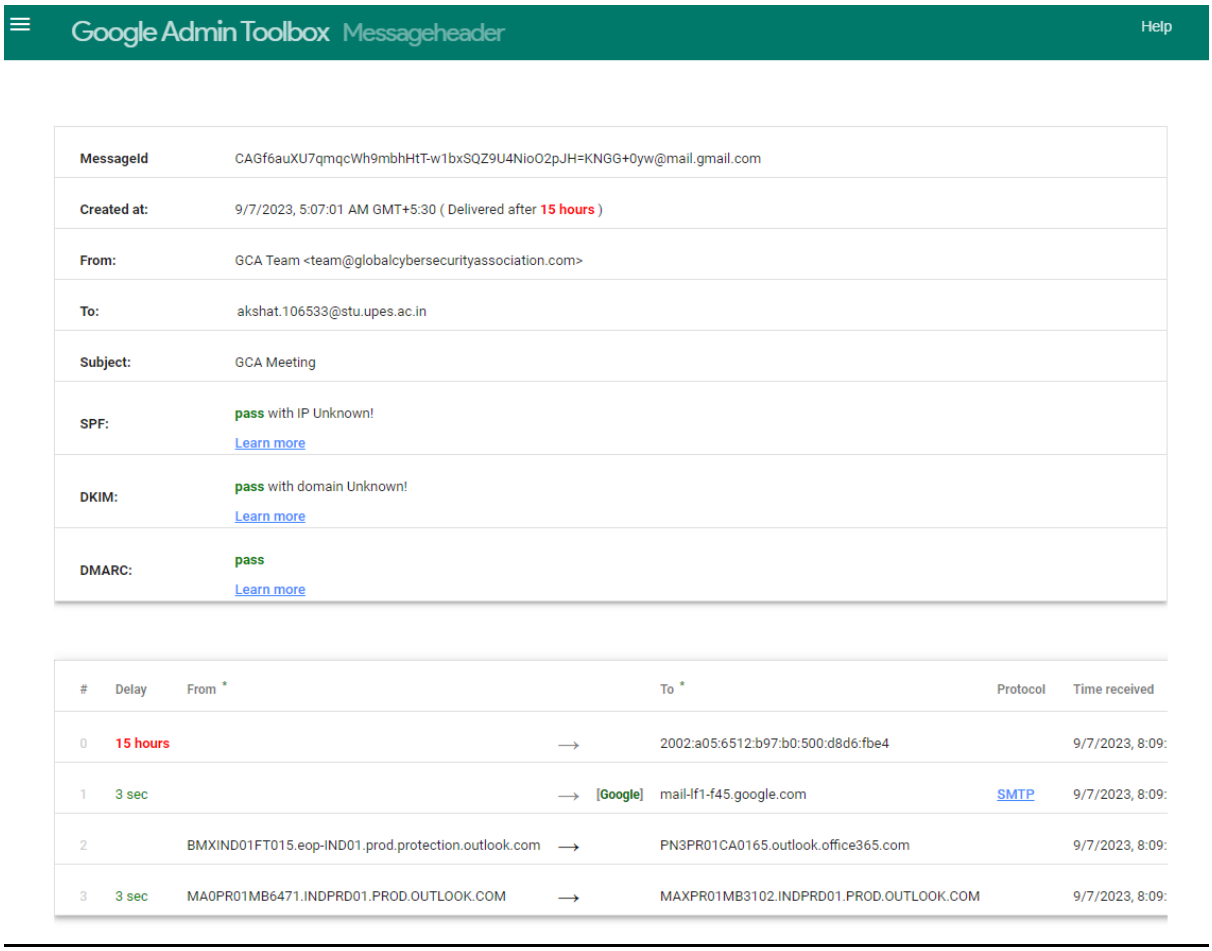
Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	deliver1.ieee.org 192.28.153.162	mx.google.com	ESMTPS	3/22/2023 12:51:52 PM	
2	0 seconds		2002:a05:7022:222:b0:5f:ad2c:a982	SMTP	3/22/2023 12:51:52 PM	

EMAIL 3

OUTLOOK ORIGINAL HEADER VIEW



https://toolbox.googleapps.com/



https://whois.domaintools.com/

DomainTools PROFILE CONNECT MONITOR SUPPORT Whois Lookup

IP Information for 209.85.167.45

Quick Stats

IP Location	United States Mountain View Google
ASN	AS15169 GOOGLE, US (registered Mar 30, 2000)
Resolve Host	mail-lf1-f45.google.com
Whois Server	whois.arin.net
IP Address	209.85.167.45
Reverse IP	1 website uses this address.

```
NetRange:       209.85.128.0 - 209.85.255.255
CIDR:           209.85.128.0/17
NetName:        GOOGLE
NetHandle:      NET-209-85-128-0-1
Parent:         NET209 (NET-209-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Google LLC (GOGL)
RegDate:        2006-01-13
Updated:        2012-02-24
Ref:            https://rdap.arin.net/registry/ip/209.85.128.0

OrgName:        Google LLC
OrgId:          GOGL
Address:        1600 Amphitheatre Parkway
City:           Mountain View
StateProv:      CA
PostalCode:     94043
Country:        US
RegDate:        2000-03-30
Updated:        2019-10-31
Comment:        Please note that the recommended way to file abuse complaints are located in

the following links.
Comment:
Comment:        To report abuse and illegal activity: https://www.google.com/contact/
Comment:
Comment:        For legal requests: http://support.google.com/legal
Comment:
Comment:        Regards,
Comment:        The Google Team
Ref:            https://rdap.arin.net/registry/entity/GOGL

OrgTechHandle: ZG39-ARIN
OrgTechName:   Google LLC
OrgTechPhone:  +1-650-253-0000
```

https://mxtoolbox.com/

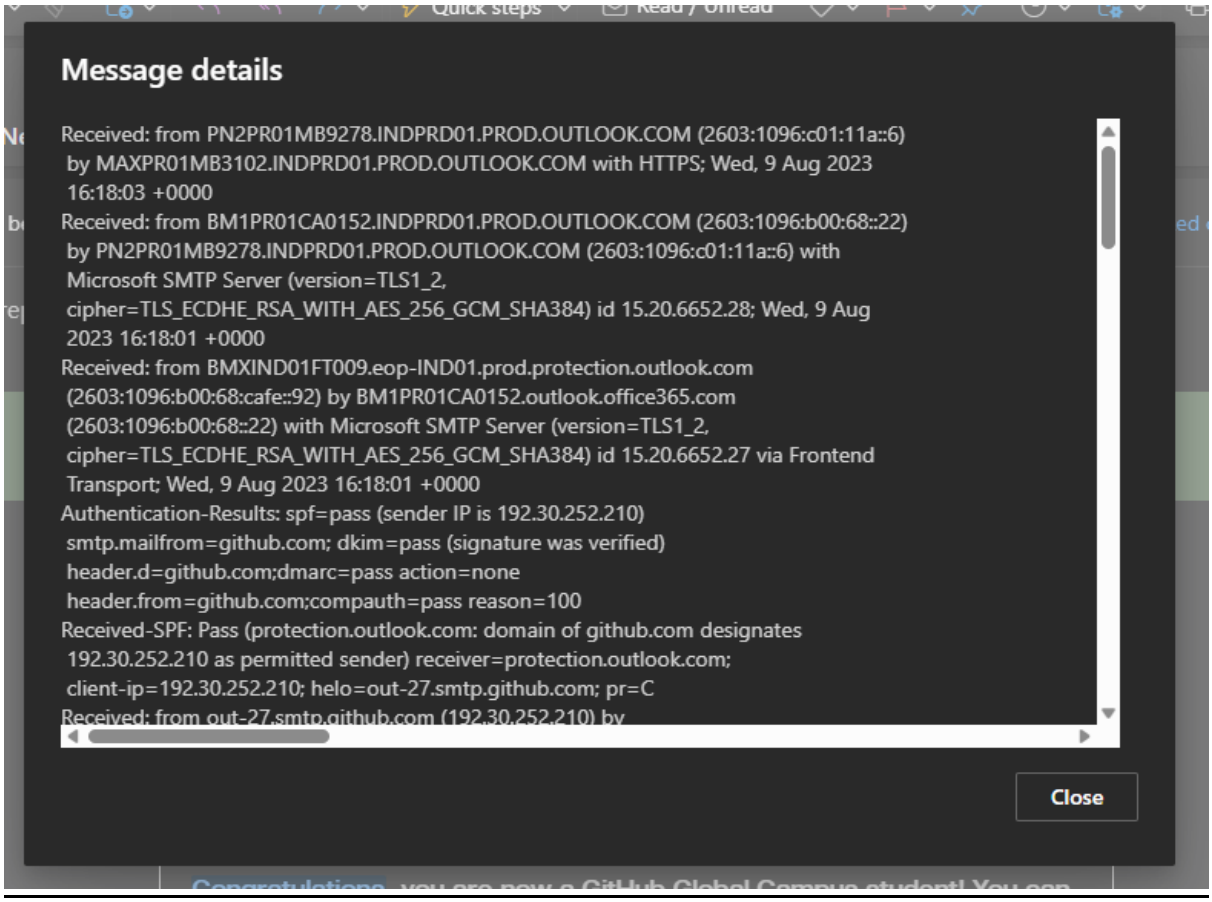
Headers Found

Header Name	Header Value
Authentication-Results	spf=pass (sender IP is 209.85.167.45) smtp.mailfrom=globalcybersecurityassociation.com; dkim=pass (signature was verified) header.d=globalcybersecurityassociation-com.20230601.gappssmtp.com;dmarc=pass action=none header.from=globalcybersecurityassociation.com;compauth=pass reason=100
Received-SPF	Pass (protection.outlook.com: domain of globalcybersecurityassociation.com designates 209.85.167.45 as permitted sender) receiver=protection.outlook.com; client-ip=209.85.167.45; helo=mail-lf1-f45.google.com; pr=C
DKIM-Signature	v=1; a=rsa-sha256; c=relaxed/relaxed; d=globalcybersecurityassociation-com.20230601.gappssmtp.com; s=20230601; t=1694097546; x=1694702346; darn=stu.upes.ac.in; h=cc:to:subject:message-id:date:from:mime-version:from:to:cc:subject :date:message-id:reply-to; bh=FuswQlhPM65tYvJRgf49frYoq6X1D5AoJk1JEeXvupw=; b=bepMk8HVAedQmqvz/1BMdlHnbj3vXwzUCdWuFlJt3UvhWpsalsCa317Mo2WM8sHHMt Zha0+bV+PBXJUxf7tiDqYJ1PTrmxtQLe8HH5+eODQNFQE0l3FWVFOfM8ExYYNvOue/Zg vTf7ldnZ3lE5H1QdBiQ1p+iyOmzLFAj73gku4awUU+dhV47k53puy4UUULWQ2cS7IFl6WdXwGmkvHQMnnUOlwCmCaYHfMAMf78YKhfmRN9QU0AwxMAih84ztmliCb05W0ktDjUpr R4YhWff04ofhggyc8leJu5M7rVa8qLk8pTNfmXSvL+Lp3lHeezl7o32rNm7a31hQh37Z MMug==
X-Google-DKIM-Signature	v=1; a=rsa-sha256; c=relaxed/relaxed; d=1e100.net; s=20221208; t=1694097546; x=1694702346; h=cc:to:subject:message-id:date:from:mime-version:x-gm-message-state :from:to:cc:subject:date:message-id:reply-to; bh=FuswQlhPM65tYvJRgf49frYoq6X1D5AoJk1JEeXvupw=; b=KA5P0w2RDBLRXlz9mAyFBLuaydL9JpOEu6bltA5DnKq70fFLI8s/Mi6Vme6FWp4lra dWowyuEv0UU/8Zk1B0o0m4VBL3WFA+wsXYymgN77FH0giR1ufELQTkAEKvWe9a3OGOTf ytUchpmulyS2h5njWREKaAs9RFRW48jSNsa+qnMWLtkgrzzcWlHeHdElBXlMCdqulSyE YncLU/n38ICP9fHaOeXVaFOslVPjB+Q+t4nFl3m94tX7spDOFNVxRSbcN1iYiyrK5QNg /7S/kZmv1iDmSThVferMQ4ZjcWJdlaYST+7vwXeX1UPXkvztd55rAAPcM0LcyMePqvEu 7z+g==
X-Gm-Message-State	AOJu0Yw/jJPYDqyal/TehMtTadQ3xer7XTAt6DHVvRxEzbEEAkYZ1pBq NtioP06zOyq/RSVtPlRrIfDhOn6sTHA1rUCoY9uHDJAP+8f7XT28
X-Google-Smtp-Source	AGHT+IFa1i1F3k4ADdMXtm+DkDKYhbYlsBsjx+cQU/PwTrsDSEDEW5ZjfPOKFjUN3yuvaFwOCe1jSigHMZanvd1iwc=
X-Received	by 2002:a05:6512:b97:b0:500:d8d6:fbe4 with SMTP id b23-20020a0565120b9700b00500d8d6fbe4mr5906961lfv.49.1694097546120; Thu, 07 Sep 2023 07:39:06 -0700 (PDT)
MIME-Version	1.0
From	GCA Team <team@globalcybersecurityassociation.com>
Date	Wed, 6 Sep 2023 15:37:01 -0800
Message-ID	<CAGf6auXU7qmqcWh9mbhHtT-w1bxSQZ9U4NioO2pJH=KNGG+0yw@mail.gmail.com>
Subject	GCA Meeting
To	akshat.106533@stu.upes.ac.in
Cc	Akashdeep Bhardwaj <bhrdwh@yahoo.com>
Content-Type	multipart/alternative; boundary="00000000000073a8480604c5d22e"
Return-Path	team@globalcybersecurityassociation.com
X-MS-Exchange-Organization-	07 Sep 2023 14:39:09.4032 (UTC)

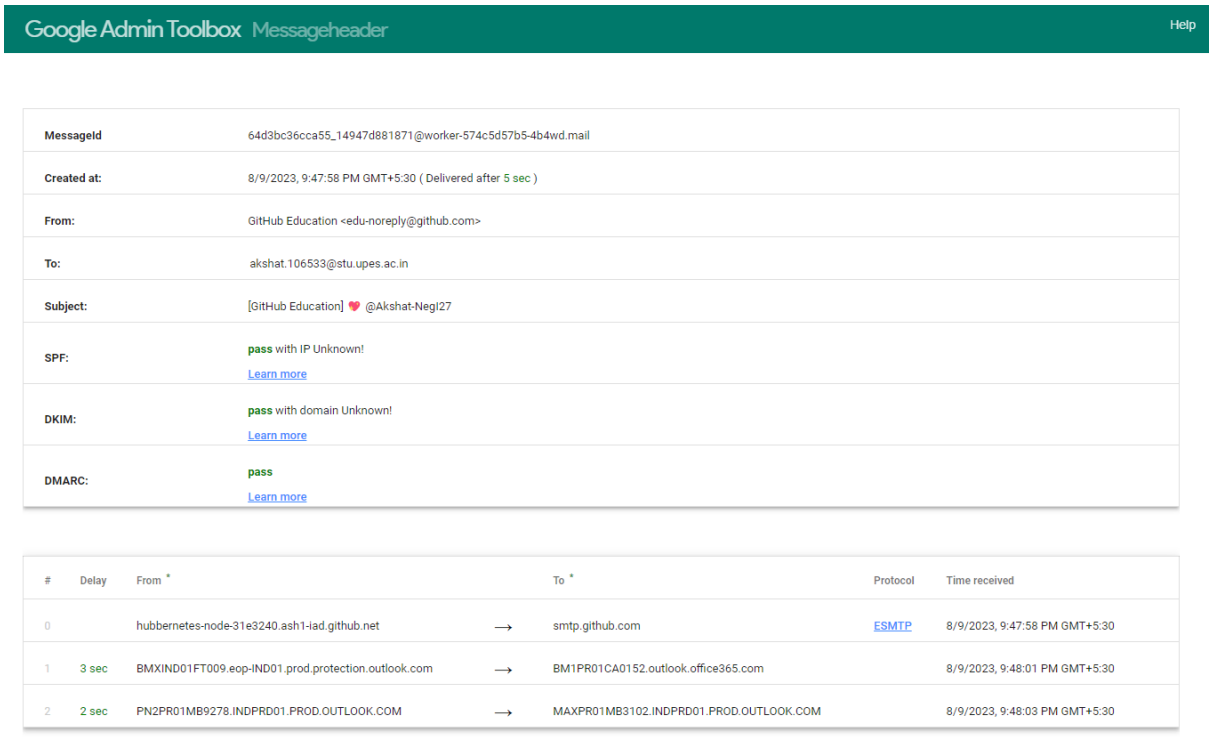
Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*		mail-lf1-f45.google.com	SMTP	9/7/2023 2:39:09 PM	
2	0 seconds	mail-lf1-f45.google.com 209.85.167.45	BMXIND01FT015.mail.protection.outlook.com 10.13.170.65	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	9/7/2023 2:39:09 PM	✖
3	0 seconds	BMXIND01FT015.eop-IND01.prod.protection.outlook.com 2603:1096:c01:de:cafe::1b	PN3PR01CA0165.outlook.office365.com 2603:1096:c01:de::9	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	9/7/2023 2:39:09 PM	✔
4	0 seconds	PN3PR01CA0165.INDPRD01.PROD.OUTLOOK.COM 2603:1096:c01:de::9	MA0PR01MB6471.INDPRD01.PROD.OUTLOOK.COM 2603:1096:a01:75::14	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	9/7/2023 2:39:09 PM	✔
5	3 seconds	MA0PR01MB6471.INDPRD01.PROD.OUTLOOK.COM 2603:1096:a01:75::14	MAXPR01MB3102.INDPRD01.PROD.OUTLOOK.COM	HTTPS	9/7/2023 2:39:12 PM	✔

EMAIL 4

OUTLOOK ORIGINAL HEADER VIEW



https://toolbox.googleapps.com/



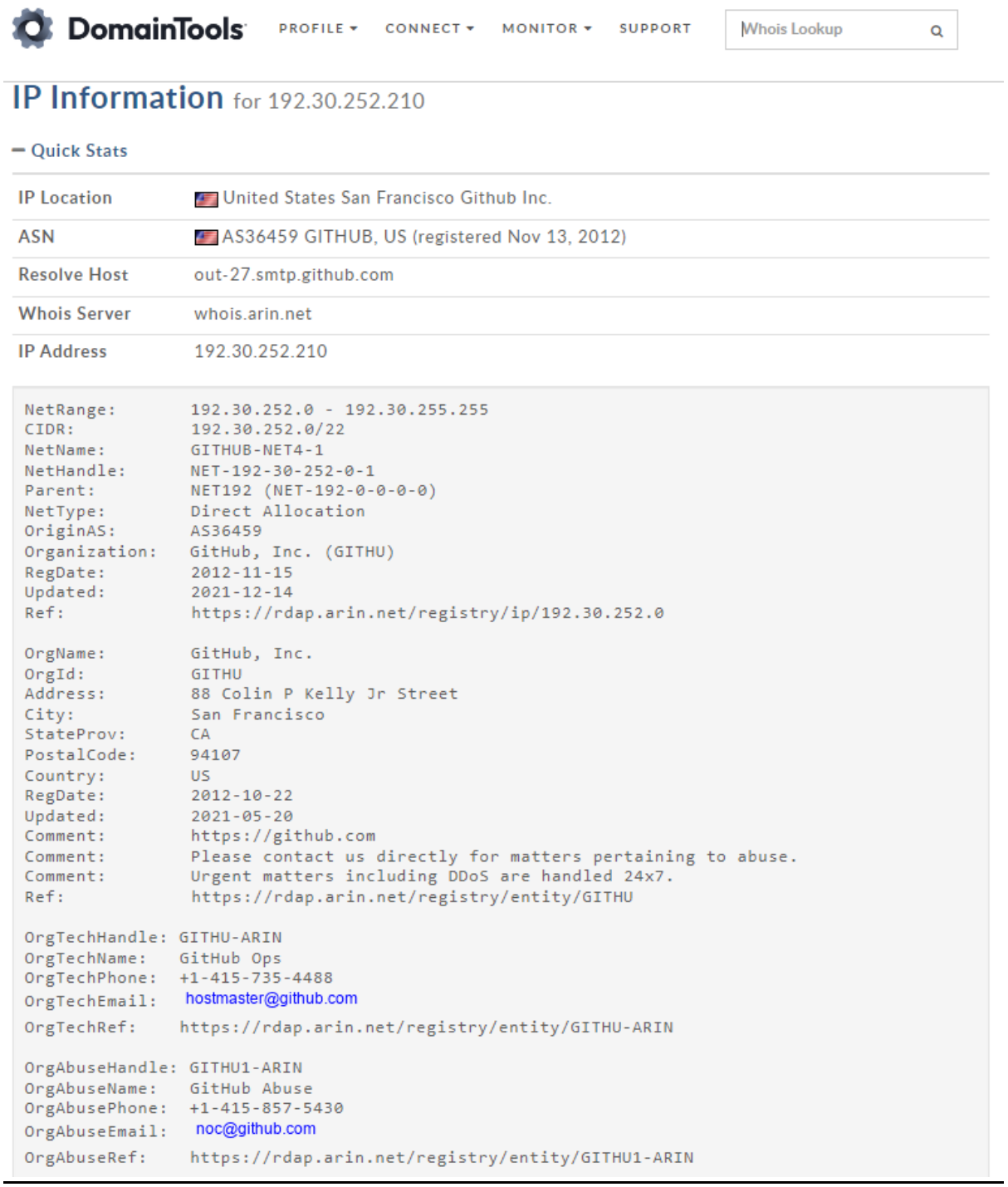
Google Admin Toolbox Messageheader

Help

MessageId	64d3bc36cca55_14947d881871@worker-574c5d57b5-4b4wd.mail
Created at:	8/9/2023, 9:47:58 PM GMT+5:30 (Delivered after 5 sec)
From:	GitHub Education <edu-noreply@github.com>
To:	akshat.106533@stu.upes.ac.in
Subject:	[GitHub Education] 💖 @Akshat-Negi27
SPF:	**pass** with IP Unknown! Learn more
DKIM:	**pass** with domain Unknown! Learn more
DMARC:	**pass** Learn more

#	Delay	From *		To *	Protocol	Time received
0		hubbernetes-node-31e3240.ash1-iad.github.net	→	smtp.github.com	ESMTP	8/9/2023, 9:47:58 PM GMT+5:30
1	3 sec	BMXIND01FT009.eop-IND01.prod.protection.outlook.com	→	BM1PR01CA0152.outlook.office365.com		8/9/2023, 9:48:01 PM GMT+5:30
2	2 sec	PN2PR01MB9278.INDPRD01.PROD.OUTLOOK.COM	→	MAXPR01MB3102.INDPRD01.PROD.OUTLOOK.COM		8/9/2023, 9:48:03 PM GMT+5:30

https://whois.domaintools.com/



DomainTools PROFILE CONNECT MONITOR SUPPORT Whois Lookup

IP Information for 192.30.252.210

Quick Stats

IP Location	United States San Francisco Github Inc.
ASN	AS36459 GITHUB, US (registered Nov 13, 2012)
Resolve Host	out-27.smtp.github.com
Whois Server	whois.arin.net
IP Address	192.30.252.210

```
NetRange:       192.30.252.0 - 192.30.255.255
CIDR:           192.30.252.0/22
NetName:        GITHUB-NET4-1
NetHandle:      NET-192-30-252-0-1
Parent:         NET192 (NET-192-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS36459
Organization:   GitHub, Inc. (GITHU)
RegDate:        2012-11-15
Updated:        2021-12-14
Ref:            https://rdap.arin.net/registry/ip/192.30.252.0

OrgName:        GitHub, Inc.
OrgId:          GITHU
Address:        88 Colin P Kelly Jr Street
City:           San Francisco
StateProv:      CA
PostalCode:     94107
Country:        US
RegDate:        2012-10-22
Updated:        2021-05-20
Comment:        https://github.com
Comment:        Please contact us directly for matters pertaining to abuse.
Comment:        Urgent matters including DDoS are handled 24x7.
Ref:            https://rdap.arin.net/registry/entity/GITHU

OrgTechHandle: GITHU-ARIN
OrgTechName:   GitHub Ops
OrgTechPhone:  +1-415-735-4488
OrgTechEmail:  hostmaster@github.com
OrgTechRef:    https://rdap.arin.net/registry/entity/GITHU-ARIN

OrgAbuseHandle: GITHU1-ARIN
OrgAbuseName:   GitHub Abuse
OrgAbusePhone:  +1-415-857-5430
OrgAbuseEmail:  noc@github.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/GITHU1-ARIN
```

https://mxtoolbox.com/

Headers Found

Header Name	Header Value
Authentication-Results	spf=pass (sender IP is 192.30.252.210) smtp.mailfrom=github.com; dkim=pass (signature was verified) header.d=github.com;dmarc=pass action=none header.from=github.com;compauth=pass reason=100
Received-SPF	Pass (protection.outlook.com: domain of github.com designates 192.30.252.210 as permitted sender) receiver=protection.outlook.com; client-ip=192.30.252.210; helo=out-27.smtp.github.com; pr=C
DKIM-Signature	v=1; a=rsa-sha256; c=relaxed/relaxed; d=github.com; s=pf2023; t=1691597878; bh=5dPkDnlth6nsy3Guoy0Fov2lo/PWmrj/JLwdrlUxZbY=; h=Date:From:To:Subject:From; b=QllOaxU47i/fApvsQfxyMadwLWn7ZvH/INKjxjYXfB18uyp4UhVyY2pp/dGe0fHkr vv0Xo8uKHi3j+DS7U1OJbsDAP3aF6gE/2HVnP6tlghBkKlfseGoZd1H7mNi5L/vjk5 0WbvmrQaQuCMWGQ8gFNszNlDFne/M/HuVfqQ9bMk=
Date	Wed, 09 Aug 2023 16:17:58 +0000
From	GitHub Education <edu-noreply@github.com>
To	akshat.106533@stu.upes.ac.in
Message-ID	<64d3bc36cca55_14947d881871@worker-574c5d57b5-4b4wd.mail>
Subject	=?UTF-8?Q?[GitHub_Education]_=F0=9F=92=96_@Akshat-Negl27?=
Mime-Version	1.0
Content-Type	multipart/alternative; boundary="--==_mimepart_64d3bc366db20_14947d8817fb"; charset=UTF-8
Content-Transfer-Encoding	7bit
Return-Path	edu-noreply@github.com
X-MS-Exchange-Organization-ExpirationStartTime	09 Aug 2023 16:18:00.7809 (UTC)
X-MS-Exchange-Organization-ExpirationStartTimeReason	OriginalSubmit
X-MS-Exchange-Organization-ExpirationInterval	1:00:00:00.0000000
X-MS-Exchange-Organization-ExpirationIntervalReason	OriginalSubmit
X-MS-Exchange-Organization-Network-Message-Id	d42a63ac-3717-4cd2-960b-08db98f43393
X-EOPAttributedMessage	0
X-EOPTenantAttributedMessage	91cc1fb6-1275-4acf-b3ea-c213ec16257b:0

Relay (seconds)

Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	github.com 10.56.104.61	smtp.github.com	ESMTP	8/9/2023 4:17:58 PM	✓
2	2 seconds	out-27.smtp.github.com 192.30.252.210	BMXIND01FT009.mail.protection.outlook.com 10.13.170.79	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	8/9/2023 4:18:00 PM	✗
3	1 Second	BMXIND01FT009.eop-IND01.prod.protection.outlook.com 2603:1096:b00:68:cafe::92	BM1PR01CA0152.outlook.office365.com 2603:1096:b00:68::22	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	8/9/2023 4:18:01 PM	✓
4	0 seconds	BM1PR01CA0152.INDPRD01.PROD.OUTLOOK.COM 2603:1096:b00:68::22	PN2PR01MB9278.INDPRD01.PROD.OUTLOOK.COM 2603:1096:c01:11a::6	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	8/9/2023 4:18:01 PM	✓
5	2 seconds	PN2PR01MB9278.INDPRD01.PROD.OUTLOOK.COM 2603:1096:c01:11a::6	MAXPR01MB3102.INDPRD01.PROD.OUTLOOK.COM	HTTPS	8/9/2023 4:18:03 PM	✓

EMAIL 5

OUTLOOK ORIGINAL HEADER VIEW

Original Message

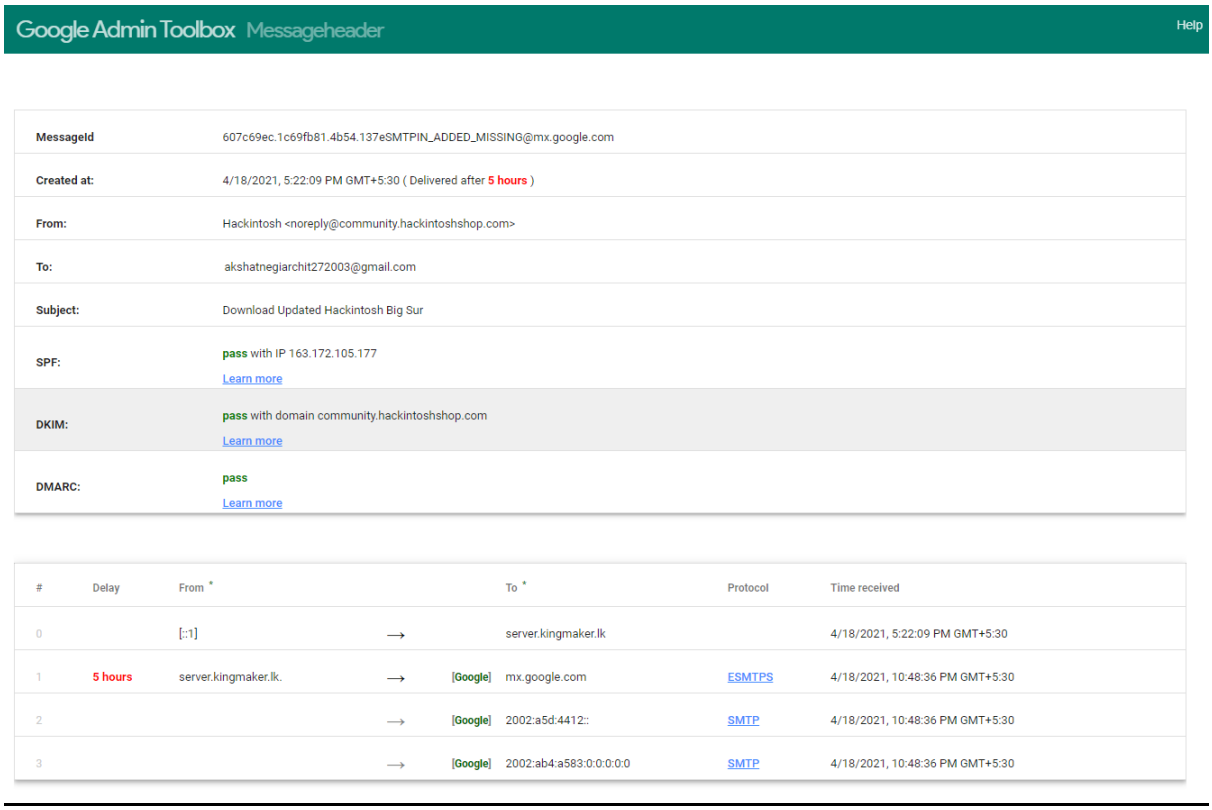
Message ID	<607c69ec.1c69fb81.4b54.137eSMTPIN_ADDED_MISSING@mx.google.com>
Created at:	Sun, Apr 18, 2021 at 5:22 PM (Delivered after 19587 seconds)
From:	Hackintosh <noreply@community.hackintoshshop.com>
To:	akshatnegiarchit272003@gmail.com
Subject:	Download Updated Hackintosh Big Sur
SPF:	PASS with IP 163.172.105.177 Learn more
DKIM:	'PASS' with domain community.hackintoshshop.com Learn more
DMARC:	'PASS' Learn more

Download Original

Copy to clipboard

```
Delivered-To: akshatnegiarchit272003@gmail.com
Received: by 2002:ab4:a583:0:0:0:0:0 with SMTP id dq3csp2204167ecb;
        Sun, 18 Apr 2021 10:18:36 -0700 (PDT)
X-Google-Smtp-Source: ABdhPJziuL/kLZINQyu76TqVSDfhKHgyvdNDKrzajQE4TGrIFmjSOcfeujW4jAnnJMfmQEKHc2rO
X-Received: by 2002:a5d:4412:: with SMTP id z18mr10492681wrq.28.1618766316769;
        Sun, 18 Apr 2021 10:18:36 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1618766316; cv=none;
        d=google.com; s=arc-20160816;
        b=OwilK/NXPotZ6ZlcTZs7tyUx0yZjYijnlFHcI6cmYo6JxVYzkVDma/3vYAqR9d9SVB
         G7G2+fjRMlGHNjmrjif2PeGLmLLjr4aBgJhMsykjLzyCS1mHUhkV8fv/D2yrS4zX6+jT
         HppG7cERA0MWI1/fqOHvKnmg+zJdFvEv2PfaTb1pYOAIg6BCCg+5JxoXDYkd9T94ETZf
         9ZUXU/ZsgMXAOclzSEqF+S6ZOsiX1toUZUAiqfT+nbFNOfqCQR3ds4jXVccScWecSoFO
         dC/aH9UqRMx9oyWU35Q2ortb1XE3IQRqCuL2gfyrA2uB20yBYWDY4g9SYakMBNlI6JYz
         5nLA==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=list-unsubscribe:content-transfer-encoding:precedence
         :auto-submitted:date:subject:from:to:mime-version:dkim-signature
         :message-id;
```

https://toolbox.googleapps.com/



https://whois.domaintools.com/

DomainTools PROFILE CONNECT MONITOR SUPPORT WHOIS

IP Information for 163.172.105.177

— Quick Stats

IP Location	France Paris Online Sas
ASN	AS12876 AS12876 SCALEWAY S.A.S., FR (registered Dec 20, 1999)
Resolve Host	163-172-105-177.rev.poneytelecom.eu
Whois Server	whois.ripe.net
IP Address	163.172.105.177

```
% Abuse contact for '163.172.0.0 - 163.172.255.255' is '
 abuse@online.net '

inetnum:        163.172.0.0 - 163.172.255.255
status:         LEGACY
mnt-routes:     MNT-TISCALIFR
org:            ORG-ONLI1-RIPE
netname:        SCALEWAY-DEDIBOX
descr:          Scaleway Dedibox - Paris, France
remarks:        Abuse reports : https://abuse.online.net
/
country:        FR
admin-c:        MM42047-RIPE
tech-c:         MM42047-RIPE
mnt-by:         ONLINE-NET-MNT
created:        2015-09-11T09:44:28Z
last-modified:  2022-05-04T17:24:57Z
source:         RIPE

organisation:   ORG-ONLI1-RIPE
mnt-ref:        MNT-TISCALIFR-B2B
org-name:       Scaleway
org-type:       OTHER
address:        8 rue de la ville l'eveque 75008 PARIS
e-mail:          noc+ripe@as12876.net
abuse-c:        AR32851-RIPE
mnt-ref:        ONLINE-NET-MNT
mnt-by:         ONLINE-NET-MNT
```

https://mxtoolbox.com/

Header Name	Header Value
Delivered-To	akshatnegiarchit272003@gmail.com
X-Google-Smtp-Source	ABdhPJziuL/kLZlNQyu76TqVSDfhKHgyvdNDKrzajQE4TGrlFmjSOcfeujW4jAnnJMfmQEKHc2rO
X-Received	by 2002:a5d:4412:: with SMTP id z18mr10492681wrq.28.1618766316769; Sun, 18 Apr 2021 10:18:36 -0700 (PDT)
ARC-Seal	i=1; a=rsa-sha256; t=1618766316; cv=none; d=google.com; s=arc-20160816; b=OwilK/NXPotZ6ZlcTZs7tyUx0yZjYijnlFHcl6cmYo6JxVYzkVDma/3vYAqR9d9SVB G7G2+fjR MlGHNjmrjif2PeGLmLLjr4aBgJhMsykjLzyCS1mHUhkV8fv/D2yrS4zX6+jT HppG7cERA0MWl1/fqOHvKnmg+zJdFvEv2PfaTb1pYOAlg6BCCg+5JxoXDYkd9T94ETZf 9ZUXU/ZsgMXAOclzSEqF+S6ZOsiX1toUZUAiqfT+nbFNOfqCQR3ds4jXVccScWecSoFO dC/aH9UqRMx9oyWU35Q2ortb1XE3lQRqCuL2gfyrA2uB20yBYWDY4g9SYakMBNll6JYz 5nLA==
ARC-Message-Signature	i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816; h=list-unsubscribe:content-transfer-encoding:precedence :auto-submitted:date:subject:from:to:mime-version:dkim-signature :message-id; bh=7vFMAEcucbYhDqLSfCxx7a0dldcYt7DJCSo54xTo8/Q=; b=ALn0kdYGBY5XlgMnaWlNGSFtXMwe0KM2Vo5dcG6bQurCEYA fp3S/rzFm+V86i94fqn VpstEHg5cYrNWSP781fLKHsgG/WqOCkdkr7aKPt5Touk65f3OhGpQNSr8KAUlGQsdvWC l/b4+EDzmo7Z78p0j3ZzcYLq+q+kmT9orq5VaP/1QJhcMF WmKClakol0O5MGMf/Dli+3 pM5x+qYP22lOZMqhB46/E+ekq5WyM7h2jmtYP8gpa6kRUyaOiW05lVEYZVO0ThtLXbLU UfkNAFD5OiQoxB4P9mN+Slp5kquxvEb1RkQkAmu1f Z+WFdAhROR3vc8HTFR/8cgXEPko 8+gg==
ARC-Authentication-Results	i=1; mx.google.com; dkim=pass header.i=@community.hackintoshshop.com header.s=default header.b=GdEVNvQy; spf=pass (google.com: domain of noreply@community.hackintoshshop.com designates 163.172.105.177 as permitted sender) smtp.mailfrom=noreply@community.hackintoshshop.com; dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=community.hackintoshshop.com
Return-Path	<noreply@community.hackintoshshop.com>
Received-SPF	pass (google.com: domain of noreply@community.hackintoshshop.com designates 163.172.105.177 as permitted sender) client-ip=163.172.105.177;
Authentication-Results	mx.google.com; dkim=pass header.i=@community.hackintoshshop.com header.s=default header.b=GdEVNvQy; spf=pass (google.com: domain of noreply@community.hackintoshshop.com designates 163.172.105.177 as permitted sender) smtp.mailfrom=noreply@community.hackintoshshop.com; dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=community.hackintoshshop.com
Message-ID	<607c69ec.1c69fb81.4b54.137eSMTPIN_ADDED_MISSING@mx.google.com>
DKIM-Signature	v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed; d=community.hackintoshshop.com; s=default; h=List-Unsubscribe: Content-Transfer-Encoding:Content-Type:Date:Subject:From:To:MIME-Version: Sender:Reply-To:Message-ID:Cc:Content-ID:Content-Description:Resent-Date: Resent-From:Resent-Sender:Resent-To:Resent-Cc:Resent-Message-ID:In-Reply-To: References:List-Id:List-Help:List-Subscribe:List-Post:List-Owner:List-Archive ; bh=7vFMAEcucbYhDqLSfCxx7a0dldcYt7DJCSo54xTo8/Q=; b=GdEVNvQypEea8B+v1GYxO3bC d9pr2/b1OM/fzuPjDcnN1VY803nWkOr7JKM4WM3ZXSVLeQzRzotpt6LsOkmjynerMkTXoV1iEPZRF oXbgfTAy+N5exvVZDbTtjGiYZ1NCWd/kex7xYO9jSDr5Hd5bHo5AlPti5EUv88uZj4Xq72Y9fKAKa Ibf+MMWeYkxJ4wRF4hNtcZCK5olLQu5hmBknhkbgulp009DOtceLVqAWu36aUD6pE3elzlJ4NxlBy 34nrwSto84Rog2iiNEskHXjdZjiUP24dclsi1HQzM6exQlKqhOluEdFORDBse4sdy2YsmwARe0jnq sAdCSYXutQ==;
MIME-Version	1.0
To	akshatnegiarchit272003@gmail.com
From	Hackintosh <noreply@community.hackintoshshop.com>
Subject	Download Updated Hackintosh Big Sur
Date	Sun, 18 Apr 2021 11:52:09 +0000
Auto-Submitted	auto-generated
Precedence	bulk
Content-Type	multipart/alternative; boundary="--==_mimepart_515f6008709aef5983053b2ebebc1fef"; charset=UTF-8

Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	::1	server.kingmaker.lk	esmtp (Exim 4.94) (envelope-from <noreply@community.hackintoshshop.com>)	4/18/2021 11:52:09 AM	✖
2	5 hour	server.kingmaker.lk 163.172.105.177	mx.google.com	ESMTPS	4/18/2021 5:18:36 PM	✔
3	0 seconds		2002:ab4:a583:0:0:0:0:0	SMTP	4/18/2021 5:18:36 PM	

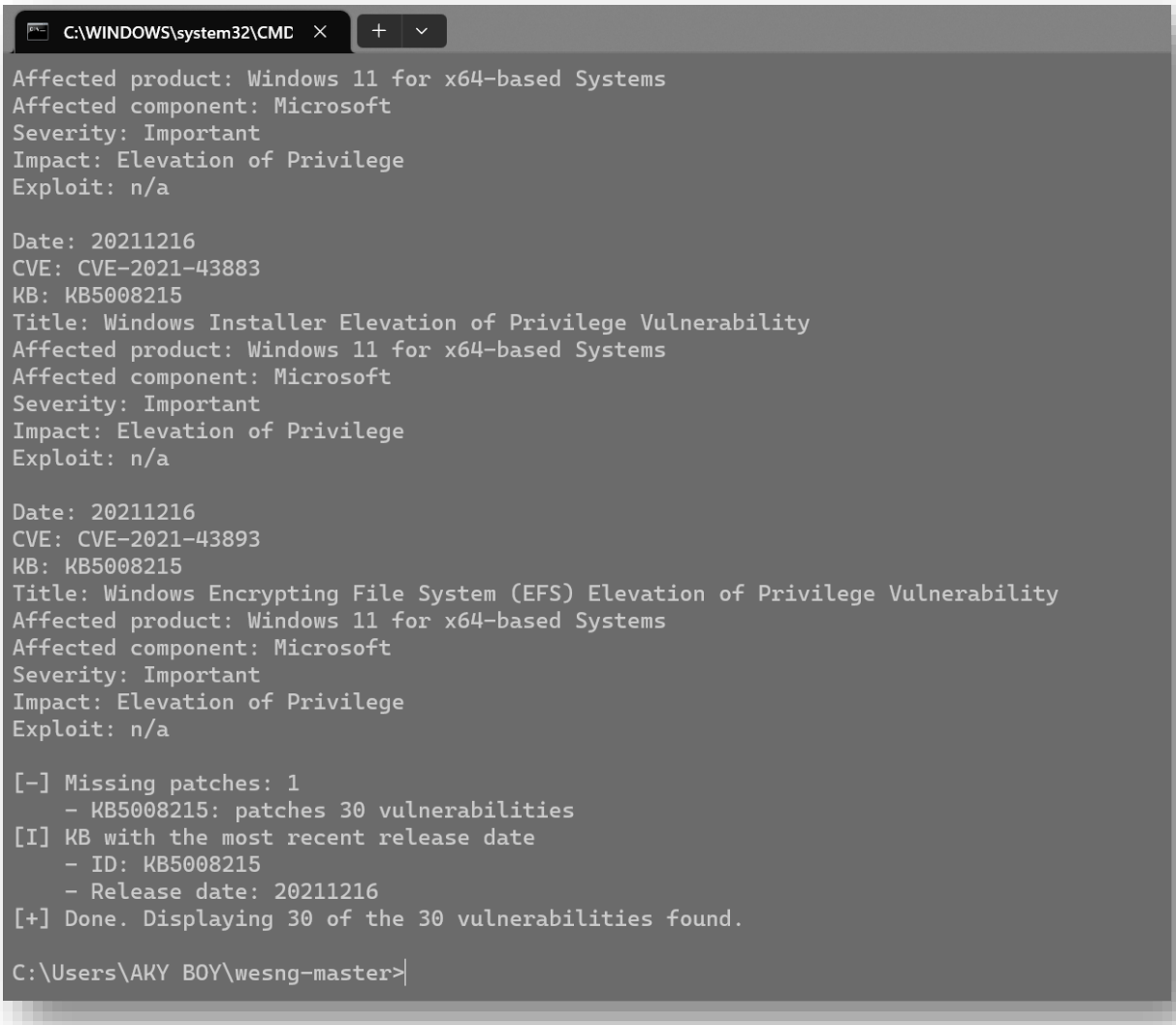
LAB EXPERIMENT – 3

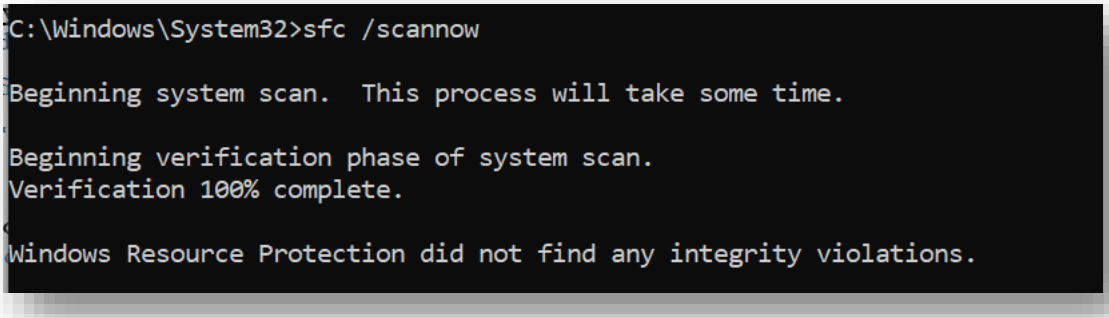
Understanding Vulnerabilities in Local Operating Systems

Windows Vulnerability CHECK

STEP-1 Python --version
STEP-2 pip3 install chardet
STEP-3 git clone https://github.com/bitsadmin/wesng.git
STEP-4 systeminfo
STEP-5 systeminfo > sysinfo.txt
STEP-6 cd wesng-master
STEP-7 dir
STEP-8 python wes.py ..\sysinfo.txt
STEP-9 python wes.py ..\sysinfo.txt -s critical
STEP-10 python wes.py ..\sysinfo.txt -s critical > critical.txt

Type of OS	Vulnerability	Vulnerability Details	Mitigation Steps
Windows 11	CVE-2023-24054	Elevation of privilege vulnerability in Windows Update Assistant	Install the latest security updates from Microsoft.
Windows 11	CVE-2023-21999	Remote code execution vulnerability in Microsoft Exchange Server	Install the latest security updates from Microsoft.
Windows 11	CVE-2023-21996	Denial-of-service vulnerability in Microsoft Exchange Server	Install the latest security updates from Microsoft.
Windows 11	CVE-2023-21995	Remote code execution vulnerability in Microsoft Exchange Server	Install the latest security updates from Microsoft.
Windows 11	CVE-2023-21985	Remote code execution vulnerability in Windows Print Spooler	Disable the Print Spooler service if not in use.
Kali Linux	CVE-2023-24056	Elevation of privilege vulnerability in OpenSSH	Upgrade to the latest version of OpenSSH.
Kali Linux	CVE-2023-24055	Remote code execution vulnerability in Samba	Upgrade to the latest version of Samba.
Kali Linux	CVE-2023-24053	Denial-of-service vulnerability in Apache HTTP Server	Upgrade to the latest version of Apache HTTP Server.
Kali Linux	CVE-2023-24052	Remote code execution vulnerability in BIND	Upgrade to the latest version of BIND.
Kali Linux	CVE-2023-24051	Remote code execution vulnerability in MySQL	Upgrade to the latest version of MySQL.


C:\WINDOWS\system32\CMD
Affected product: Windows 11 for x64-based Systems
Affected component: Microsoft
Severity: Important
Impact: Elevation of Privilege
Exploit: n/a
Date: 20211216
CVE: CVE-2021-43883
KB: KB5008215
Title: Windows Installer Elevation of Privilege Vulnerability
Affected product: Windows 11 for x64-based Systems
Affected component: Microsoft
Severity: Important
Impact: Elevation of Privilege
Exploit: n/a
Date: 20211216
CVE: CVE-2021-43893
KB: KB5008215
Title: Windows Encrypting File System (EFS) Elevation of Privilege Vulnerability
Affected product: Windows 11 for x64-based Systems
Affected component: Microsoft
Severity: Important
Impact: Elevation of Privilege
Exploit: n/a
[-] Missing patches: 1
- KB5008215: patches 30 vulnerabilities
[I] KB with the most recent release date
- ID: KB5008215
- Release date: 20211216
[+] Done. Displaying 30 of the 30 vulnerabilities found.
C:\Users\AKY BOY\wesng-master>

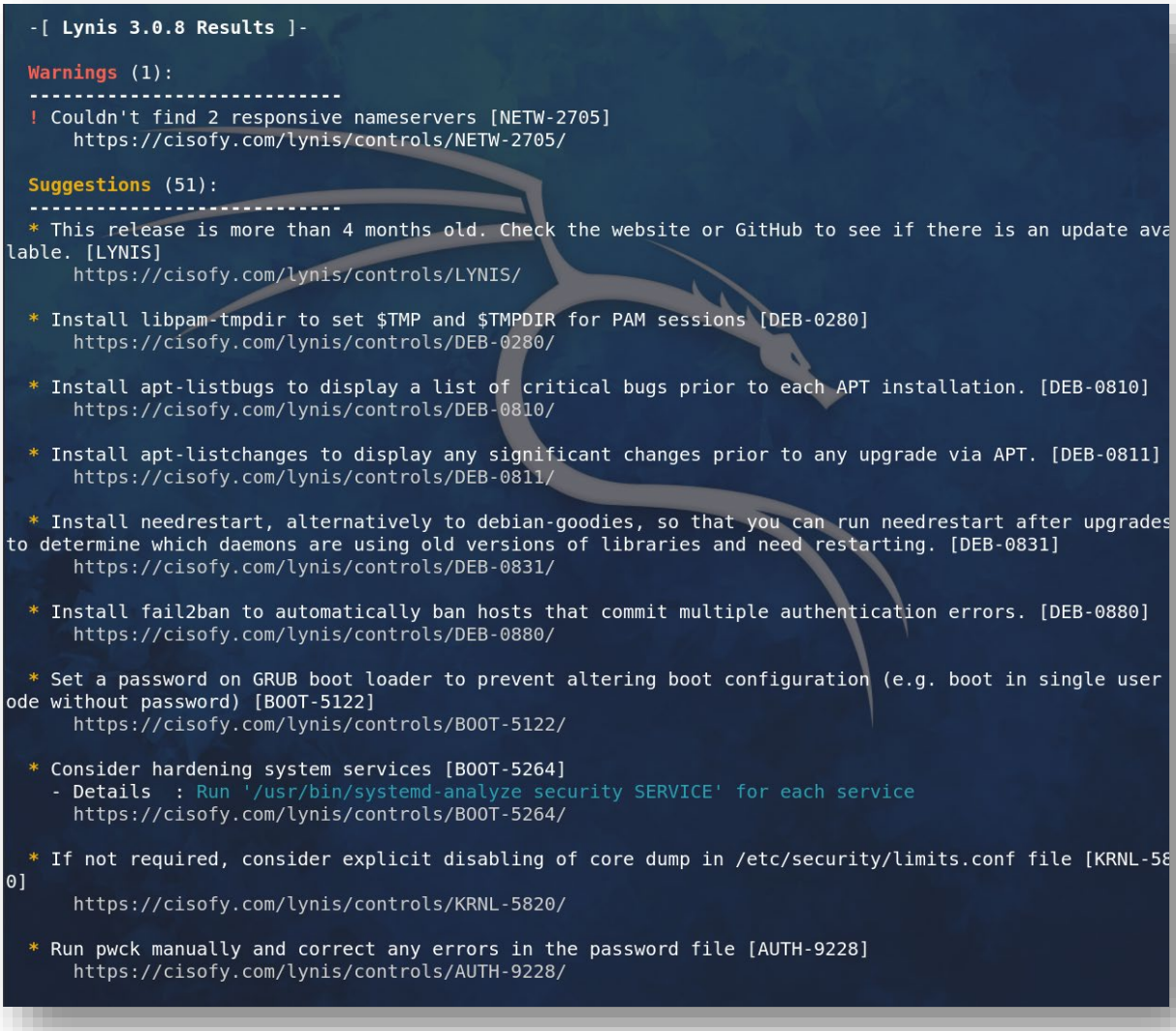

C:\Windows\System32>sfc /scannow
Beginning system scan. This process will take some time.
Beginning verification phase of system scan.
Verification 100% complete.
Windows Resource Protection did not find any integrity violations.

```
Date: 20211215
CVE: CVE-2021-43217
KB: KB5008215
Title: Windows Encrypting File System (EFS) Remote Code Execution Vulnerability
Affected product: Windows 11 for x64-based Systems
Affected component: Microsoft
Severity: Critical
Impact: Remote Code Execution
Exploit: n/a

Date: 20211214
CVE: CVE-2021-43233
KB: KB5008215
Title: Remote Desktop Client Remote Code Execution Vulnerability
Affected product: Windows 11 for x64-based Systems
Affected component: Microsoft
Severity: Critical
Impact: Remote Code Execution
Exploit: n/a

[-] Missing patches: 1
    - KB5008215: patches 2 vulnerabilities
[I] KB with the most recent release date
    - ID: KB5008215
    - Release date: 20211215
[+] Done. Displaying 2 of the 30 vulnerabilities found.

C:\Users\AKY BOY\wesng-master>
```

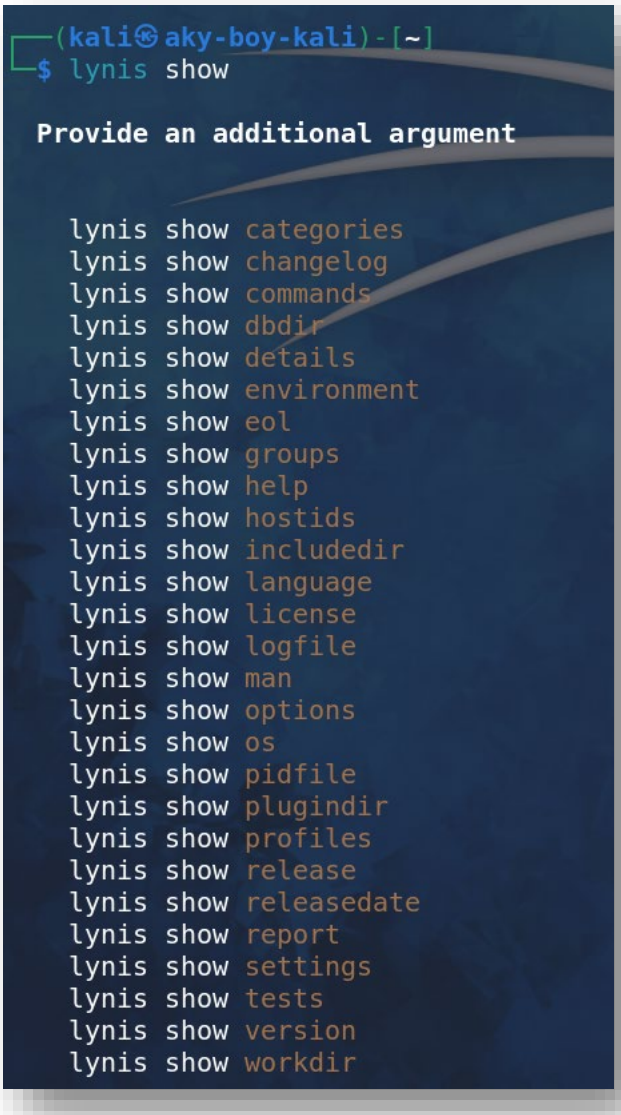
USING LYNIS

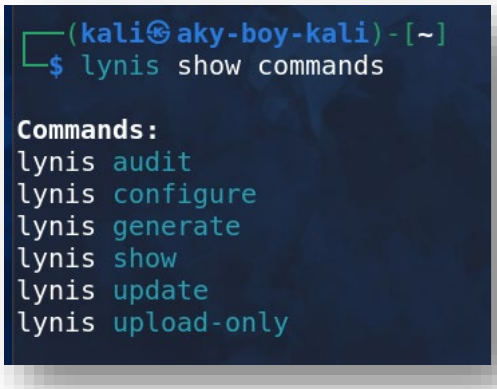
- Install Lynis using command: **sudo apt install lynis**
- Check audit using: **lynis audit system --quick**

- Warnings and Suggestions by Lynis after detecting OS.

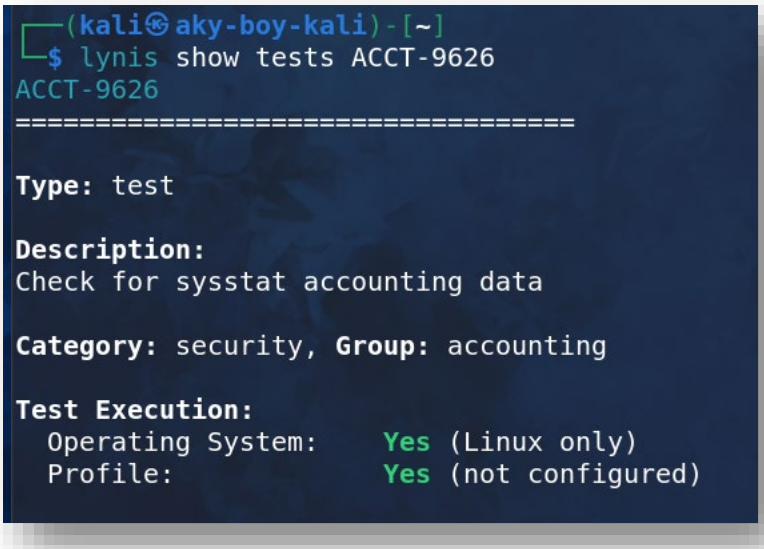


- To view all commands: **lynis show** and to view audit commands: **lynis show commands**





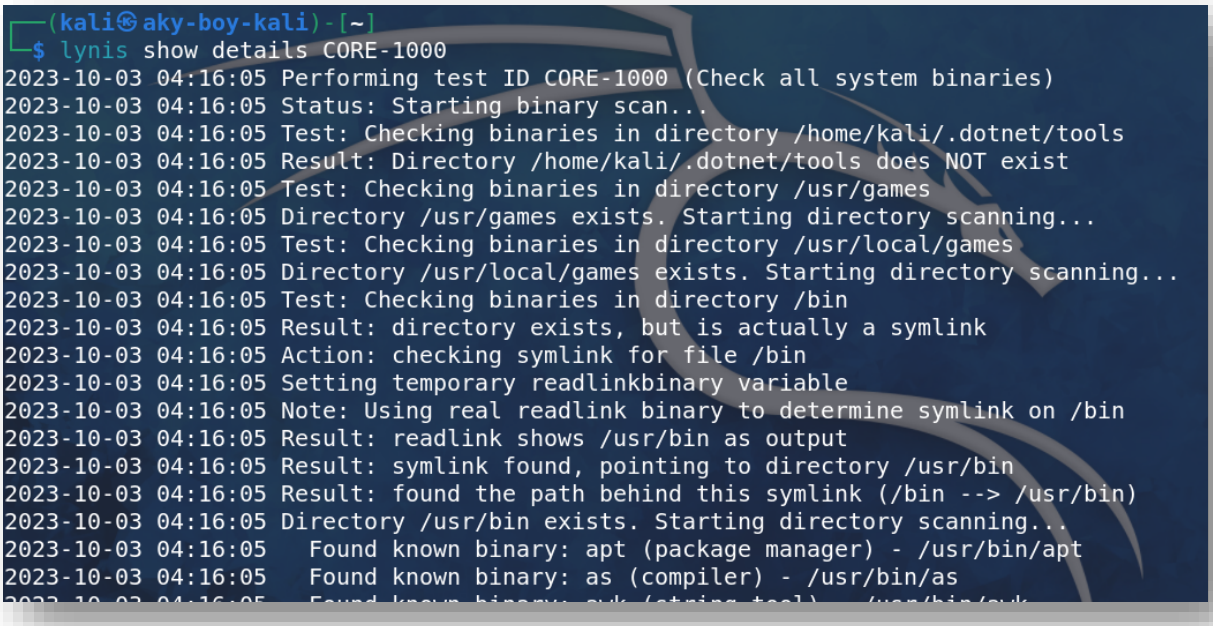
- **Lynis show tests ACCT – 9626** to view particular test.

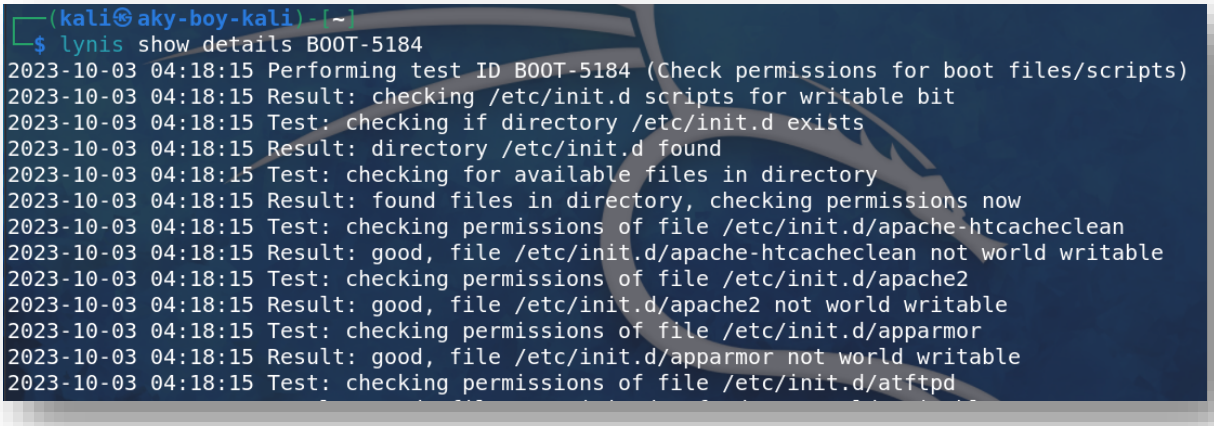


- To view all test together: **Lynis show tests**

```
┌──(kali㉿aky-boy-kali)-[~]
└─$ lynis show tests
# Test       OS         Description
# ================================================================================
ACCT-2754  FreeBSD    Check for available FreeBSD accounting information (security)
ACCT-2760  OpenBSD    Check for available OpenBSD accounting information (security)
ACCT-9622  Linux      Check for available Linux accounting information (security)
ACCT-9626  Linux      Check for sysstat accounting data (security)
ACCT-9628  Linux      Check for auditd (security)
ACCT-9630  Linux      Check for auditd rules (security)
ACCT-9632  Linux      Check for auditd configuration file (security)
ACCT-9634  Linux      Check for auditd log file (security)
ACCT-9636  Linux      Check for Snoopy wrapper and logger (security)
ACCT-9650  Solaris    Check Solaris audit daemon (security)
ACCT-9652  Solaris    Check auditd SMF status (security)
ACCT-9654  Solaris    Check BSM auditing in /etc/system (security)
ACCT-9656  Solaris    Check BSM auditing in module list (security)
ACCT-9660  Solaris    Check location of audit events (security)
ACCT-9662  Solaris    Check Solaris auditing stats (security)
ACCT-9670  Linux      Check for cmd tooling (security)
ACCT-9672  Linux      Check cmd configuration file (security)
AUTH-9204             Check users with an UID of zero (security)
AUTH-9208             Check non-unique accounts in passwd file (security)
AUTH-9212             Test group file (security)
AUTH-9216             Check group and shadow group files (security)
AUTH-9218  FreeBSD    Check harmful login shells (security)
AUTH-9222             Check for non unique groups (security)
AUTH-9226             Check non unique group names (security)
AUTH-9228             Check password file consistency with pwck (security)
AUTH-9229             Check password hashing methods (security)
AUTH-9230             Check group password hashing rounds (security)
AUTH-9234             Query user accounts (security)
AUTH-9240             Query NIS+ authentication support (security)
AUTH-9242             Query NIS authentication support (security)
AUTH-9250             Checking sudoers file (security)
AUTH-9252             Check sudoers file (security)
AUTH-9254  Solaris    Solaris passwordless accounts (security)
AUTH-9262             Checking presence password strength testing tools (PAM) (security)
AUTH-9264             Checking presence pam.conf (security)
AUTH-9266             Checking presence pam.d files (security)
AUTH-9268             Checking presence pam.d files (security)
AUTH-9278             Checking LDAP pam status (security)
```

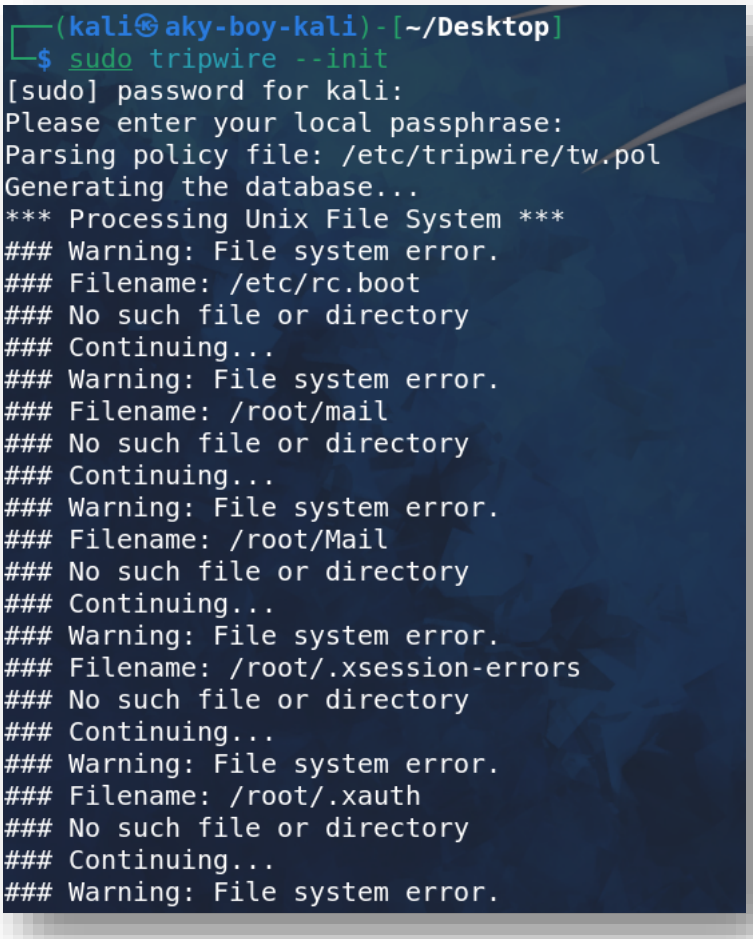
- Some individual details of particular tests.





USING TRIPWIRE

- Install tripwire using: **sudo apt install tripwire** and do the configuration using same password.
- **Sudo tripwire --init**

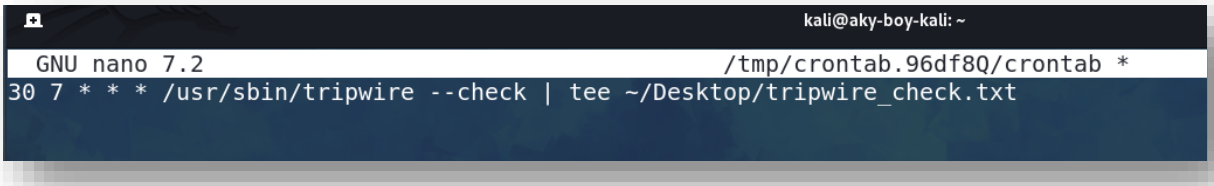


- Table below is the Integrity report generated by Tripwire.
- **Sudo apt tripwire –check > tripwire.txt**

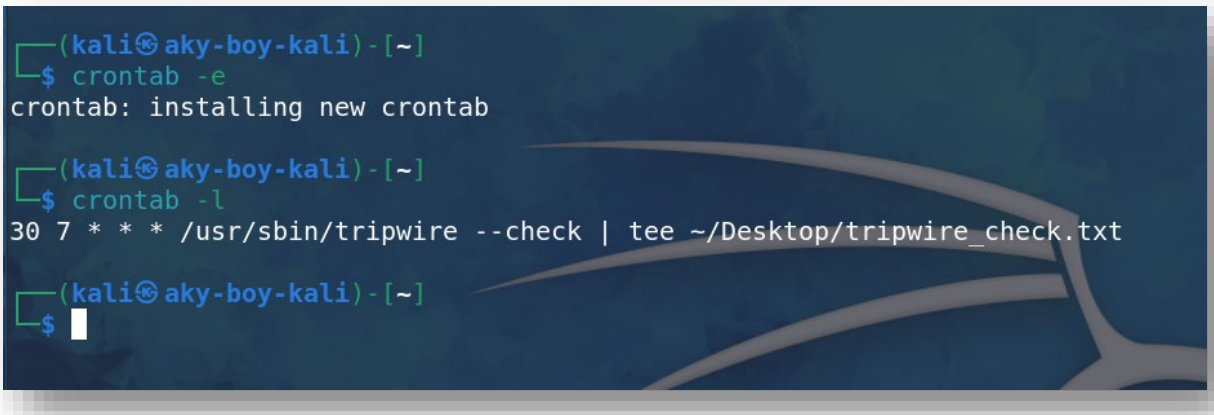
```
Open Source Tripwire(R) 2.4.3.7 Integrity Check Report

Report generated by:          root
Report created on:            Tue 03 Oct 2023 05:39:24 AM EDT
Database last updated on:     Never

================================================================================
Report Summary:
================================================================================

Host name:                    aky-boy-kali
Host IP address:              192.168.230.128
Host ID:                      None
Policy file used:             /etc/tripwire/tw.pol
Configuration file used:      /etc/tripwire/tw.cfg
Database file used:           /var/lib/tripwire/aky-boy-kali.twd
Command line used:            tripwire --check

================================================================================
Rule Summary:
================================================================================

--------------------------------------------------------------------------------
  Section: Unix File System
--------------------------------------------------------------------------------

  Rule Name                     Severity Level    Added    Removed  Modified
  ---------                     --------------    -----    -------  --------
* Other binaries                66                9        6        1384
  Tripwire Binaries             100               0        0        0
* Other libraries               66                6604     410      26864
  Root file-system executables  100               0        0        0
  Tripwire Data Files           100               0        0        0
* System boot changes           100               28       0        14
  Root file-system libraries    100               0        0        0
  (/lib)
* Critical system boot files    100               4961     0        12
* Other configuration files     66                25       16       386
  (/etc)
* Boot Scripts                  100               0        0        2
* Security Control              66                0        0        2
* Root config files             100               1        0        2
* Devices & Kernel information  100               154655   125741   31361
  Invariant Directories         66                0        0        0
```

BONUS: Crontab Scheduling

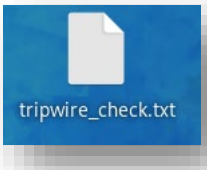
- To view the number of Crontabs: **crontab -l**



- To install or schedule new crontab using the nano editor: **crontab -e**



- File auto-generated at 7:30 according to 24hr clock with the Integrity Report using Tripwire.

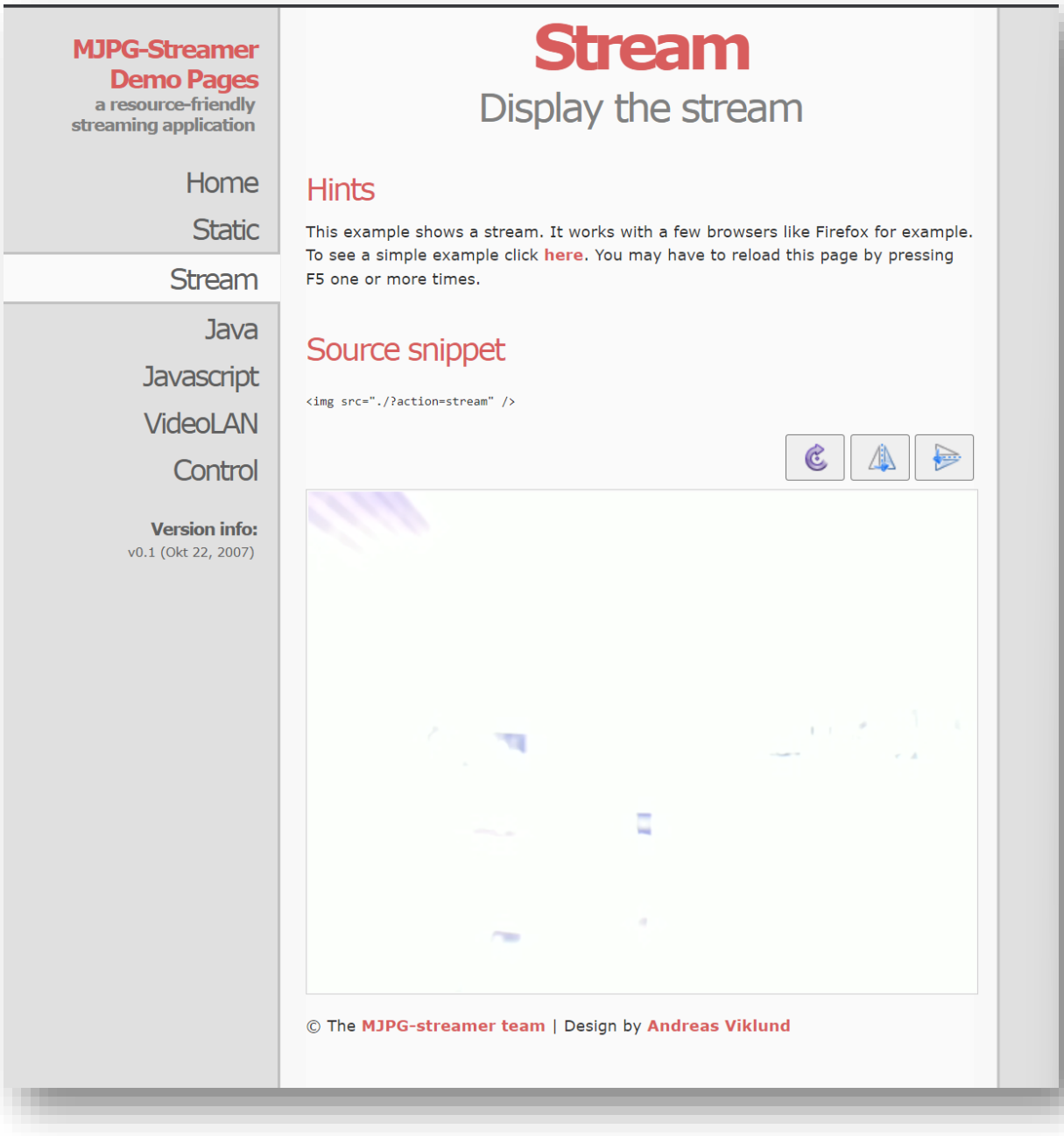


LAB EXPERIMENT – 4

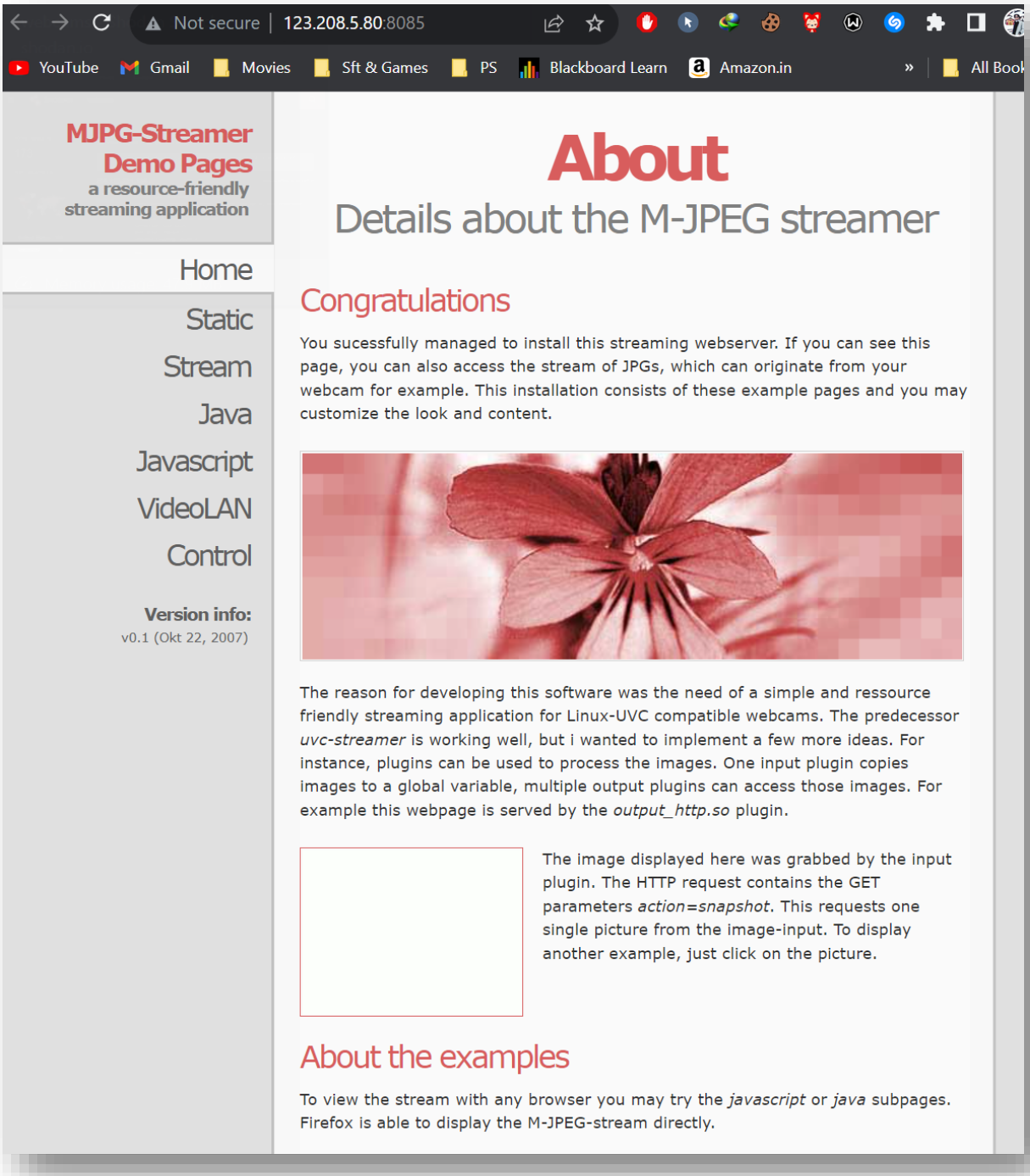
Vulnerabilities in Live IOT devices on Internet

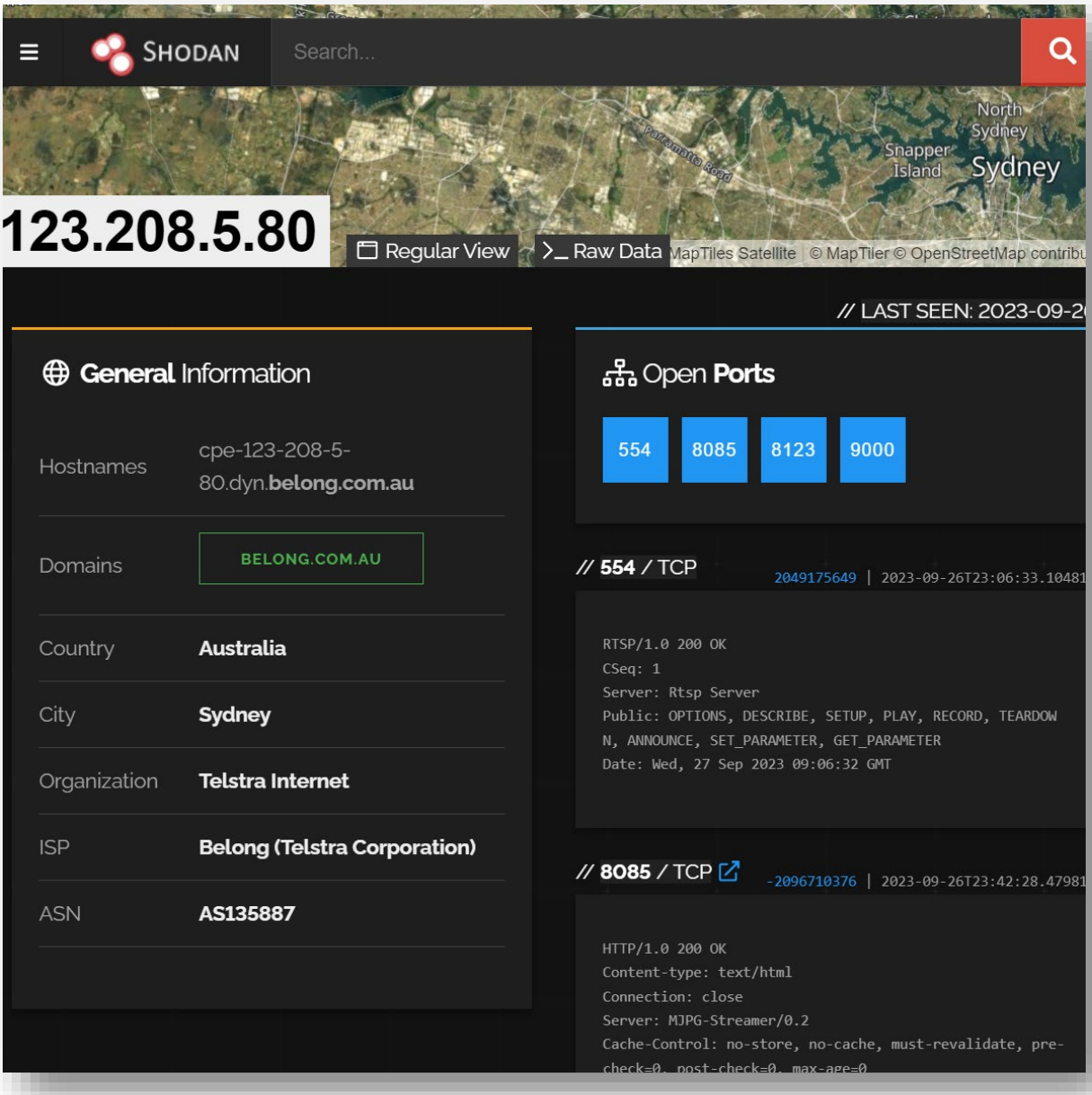
IP Address	Device	Open Ports	Geolocation	Mode/Make	Product Version	Admin Password
123.208.5.80	Webcam	554,**8085**,2123,9000	Sydney, Australia	Telstra Internet	v0.1.2	Not found
182.138.139.41	Webcam	**8081**	China, Chengdu	CHINANET Sichuan province network	V0.1.1	Not Found
81.174.128.10	webserver	**4444**	United Kingdom, Pontypridd	British Telecommunications PLC	v0.1	Admin page found
124.246.151.142	MJPG-Streamer	**9000**	Japan, Chino	LCV Corporation	v0.2	Not Found
90.187.8.29	MJPG-Streamer	**443**,22,80,1900,5353,**8080**,8081	Germany, Hamburg	Vodafone Deutschland GmbH	v 0.2	Admin Page

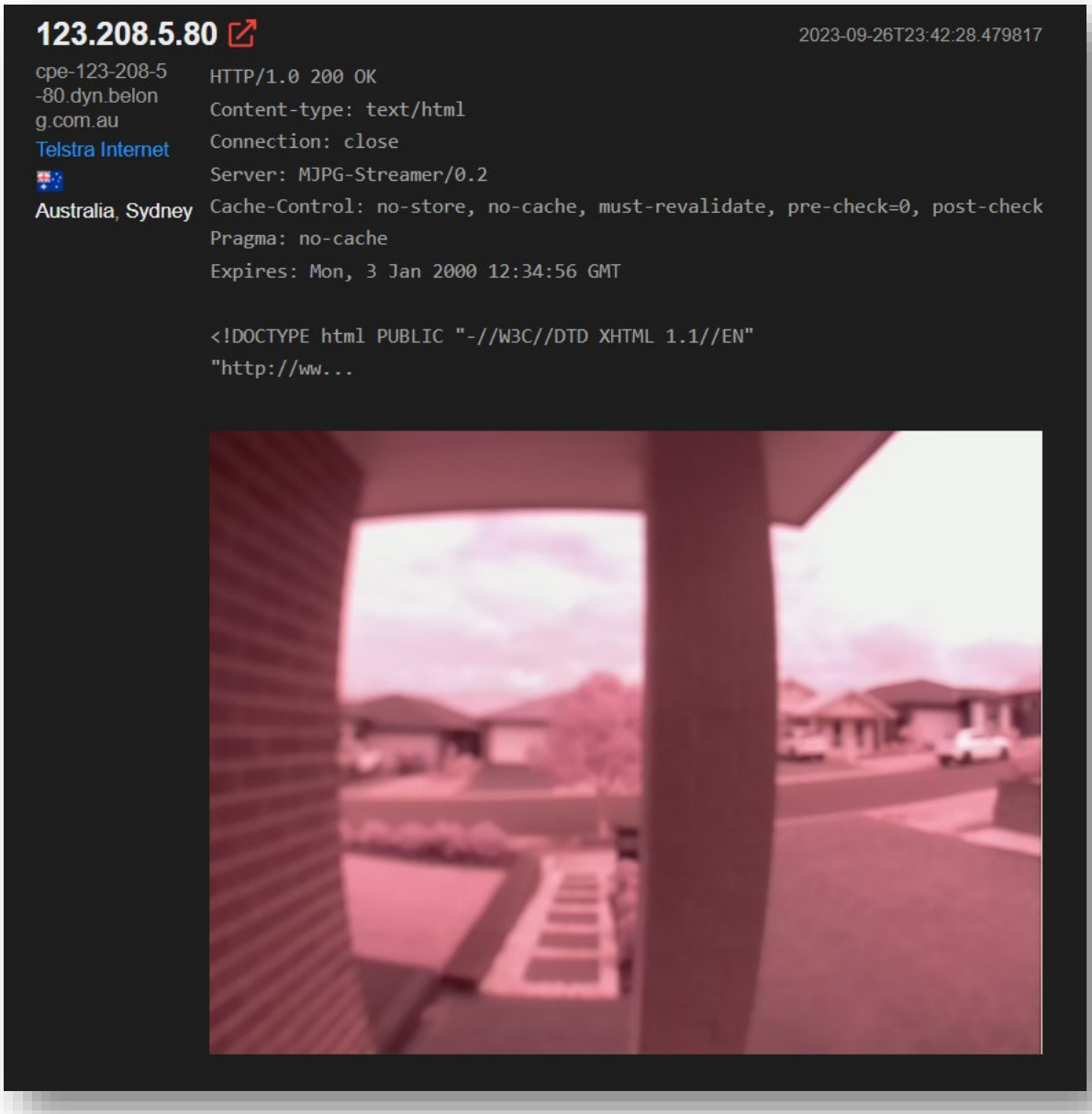
DEVICE 1

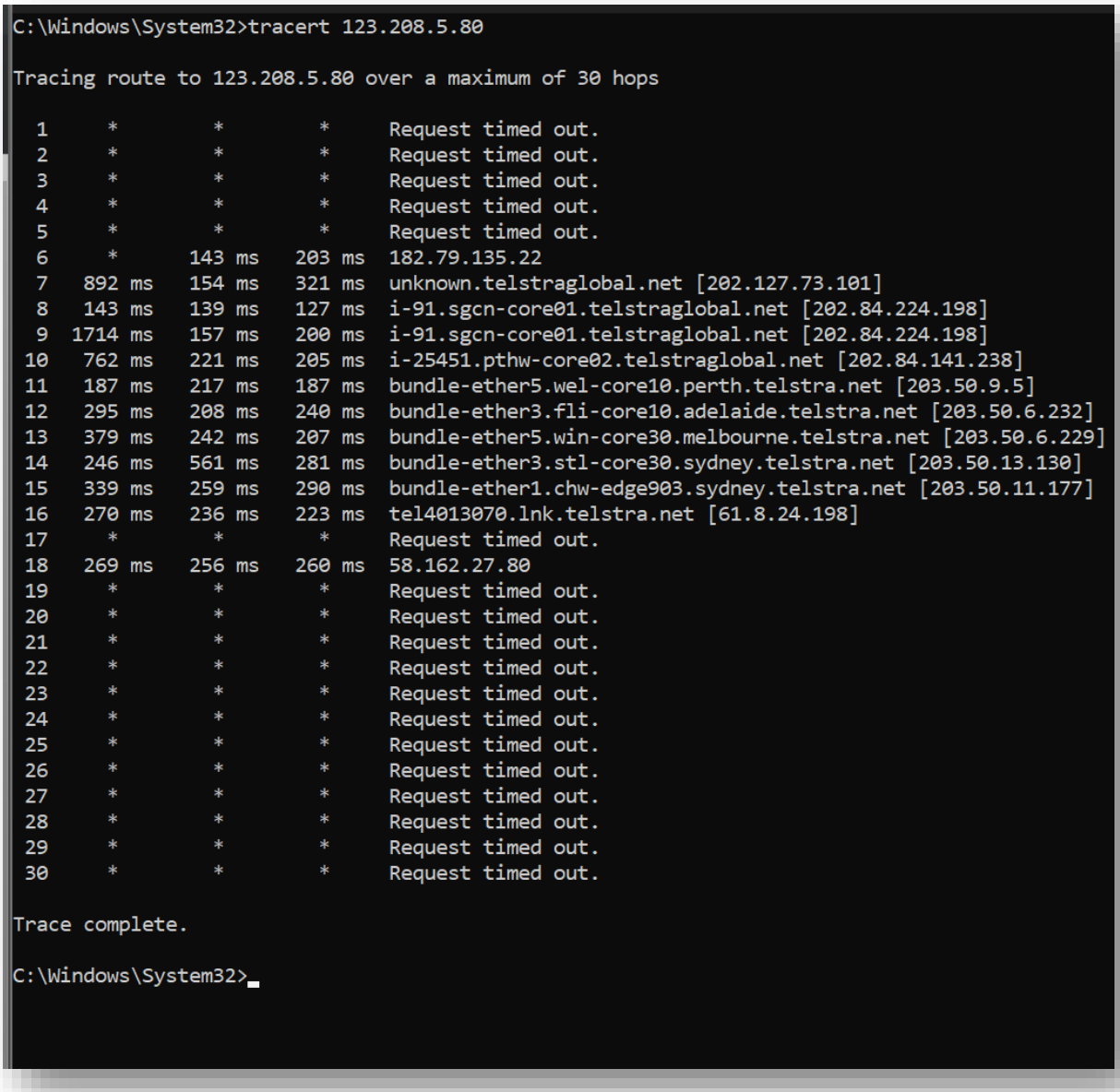

MJPG-Streamer
Demo Pages
a resource-friendly
streaming application
Home
Static
Stream
Java
Javascript
VideoLAN
Control
Version info:
v0.1 (Okt 22, 2007)
Stream
Display the stream
Hints
This example shows a stream. It works with a few browsers like Firefox for example. To see a simple example click here. You may have to reload this page by pressing F5 one or more times.
Source snippet

© The MJPG-streamer team | Design by Andreas Viklund


Not secure | 123.208.5.80:8085
YouTube
Gmail
Movies
Sft & Games
PS
Blackboard Learn
Amazon.in
All Book
MJPG-Streamer
Demo Pages
a resource-friendly
streaming application
Home
Static
Stream
Java
Javascript
VideoLAN
Control
Version info:
v0.1 (Okt 22, 2007)
About
Details about the M-JPEG streamer
Congratulations
You sucessfully managed to install this streaming webserver. If you can see this page, you can also access the stream of JPGs, which can originate from your webcam for example. This installation consists of these example pages and you may customize the look and content.
The reason for developing this software was the need of a simple and ressource friendly streaming application for Linux-UVC compatible webcams. The predecessor uvc-streamer is working well, but i wanted to implement a few more ideas. For instance, plugins can be used to process the images. One input plugin copies images to a global variable, multiple output plugins can access those images. For example this webpage is served by the output_http.so plugin.
The image displayed here was grabbed by the input plugin. The HTTP request contains the GET parameters action=snapshot. This requests one single picture from the image-input. To display another example, just click on the picture.
About the examples
To view the stream with any browser you may try the javascript or java subpages. Firefox is able to display the M-JPEG-stream directly.

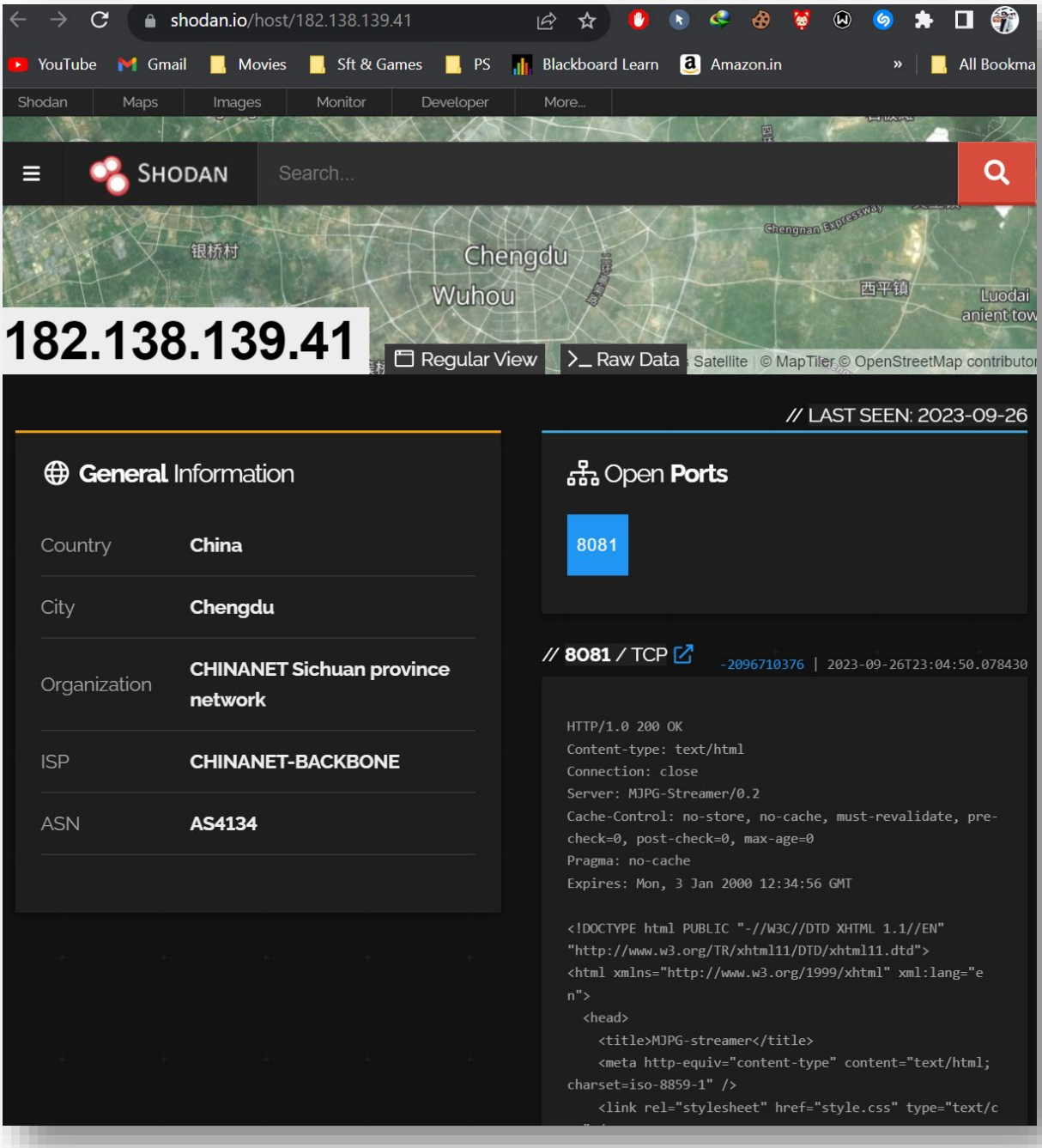

SHODAN
Search...
North Sydney
Snapper Island
Sydney
123.208.5.80
Regular View
Raw Data
MapTiles Satellite
© MapTiler © OpenStreetMap contribu
// LAST SEEN: 2023-09-2
General Information
Hostnames
cpe-123-208-5-80.dyn.belong.com.au
Domains
BELONG.COM.AU
Country
Australia
City
Sydney
Organization
Telstra Internet
ISP
Belong (Telstra Corporation)
ASN
AS135887
Open Ports
554
8085
8123
9000
// 554 / TCP
2049175649 | 2023-09-26T23:06:33.10481
RTSP/1.0 200 OK
CSeq: 1
Server: Rtsp Server
Public: OPTIONS, DESCRIBE, SETUP, PLAY, RECORD, TEARDOWN, ANNOUNCE, SET_PARAMETER, GET_PARAMETER
Date: Wed, 27 Sep 2023 09:06:32 GMT
// 8085 / TCP
-2096710376 | 2023-09-26T23:42:28.47981
HTTP/1.0 200 OK
Content-type: text/html
Connection: close
Server: MJPG-Streamer/0.2
Cache-Control: no-store, no-cache, must-revalidate, pre-check=0, post-check=0, max-age=0

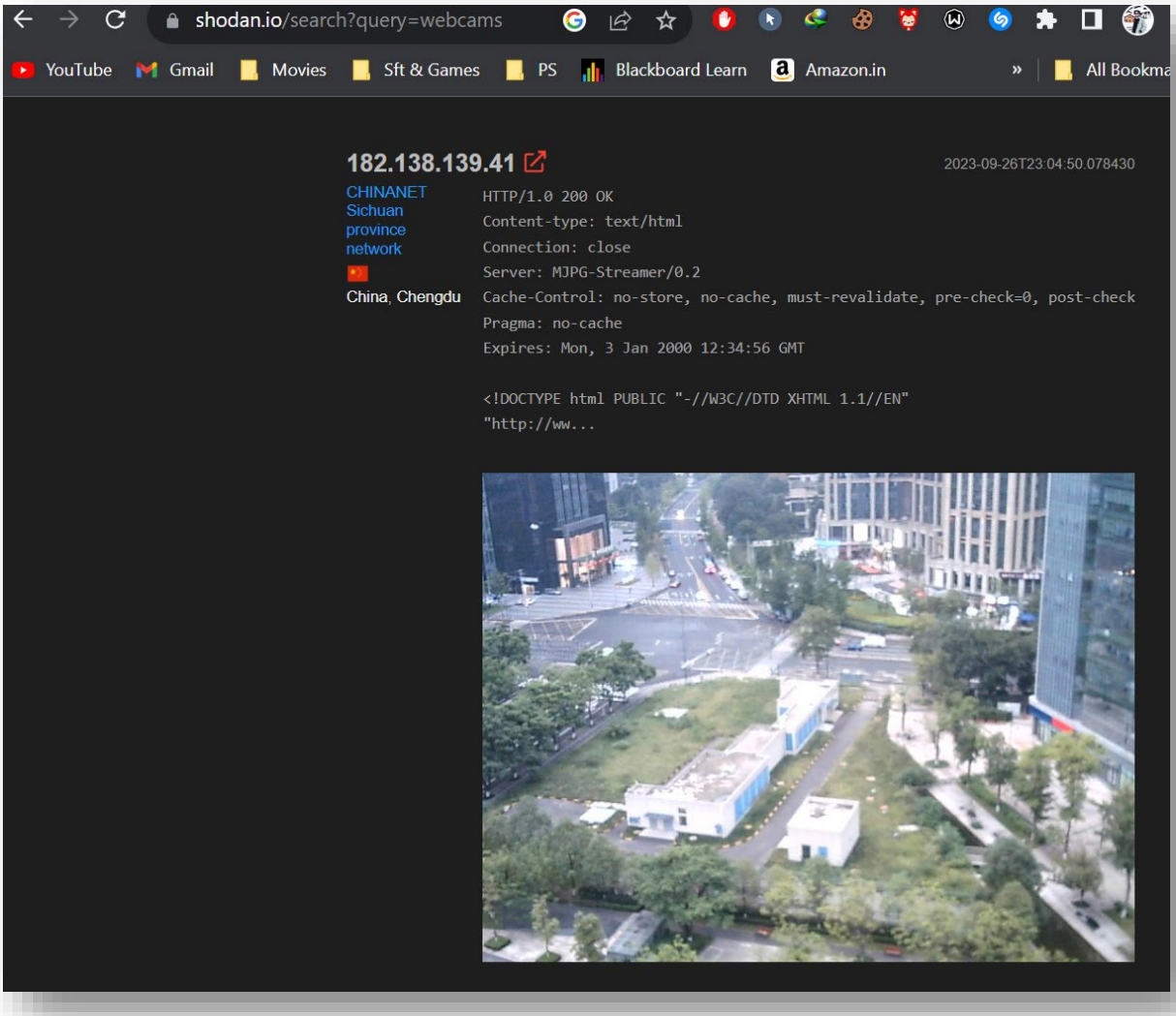

123.208.5.80
2023-09-26T23:42:28.479817
cpe-123-208-5-80.dyn.belong.com.au
Telstra Internet
Australia, Sydney
HTTP/1.0 200 OK
Content-type: text/html
Connection: close
Server: MJPG-Streamer/0.2
Cache-Control: no-store, no-cache, must-revalidate, pre-check=0, post-check
Pragma: no-cache
Expires: Mon, 3 Jan 2000 12:34:56 GMT
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN"
"http://ww...


C:\Windows\System32>tracert 123.208.5.80
Tracing route to 123.208.5.80 over a maximum of 30 hops
1 * * * Request timed out.
2 * * * Request timed out.
3 * * * Request timed out.
4 * * * Request timed out.
5 * * * Request timed out.
6 * 143 ms 203 ms 182.79.135.22
7 892 ms 154 ms 321 ms unknown.telstraglobal.net [202.127.73.101]
8 143 ms 139 ms 127 ms i-91.sgcn-core01.telstraglobal.net [202.84.224.198]
9 1714 ms 157 ms 200 ms i-91.sgcn-core01.telstraglobal.net [202.84.224.198]
10 762 ms 221 ms 205 ms i-25451.pthw-core02.telstraglobal.net [202.84.141.238]
11 187 ms 217 ms 187 ms bundle-ether5.wel-core10.perth.telstra.net [203.50.9.5]
12 295 ms 208 ms 240 ms bundle-ether3.fli-core10.adelaide.telstra.net [203.50.6.232]
13 379 ms 242 ms 207 ms bundle-ether5.win-core30.melbourne.telstra.net [203.50.6.229]
14 246 ms 561 ms 281 ms bundle-ether3.stl-core30.sydney.telstra.net [203.50.13.130]
15 339 ms 259 ms 290 ms bundle-ether1.chw-edge903.sydney.telstra.net [203.50.11.177]
16 270 ms 236 ms 223 ms tel4013070.lnk.telstra.net [61.8.24.198]
17 * * * Request timed out.
18 269 ms 256 ms 260 ms 58.162.27.80
19 * * * Request timed out.
20 * * * Request timed out.
21 * * * Request timed out.
22 * * * Request timed out.
23 * * * Request timed out.
24 * * * Request timed out.
25 * * * Request timed out.
26 * * * Request timed out.
27 * * * Request timed out.
28 * * * Request timed out.
29 * * * Request timed out.
30 * * * Request timed out.
Trace complete.
C:\Windows\System32>

DEVICE 2

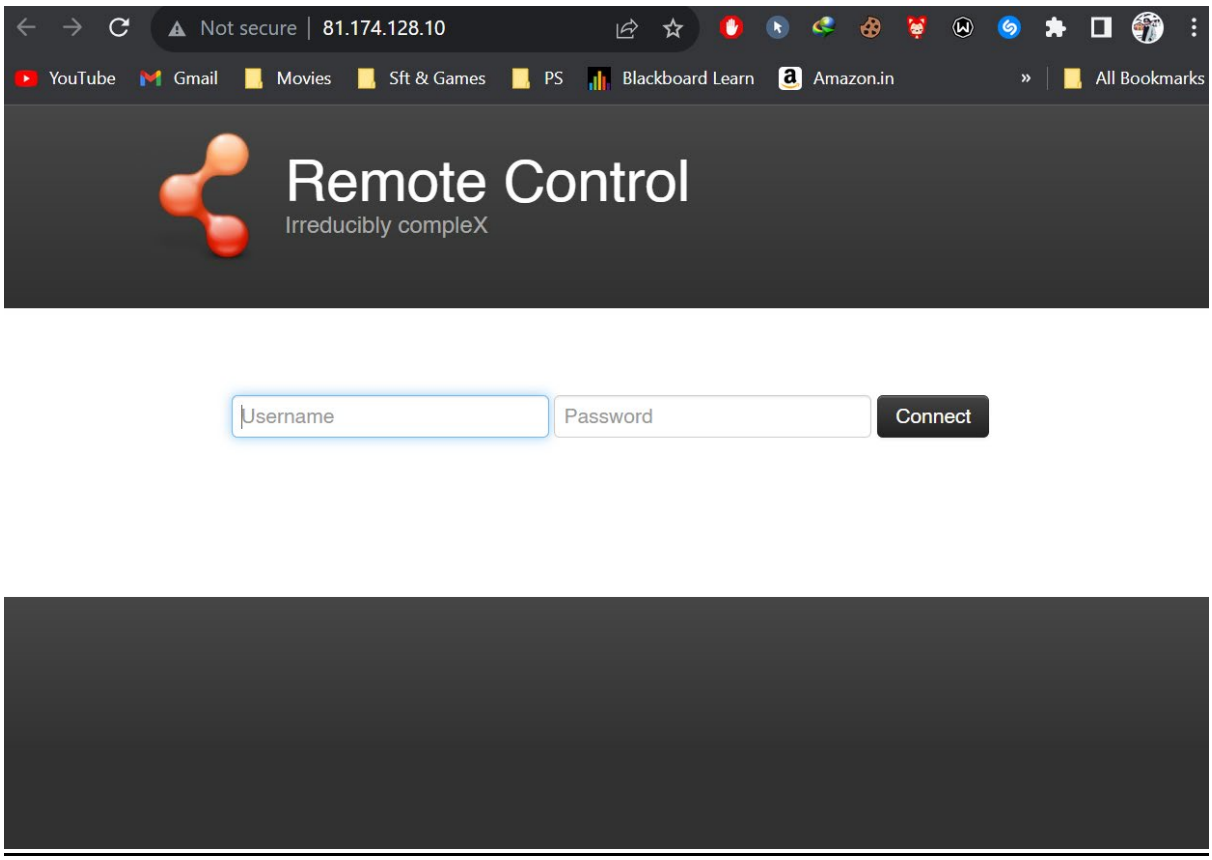

Not secure | 182.138.139.41:8081
YouTube
Gmail
Movies
Sft & Games
PS
Blackboard Learn
Amazon.in
MJPG-Streamer Demo Pages
a resource-friendly streaming application
Home Static Stream Java Javascript VideoLAN Control
Version info:
v0.1 (Okt 22, 2007)
About
Details about the M-JPEG streamer
Congratulations
You sucessfully managed to install this streaming webserver. If you can see this page, you can also access the stream of JPGs, which can originate from your webcam for example. This installation consists of these example pages and you may customize the look and content.
The reason for developing this software was the need of a simple and ressource friendly streaming application for Linux-UVC compatible webcams. The predecessor uvc-streamer is working well, but i wanted to implement a few more ideas. For instance, plugins can be used to process the images. One input plugin copies images to a global variable, multiple output plugins can access those images. For example this webpage is served by the output_http.so plugin.


shodan.io/host/182.138.139.41
YouTube
Gmail
Movies
Sft & Games
PS
Blackboard Learn
Amazon.in
All Bookma
Shodan
Maps
Images
Monitor
Developer
More...
SHODAN
Search...
Chengdu
Wuhou
Chengnan Expressway
Luodai
182.138.139.41
Regular View
Raw Data
Satellite
© MapTiler © OpenStreetMap contributor
// LAST SEEN: 2023-09-26
General Information
Country
China
City
Chengdu
Organization
CHINANET Sichuan province network
ISP
CHINANET-BACKBONE
ASN
AS4134
Open Ports
8081
// 8081 / TCP
-2096710376 | 2023-09-26T23:04:50.078430
HTTP/1.0 200 OK
Content-type: text/html
Connection: close
Server: MJPG-Streamer/0.2
Cache-Control: no-store, no-cache, must-revalidate, pre-check=0, post-check=0, max-age=0
Pragma: no-cache
Expires: Mon, 3 Jan 2000 12:34:56 GMT
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en">
<head>
<title>MJPG-streamer</title>
<meta http-equiv="content-type" content="text/html; charset=iso-8859-1" />
<link rel="stylesheet" href="style.css" type="text/c




```
C:\Windows\System32>tracert 182.138.139.41

Tracing route to 182.138.139.41 over a maximum of 30 hops

  1     4 ms     3 ms     8 ms  192.168.153.182
  2     *      174 ms   153 ms  10.206.17.17
  3     *        *        *     Request timed out.
  4     *        *       84 ms  10.206.248.177
  5    74 ms    72 ms    78 ms  125.16.168.245
  6   188 ms   185 ms   293 ms  116.119.57.144
  7   241 ms   158 ms   151 ms  unknown.telstraglobal.net [202.127.73.101]
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *     Transmit error: code 1232.

Trace complete.
```

Device 3 & BONUS



NETCRAFT

Site report for http://cs.rin.ru

▸ Look up another site?

Share:

Background

Site title	CS.RIN.RU - Steam Underground Community	**Date first seen**	February 2004
Site rank	6203	**Netcraft Risk Rating**	0/10
Description	CS.RIN.RU - Steam Underground Community	**Primary language**	Russian

Network

Site	http://cs.rin.ru	**Domain**	rin.ru
Netblock Owner	FlokiNET Ltd	**Nameserver**	joan.ns.cloudflare.com
Hosting company	FlokiNet	**Domain registrar**	unknown
Hosting country	RO	**Nameserver organisation**	whois.cloudflare.com
IPv4 address	185.100.87.208 (VirusTotal)	**Organisation**	unknown
IPv4 autonomous systems	AS200651	**DNS admin**	dns@cloudflare.com

---

Web Browser Targeting

Web browser targeting enables software applications to make use of specific functions of the browser as well as optimizing the application for specific browser versions.

Technology	Description	Popular sites using this technology
X-Content-Type-Options	Browser MIME type sniffing is disabled	www.linkedin.com, www.arco.co.uk, www.facebook.com
X-Frame-Options Deny	Prevents the web page being embedded in a frame	www.instagram.com, www.bbc.co.uk, www.geeksforgeeks.org
Strict Transport Security	Web security policy mechanism whereby a web server declares that complying user agents are to interact with it using only secure HTTP connections	www.amazon.com, mail-redir.mention.com, l.facebook.com
Strict-Transport-Security (preload)	*No description*	www.canva.com, www.amazon.de, www.amazon.co.uk
Referrer Policy	Restrict referrer information included in subsequent requests	www.binance.com, www.udemy.com, www.tiktok.com
Stylesheet with SRI	*No description*	www.cvedetails.com, www.pdfdrive.com, www.politico.com
X-XSS-Protection Block	Block pages on which cross-site scripting is detected	www.ebay.com, teams.microsoft.com, discord.com
Content Security Policy	Detect and mitigate attacks in the browser	arco.okta.com

---

LAB EXPERIMENT – 4

Type of Target	Information Obtained
E.g. Website / Domain	• IP Address - 91.201.40.166 • Geolocation - Moskva - Moskva - Llc Ruweb • Hosted by - Private Person • Physical address - Russia • Services provided – Pirated Games • Server names - MILES.NS.CLOUDFLARE.COM JOAN.NS.CLOUDFLARE.COM • Server OS - Linux • Top Management - None
E.g. Person	• Name - Palak Singhla • Location – Himachal Pradesh • Phone – No Info • Office Address – CU, Chandigarh • Home Address - Solan, Himachal Pradesh • Role – Twitter Friend • Credit Card – No Info • Hobbies – Chatting and Gossips • Buying Habits – No Habits at all • Friends – Aditi, Shreya, Ananya

Perform Internet Footprinting Internet

	• Social Media Posts → 6 Pictures Captured • Twitter / Facebook - palak_016

Used Grabify and got the ip using social engineering on Instagram.

Link Used – https://grabify.link

Original URL - https://www.upes.ac.in/

Geo Location - https://www.google.com/intl/en_in/earth/about/

Website Information - https://whois.domaintools.com/rin.ru

Target 1

Young Teen

Source – Instagram

Method – Social Engineering

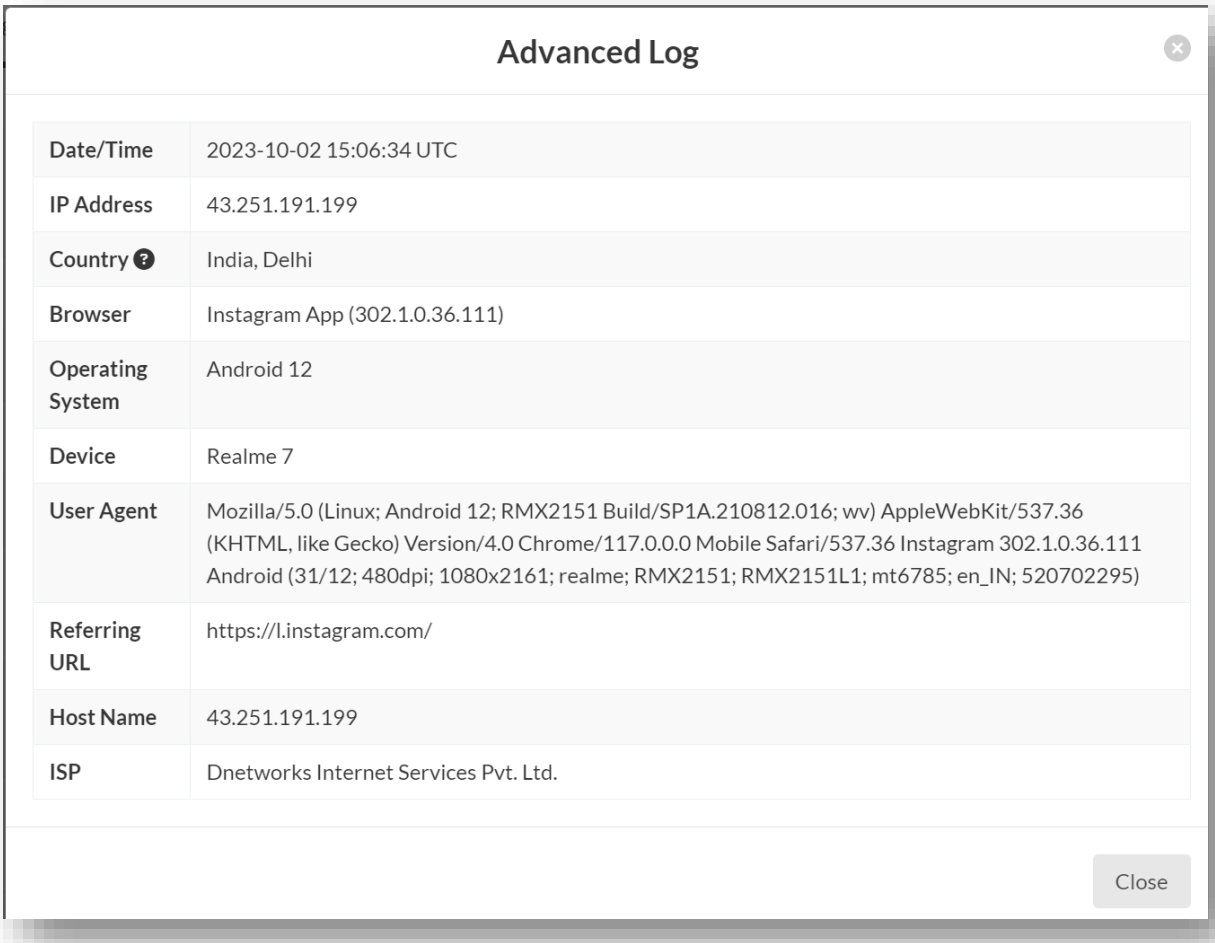
IP - 43.251.191.199

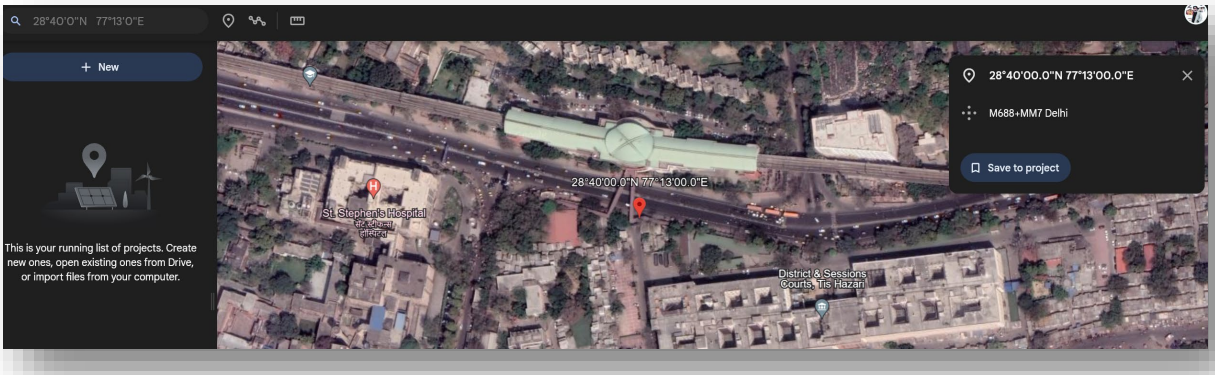
Coordinates - 28.666775, 77.216681 (28°40'0"N 77°13'0"E)

Geo Location – Delhi, India

ISP – Dnetworks Internet Services Pvt. Ltd.

Device – Real ME 7 Pro





Target 2

Student at CU

Source – Instagram

Method – Social Engineering

IP - 103.41.26.231

Coordinates - 32.039330, 75.403180 (32°2'22"N 75°24'11"E)

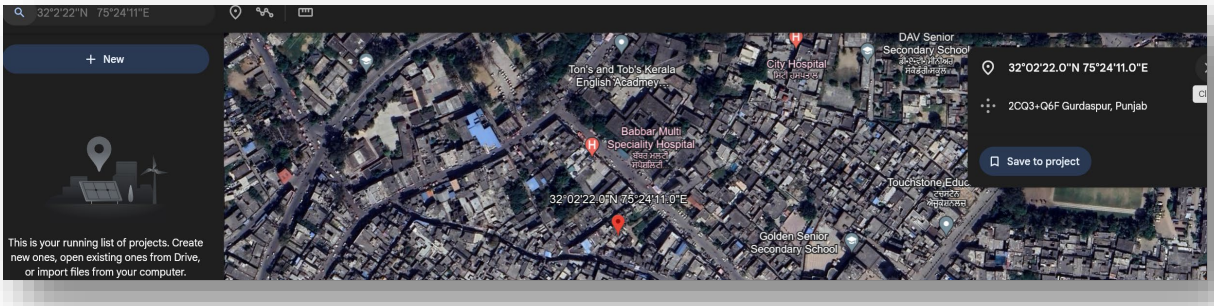
Geo Location – Gurdaspur, Punjab, India

ISP – Fastway Transmission Private Limited

Device – Vivo Y20G (2021)

Date/Time	2023-10-02 15:29:15 UTC
IP Address	103.41.26.231
Country	India, Bhiwani
Browser	Instagram App (302.1.0.36.111)
Operating System	Android 10
Device	Vivo Y20G (2021)
User Agent	Mozilla/5.0 (Linux; Android 10; V2065 Build/QP1A.190711.020; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/117.0.0.0 Mobile Safari/537.36 Instagram 302.1.0.36.111 Android (29/10; 300dpi; 720x1475; vivo; V2065; 2026; mt6765; en_US; 520702291)
Referring URL	http://instagram.com/
Host Name	231.26.41.103.netplus.co.in
ISP	Netplus Broadband Services Private Limited

IP Address	103.41.26.231
Country	India [IN]
Region	Punjab
City	Gurdaspur
Coordinates of City	32.039330, 75.403180 (32°2'22"N 75°24'11"E)
ISP	Fastway Transmission Private Limited
Local Time	02 Oct, 2023 09:04 PM (UTC +05:30)
Domain	fastway.in
Net Speed	(DSL) Broadband/Cable/Fiber/Mobile
IDD & Area Code	(91) 080
ZIP Code	143515
Weather Station	Batala (INXX0015)



Target 3

Student at CU's Friend at Home

Source – Instagram

Method – Social Engineering

IP - 223.187.100.126

Coordinates - 30.916670, 77.116670 (30°55'0"N 77°7'0"E)

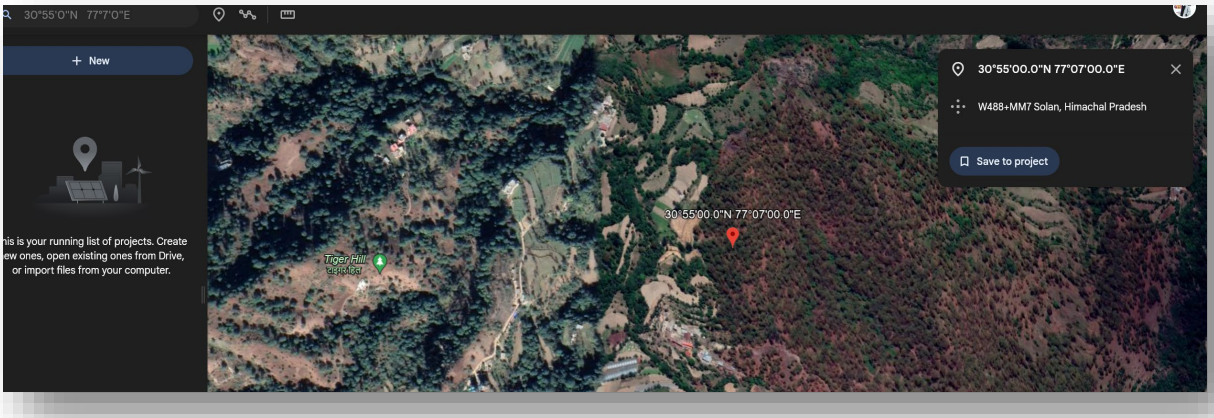
Geo Location – Solan, Himachal Pradesh, India

ISP – Bharti Airtel Ltd.

Device – Apple iPhone (iOS 12.3.1)

Date/Time	2023-10-02 15:35:26 UTC
IP Address	223.187.100.126
Country	India, Delhi
Browser	Mobile Safari (12.1.1)
Operating System	iOS 12.3.1
Device	Apple iPhone
User Agent	Mozilla/5.0 (iPhone; CPU iPhone OS 12_3_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Mobile/15E148 Safari/604.1
Referring URL	*no referrer*
Host Name	223.187.100.126
ISP	Bharti Airtel Ltd. AS for GPRS Service

IP Address	223.187.100.126
Country	India [IN]
Region	Himachal Pradesh
City	Solan
Coordinates of City	30.916670, 77.116670 (30°55'0"N 77°7'0"E)
ISP	Bharti Airtel Ltd.
Local Time	02 Oct, 2023 09:08 PM (UTC +05:30)
Domain	airtel.in
Net Speed	(DSL) Broadband/Cable/Fiber/Mobile
IDD & Area Code	(91) 098
ZIP Code	173210
Weather Station	Shimla (INXX0195)
Mobile Carrier	AirTel
Mobile Country Code - MCC	404
Mobile Network Code - MNC	02/03/10/16/31/40/45/49/70/90/92/93/94/95/96/97/98/51/52/53/54/56
Elevation	1378m



Target – Website

Whois Record for Rin.ru

− Domain Profile

Registrar	RU-CENTER-RU IANA ID: – URL: https://www.nic.ru/whois Whois Server: –
Registrar Status	REGISTERED,
Dates	8,662 days old Created on 2000-01-14 Expires on 2024-01-31
Name Servers	JOAN.NS.CLOUDFLARE.COM. (has 25,220,938 domains) MILES.NS.CLOUDFLARE.COM. (has 25,220,938 domains)
IP Address	91.201.40.166 - 1 other site is hosted on this server
IP Location	- Moskva - Moskva - Llc Ruweb
ASN	AS210079 EUROBYTE EuroByte LLC, RU (registered Oct 11, 2018)
Hosting History	6 changes on 6 unique name servers over 10 years

Whois Record (last updated on 2023-10-02)

```
domain:         RIN.RU
nserver:        joan.ns.cloudflare.com.
nserver:        miles.ns.cloudflare.com.
state:          REGISTERED, DELEGATED, VERIFIED
person:         Private Person
registrar:      RU-CENTER-RU
admin-contact:  https://www.nic.ru/whois
created:        2000-01-14T16:01:52Z
paid-till:      2024-01-31T21:00:00Z
free-date:      2024-03-03
source:         TCI
```

LAB EXPERIMENT – 6

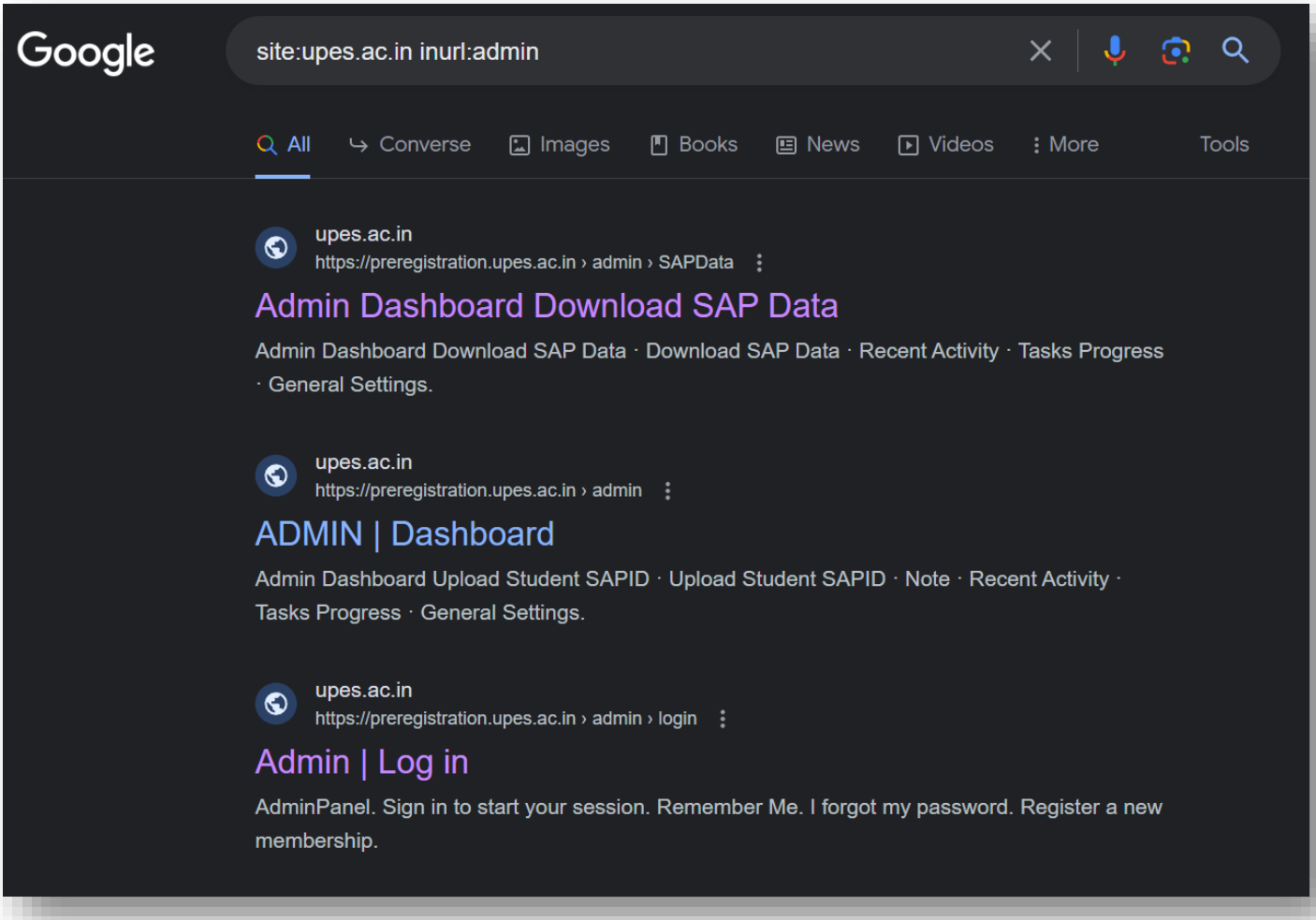
Hack using Search Engines

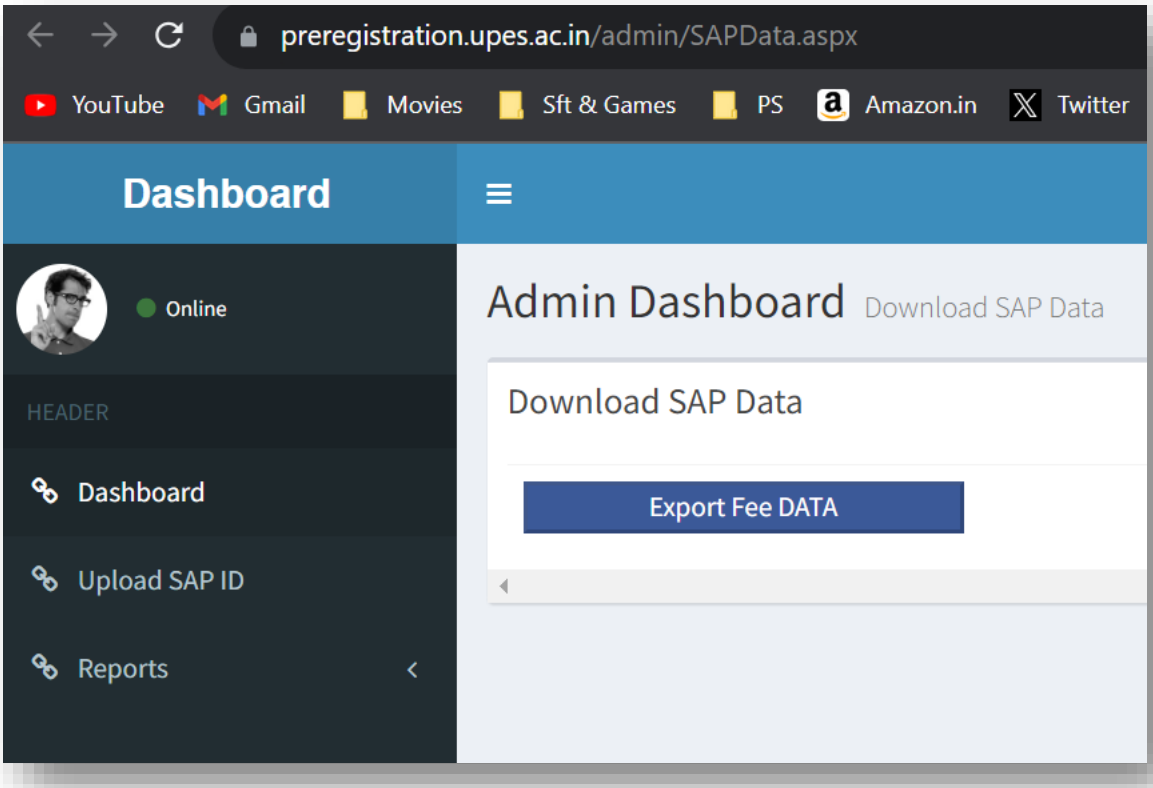
Akshat site:upesac.in intitle:

Intitle

Intext

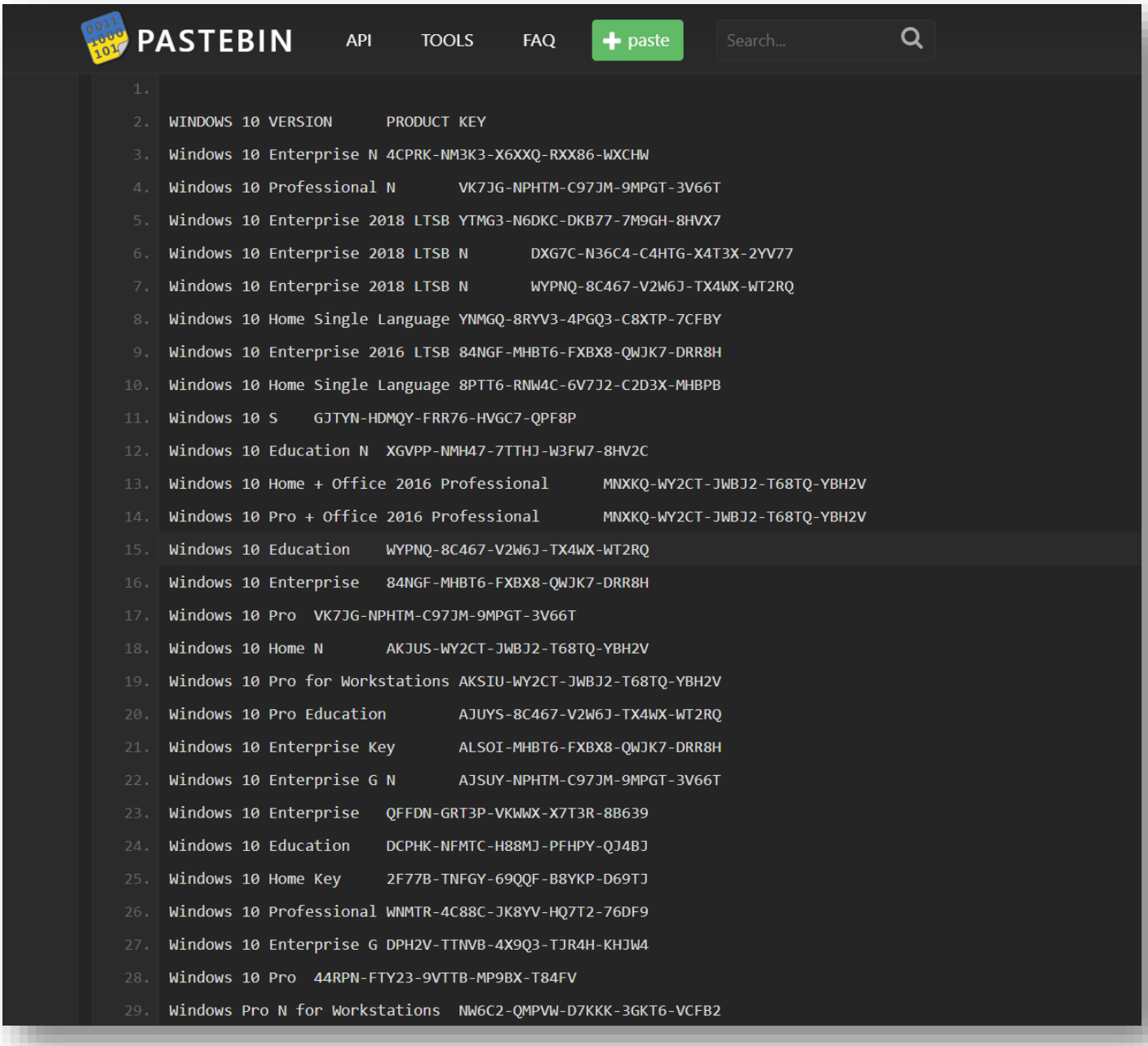
Inurl



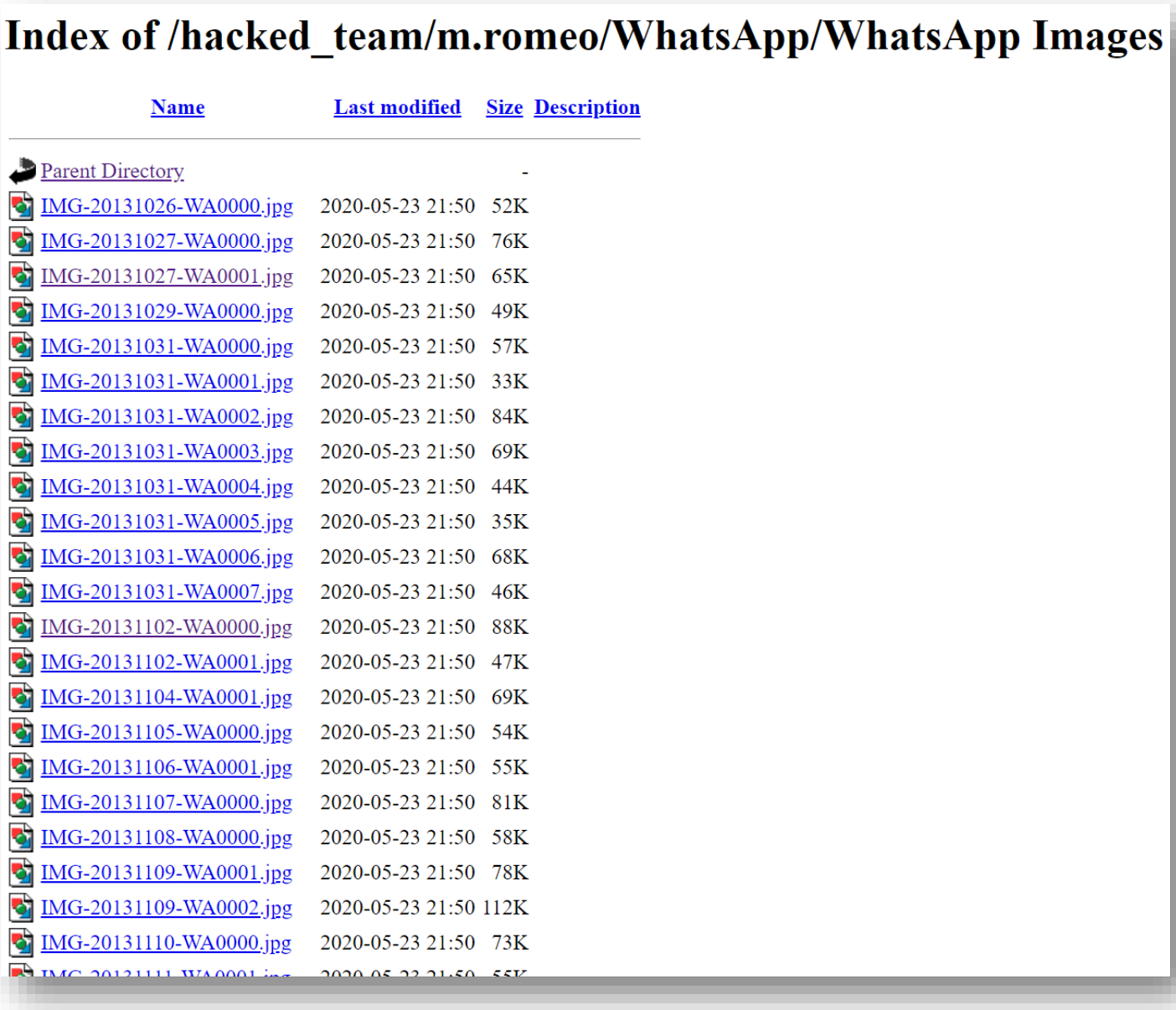


Sl No.	Gender	Title	First Name	Middle Name	Last Name	Application No.	Date of Birth	Nationality	Communication Lang.	Marital Status	University	Building
1	Female	3	Vanya		kalra	102205608	12.04.2005	IN	EN	0	UPES	Opp. Mbd mall ludhiana
2	Female	3	Janhvi	Vikram	Mayee	102205658	25.02.2006	IN	EN	0	UPES	B1/404, Parkwoods, Behind DMart, Ghodbunder Road, Kavesar
3	Female	3	Meghna		Chaturvedi	102205679	25.05.2005	IN	EN	0	UPES	South Bopal
4	Female	3	anika		goyal	102205713	17.04.2005	IN	EN	0	UPES	sector 12 mahavir drishti c204
5	Female	3	Vani		Gupta	102205769	23.09.2005	IN	EN	0	UPES	126, Satya Niketan, Moti Bagh 2, New Delhi110021
6	Male	1	SAMYAK	ASHOKKUMAR	GADHIRE	102205770	31.10.2005	IN	EN	0	UPES	ALLURE BEGONIA CHS, NEHRU NAGAR
7	Female	3	ADYA		BHARGAVA	102205772	19.12.2004	IN	EN	0	UPES	RAJPUR ROAD
8	Male	1	Uday		Grover	102205775	11.04.2005	IN	EN	0	UPES	Vasant Kunj
9	Male	1	Shashank	Rajaneesh	Hebbar	102205776	17.01.2005	IN	EN	0	UPES	BRIGADE METROPOLIS, WHITEFIELD MAIN ROAD
10	Female	3	Mrunal	Nilesh	Aitawadekar	102205786	27.01.2005	IN	EN	0	UPES	G1, Shivdatta Ratna apt, 100 ft road, Vishrambagh, Sangli
11	Male	1	Ashmit	Mohit	Nand	102205790	24.06.2005	IN	EN	0	UPES	Gachibowli, Hyderabad
12	Female	3	Vishaka	Vishal	Ghumbre	102205816	01.05.2005	IN	EN	0	UPES	A 1402 arihant anaya sec 35G kharghar navi mumbai
13	Female	3	Divyanshi		Singh	102205818	26.10.2004	IN	EN	0	UPES	Near Kanchan kaya yoga center,
14	Female	3	Dia	Amitkumar	Gosar	102205847	15.10.2005	IN	EN	0	UPES	A703, Jay Balaji, CHS
15	Female	3	Devishi		Wahi	102205865	08.04.2005	IN	EN	0	UPES	Delhi road
16	Male	1	Ayush		NAIR	102205891	01.12.2005	IN	EN	0	UPES	C3/1003, Lotus Pond Apt
17	Female	3	Mahak	Avinash	Zawar	102205892	10.07.2005	IN	EN	0	UPES	18,ASHISH,ANAND NAGAR GULMOHAR ROAD, AHMEDNAGAR
18	Male	1	Nitai		Gandhar	102205895	10.08.2005	IN	EN	0	UPES	57, sec 7, Urban Estate, Gurugram, Haryana
19	Female	3	Ashna		Das	102205908	23.06.2004	IN	EN	0	UPES	Shivoham Gardenia
20	Female	3	Neha	Ganesh	Kumbhar	102205909	21.05.2005	FO	EN	0	UPES	
21	Male	1	DHAIRYA		TIWARI	102205919	26.10.2005	IN	EN	0	UPES	MEDIA TIMES APARTMENT, ABHAY KHAND4, INDIRAPURAM, GHAZIAB
22	Female	3	Shagal		Maheshwari	102205921	05.11.2005	IN	EN	0	UPES	gumasta nagar
23	Female	3	Nayanika		Tyagi	102205924	06.12.2005	IN	EN	0	UPES	
24	Female	3	Tanvi		Gupta	102205925	01.03.2005	IN	EN	0	UPES	Chandrakala Colony
25	Female	3	Reetika		Madan	102205936	21.12.2004	IN	EN	0	UPES	B5, Dhawalgiri Apartment
26	Female	3	Muskaan		Mehra	102205951	02.04.2004	IN	EN	0	UPES	29 ba Basant avenue backside of adlakha hospital
27	Male	1	Hanskumar	Sachin	Gala	102205953	26.01.2005	IN	EN	0	UPES	garodia nagar
28	Female	3	Ananya	Gurunath	Borkar	102205956	29.09.2005	IN	EN	0	UPES	RESTAURANT GOREGAON E
29	Female	3	Ananya		Udasi	102205957	14.12.2005	IN	EN	0	UPES	Survey No. 148, Golden Mile Road
30	Female	3	VIDHI	VIPUL	AMBADE	102205964	20.06.2003	IN	EN	0	UPES	BEHIND HOTEL ASHOK, AATH RASTA SQUARE,
31	Female	3	Ishita		Jauhari	102205976	14.05.2005	IN	EN	0	UPES	4E Peach, SFS Cyberpalms
32	Female	3	Anmoldeep	Kaur	Sandhu	102205986	07.08.2005	IN	EN	0	UPES	57a Subhash colony ambala cantt
33	Female	3	Anshika		Pundir	102205992	04.03.2006	IN	EN	0	UPES	Kahna green city
34	Female	3	Reva	Rohit	Rajgariah	102205999	25.04.2004	IN	EN	0	UPES	vasant nagri
35	Female	3	Aditi		Madhavan	102206008	03.03.2005	IN	EN	0	UPES	Salarpuria Magnificia
36	Female	3	NANDINI		CHADHA	102206013	10.08.2005	IN	EN	0	UPES	CH/KG 20.KAVI NAGAR G BLOCK GHAZIABAD
37	Female	3	Miya	Martha	Sanooj	102206087	19.02.2005	IN	EN	0	UPES	ElectraPark Apartment,

inurl:pastebin "Windows 10 Product Keys*"



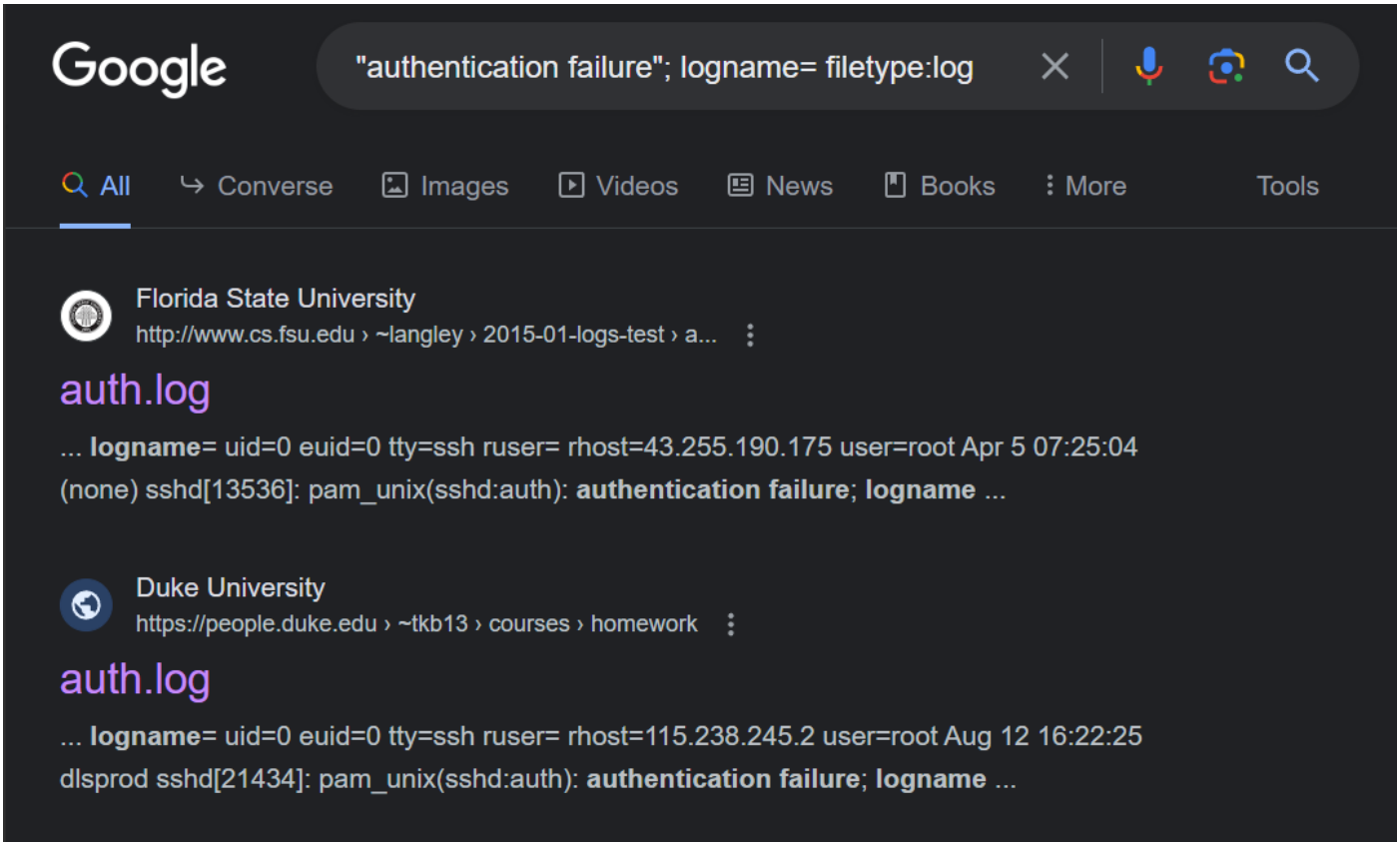
intitle:"Index of" "WhatsApp Images"



Index of /hacked_team/m.romeo/WhatsApp/WhatsApp Images

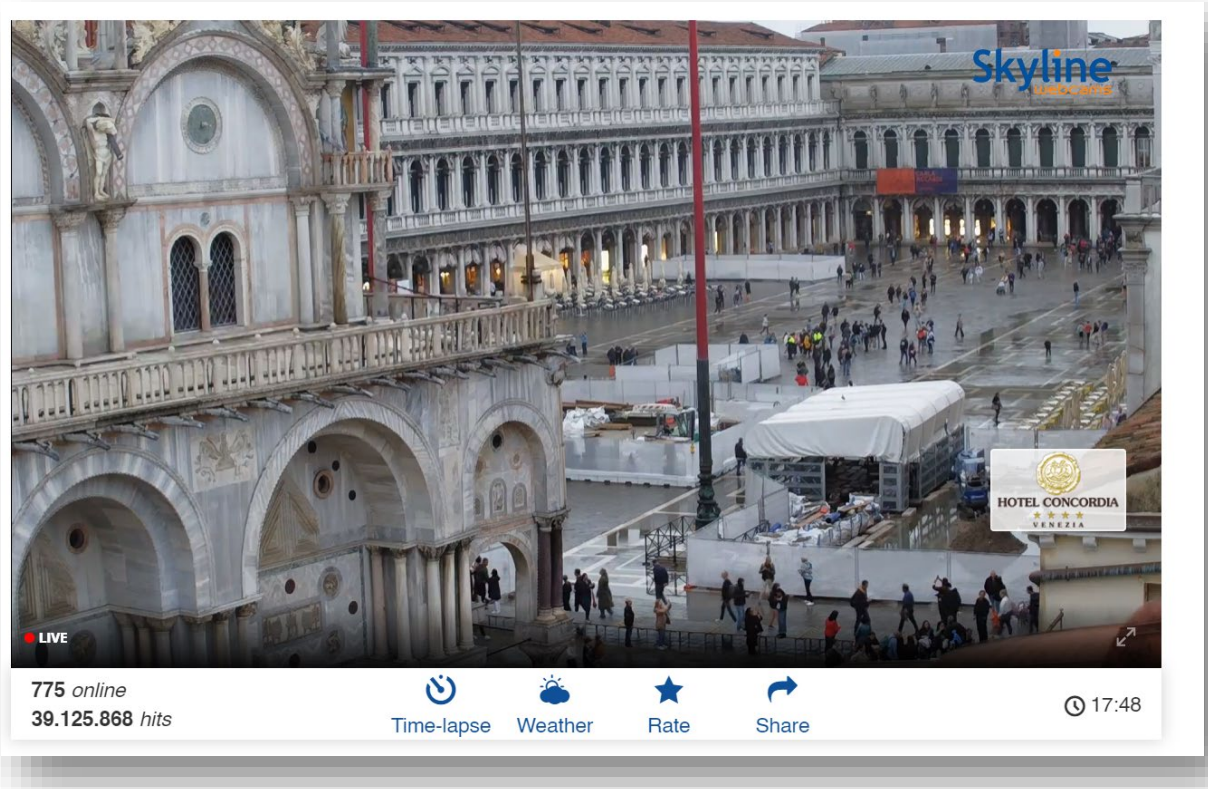
Name	Last modified	Size	Description
Parent Directory		-	
IMG-20131026-WA0000.jpg	2020-05-23 21:50	52K	
IMG-20131027-WA0000.jpg	2020-05-23 21:50	76K	
IMG-20131027-WA0001.jpg	2020-05-23 21:50	65K	
IMG-20131029-WA0000.jpg	2020-05-23 21:50	49K	
IMG-20131031-WA0000.jpg	2020-05-23 21:50	57K	
IMG-20131031-WA0001.jpg	2020-05-23 21:50	33K	
IMG-20131031-WA0002.jpg	2020-05-23 21:50	84K	
IMG-20131031-WA0003.jpg	2020-05-23 21:50	69K	
IMG-20131031-WA0004.jpg	2020-05-23 21:50	44K	
IMG-20131031-WA0005.jpg	2020-05-23 21:50	35K	
IMG-20131031-WA0006.jpg	2020-05-23 21:50	68K	
IMG-20131031-WA0007.jpg	2020-05-23 21:50	46K	
IMG-20131102-WA0000.jpg	2020-05-23 21:50	88K	
IMG-20131102-WA0001.jpg	2020-05-23 21:50	47K	
IMG-20131104-WA0001.jpg	2020-05-23 21:50	69K	
IMG-20131105-WA0000.jpg	2020-05-23 21:50	54K	
IMG-20131106-WA0001.jpg	2020-05-23 21:50	55K	
IMG-20131107-WA0000.jpg	2020-05-23 21:50	81K	
IMG-20131108-WA0000.jpg	2020-05-23 21:50	58K	
IMG-20131109-WA0001.jpg	2020-05-23 21:50	78K	
IMG-20131109-WA0002.jpg	2020-05-23 21:50	112K	
IMG-20131110-WA0000.jpg	2020-05-23 21:50	73K	

"authentication failure"; logname= filetype:log

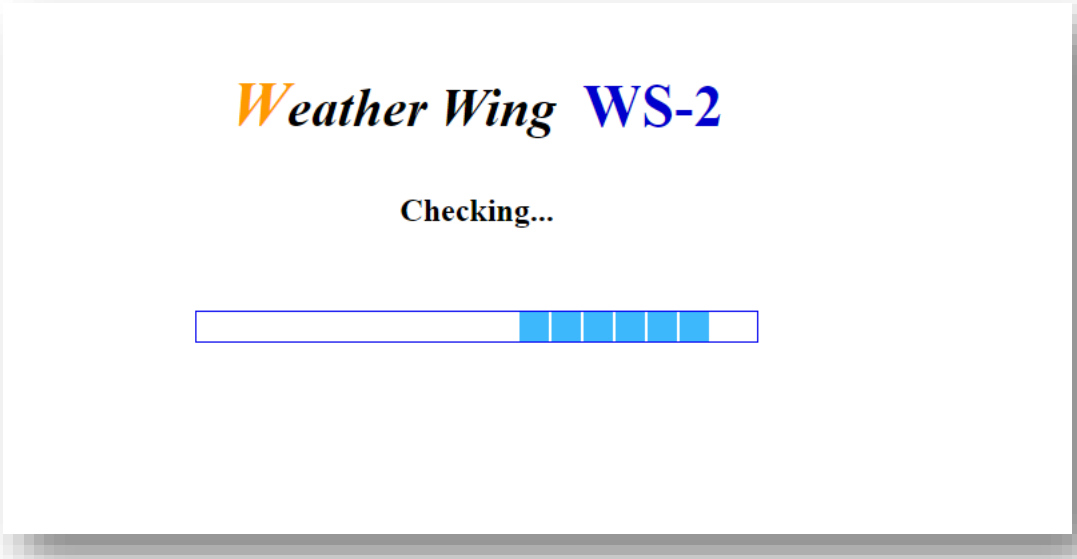



```
-- Logs begin at Sat 2020-09-19 17:06:29 UTC. --
Nov 13 22:08:17 test-server su[25225]: pam_unix(su:session): session closed for user balena
Nov 13 22:08:27 test-server sshd[25307]: Invalid user dc from 42.194.204.223 port 33450
Nov 13 22:08:27 test-server sshd[25307]: pam_unix(sshd:auth): check pass; user unknown
Nov 13 22:08:27 test-server sshd[25307]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=s
Nov 13 22:08:28 test-server sshd[25304]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=s
Nov 13 22:08:30 test-server sshd[25307]: Failed password for invalid user dc from 42.194.204.223 port 33450 ssh2
Nov 13 22:08:30 test-server sshd[25306]: Invalid user ok from 101.36.179.145 port 35294
Nov 13 22:08:30 test-server sshd[25306]: pam_unix(sshd:auth): check pass; user unknown
Nov 13 22:08:30 test-server sshd[25306]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=s
Nov 13 22:08:30 test-server sshd[25307]: Received disconnect from 42.194.204.223 port 33450:11: Bye Bye [preauth]
Nov 13 22:08:30 test-server sshd[25307]: Disconnected from invalid user dc 42.194.204.223 port 33450 [preauth]
Nov 13 22:08:31 test-server sshd[25304]: Failed password for root from 112.85.42.98 port 12620 ssh2
Nov 13 22:08:31 test-server sshd[25306]: Failed password for invalid user ok from 101.36.179.145 port 35294 ssh2
Nov 13 22:08:32 test-server sshd[25306]: Received disconnect from 101.36.179.145 port 35294:11: Bye Bye [preauth]
Nov 13 22:08:32 test-server sshd[25306]: Disconnected from invalid user ok 101.36.179.145 port 35294 [preauth]
Nov 13 22:08:34 test-server sshd[25304]: Failed password for root from 112.85.42.98 port 12620 ssh2
Nov 13 22:08:35 test-server sshd[25321]: Invalid user database from 123.207.100.182 port 50836
Nov 13 22:08:35 test-server sshd[25321]: pam_unix(sshd:auth): check pass; user unknown
Nov 13 22:08:35 test-server sshd[25321]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=s
Nov 13 22:08:36 test-server sshd[25323]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=s
Nov 13 22:08:37 test-server sshd[25321]: Failed password for invalid user database from 123.207.100.182 port 5083
Nov 13 22:08:37 test-server sshd[25321]: Received disconnect from 123.207.100.182 port 50836:11: Bye Bye [preauth
Nov 13 22:08:37 test-server sshd[25321]: Disconnected from invalid user database 123.207.100.182 port 50836 [prea
Nov 13 22:08:37 test-server sshd[25304]: Failed password for root from 112.85.42.98 port 12620 ssh2
Nov 13 22:08:37 test-server sshd[25323]: Failed password for root from 61.177.172.158 port 40796 ssh2
Nov 13 22:08:39 test-server sshd[25323]: Failed password for root from 61.177.172.158 port 40796 ssh2
Nov 13 22:08:41 test-server sshd[25304]: Failed password for root from 112.85.42.98 port 12620 ssh2
Nov 13 22:08:42 test-server sshd[25323]: Failed password for root from 61.177.172.158 port 40796 ssh2
Nov 13 22:08:42 test-server sshd[25323]: Received disconnect from 61.177.172.158 port 40796:11:  [preauth]
Nov 13 22:08:42 test-server sshd[25323]: Disconnected from authenticating user root 61.177.172.158 port 40796 [pr
Nov 13 22:08:42 test-server sshd[25323]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser=
Nov 13 22:08:44 test-server sshd[25304]: Failed password for root from 112.85.42.98 port 12620 ssh2
```

https://www.skylinewebcams.com/en/webcam/italia/veneto/venezia/piazza-san-marco.html



intitle:"Weather Wing WS-2"




185.230.194
http://185.230.194.209
Weather Wing WS-2
No-IP
http://rubizzano.hopto.org › ...
Weather Wing WS-2
88.147.94
http://88.147.94.223
Weather Wing WS-2
No-IP
http://rubizzano.hopto.org
Weather Wing WS-2
Weather Wing WS-2. Checking... Weather Wing. [Temp] 14.2 oC [Hum] 86 % [Bar] 1018.5 hPa [Rain] 0.0 mm [WS] 0.4 m/s [WD] SSW. 23/09/28 04:16.
89.150.61
http://89.150.61.163
Weather Wing WS-2
ns0.it
http://stazionemeteoloro.ns0.it
Weather Wing WS-2
82.49.87
http://82.49.87.239
Weather Wing WS-2

Ways to Prevent Yourself from Google Dork Method

1. Securely configure web applications:

Ensure that your web applications are properly secured, following industry best practices. This includes implementing strong authentication mechanisms, input validation, and access controls to prevent unauthorized access or leakage of sensitive information.

2. Limit search engine indexing:

Use robots.txt or meta tags to instruct search engines not to index certain parts of your website or specific files. This can help prevent sensitive information from being exposed through search engine results.

3. Implement access controls:

Control access to sensitive information by implementing proper authorization mechanisms. Ensure that only authorized users can access sensitive data or perform sensitive actions.

4. Regularly review and update security configurations:

Regularly review and update security configurations for your web applications, content management systems (CMS), and any other platforms you use. This includes keeping software up to date, applying security patches, and following vendor recommendations.

5. Avoid storing sensitive information in plain text:

Do not store sensitive information, such as passwords, API keys, or database credentials, in plain text within your web applications or configuration files. Utilize encryption and secure storage mechanisms to protect sensitive data.

6. Use secure coding practices:

Adhere to secure coding practices, such as input validation, output encoding, and proper handling of user-supplied data. These practices can help prevent common vulnerabilities like SQL injection, cross-site scripting (XSS), and command injection.

7. Implement web application firewalls (WAF):

Consider implementing a WAF to provide an additional layer of protection against attacks targeting your web applications. WAFs can help detect and block suspicious or malicious requests, including those generated by Google dorks.

8. Regularly monitor and audit your web applications:

Implement monitoring and auditing mechanisms to detect and respond to potential security incidents or unauthorized access attempts. This can include log monitoring, intrusion detection systems (IDS), or security information and event management (SIEM) solutions.

9. Educate users and developers:

Provide security awareness training to users and developers to help them understand the risks associated with Google dorks and the importance of following secure coding practices. Encourage them to report any suspicious activities or potential vulnerabilities they encounter.

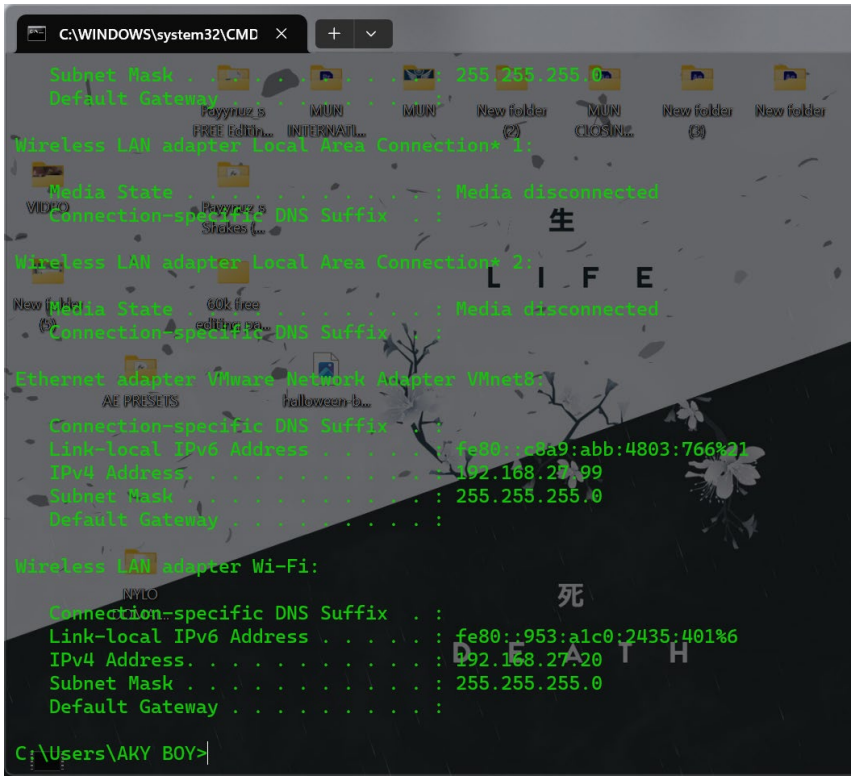
10. Stay informed about security vulnerabilities:

Stay up to date with security news and vulnerabilities related to the software and platforms you use. Subscribe to security mailing lists, follow security blogs, and apply security patches promptly to mitigate known vulnerabilities.

LAB EXPERIMENT – 7

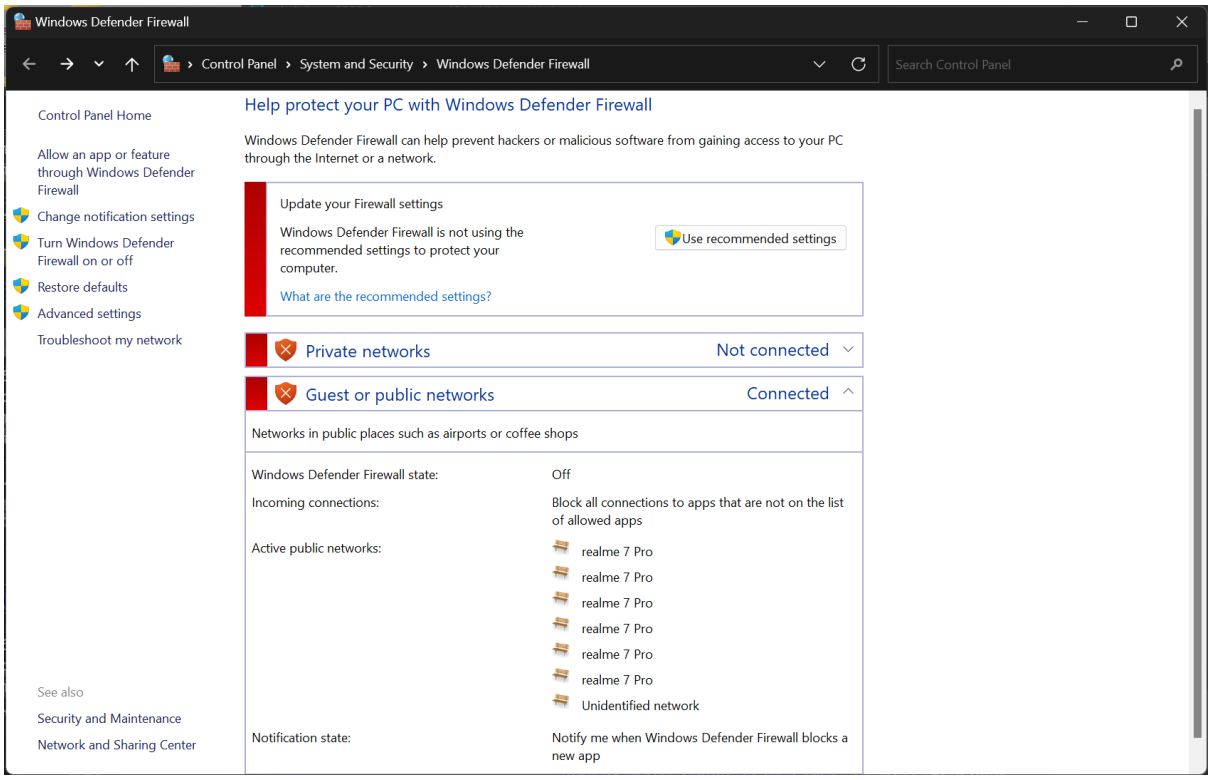
LAN KALI LINUX

IP CONFIG to check the IP for the Device.

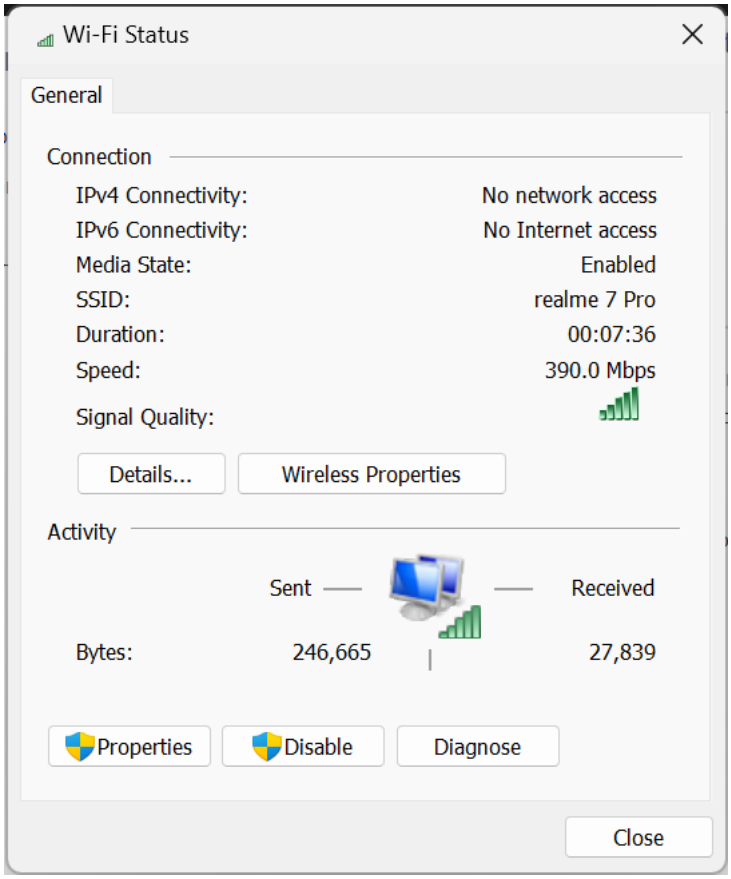


CONFIGURATION IP

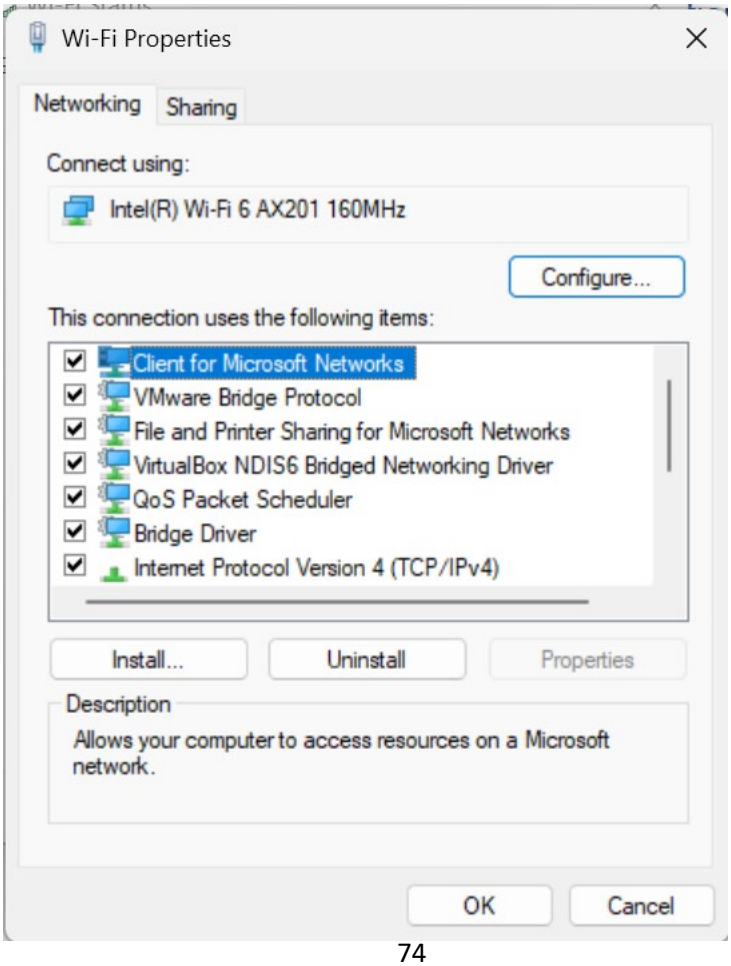
Turn off the Firewall for the both the devices.



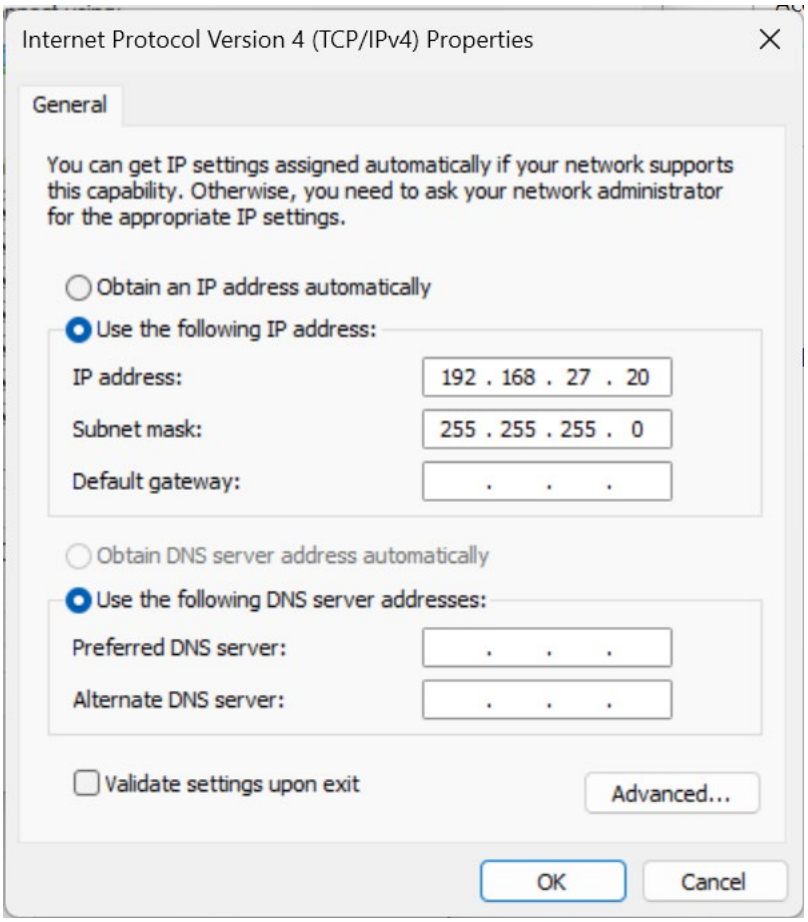
Go for the Properties



Go for the IPV4 to configure the custom Static IP for your device.



IP for my device is 192.168.27.20

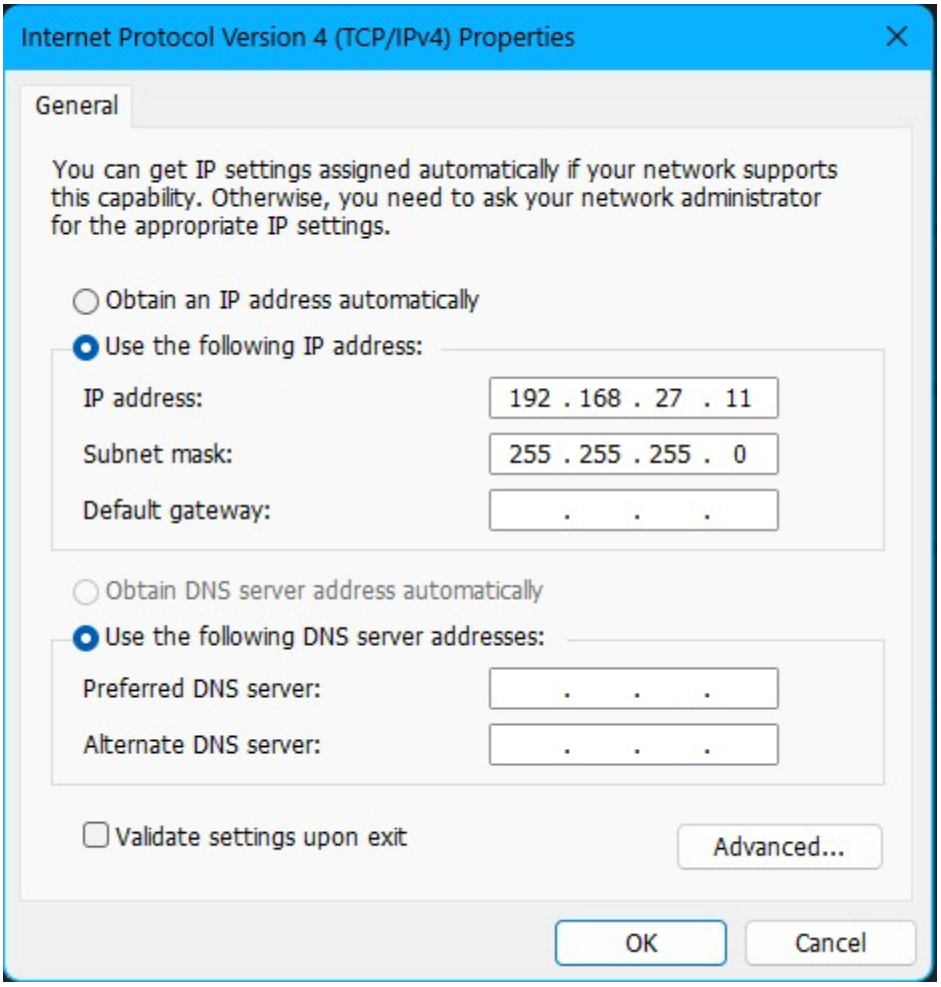


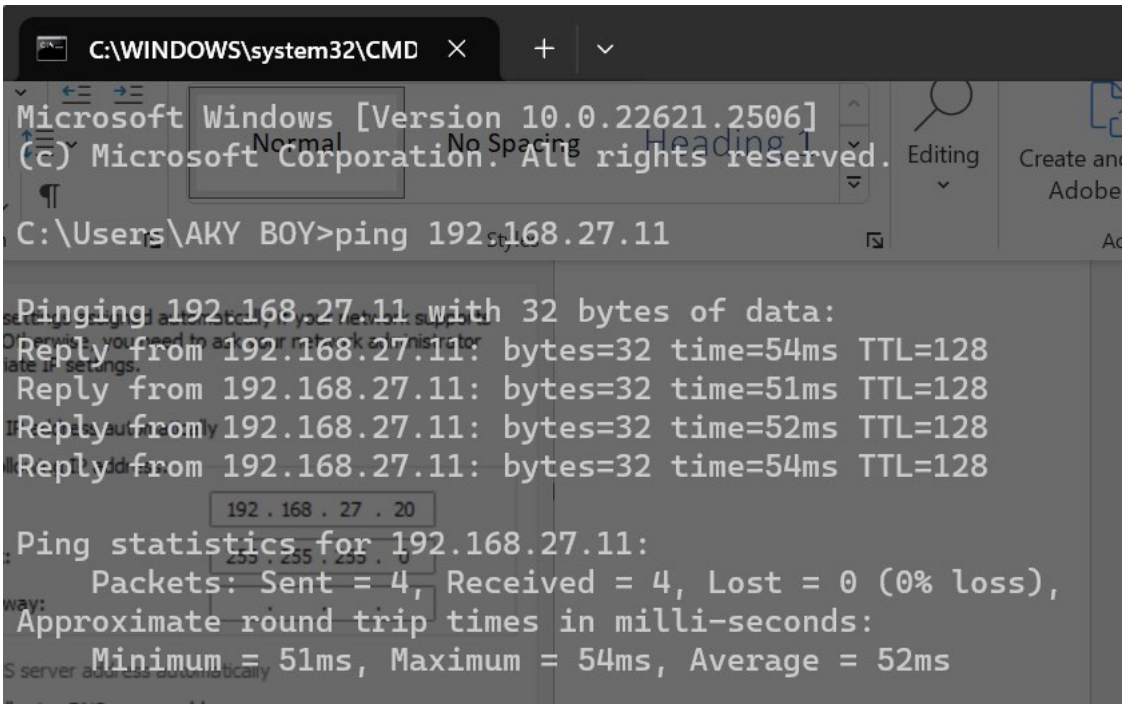
2nd DEVICE IP – 192.168.27.10

3rd Deevce IP – 192.168.27.11

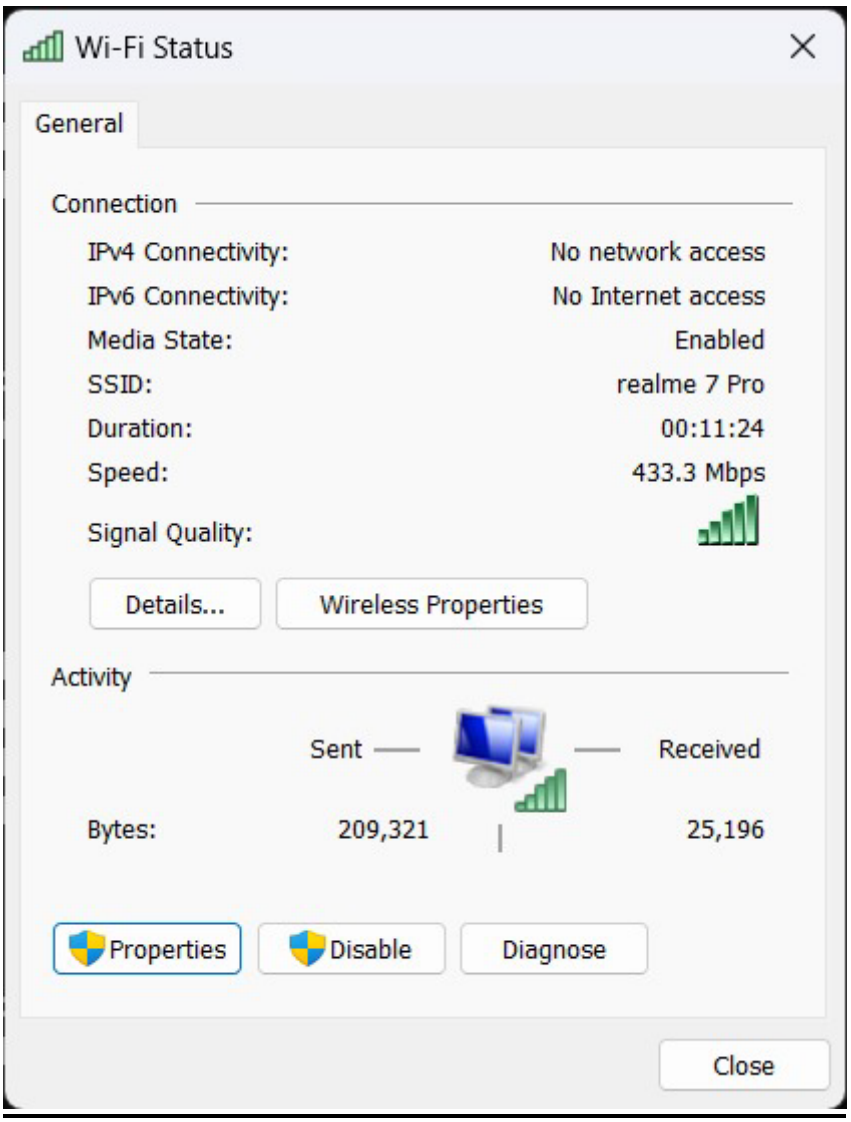
4th Device IP – 192.168.27.12

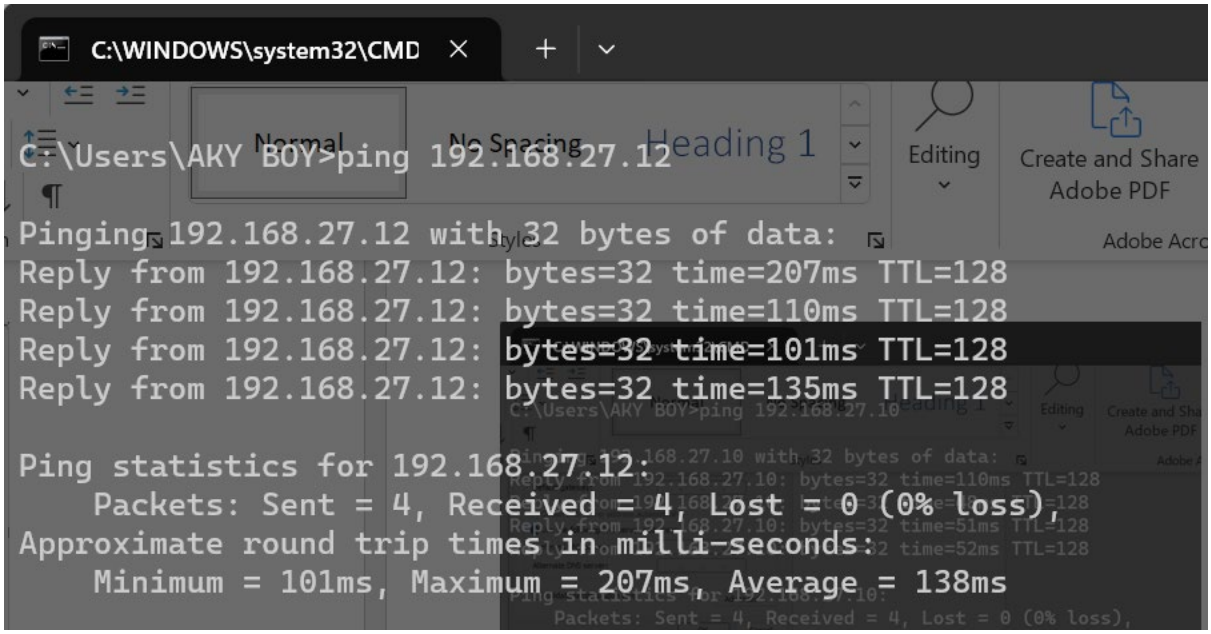
3rd DEVICE


Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 27 . 11
Subnet mask: 255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

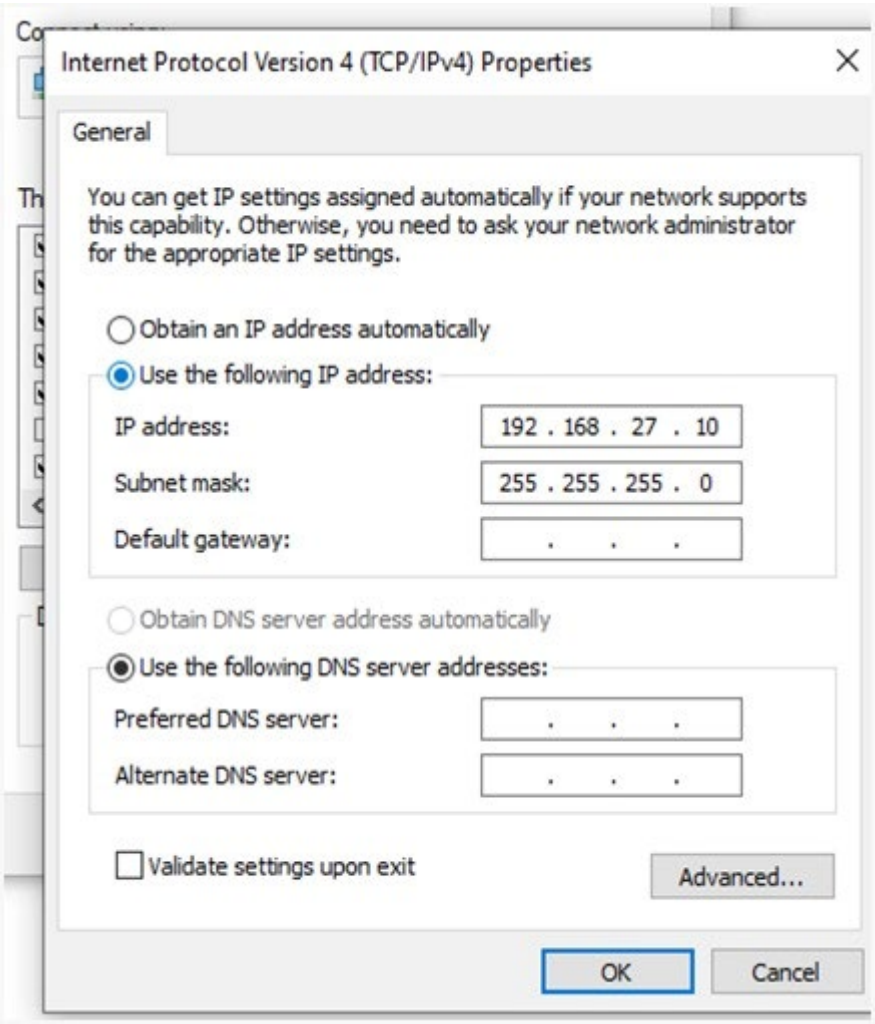

C:\WINDOWS\system32\CMD
Microsoft Windows [Version 10.0.22621.2506]
(c) Microsoft Corporation. All rights reserved.
C:\Users\AKY BOY>ping 192.168.27.11
Pinging 192.168.27.11 with 32 bytes of data:
Reply from 192.168.27.11: bytes=32 time=54ms TTL=128
Reply from 192.168.27.11: bytes=32 time=51ms TTL=128
Reply from 192.168.27.11: bytes=32 time=52ms TTL=128
Reply from 192.168.27.11: bytes=32 time=54ms TTL=128
Ping statistics for 192.168.27.11:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 51ms, Maximum = 54ms, Average = 52ms

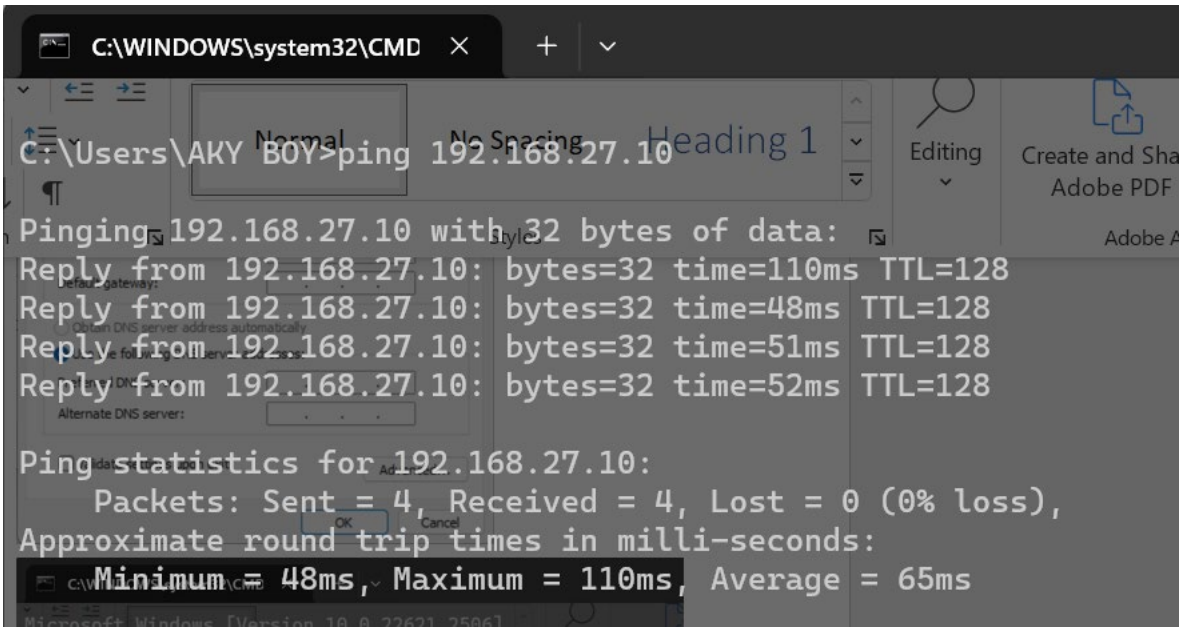
2nd DEVICE


Wi-Fi Status
General
Connection
IPv4 Connectivity: No network access
IPv6 Connectivity: No Internet access
Media State: Enabled
SSID: realme 7 Pro
Duration: 00:11:24
Speed: 433.3 Mbps
Signal Quality:
Details...
Wireless Properties
Activity
Sent
Received
Bytes: 209,321 25,196
Properties
Disable
Diagnose
Close

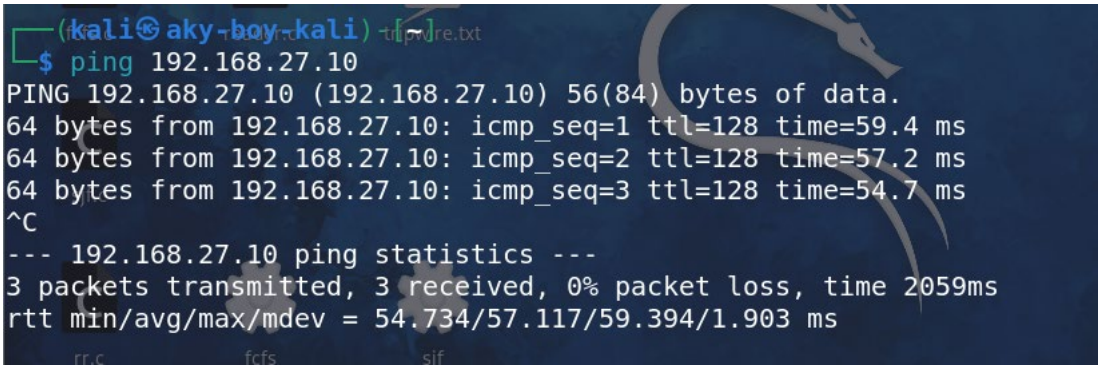

C:\WINDOWS\system32\CMD
C:\Users\AKY BOY>ping 192.168.27.12
Pinging 192.168.27.12 with 32 bytes of data:
Reply from 192.168.27.12: bytes=32 time=207ms TTL=128
Reply from 192.168.27.12: bytes=32 time=110ms TTL=128
Reply from 192.168.27.12: bytes=32 time=101ms TTL=128
Reply from 192.168.27.12: bytes=32 time=135ms TTL=128
Ping statistics for 192.168.27.12:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 101ms, Maximum = 207ms, Average = 138ms

4th DEVICE

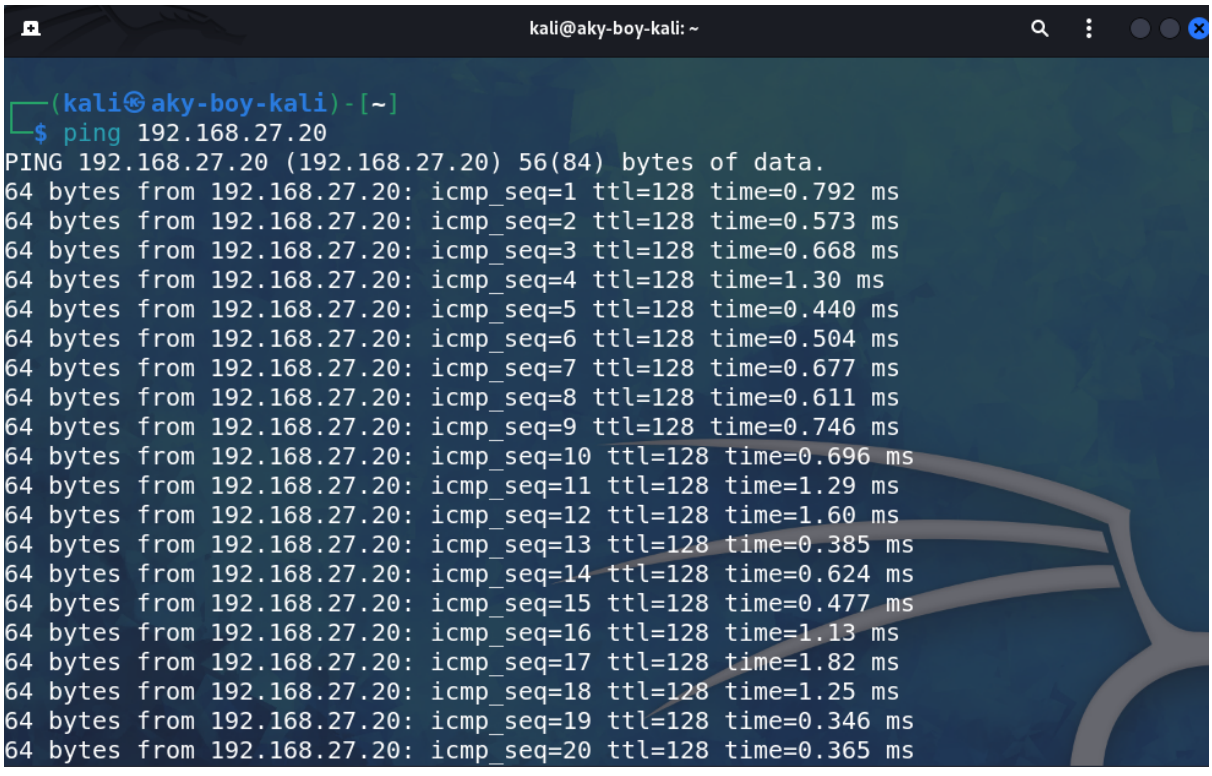

Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 27 . 10
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel


C:\WINDOWS\system32\CMD
C:\Users\AKY BOY>ping 192.168.27.10
Pinging 192.168.27.10 with 32 bytes of data:
Reply from 192.168.27.10: bytes=32 time=110ms TTL=128
Reply from 192.168.27.10: bytes=32 time=48ms TTL=128
Reply from 192.168.27.10: bytes=32 time=51ms TTL=128
Reply from 192.168.27.10: bytes=32 time=52ms TTL=128
Ping statistics for 192.168.27.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 48ms, Maximum = 110ms, Average = 65ms

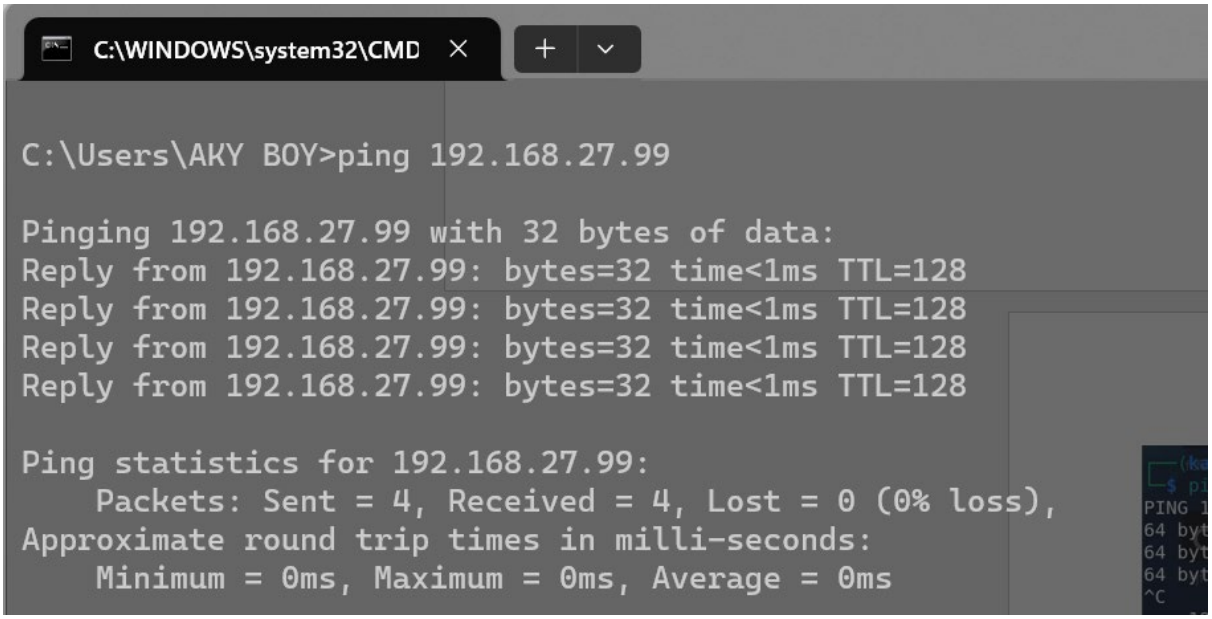
SELF VM TO OTHER DEVICE WINDOWS



PING FROM VM TO SELF DEVICE

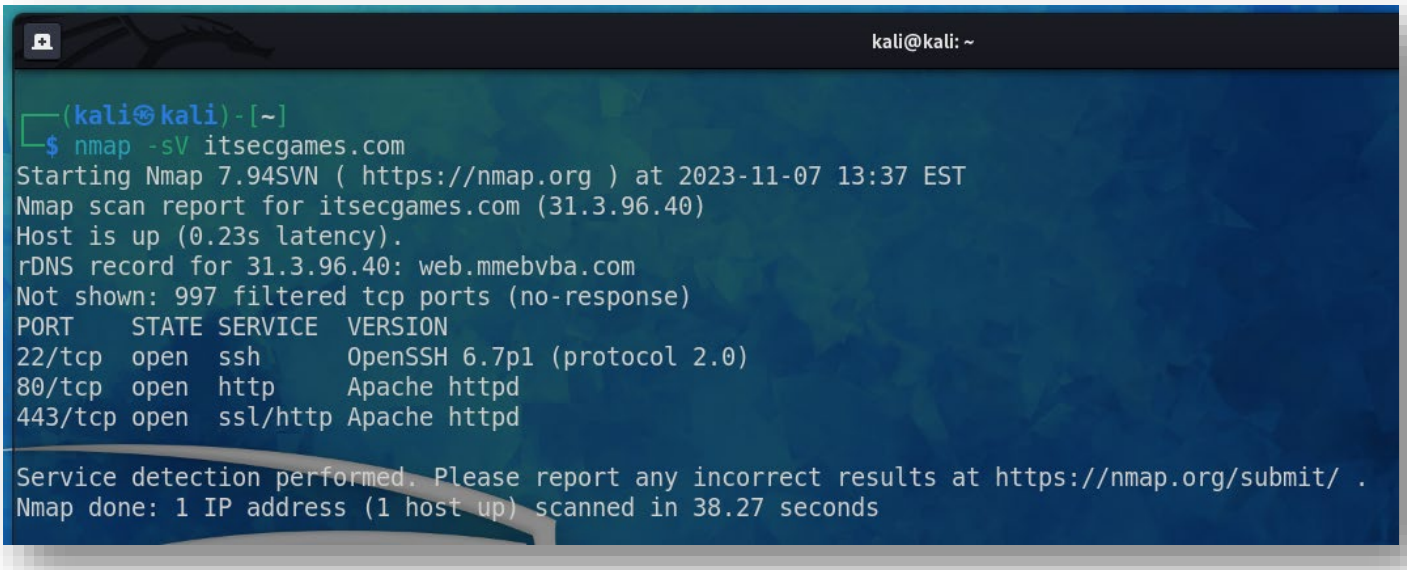


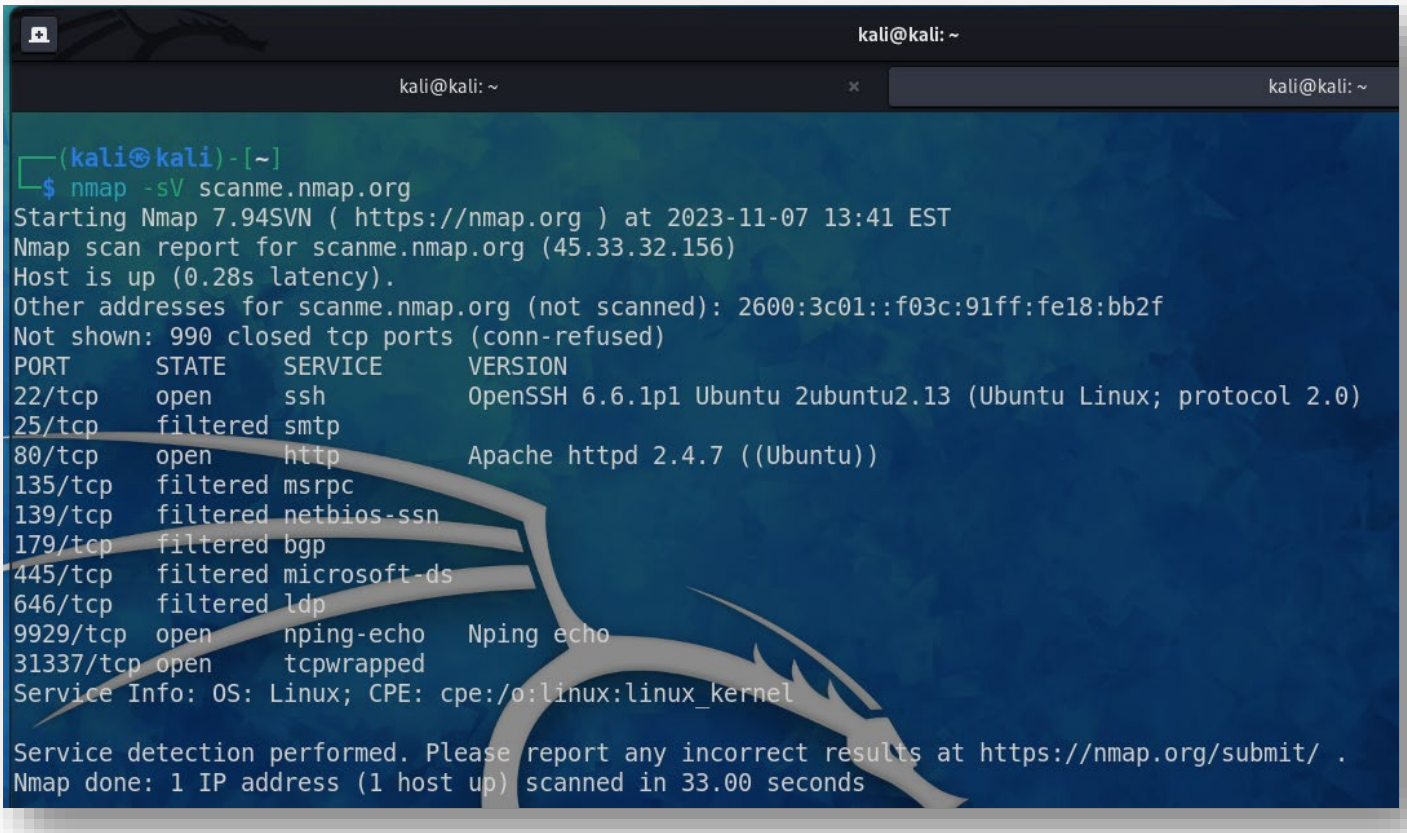
PING FROM WINDOWS TO SELF VM

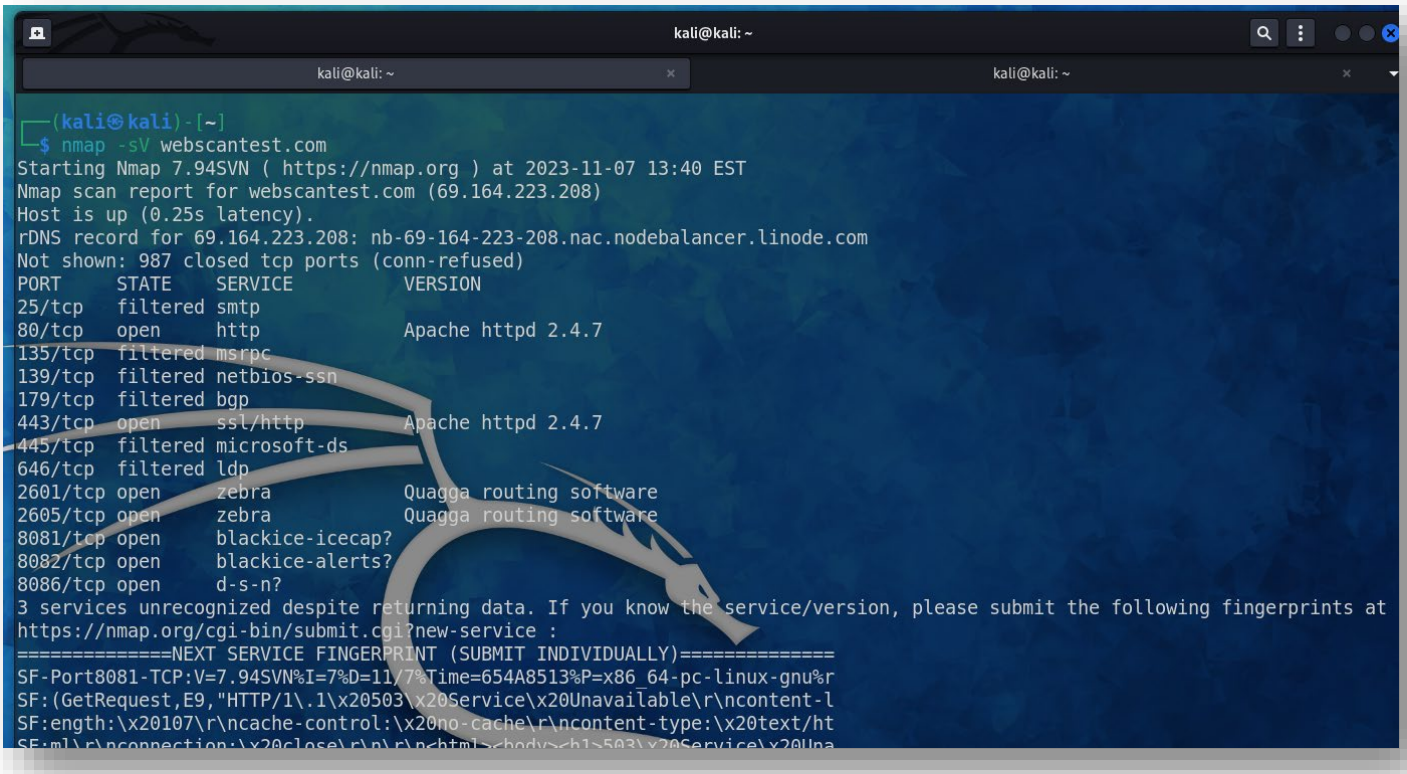


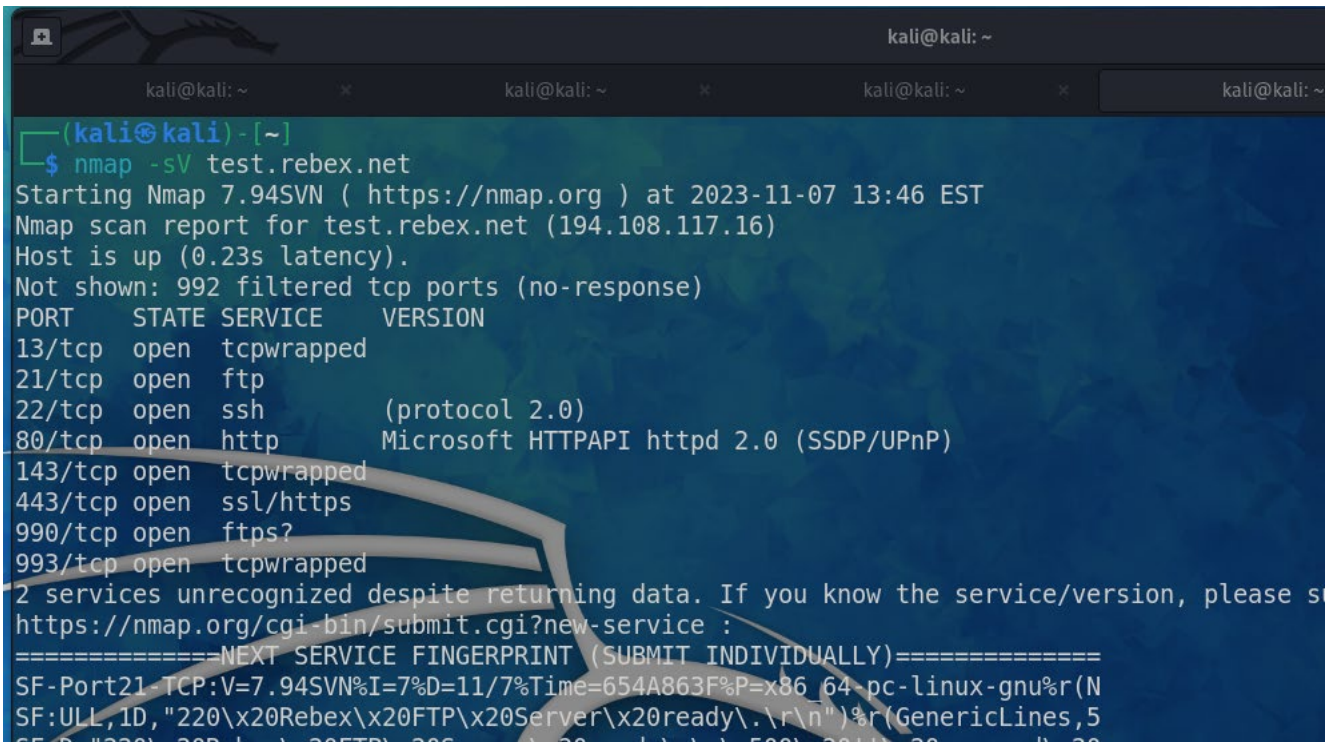
LAB EXPERIMENT – 8

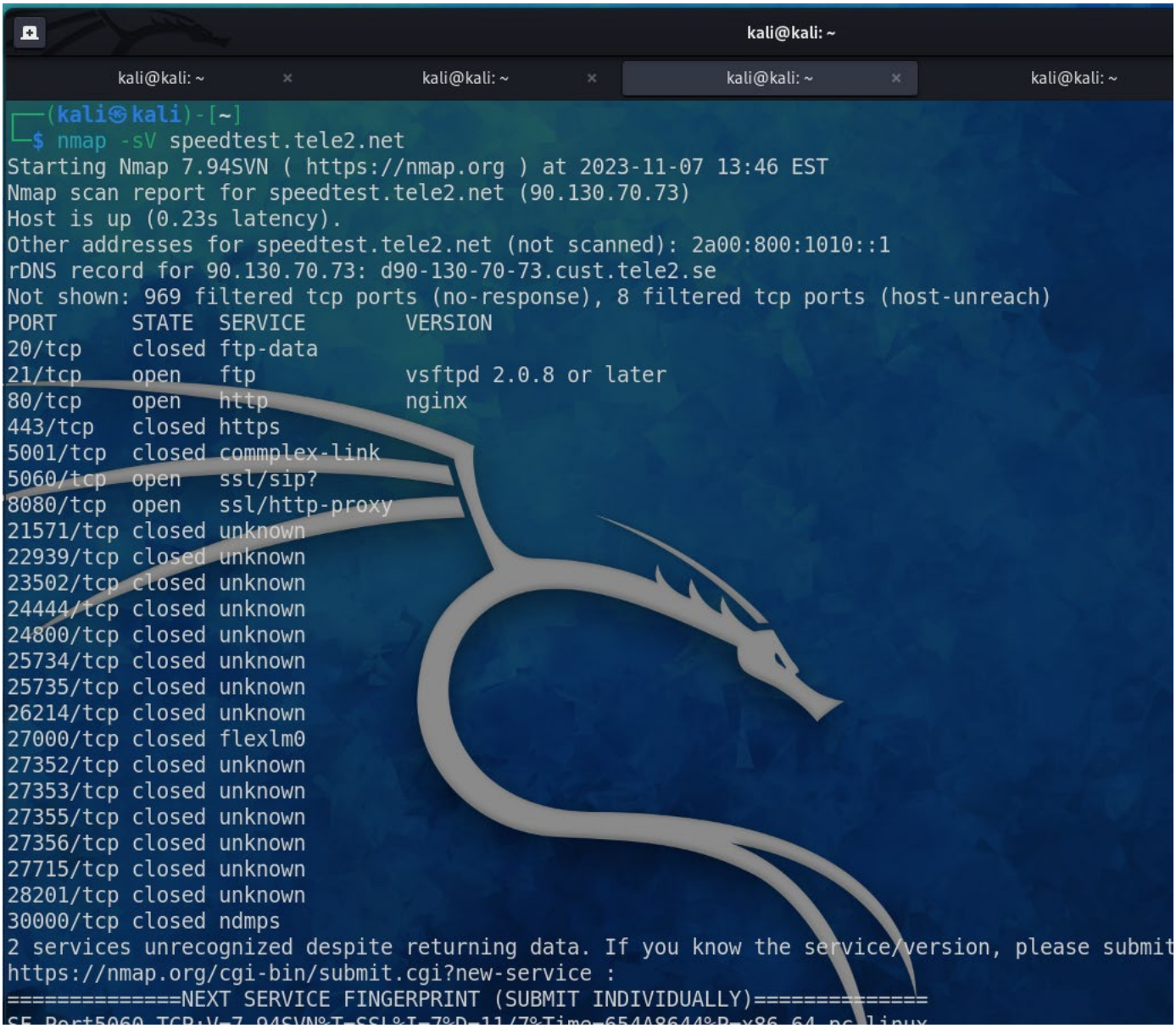
Network Scanning Tool - NMAP





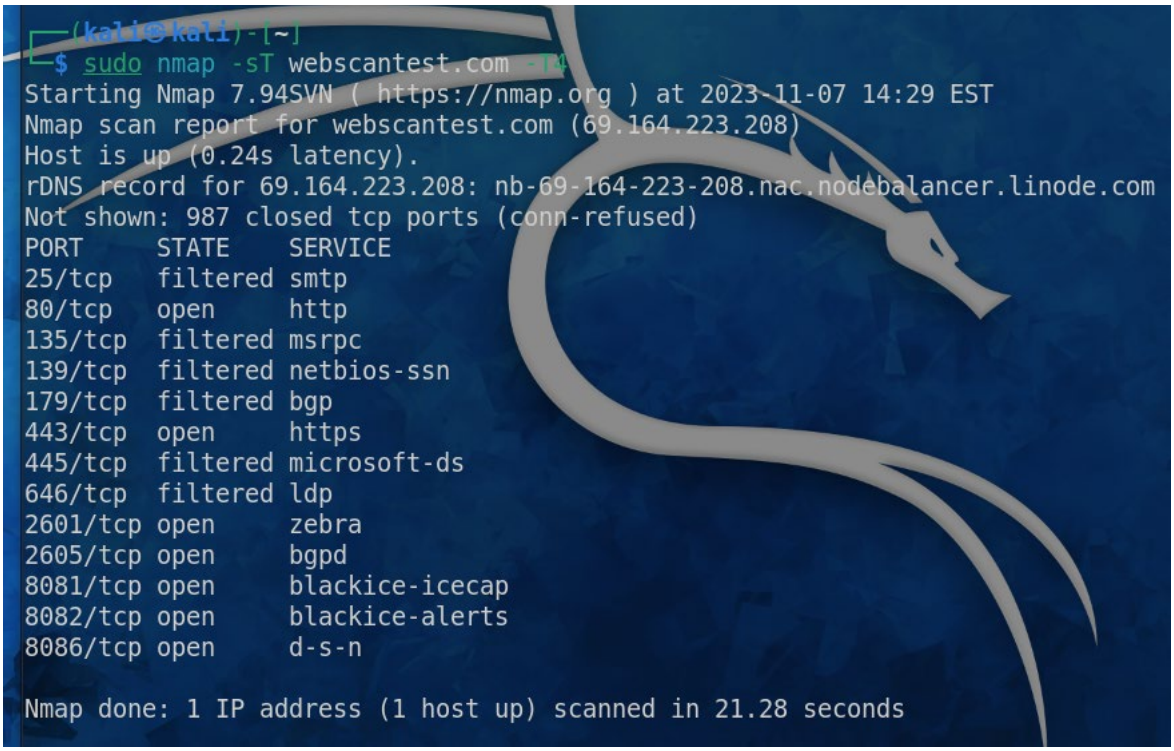

kali@kali: ~
kali@kali: ~
kali@kali: ~
┌──(kali㉿kali)-[~]
└─$ nmap -sV webscantest.com
Starting Nmap 7.94SVN (https://nmap.org) at 2023-11-07 13:40 EST
Nmap scan report for webscantest.com (69.164.223.208)
Host is up (0.25s latency).
rDNS record for 69.164.223.208: nb-69-164-223-208.nac.nodebalancer.linode.com
Not shown: 987 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
25/tcp filtered smtp
80/tcp open http Apache httpd 2.4.7
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
179/tcp filtered bgp
443/tcp open ssl/http Apache httpd 2.4.7
445/tcp filtered microsoft-ds
646/tcp filtered ldp
2601/tcp open zebra Quagga routing software
2605/tcp open zebra Quagga routing software
8081/tcp open blackice-icecap?
8082/tcp open blackice-alerts?
8086/tcp open d-s-n?
3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at
https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port8081-TCP:V=7.94SVN%I=7%D=11/7%Time=654A8513%P=x86_64-pc-linux-gnu%r
SF:(GetRequest,E9,"HTTP/1\.1\x20503\x20Service\x20Unavailable\r\ncontent-l
SF:ength:\x20107\r\ncache-control:\x20no-cache\r\ncontent-type:\x20text/ht


kali@kali: ~
kali@kali: ~
kali@kali: ~
kali@kali: ~
kali@kali: ~
┌──(kali㉿kali)-[~]
└─$ nmap -sV test.rebex.net
Starting Nmap 7.94SVN (https://nmap.org) at 2023-11-07 13:46 EST
Nmap scan report for test.rebex.net (194.108.117.16)
Host is up (0.23s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
13/tcp open tcpwrapped
21/tcp open ftp
22/tcp open ssh (protocol 2.0)
80/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
143/tcp open tcpwrapped
443/tcp open ssl/https
990/tcp open ftps?
993/tcp open tcpwrapped
2 services unrecognized despite returning data. If you know the service/version, please s
https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port21-TCP:V=7.94SVN%I=7%D=11/7%Time=654A863F%P=x86_64-pc-linux-gnu%r(N
SF:ULL,1D,"220\x20Rebex\x20FTP\x20Server\x20ready\.\r\n")%r(GenericLines,5


kali@kali: ~
kali@kali: ~
kali@kali: ~
kali@kali: ~
kali@kali: ~
(kali㉿kali)-[~]
$ nmap -sV speedtest.tele2.net
Starting Nmap 7.94SVN (https://nmap.org) at 2023-11-07 13:46 EST
Nmap scan report for speedtest.tele2.net (90.130.70.73)
Host is up (0.23s latency).
Other addresses for speedtest.tele2.net (not scanned): 2a00:800:1010::1
rDNS record for 90.130.70.73: d90-130-70-73.cust.tele2.se
Not shown: 969 filtered tcp ports (no-response), 8 filtered tcp ports (host-unreach)
PORT STATE SERVICE VERSION
20/tcp closed ftp-data
21/tcp open ftp vsftpd 2.0.8 or later
80/tcp open http nginx
443/tcp closed https
5001/tcp closed commplex-link
5060/tcp open ssl/sip?
8080/tcp open ssl/http-proxy
21571/tcp closed unknown
22939/tcp closed unknown
23502/tcp closed unknown
24444/tcp closed unknown
24800/tcp closed unknown
25734/tcp closed unknown
25735/tcp closed unknown
26214/tcp closed unknown
27000/tcp closed flexlm0
27352/tcp closed unknown
27353/tcp closed unknown
27355/tcp closed unknown
27356/tcp closed unknown
27715/tcp closed unknown
28201/tcp closed unknown
30000/tcp closed ndmps
2 services unrecognized despite returning data. If you know the service/version, please submit
https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

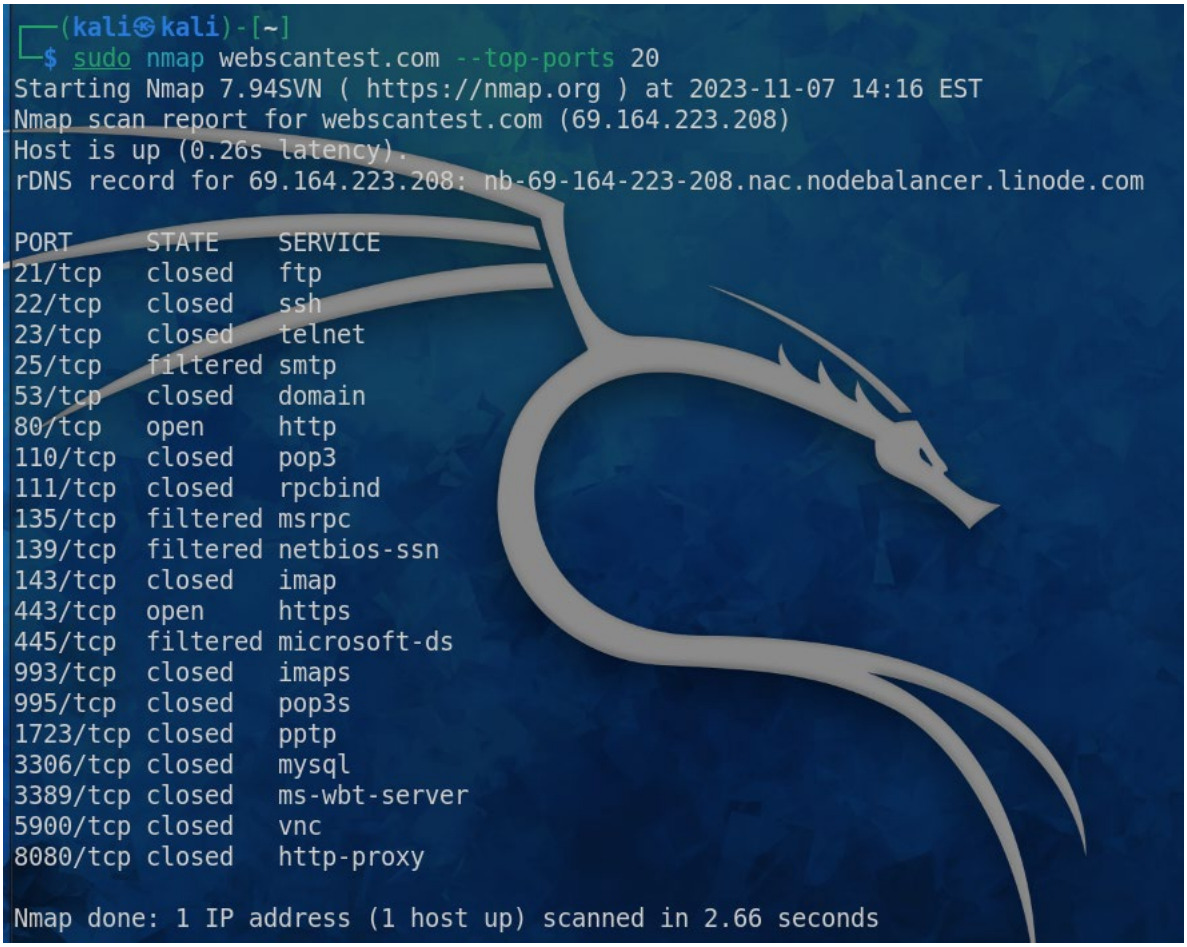
Traceroute port 80 using nmap

To run the scans faster if you have faster internet use -T4 and for normal scan you can use -T3 or it's the default way.

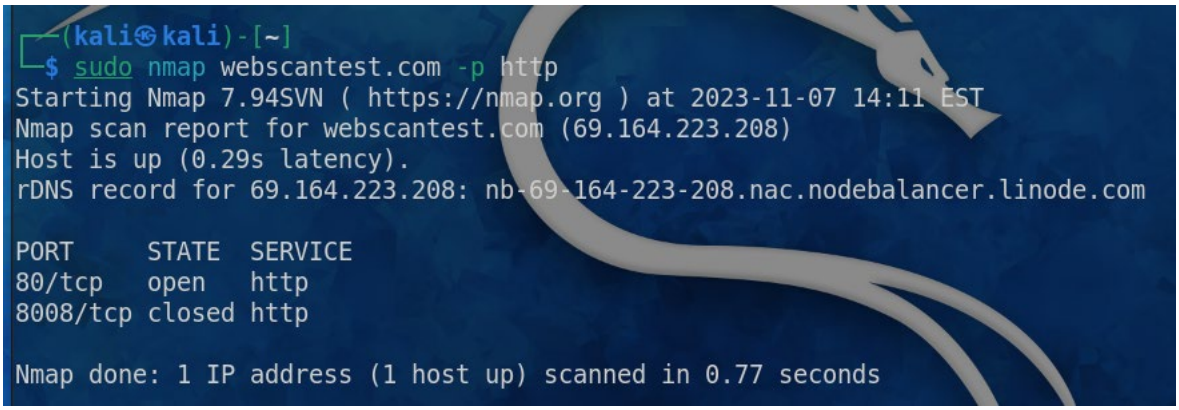


To show the top ports from ranges 20.

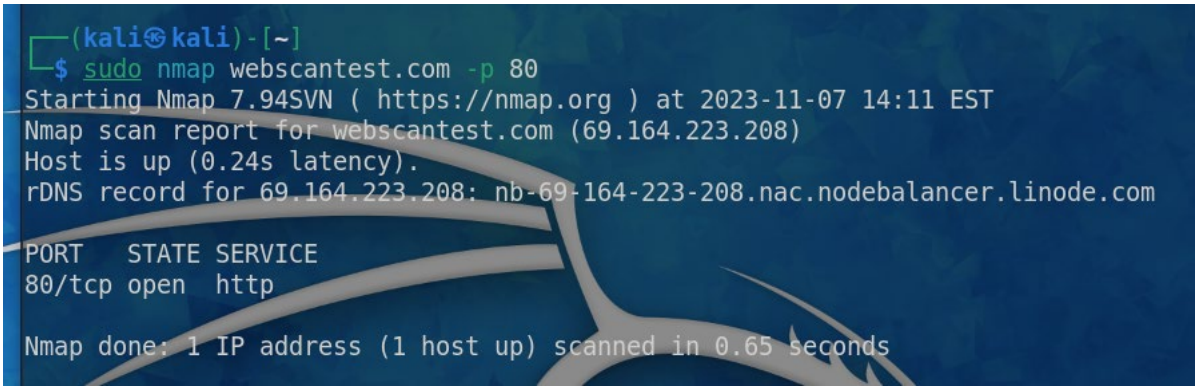
And to show all the 65535 ports use -p-



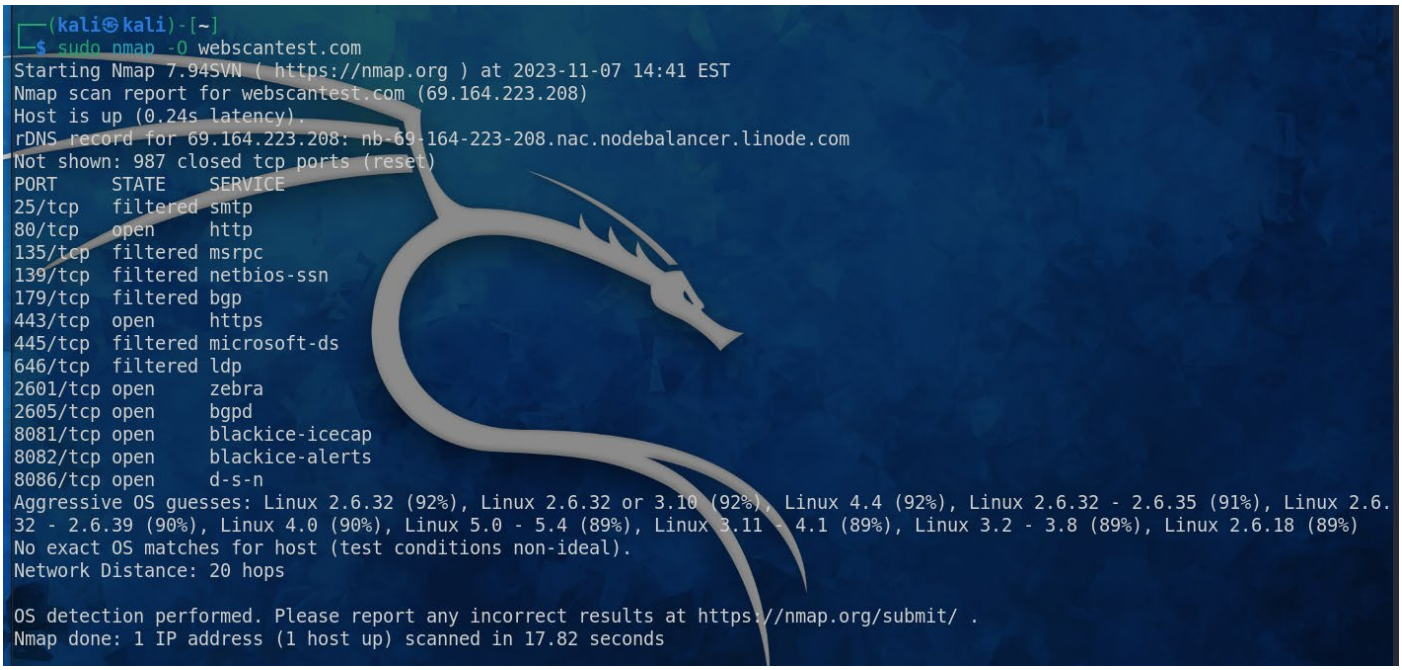
Specific Protocol Type filtered SCAN



Specific Port Type filtered SCAN

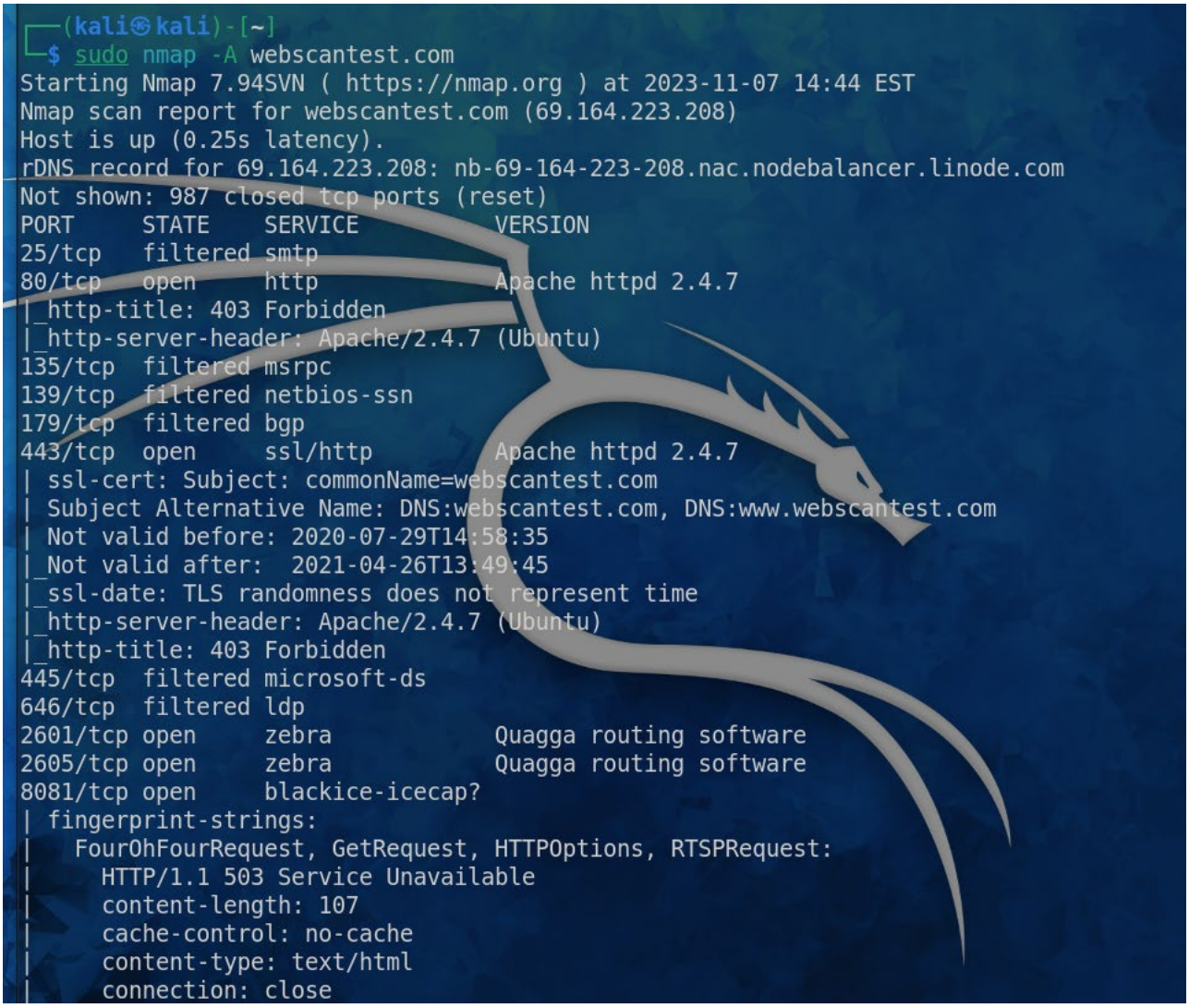


For OS Detection on particular domain, we use -O



WARNING

This command is basically the mixture of all the commands and functionality of the nmap that is the -A which tells you about the Service Version + OS Detection + Scanning Ports + TraceRoute

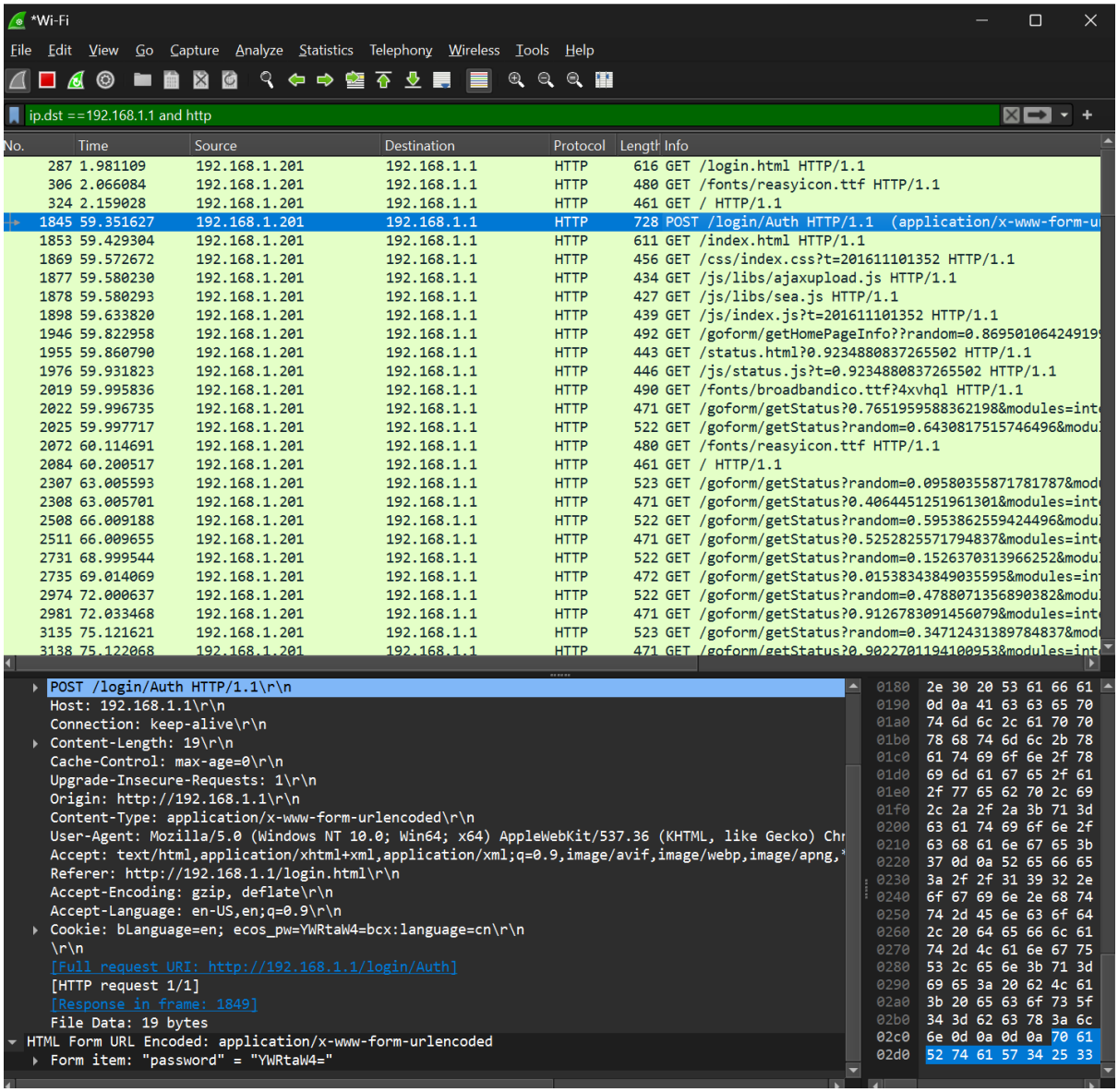


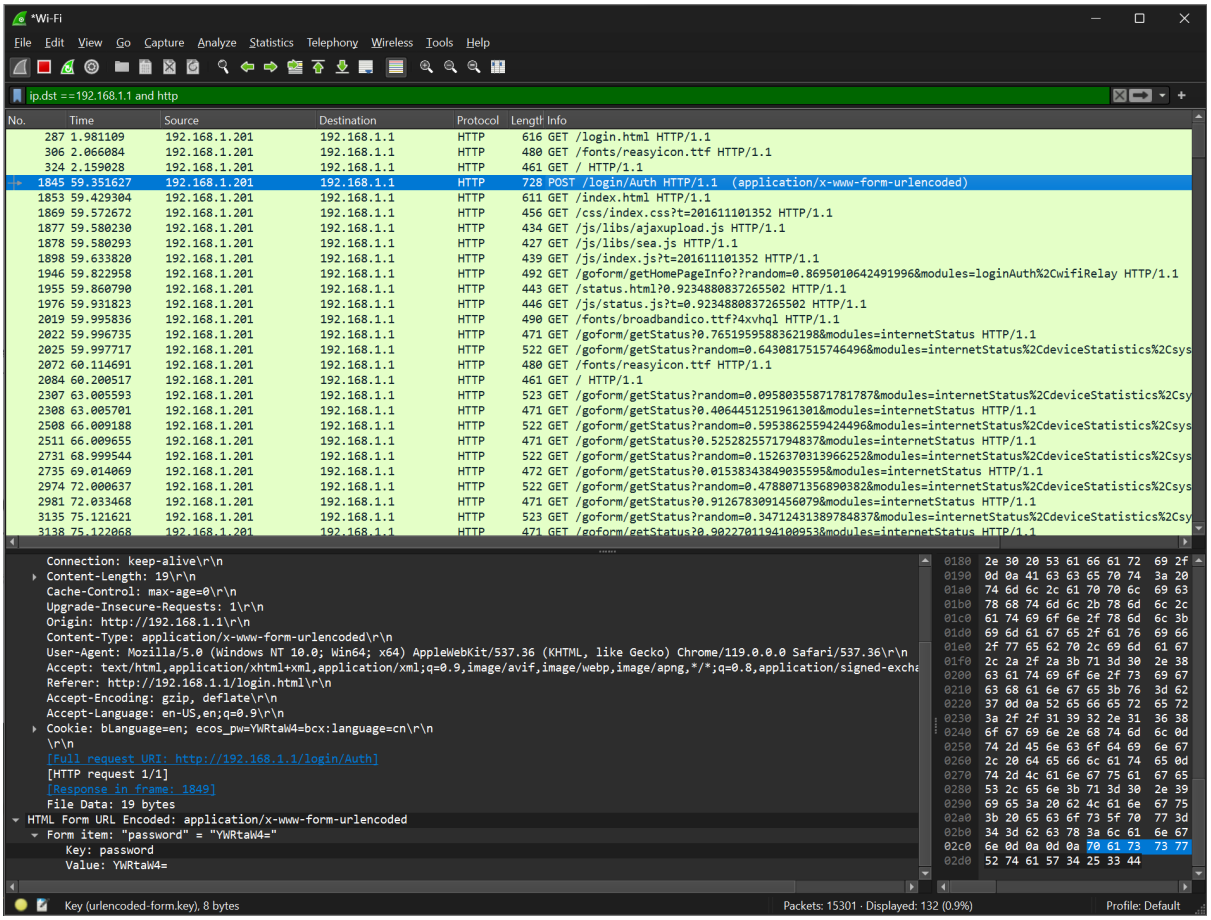
This command shows you the live data, just like verbosity that is -v

LAB EXPERIMENT – 9

Network Traffic Sniffing – Wireshark

Own Router Traffic Analysis

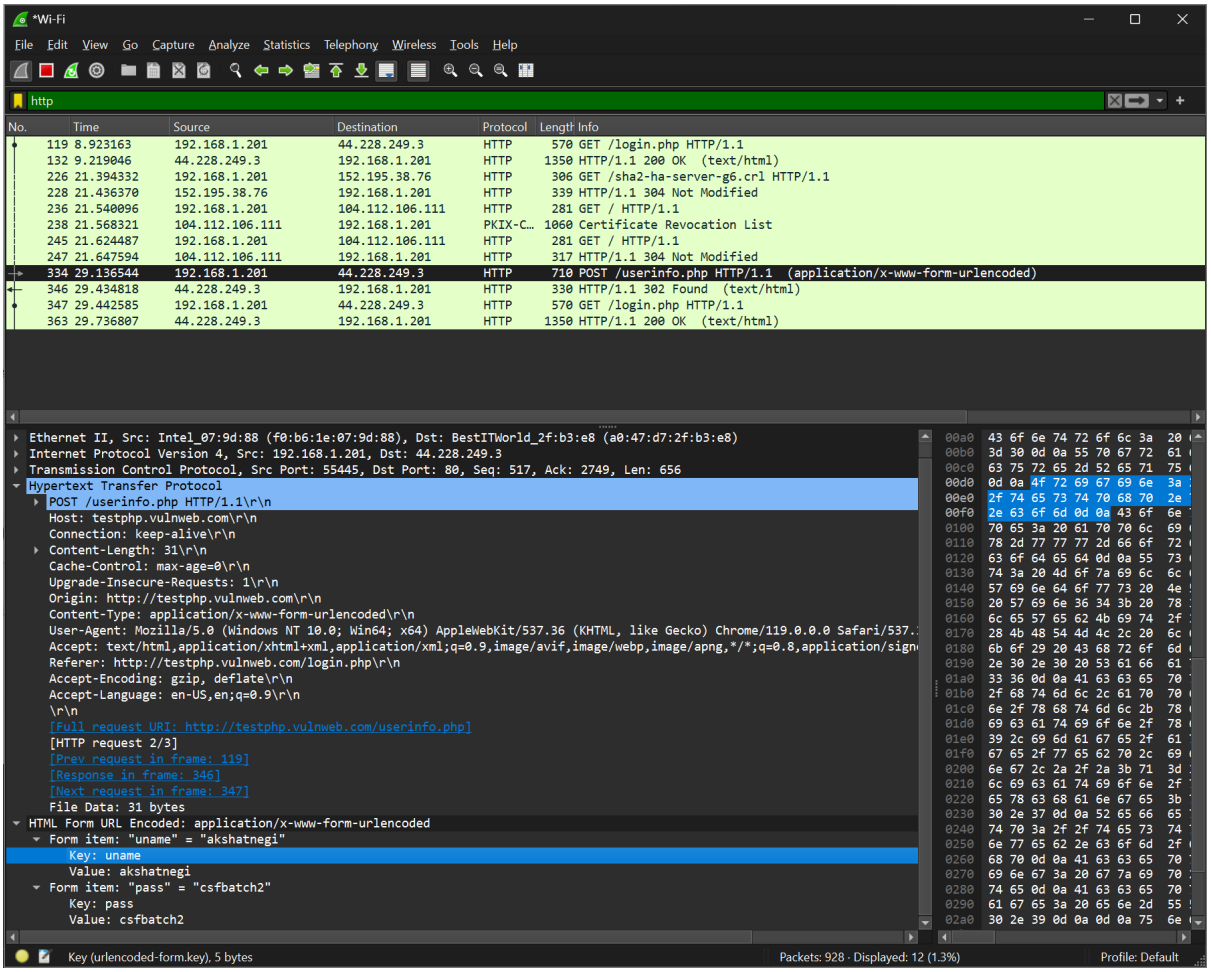


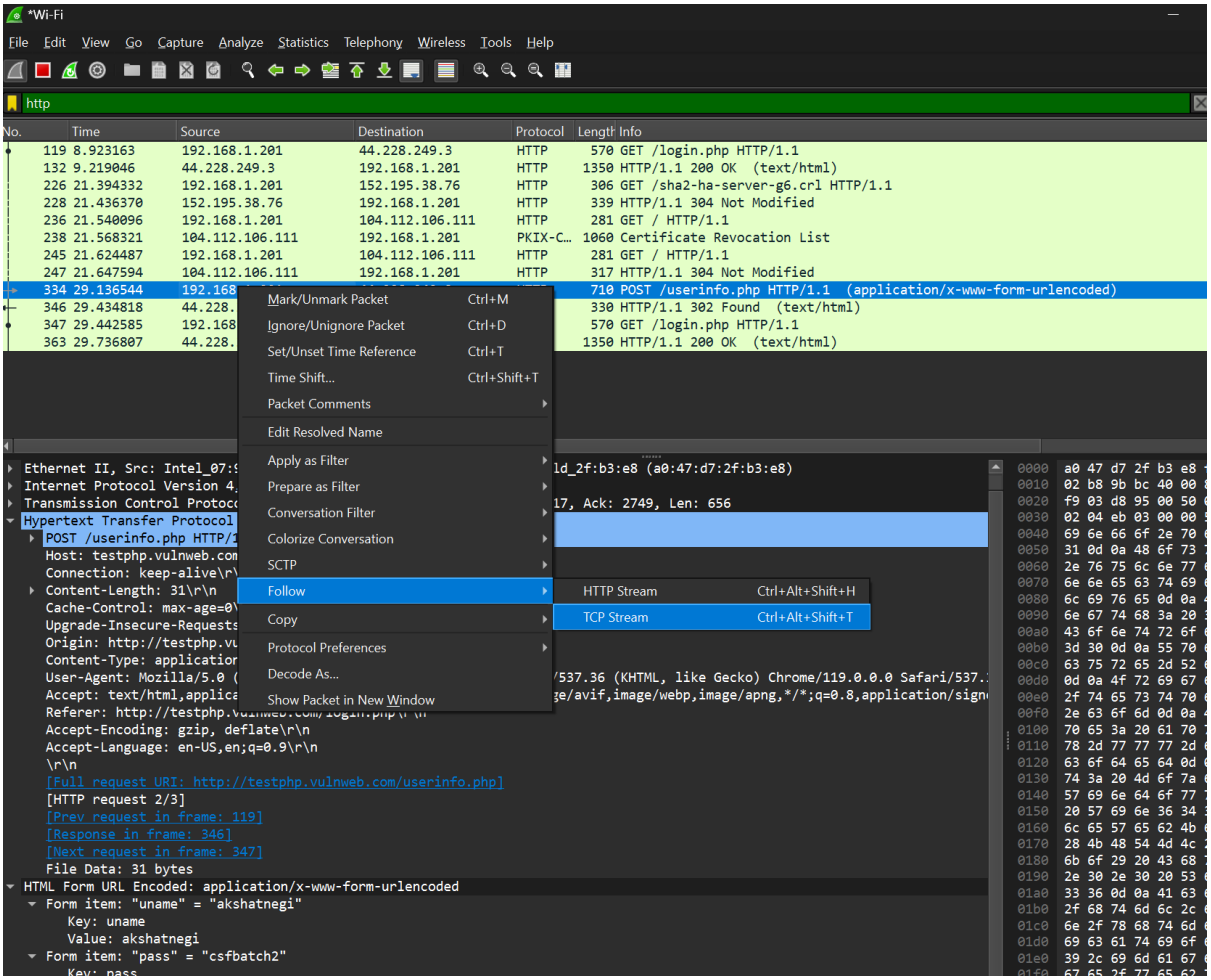

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.dst ==192.168.1.1 and http
No. Time Source Destination Protocol Length Info
287 1.981109 192.168.1.201 192.168.1.1 HTTP 616 GET /login.html HTTP/1.1
306 2.066084 192.168.1.201 192.168.1.1 HTTP 480 GET /fonts/reasyicon.ttf HTTP/1.1
324 2.159028 192.168.1.201 192.168.1.1 HTTP 461 GET / HTTP/1.1
1845 59.351627 192.168.1.201 192.168.1.1 HTTP 728 POST /login/Auth HTTP/1.1 (application/x-www-form-urlencoded)
1853 59.429304 192.168.1.201 192.168.1.1 HTTP 611 GET /index.html HTTP/1.1
1869 59.572672 192.168.1.201 192.168.1.1 HTTP 456 GET /css/index.css?t=201611101352 HTTP/1.1
1877 59.580230 192.168.1.201 192.168.1.1 HTTP 434 GET /js/libs/ajaxupload.js HTTP/1.1
1878 59.580293 192.168.1.201 192.168.1.1 HTTP 427 GET /js/libs/sea.js HTTP/1.1
1898 59.633820 192.168.1.201 192.168.1.1 HTTP 439 GET /js/index.js?t=201611101352 HTTP/1.1
1946 59.822958 192.168.1.201 192.168.1.1 HTTP 492 GET /goform/getHomePageInfo??random=0.8695010642491996&modules=loginAuth%2CwifiRelay HTTP/1.1
1955 59.860790 192.168.1.201 192.168.1.1 HTTP 443 GET /status.html?0.9234880837265502 HTTP/1.1
1976 59.931823 192.168.1.201 192.168.1.1 HTTP 446 GET /js/status.js?t=0.9234880837265502 HTTP/1.1
2019 59.995836 192.168.1.201 192.168.1.1 HTTP 490 GET /fonts/broadbandico.ttf?4xvhql HTTP/1.1
2022 59.996735 192.168.1.201 192.168.1.1 HTTP 471 GET /goform/getStatus?0.7651959588362198&modules=internetStatus HTTP/1.1
2025 59.997717 192.168.1.201 192.168.1.1 HTTP 522 GET /goform/getStatus?random=0.6430817515746496&modules=internetStatus%2CdeviceStatistics%2Csys
2072 60.114691 192.168.1.201 192.168.1.1 HTTP 480 GET /fonts/reasyicon.ttf HTTP/1.1
2084 60.200517 192.168.1.201 192.168.1.1 HTTP 461 GET / HTTP/1.1
2307 63.005593 192.168.1.201 192.168.1.1 HTTP 523 GET /goform/getStatus?random=0.09580355871781787&modules=internetStatus%2CdeviceStatistics%2Csy
2308 63.005701 192.168.1.201 192.168.1.1 HTTP 471 GET /goform/getStatus?0.40644512519613O1&modules=internetStatus HTTP/1.1
2508 66.009188 192.168.1.201 192.168.1.1 HTTP 522 GET /goform/getStatus?random=0.5953862559424496&modules=internetStatus%2CdeviceStatistics%2Csys
2511 66.009655 192.168.1.201 192.168.1.1 HTTP 471 GET /goform/getStatus?0.5252825571794837&modules=internetStatus HTTP/1.1
2731 68.999544 192.168.1.201 192.168.1.1 HTTP 522 GET /goform/getStatus?random=0.1526370313966252&modules=internetStatus%2CdeviceStatistics%2Csys
2735 69.014069 192.168.1.201 192.168.1.1 HTTP 472 GET /goform/getStatus?0.01538343849035595&modules=internetStatus HTTP/1.1
2974 72.000637 192.168.1.201 192.168.1.1 HTTP 522 GET /goform/getStatus?random=0.4788071356890382&modules=internetStatus%2CdeviceStatistics%2Csys
2981 72.033468 192.168.1.201 192.168.1.1 HTTP 471 GET /goform/getStatus?0.9126783091456079&modules=internetStatus HTTP/1.1
3135 75.121621 192.168.1.201 192.168.1.1 HTTP 523 GET /goform/getStatus?random=0.34712431389784837&modules=internetStatus%2CdeviceStatistics%2Csy
3138 75.122068 192.168.1.201 192.168.1.1 HTTP 471 GET /goform/getStatus?0.9022701194100953&modules=internetStatus HTTP/1.1
Connection: keep-alive\r\n
Content-Length: 19\r\n
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
Origin: http://192.168.1.1\r\n
Content-Type: application/x-www-form-urlencoded\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-excha
Referer: http://192.168.1.1/login.html\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
Cookie: bLanguage=en; ecos_pw=YWRtaW4=bcx:language=cn\r\n
\r\n
[Full request URI: http://192.168.1.1/login/Auth]
[HTTP request 1/1]
[Response in frame: 1849]
File Data: 19 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "password" = "YWRtaW4="
Key: password
Value: YWRtaW4=
0180 2e 30 20 53 61 66 61 72 69 2f
0190 0d 0a 41 63 63 65 70 74 3a 20
01a0 74 6d 6c 2c 61 70 70 6c 69 63
01b0 78 68 74 6d 6c 2b 78 6d 6c 2c
01c0 61 74 69 6f 6e 2f 78 6d 6c 3b
01d0 69 6d 61 67 65 2f 61 76 69 66
01e0 2f 77 65 62 70 2c 69 6d 61 67
01f0 2c 2a 2f 2a 3b 71 3d 30 2e 38
0200 63 61 74 69 6f 6e 2f 73 69 67
0210 63 68 61 6e 67 65 3b 76 3d 62
0220 37 0d 0a 52 65 66 65 72 65 72
0230 3a 2f 2f 31 39 32 2e 31 36 38
0240 6f 67 69 6e 2e 68 74 6d 6c 0d
0250 74 2d 45 6e 63 6f 64 69 6e 67
0260 2c 20 64 65 66 6c 61 74 65 0d
0270 74 2d 4c 61 6e 67 75 61 67 65
0280 53 2c 65 6e 3b 71 3d 30 2e 39
0290 69 65 3a 20 62 4c 61 6e 67 75
02a0 3b 20 65 63 6f 73 5f 70 77 3d
02b0 34 3d 62 63 78 3a 6c 61 6e 67
02c0 6e 0d 0a 0d 0a 70 61 73 73 77
02d0 52 74 61 57 34 25 33 44
Key (urlencoded-form.key), 8 bytes
Packets: 15301 · Displayed: 132 (0.9%)
Profile: Default

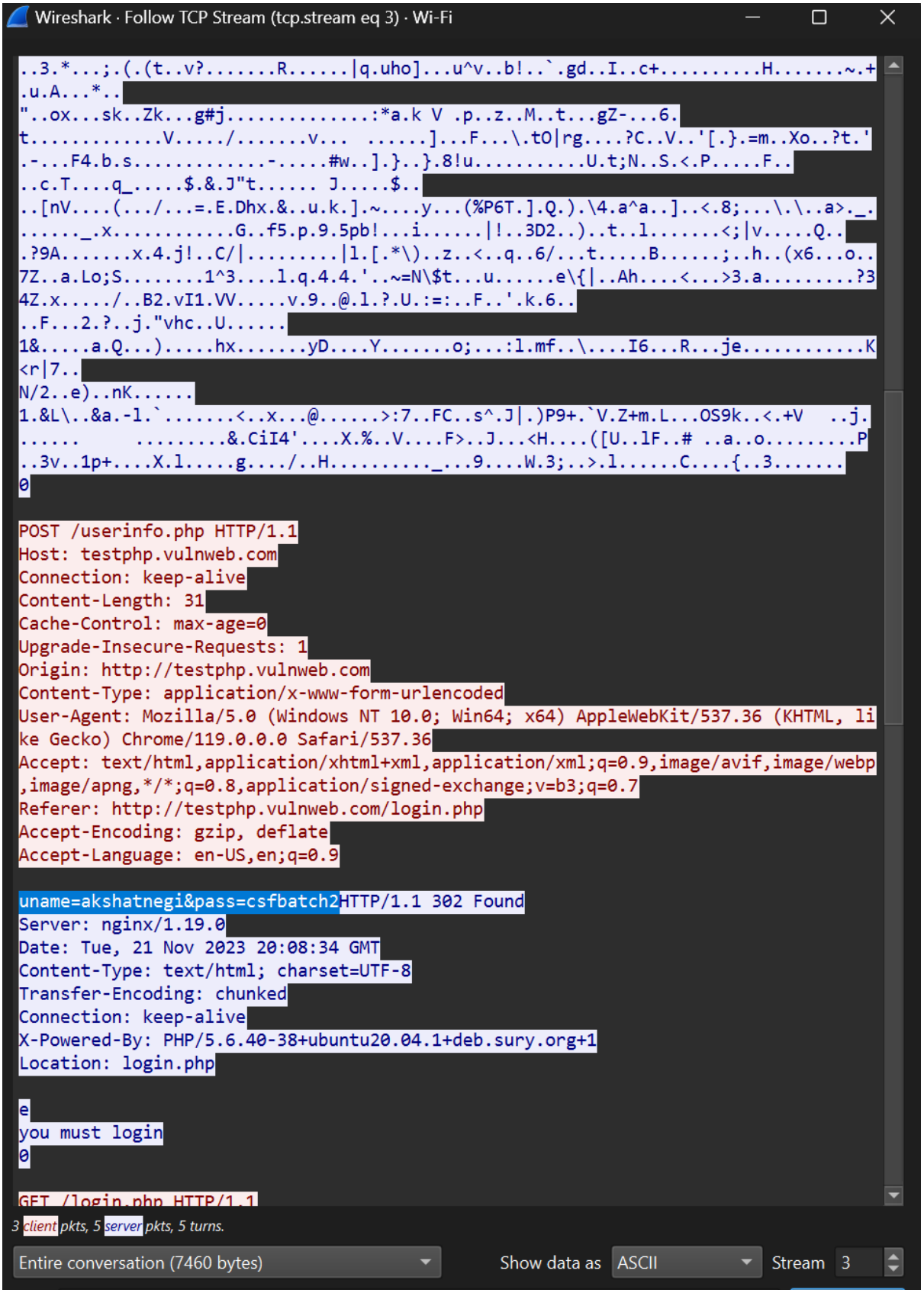
Information Gathering from the following website:

http://testphp.vulnweb.com/login.php

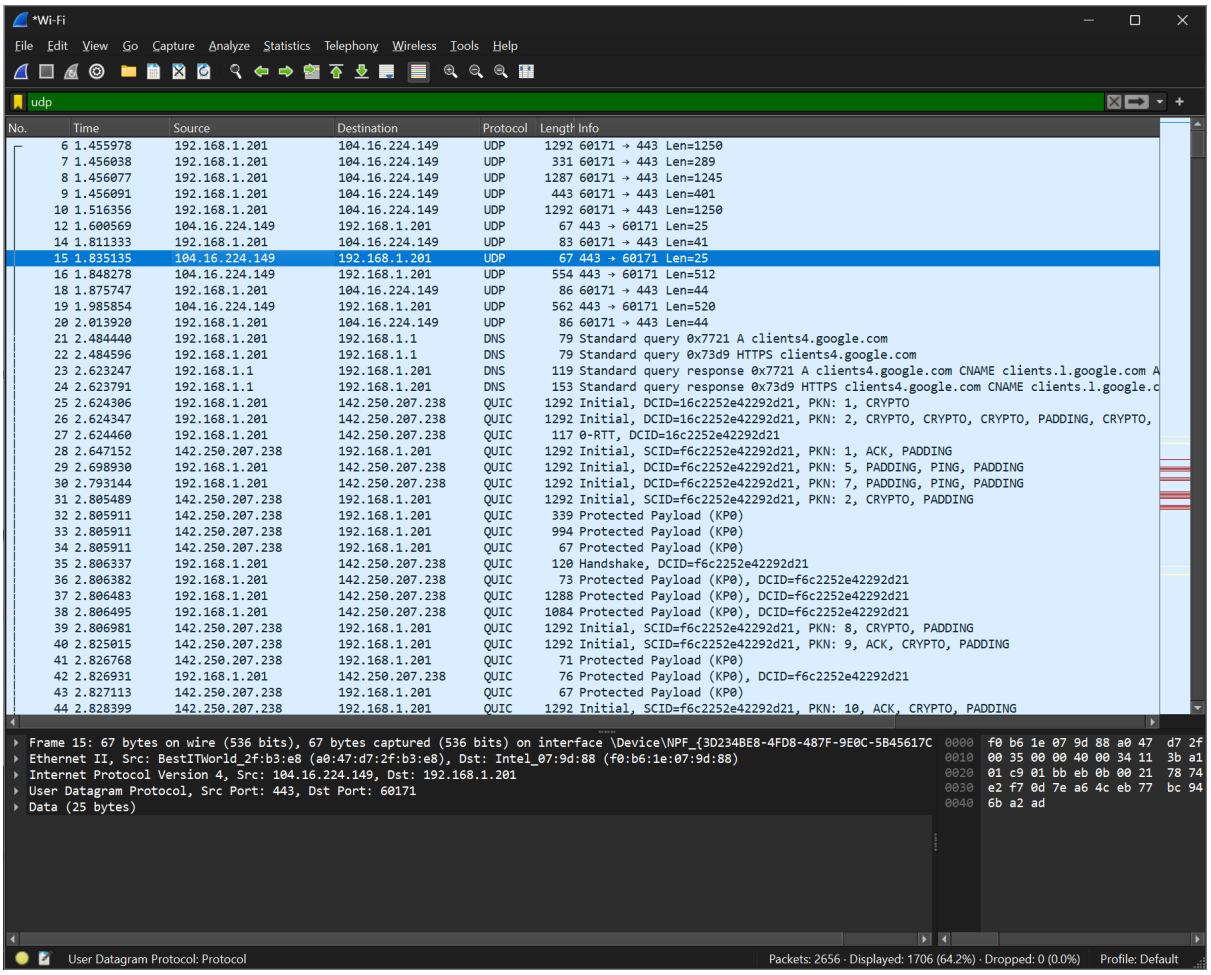
Gathered the username and password using the HyperTEXT Transfer Protocol



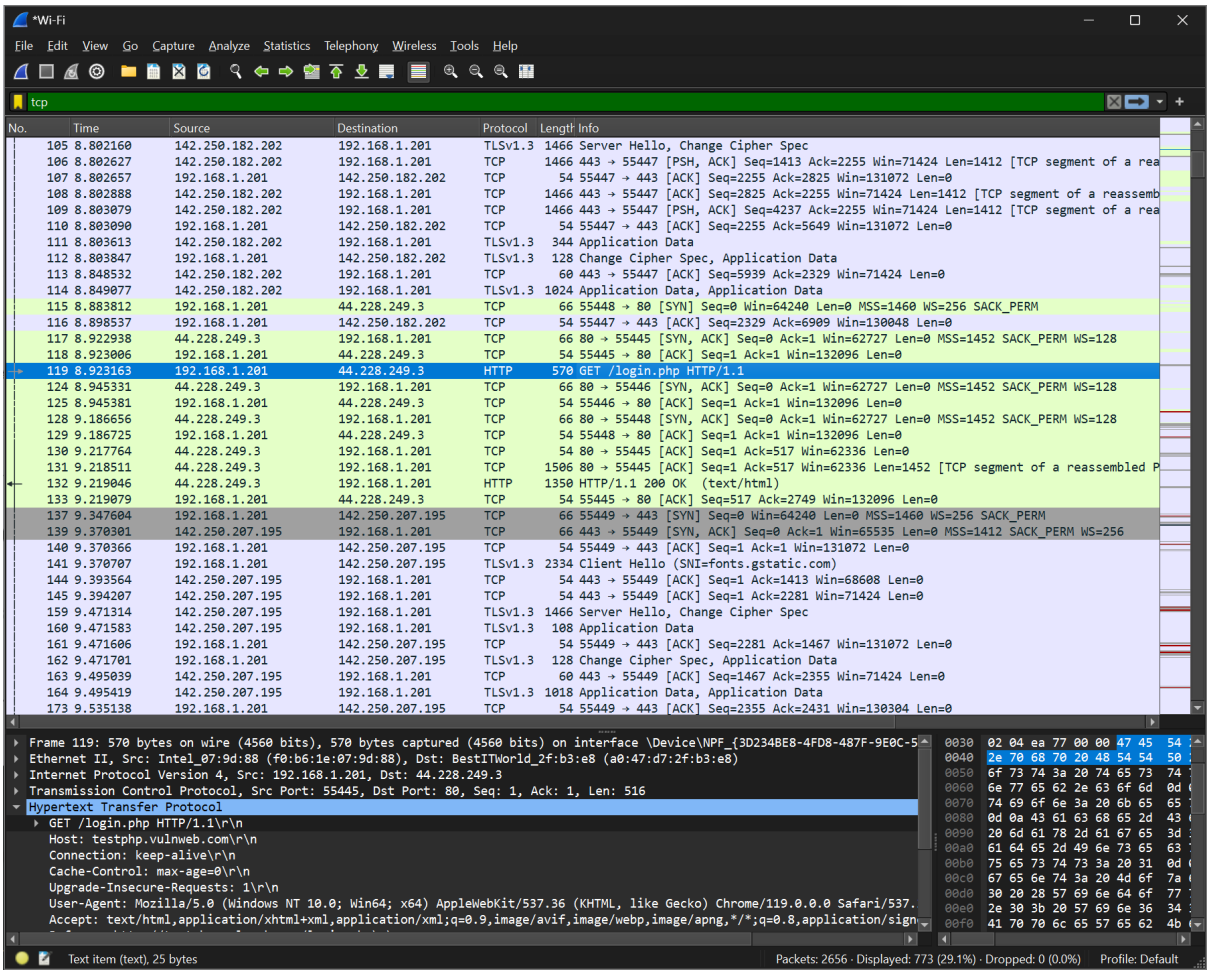

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
119 8.923163 192.168.1.201 44.228.249.3 HTTP 570 GET /login.php HTTP/1.1
132 9.219046 44.228.249.3 192.168.1.201 HTTP 1350 HTTP/1.1 200 OK (text/html)
226 21.394332 192.168.1.201 152.195.38.76 HTTP 306 GET /sha2-ha-server-g6.crl HTTP/1.1
228 21.436370 152.195.38.76 192.168.1.201 HTTP 339 HTTP/1.1 304 Not Modified
236 21.540096 192.168.1.201 104.112.106.111 HTTP 281 GET / HTTP/1.1
238 21.568321 104.112.106.111 192.168.1.201 PKIX-C... 1060 Certificate Revocation List
245 21.624487 192.168.1.201 104.112.106.111 HTTP 281 GET / HTTP/1.1
247 21.647594 104.112.106.111 192.168.1.201 HTTP 317 HTTP/1.1 304 Not Modified
334 29.136544 192.168 710 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
346 29.434818 44.228. 330 HTTP/1.1 302 Found (text/html)
347 29.442585 192.168 570 GET /login.php HTTP/1.1
363 29.736807 44.228. 1350 HTTP/1.1 200 OK (text/html)
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comments
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
HTTP Stream Ctrl+Alt+Shift+H
TCP Stream Ctrl+Alt+Shift+T
Ethernet II, Src: Intel_07:
Internet Protocol Version 4,
Transmission Control Protoc
Hypertext Transfer Protocol
POST /userinfo.php HTTP/1
Host: testphp.vulnweb.com
Connection: keep-alive\r\
Content-Length: 31\r\n
Cache-Control: max-age=0\
Upgrade-Insecure-Requests
Origin: http://testphp.vu
Content-Type: applicatior
User-Agent: Mozilla/5.0 (
Accept: text/html,applica
Referer: http://testphp.vulnweb.com/login.php\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
\r\n
[Full request URI: http://testphp.vulnweb.com/userinfo.php]
[HTTP request 2/3]
[Prev request in frame: 119]
[Response in frame: 346]
[Next request in frame: 347]
File Data: 31 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "uname" = "akshatnegi"
Key: uname
Value: akshatnegi
Form item: "pass" = "csfbatch2"
ld_2f:b3:e8 (a0:47:d7:2f:b3:e8)
17, Ack: 2749, Len: 656
/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.
ge/avif,image/webp,image/apng,*/*;q=0.8,application/sign
0000 a0 47 d7 2f b3 e8
0010 02 b8 9b bc 40 00
0020 f9 03 d8 95 00 50
0030 02 04 eb 03 00 00
0040 69 6e 66 6f 2e 70
0050 31 0d 0a 48 6f 73
0060 2e 76 75 6c 6e 77
0070 6e 6e 65 63 74 69
0080 6c 69 76 65 0d 0a
0090 6e 67 74 68 3a 20
00a0 43 6f 6e 74 72 6f
00b0 3d 30 0d 0a 55 70
00c0 63 75 72 65 2d 52
00d0 0d 0a 4f 72 69 67
00e0 2f 74 65 73 74 70
00f0 2e 63 6f 6d 0d 0a
0100 70 65 3a 20 61 70
0110 78 2d 77 77 77 2d
0120 63 6f 64 65 64 0d
0130 74 3a 20 4d 6f 7a
0140 57 69 6e 64 6f 77
0150 20 57 69 6e 36 34
0160 6c 65 57 65 62 4b
0170 28 4b 48 54 4d 4c
0180 6b 6f 29 20 43 68
0190 2e 30 2e 30 20 53
01a0 33 36 0d 0a 41 63
01b0 2f 68 74 6d 6c 2c
01c0 6e 2f 78 68 74 6d
01d0 69 63 61 74 69 6f
01e0 39 2c 69 6d 61 67


Wireshark · Follow TCP Stream (tcp.stream eq 3) · Wi-Fi
..3.*...;.(.(t..v?.......R.......|q.uho]...u^v..b!..`.gd..I..c+..........H.......~.+
.u.A...*..
"..ox...sk..Zk...g#j..............:*a.k V .p..z..M..t...gZ-...6.
t.............V...../.......v... ......]...F...\.tO|rg....?C..V..'[.}.=m..Xo..?t.'
.-...F4.b.s.............-.....#w..].}..}.8!u...........U.t;N..S.<.P.....F..
..c.T....q_.....$.&.J"t..... J.....$..
..[nV....(.../...=.E.Dhx.&..u.k.].~....y...(%P6T.].Q.).\4.a^a..]..<.8;...\.\..a>._.
......_.x............G..f5.p.9.5pb!...i......|!..3D2..)..t..l.......<;|v.....Q..
.?9A.......x.4.j!..C/|.........|1.[.*\)..z..<..q..6/...t.....B......;..h..(x6...o..
7Z..a.Lo;S........1^3....l.q.4.4.'..~=N\$t...u......e\{|..Ah....<...>3.a.........?3
4Z.x...../..B2.vI1.VV.....v.9..@.l.?.U.:=:..F..'.k.6..
..F...2.?..j."vhc..U.....
1&.....a.Q...).....hx.......yD....Y.......o;...:l.mf..\....I6...R...je...........K
<r|7..
N/2..e)..nK......
1.&L\..&a.-l.`.......<..x...@......>:7..FC..s^.J|.)P9+.`V.Z+m.L...OS9k..<.+V ..j.
....&.CiI4'....X.%..V....F>..J...<H....([U..lF..# ..a..o.........P
..3v..1p+....X.l.....g..../..H..........._...9....W.3;..>.l......C....{..3.......
0
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Connection: keep-alive
Content-Length: 31
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://testphp.vulnweb.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li
ke Gecko) Chrome/119.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
uname=akshatnegi&pass=csfbatch2HTTP/1.1 302 Found
Server: nginx/1.19.0
Date: Tue, 21 Nov 2023 20:08:34 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Location: login.php
e
you must login
0
GET /login.php HTTP/1.1
3 client pkts, 5 server pkts, 5 turns.
Entire conversation (7460 bytes)
Show data as
ASCII
Stream
3

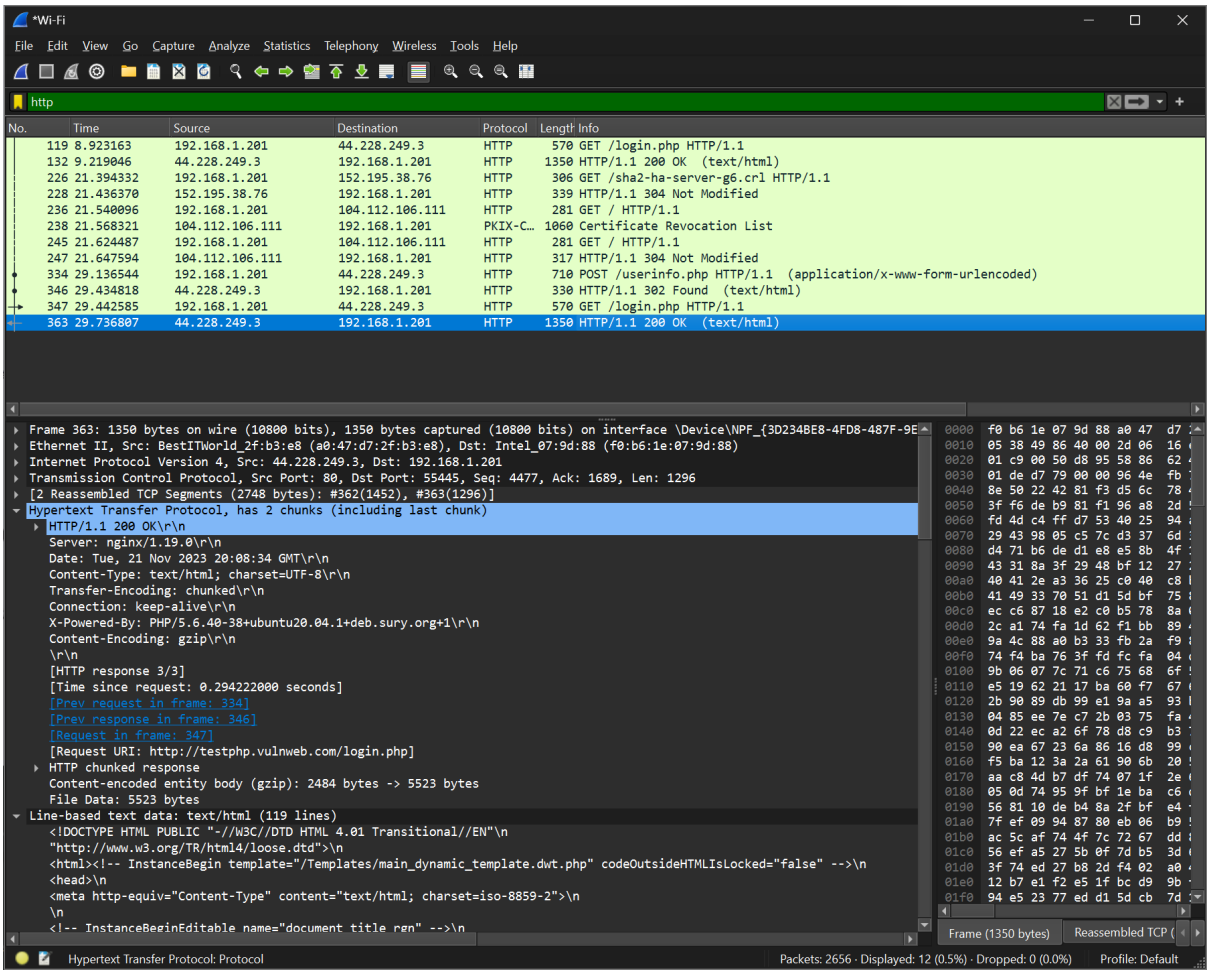
UDP Filter


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp
No. Time Source Destination Protocol Length Info
6 1.455978 192.168.1.201 104.16.224.149 UDP 1292 60171 → 443 Len=1250
7 1.456038 192.168.1.201 104.16.224.149 UDP 331 60171 → 443 Len=289
8 1.456077 192.168.1.201 104.16.224.149 UDP 1287 60171 → 443 Len=1245
9 1.456091 192.168.1.201 104.16.224.149 UDP 443 60171 → 443 Len=401
10 1.516356 192.168.1.201 104.16.224.149 UDP 1292 60171 → 443 Len=1250
12 1.600569 104.16.224.149 192.168.1.201 UDP 67 443 → 60171 Len=25
14 1.811333 192.168.1.201 104.16.224.149 UDP 83 60171 → 443 Len=41
15 1.835135 104.16.224.149 192.168.1.201 UDP 67 443 → 60171 Len=25
16 1.848278 104.16.224.149 192.168.1.201 UDP 554 443 → 60171 Len=512
18 1.875747 192.168.1.201 104.16.224.149 UDP 86 60171 → 443 Len=44
19 1.985854 104.16.224.149 192.168.1.201 UDP 562 443 → 60171 Len=520
20 2.013920 192.168.1.201 104.16.224.149 UDP 86 60171 → 443 Len=44
21 2.484440 192.168.1.201 192.168.1.1 DNS 79 Standard query 0x7721 A clients4.google.com
22 2.484596 192.168.1.201 192.168.1.1 DNS 79 Standard query 0x73d9 HTTPS clients4.google.com
23 2.623247 192.168.1.1 192.168.1.201 DNS 119 Standard query response 0x7721 A clients4.google.com CNAME clients.l.google.com A
24 2.623791 192.168.1.1 192.168.1.201 DNS 153 Standard query response 0x73d9 HTTPS clients4.google.com CNAME clients.l.google.c
25 2.624306 192.168.1.201 142.250.207.238 QUIC 1292 Initial, DCID=16c2252e42292d21, PKN: 1, CRYPTO
26 2.624347 192.168.1.201 142.250.207.238 QUIC 1292 Initial, DCID=16c2252e42292d21, PKN: 2, CRYPTO, CRYPTO, CRYPTO, PADDING, CRYPTO,
27 2.624460 192.168.1.201 142.250.207.238 QUIC 117 0-RTT, DCID=16c2252e42292d21
28 2.647152 142.250.207.238 192.168.1.201 QUIC 1292 Initial, SCID=f6c2252e42292d21, PKN: 1, ACK, PADDING
29 2.698930 192.168.1.201 142.250.207.238 QUIC 1292 Initial, DCID=f6c2252e42292d21, PKN: 5, PADDING, PING, PADDING
30 2.793144 192.168.1.201 142.250.207.238 QUIC 1292 Initial, DCID=f6c2252e42292d21, PKN: 7, PADDING, PING, PADDING
31 2.805489 142.250.207.238 192.168.1.201 QUIC 1292 Initial, SCID=f6c2252e42292d21, PKN: 2, CRYPTO, PADDING
32 2.805911 142.250.207.238 192.168.1.201 QUIC 339 Protected Payload (KP0)
33 2.805911 142.250.207.238 192.168.1.201 QUIC 994 Protected Payload (KP0)
34 2.805911 142.250.207.238 192.168.1.201 QUIC 67 Protected Payload (KP0)
35 2.806337 192.168.1.201 142.250.207.238 QUIC 120 Handshake, DCID=f6c2252e42292d21
36 2.806382 192.168.1.201 142.250.207.238 QUIC 73 Protected Payload (KP0), DCID=f6c2252e42292d21
37 2.806483 192.168.1.201 142.250.207.238 QUIC 1288 Protected Payload (KP0), DCID=f6c2252e42292d21
38 2.806495 192.168.1.201 142.250.207.238 QUIC 1084 Protected Payload (KP0), DCID=f6c2252e42292d21
39 2.806981 142.250.207.238 192.168.1.201 QUIC 1292 Initial, SCID=f6c2252e42292d21, PKN: 8, CRYPTO, PADDING
40 2.825015 142.250.207.238 192.168.1.201 QUIC 1292 Initial, SCID=f6c2252e42292d21, PKN: 9, ACK, CRYPTO, PADDING
41 2.826768 142.250.207.238 192.168.1.201 QUIC 71 Protected Payload (KP0)
42 2.826931 192.168.1.201 142.250.207.238 QUIC 76 Protected Payload (KP0), DCID=f6c2252e42292d21
43 2.827113 142.250.207.238 192.168.1.201 QUIC 67 Protected Payload (KP0)
44 2.828399 142.250.207.238 192.168.1.201 QUIC 1292 Initial, SCID=f6c2252e42292d21, PKN: 10, ACK, CRYPTO, PADDING
Frame 15: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_{3D234BE8-4FD8-487F-9E0C-5B45617C
Ethernet II, Src: BestITWorld_2f:b3:e8 (a0:47:d7:2f:b3:e8), Dst: Intel_07:9d:88 (f0:b6:1e:07:9d:88)
Internet Protocol Version 4, Src: 104.16.224.149, Dst: 192.168.1.201
User Datagram Protocol, Src Port: 443, Dst Port: 60171
Data (25 bytes)
0000 f0 b6 1e 07 9d 88 a0 47 d7 2f
0010 00 35 00 00 40 00 34 11 3b a1
0020 01 c9 01 bb eb 0b 00 21 78 74
0030 e2 f7 0d 7e a6 4c eb 77 bc 94
0040 6b a2 ad
User Datagram Protocol: Protocol
Packets: 2656 · Displayed: 1706 (64.2%) · Dropped: 0 (0.0%)
Profile: Default

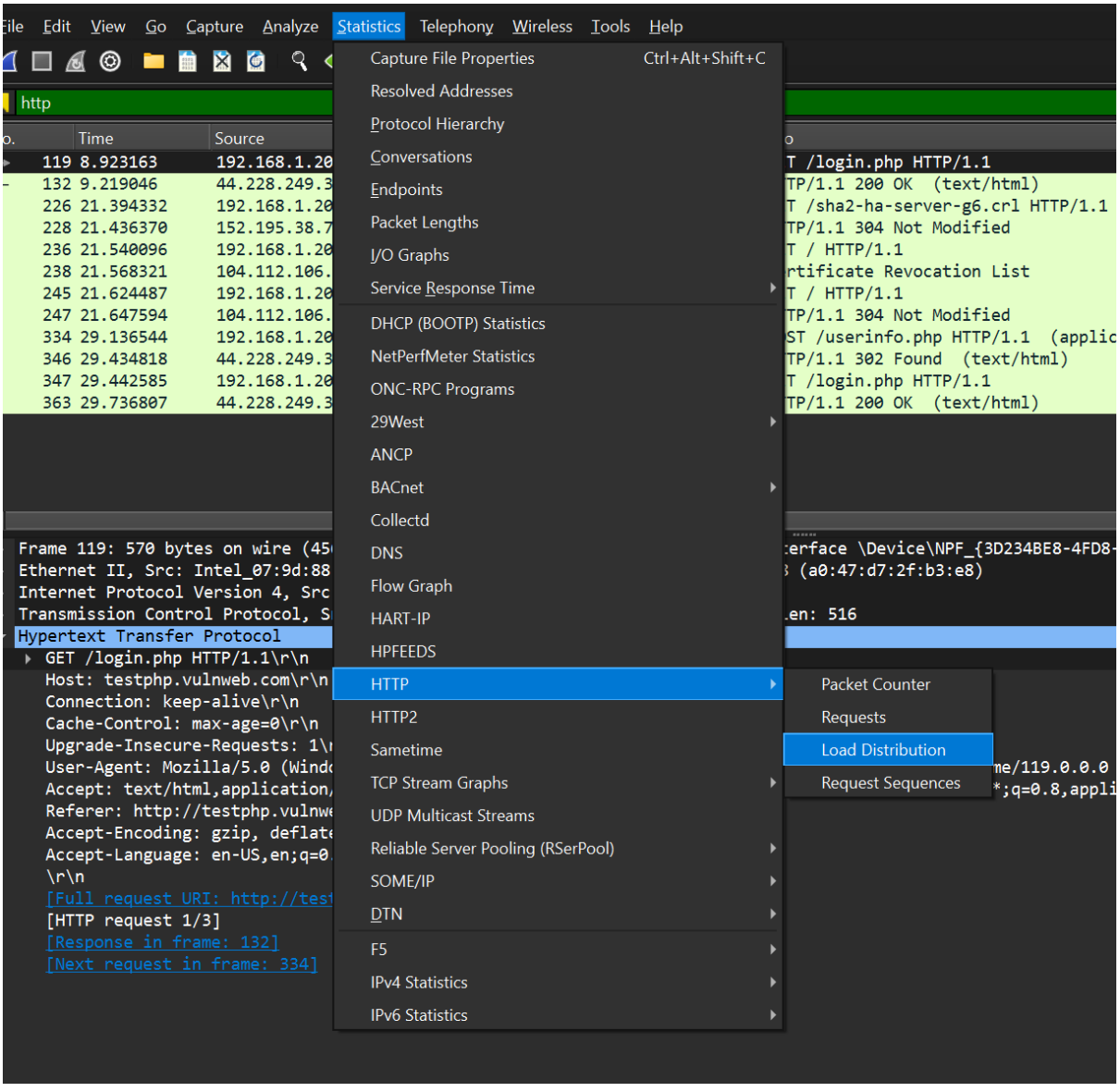
TCP Filter

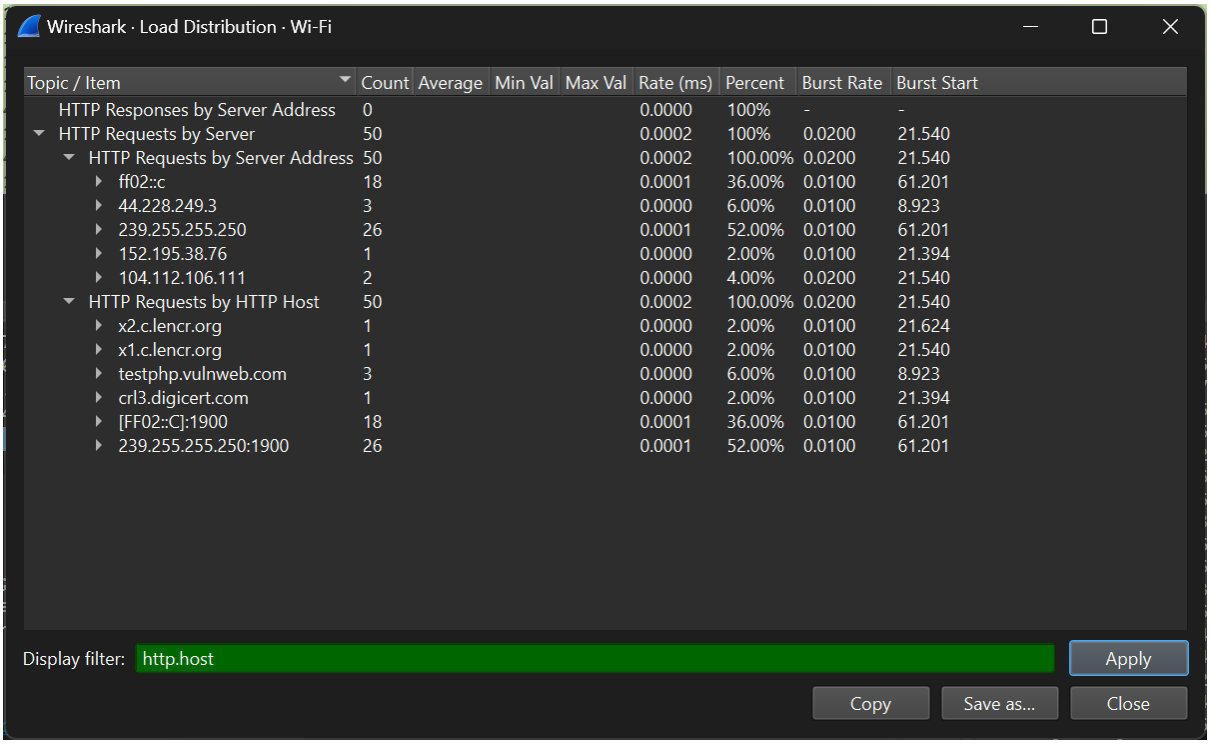

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
No. Time Source Destination Protocol Length Info
105 8.802160 142.250.182.202 192.168.1.201 TLSv1.3 1466 Server Hello, Change Cipher Spec
106 8.802627 142.250.182.202 192.168.1.201 TCP 1466 443 → 55447 [PSH, ACK] Seq=1413 Ack=2255 Win=71424 Len=1412 [TCP segment of a rea
107 8.802657 192.168.1.201 142.250.182.202 TCP 54 55447 → 443 [ACK] Seq=2255 Ack=2825 Win=131072 Len=0
108 8.802888 142.250.182.202 192.168.1.201 TCP 1466 443 → 55447 [ACK] Seq=2825 Ack=2255 Win=71424 Len=1412 [TCP segment of a reassemb
109 8.803079 142.250.182.202 192.168.1.201 TCP 1466 443 → 55447 [PSH, ACK] Seq=4237 Ack=2255 Win=71424 Len=1412 [TCP segment of a rea
110 8.803090 192.168.1.201 142.250.182.202 TCP 54 55447 → 443 [ACK] Seq=2255 Ack=5649 Win=131072 Len=0
111 8.803613 142.250.182.202 192.168.1.201 TLSv1.3 344 Application Data
112 8.803847 192.168.1.201 142.250.182.202 TLSv1.3 128 Change Cipher Spec, Application Data
113 8.848532 142.250.182.202 192.168.1.201 TCP 60 443 → 55447 [ACK] Seq=5939 Ack=2329 Win=71424 Len=0
114 8.849077 142.250.182.202 192.168.1.201 TLSv1.3 1024 Application Data, Application Data
115 8.883812 192.168.1.201 44.228.249.3 TCP 66 55448 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
116 8.898537 192.168.1.201 142.250.182.202 TCP 54 55447 → 443 [ACK] Seq=2329 Ack=6909 Win=130048 Len=0
117 8.922938 44.228.249.3 192.168.1.201 TCP 66 80 → 55445 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=0 MSS=1452 SACK_PERM WS=128
118 8.923006 192.168.1.201 44.228.249.3 TCP 54 55445 → 80 [ACK] Seq=1 Ack=1 Win=132096 Len=0
119 8.923163 192.168.1.201 44.228.249.3 HTTP 570 GET /login.php HTTP/1.1
124 8.945331 44.228.249.3 192.168.1.201 TCP 66 80 → 55446 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=0 MSS=1452 SACK_PERM WS=128
125 8.945381 192.168.1.201 44.228.249.3 TCP 54 55446 → 80 [ACK] Seq=1 Ack=1 Win=132096 Len=0
128 9.186656 44.228.249.3 192.168.1.201 TCP 66 80 → 55448 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=0 MSS=1452 SACK_PERM WS=128
129 9.186725 192.168.1.201 44.228.249.3 TCP 54 55448 → 80 [ACK] Seq=1 Ack=1 Win=132096 Len=0
130 9.217764 44.228.249.3 192.168.1.201 TCP 54 80 → 55445 [ACK] Seq=1 Ack=517 Win=62336 Len=0
131 9.218511 44.228.249.3 192.168.1.201 TCP 1506 80 → 55445 [ACK] Seq=1 Ack=517 Win=62336 Len=1452 [TCP segment of a reassembled P
132 9.219046 44.228.249.3 192.168.1.201 HTTP 1350 HTTP/1.1 200 OK (text/html)
133 9.219079 192.168.1.201 44.228.249.3 TCP 54 55445 → 80 [ACK] Seq=517 Ack=2749 Win=132096 Len=0
137 9.347604 192.168.1.201 142.250.207.195 TCP 66 55449 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
139 9.370301 142.250.207.195 192.168.1.201 TCP 66 443 → 55449 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
140 9.370366 192.168.1.201 142.250.207.195 TCP 54 55449 → 443 [ACK] Seq=1 Ack=1 Win=131072 Len=0
141 9.370707 192.168.1.201 142.250.207.195 TLSv1.3 2334 Client Hello (SNI=fonts.gstatic.com)
144 9.393564 142.250.207.195 192.168.1.201 TCP 54 443 → 55449 [ACK] Seq=1 Ack=1413 Win=68608 Len=0
145 9.394207 142.250.207.195 192.168.1.201 TCP 54 443 → 55449 [ACK] Seq=1 Ack=2281 Win=71424 Len=0
159 9.471314 142.250.207.195 192.168.1.201 TLSv1.3 1466 Server Hello, Change Cipher Spec
160 9.471583 142.250.207.195 192.168.1.201 TLSv1.3 108 Application Data
161 9.471606 192.168.1.201 142.250.207.195 TCP 54 55449 → 443 [ACK] Seq=2281 Ack=1467 Win=131072 Len=0
162 9.471701 192.168.1.201 142.250.207.195 TLSv1.3 128 Change Cipher Spec, Application Data
163 9.495039 142.250.207.195 192.168.1.201 TCP 60 443 → 55449 [ACK] Seq=1467 Ack=2355 Win=71424 Len=0
164 9.495419 142.250.207.195 192.168.1.201 TLSv1.3 1018 Application Data, Application Data
173 9.535138 192.168.1.201 142.250.207.195 TCP 54 55449 → 443 [ACK] Seq=2355 Ack=2431 Win=130304 Len=0
Frame 119: 570 bytes on wire (4560 bits), 570 bytes captured (4560 bits) on interface \Device\NPF_{3D234BE8-4FD8-487F-9E0C-5
Ethernet II, Src: Intel_07:9d:88 (f0:b6:1e:07:9d:88), Dst: BestITWorld_2f:b3:e8 (a0:47:d7:2f:b3:e8)
Internet Protocol Version 4, Src: 192.168.1.201, Dst: 44.228.249.3
Transmission Control Protocol, Src Port: 55445, Dst Port: 80, Seq: 1, Ack: 1, Len: 516
Hypertext Transfer Protocol
GET /login.php HTTP/1.1\r\n
Host: testphp.vulnweb.com\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sign
0030 02 04 ea 77 00 00 47 45 54
0040 2e 70 68 70 20 48 54 54 50
0050 6f 73 74 3a 20 74 65 73 74
0060 6e 77 65 62 2e 63 6f 6d 0d
0070 74 69 6f 6e 3a 20 6b 65 65
0080 0d 0a 43 61 63 68 65 2d 43
0090 20 6d 61 78 2d 61 67 65 3d
00a0 61 64 65 2d 49 6e 73 65 63
00b0 75 65 73 74 73 3a 20 31 0d
00c0 67 65 6e 74 3a 20 4d 6f 7a
00d0 30 20 28 57 69 6e 64 6f 77
00e0 2e 30 3b 20 57 69 6e 36 34
00f0 41 70 70 6c 65 57 65 62 4b
Text item (text), 25 bytes
Packets: 2656 · Displayed: 773 (29.1%) · Dropped: 0 (0.0%)
Profile: Default

HTTP Filtered



To check which websites are surfed on a network (only http websites)




Wireshark · Load Distribution · Wi-Fi
Topic / Item
Count
Average
Min Val
Max Val
Rate (ms)
Percent
Burst Rate
Burst Start
HTTP Responses by Server Address 0 0.0000 100% - -
HTTP Requests by Server 50 0.0002 100% 0.0200 21.540
HTTP Requests by Server Address 50 0.0002 100.00% 0.0200 21.540
ff02::c 18 0.0001 36.00% 0.0100 61.201
44.228.249.3 3 0.0000 6.00% 0.0100 8.923
239.255.255.250 26 0.0001 52.00% 0.0100 61.201
152.195.38.76 1 0.0000 2.00% 0.0100 21.394
104.112.106.111 2 0.0000 4.00% 0.0200 21.540
HTTP Requests by HTTP Host 50 0.0002 100.00% 0.0200 21.540
x2.c.lencr.org 1 0.0000 2.00% 0.0100 21.624
x1.c.lencr.org 1 0.0000 2.00% 0.0100 21.540
testphp.vulnweb.com 3 0.0000 6.00% 0.0100 8.923
crl3.digicert.com 1 0.0000 2.00% 0.0100 21.394
[FF02::C]:1900 18 0.0001 36.00% 0.0100 61.201
239.255.255.250:1900 26 0.0001 52.00% 0.0100 61.201
Display filter:
http.host
Apply
Copy
Save as...
Close

LAB EXPERIMENT – 10

Nessus Essentials for Vulnerability Scanning

LAB PRACTICE:

Which company created Nessus?

Nessus was created by Tenable, Inc. Tenable is a cybersecurity company that provides various security products and services.

Under Scan Templates in Nessus, there is a scan for what type of Ransomware?

Nessus does not specifically have a predefined scan template for a particular type of ransomware. Scan templates in Nessus are generally designed to identify vulnerabilities and security issues in systems rather than specific malware types.

When creating a new Plugin Rule, what 4 fields do you need to enter?

When creating a new Plugin Rule in Nessus, you typically need to enter the following four fields:

Name: A descriptive name for the rule.

Rule: The rule itself, specifying the conditions that trigger the rule.

Action: The action to be taken when the rule is triggered (e.g., alert, log, block).

Severity: The severity level assigned to the rule.

Is there a scan template specifically designed for mobile devices?

Yes, Nessus has scan templates that are specifically designed for mobile devices. These templates are tailored to assess the security of mobile operating systems and applications. Mobile device scan templates typically include checks for vulnerabilities and misconfigurations relevant to platforms such as Android and iOS.

Vulnerabilities by Host

Advance Dynamic Scan

127.0.0.1

0	0	0	0	20
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 20

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	141394	Apache HTTP Server Installed (Linux)
INFO	N/A	-	142640	Apache HTTP Server Site Enumeration
INFO	N/A	-	182774	Curl Installed (Linux / Unix)
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	84047	Hyper-V Virtual Machine Detection
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	147817	Java Detection and Identification (Linux / Unix)
INFO	N/A	-	151883	Libgcrypt Installed (Linux/UNIX)
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10147	Nessus Server Detection
INFO	N/A	-	14272	Netstat Portscanner (SSH)
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	148373	OpenJDK Java Detection (Linux / Unix)
INFO	N/A	-	168007	OpenSSL Installed (Linux)
INFO	N/A	-	130024	PostgreSQL Client/Server Installed (Linux)
INFO	N/A	-	174788	SQLite Local Detection (Linux)
INFO	N/A	-	42822	Strict Transport Security (STS) Detection
INFO	N/A	-	163326	Tenable Nessus Installed (Linux)
INFO	N/A	-	182848	libcurl Installed (Linux / Unix)

Vulnerabilities by Host

Basic Network Scan

127.0.0.1

0	0	1	0	55
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 56

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
INFO	N/A	-	141394	Apache HTTP Server Installed (Linux)
INFO	N/A	-	142640	Apache HTTP Server Site Enumeration
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	182774	Curl Installed (Linux / Unix)
INFO	N/A	-	55472	Device Hostname
INFO	N/A	-	54615	Device Type
INFO	N/A	-	159273	Dockerfile Detection for Linux/UNIX
INFO	N/A	-	25203	Enumerate IPv4 Interfaces via SSH
INFO	N/A	-	25202	Enumerate IPv6 Interfaces via SSH
INFO	N/A	-	33276	Enumerate MAC Addresses via SSH
INFO	N/A	-	170170	Enumerate the Network Interface configuration via SSH
INFO	N/A	-	179200	Enumerate the Network Routing configuration via SSH
INFO	N/A	-	168980	Enumerate the PATH Variables
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	86420	Ethernet MAC Addresses
INFO	N/A	-	168982	Filepaths contain Dangerous characters (Linux)
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution

127.0.0.1

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	1	0	0

Scan Information

Start time: Tue Dec 5 10:31:24 2023
End time: Tue Dec 5 10:46:42 2023

Host Information

IP: 127.0.0.1
MAC Address: 00:15:5D:1B:63:01
OS: Linux Kernel 6.5.0-kali3-amd64

Vulnerabilities

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

https://www.itu.int/rec/T-REC-X.509/en

https://en.wikipedia.org/wiki/X.509

Solution

Purchase or generate a proper SSL certificate for this service.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N)

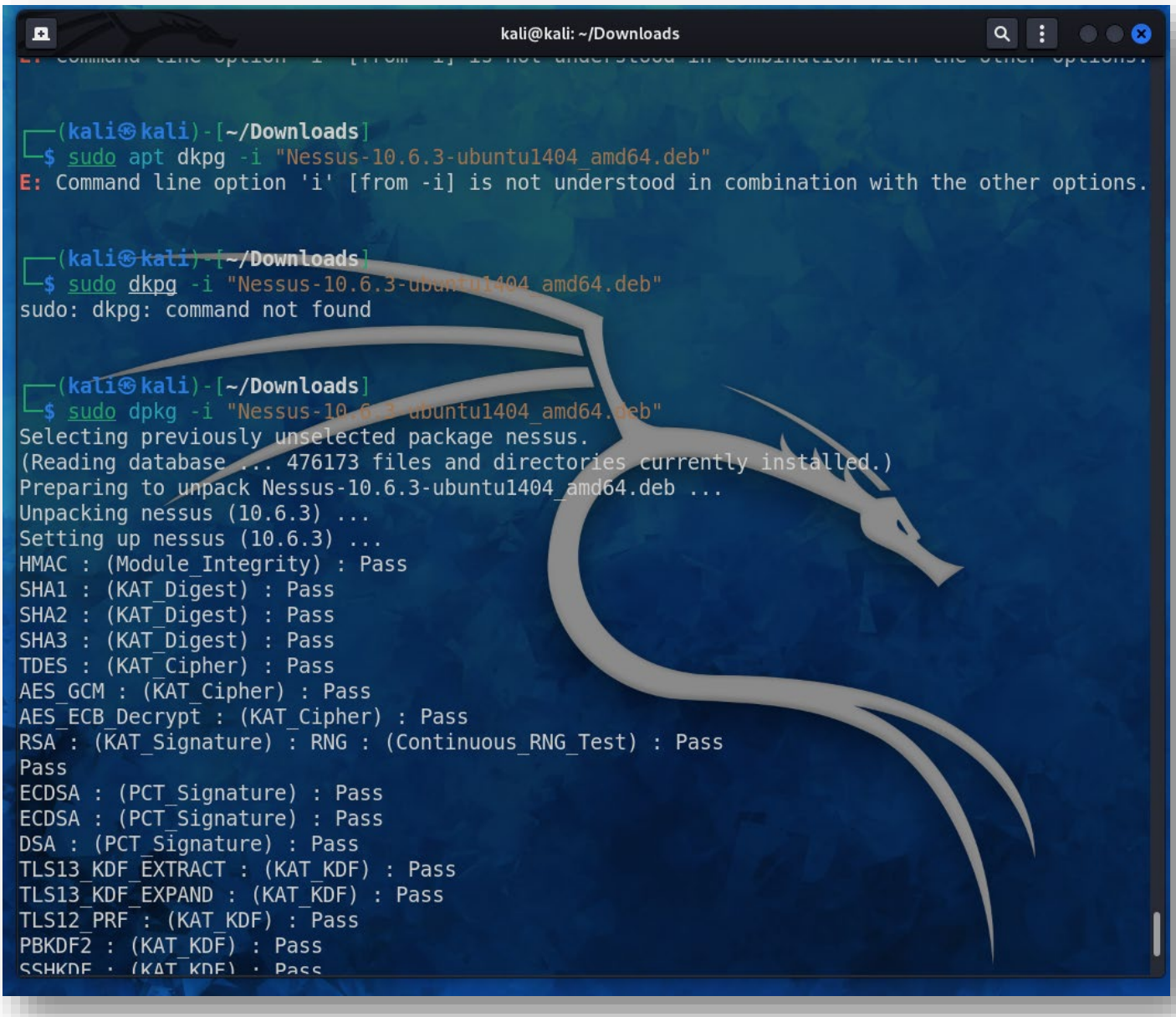
Plugin Information

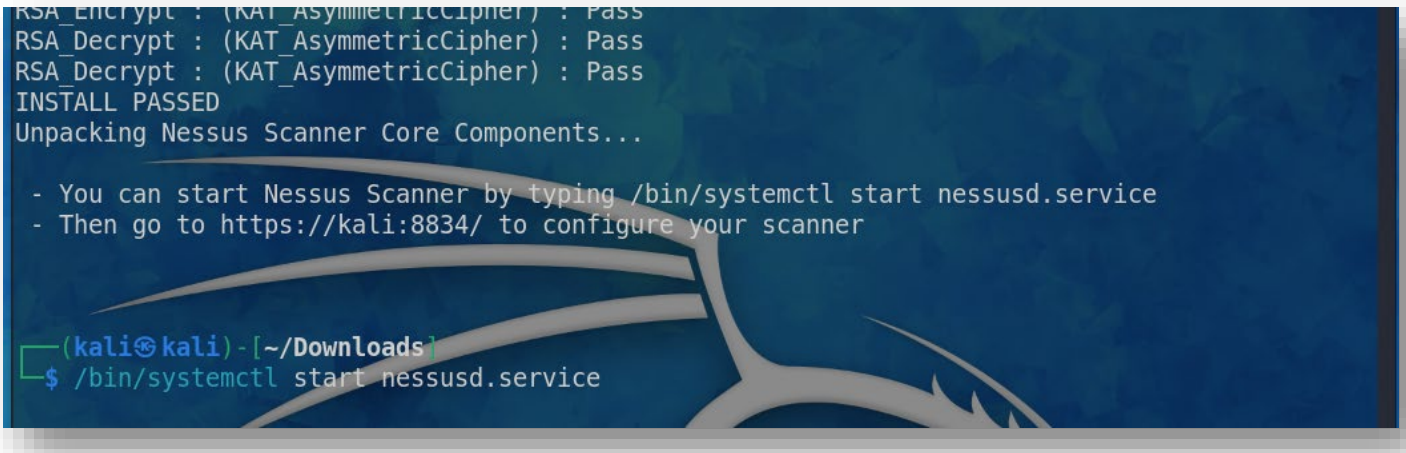
Published: 2010/12/15, Modified: 2020/04/27

Plugin Output

tcp/8834/www

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : O=Nessus Users United/OU=Nessus Server/L=New York/C=US/ST=NY/CN=kali
|-Issuer  : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus
 Certification Authority
```


kali@kali: ~/Downloads
(kali㉿kali)-[~/Downloads]
$ sudo apt dkpg -i "Nessus-10.6.3-ubuntu1404_amd64.deb"
E: Command line option 'i' [from -i] is not understood in combination with the other options.
(kali㉿kali)-[~/Downloads]
$ sudo dkpg -i "Nessus-10.6.3-ubuntu1404_amd64.deb"
sudo: dkpg: command not found
(kali㉿kali)-[~/Downloads]
$ sudo dpkg -i "Nessus-10.6.3-ubuntu1404_amd64.deb"
Selecting previously unselected package nessus.
(Reading database ... 476173 files and directories currently installed.)
Preparing to unpack Nessus-10.6.3-ubuntu1404_amd64.deb ...
Unpacking nessus (10.6.3) ...
Setting up nessus (10.6.3) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass


RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components...
- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://kali:8834/ to configure your scanner
(kali㉿kali)-[~/Downloads]
$ /bin/systemctl start nessusd.service

Welcome To Nessus Essentials

Welcome to Nessus Essentials and congratulations on taking action to secure your network! We offer the latest plugins for vulnerability scanning today, helping you identify more vulnerabilities and keep your network protected.

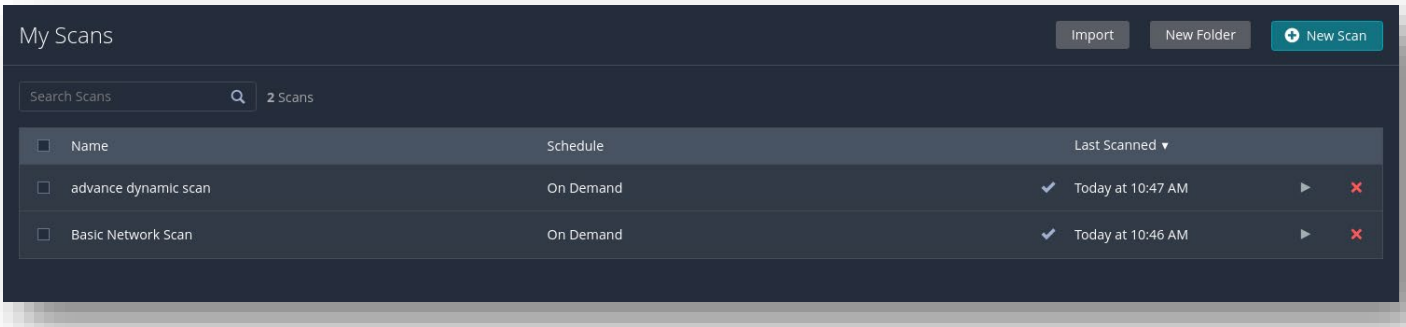
If you're looking for more advanced capabilities, such as live results and configuration checks – as well as the ability to scan unlimited IPs, check out Nessus Professional. To learn more view the Nessus Professional datasheet.

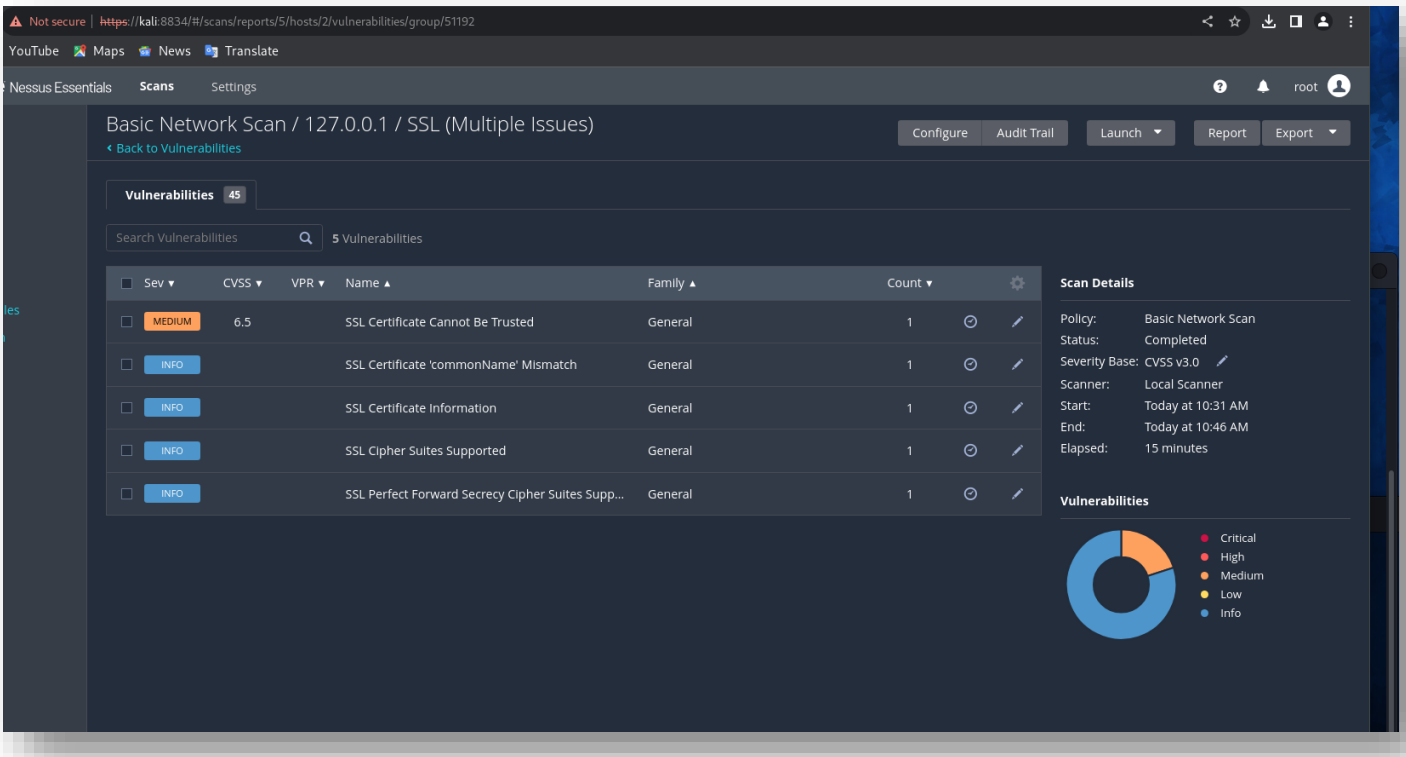
Activating Your Nessus Essentials License
Your activation code for Nessus Essentials is:
7TDJ-GSFS-LNGE-JFMT-7FP2

Download Nessus

This is a one-time code. If you uninstall and then reinstall you will need to register the scanner again and receive another activation code.

After initial installation of Nessus you will be prompted to set up and activate your scanner. For further details on activating your subscription review the installation guide.


My Scans
Import
New Folder
New Scan
Search Scans
2 Scans
Name
Schedule
Last Scanned
advance dynamic scan
On Demand
Today at 10:47 AM
Basic Network Scan
On Demand
Today at 10:46 AM


Not secure | https://kali:8834/#/scans/reports/5/hosts/2/vulnerabilities/group/51192
YouTube
Maps
News
Translate
Nessus Essentials
Scans
Settings
root
Basic Network Scan / 127.0.0.1 / SSL (Multiple Issues)
Back to Vulnerabilities
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 45
Search Vulnerabilities
5 Vulnerabilities
Sev
CVSS
VPR
Name
Family
Count
MEDIUM 6.5 SSL Certificate Cannot Be Trusted General 1
INFO SSL Certificate 'commonName' Mismatch General 1
INFO SSL Certificate Information General 1
INFO SSL Cipher Suites Supported General 1
INFO SSL Perfect Forward Secrecy Cipher Suites Supp... General 1
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 10:31 AM
End: Today at 10:46 AM
Elapsed: 15 minutes
Vulnerabilities
Critical
High
Medium
Low
Info