LOGIX ACADEMY

Lab: Email Forensics (SMTP)

Purpose

You have recently joined CyberOrg as a Security Analyst and you have been assigned the task to carry out a forensic investigation of a suspicious email header allegedly received from Facebook. Carry out a thorough investigation, and respond to the following points:

- Confirm if the email is legitimate or not
- Identify the IP address of the source SMTP server
- Identify the specific country and city where the source SMTP server is located

Solution is shared on the last page.

*** Copy header AFTER downloading this file otherwise you will miss some fields ***
(HEADER starts below this line and continues to Page 3)

Received: from MW4PR19MB6746.namprd19.prod.outlook.com (::1) by
 CY8PR19MB6938.namprd19.prod.outlook.com with HTTPS; Sun, 18 Sep 2022 19:13:39
 +0000
Received: from BN8PR07CA0029.namprd07.prod.outlook.com (2603:10b6:408:ac::42)
 by MW4PR19MB6746.namprd19.prod.outlook.com (2603:10b6:303:20b::9) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.5632.15; Sun, 18 Sep
 2022 19:13:38 +0000
Received: from BN1NAM02FT031.eop-nam02.prod.protection.outlook.com
 (2603:10b6:408:ac:cafe::87) by BN8PR07CA0029.outlook.office365.com
 (2603:10b6:408:ac::42) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.5632.19 via Frontend
 Transport; Sun, 18 Sep 2022 19:13:37 +0000
Authentication-Results: spf=none (sender IP is 89.144.21.170)
 smtp.mailfrom=facebook.com; dkim=none (message not signed)
 header.d=none;dmarc=none action=none header.from=;
Received-SPF: None (protection.outlook.com: facebook.com does not designate
 permitted sender hosts)
Received: from ghostnet.de (89.144.21.170) by
 BN1NAM02FT031.mail.protection.outlook.com (10.13.2.145) with Microsoft SMTP
 Server id 15.20.5632.12 via Frontend Transport; Sun, 18 Sep 2022 19:13:37
 +0000
X-IncomingTopHeaderMarker:

OriginalChecksum:9377C5A386D30792B842D1A9F38971885DE726853F37368B7234AA9A4F101D19;UpperCased
Checksum:F7E410CB226C6C2CEDECF4A46FC5B486B7C51D7A39B947271FBAFE69D465E90B;SizeAsReceived:326;
Count:8
From: "Facebook" <support@facebook.com>
Subject: Someone tried to log in To Your Account, User lD : Victim 1001
Reply-To: secureinternationalalerts10@gmail.com
To: victim1001@hotmail.com
Content-Type: text/html; charset="UTF-8"
Content-Transfer-Encoding: quoted-printable
Date: Sun, 18 Sep 2022 19:13:32 +0000

X-IncomingHeaderCount: 8
Return-Path: secureinternationalalerts10@gmail.com
X-MS-Exchange-Organization-ExpirationStartTime: 18 Sep 2022 19:13:37.7400
(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:
8a3a4416-fe45-4fdc-33cd-08da99a9e3d7
X-EOPAttributedMessage: 0
X-EOPTenantAttributedMessage: 84df9e7f-e9f6-40af-b435-aaaaaaaaaaaa:0
X-MS-Exchange-Organization-MessageDirectionality: Incoming
X-MS-PublicTrafficType: Email
X-MS-TrafficTypeDiagnostic: BN1NAM02FT031:EE_|MW4PR19MB6746:EE_
X-MS-Exchange-Organization-AuthSource:
BN1NAM02FT031.eop-nam02.prod.protection.outlook.com
X-MS-Exchange-Organization-AuthAs: Anonymous
X-MS-UserLastLogonTime: 9/18/2022 12:16:12 PM
X-MS-Office365-Filtering-Correlation-Id: 8a3a4416-fe45-4fdc-33cd-08da99a9e3d7
X-MS-Exchange-EOPDirect: true
X-Sender-IP: 89.144.21.170
X-SID-Result: NONE
X-MS-Exchange-Organization-PCL: 2
X-MS-Exchange-Organization-SCL: 5
X-Microsoft-Antispam: BCL:0;
X-MS-Exchange-CrossTenant-OriginalArrivalTime: 18 Sep 2022 19:13:37.6150
(UTC)
X-MS-Exchange-CrossTenant-Network-Message-Id: 8a3a4416-fe45-4fdc-33cd-08da99a9e3d7
X-MS-Exchange-CrossTenant-Id: 84df9e7f-e9f6-40af-b435-aaaaaaaaaaaa
X-MS-Exchange-CrossTenant-AuthSource:
BN1NAM02FT031.eop-nam02.prod.protection.outlook.com
X-MS-Exchange-CrossTenant-AuthAs: Anonymous
X-MS-Exchange-CrossTenant-FromEntityHeader: Internet
X-MS-Exchange-CrossTenant-RMS-PersistedConsumerOrg:
00000000-0000-0000-0000-000000000000
X-MS-Exchange-Transport-CrossTenantHeadersStamped: MW4PR19MB6746
X-MS-Exchange-Transport-EndToEndLatency: 00:00:01.6683626
X-MS-Exchange-Processed-By-BccFoldering: 15.20.5632.015
X-Microsoft-Antispam-Mailbox-Delivery:
abwl:0;wl:0;pcwl:0;kl:0;iwl:0;ijl:0;dwl:0;dkl:0;rwl:0;ucf:0;jmr:0;ex:0;psp:0;auth:0;dest:J;OFR:SpamFilterAuthJ;ENG:(5062000305)(90000117)(90002001)(91000020)(91036095)(91040095)(5061607266)(5061608174)(9050020)(9055020)(9100338)(2008001134)(2008121020)(4810004)(4910033)(8810097)(10005027)(9710001)(9610025)(9540006)(10103002)(9320005)(9215004);RF:JunkEmail;
X-Message-Info:
6hMotsjLow8tCacANDFIPxVFK5IWbneQPktA3UJ1JLJwnUydPoANjAxpSk8m1iZkzJ6qefSGmicU2vl9I3LnGXkT2aAsX1oh53WfKruJTPvSSilpWixL+zu75r+EvIyWn3dlrFbbG+pRYgWywbBVnDgCZOjyoHvoEY/WYtIh/b9MmlMp/maP+j0sa6uTsUt6dMXsLtwL44QbDX2Mj3swNQ==
X-Message-Delivery: Vj0xLjE7dXM9MDtsPTA7YT0wO0Q9MjtHRD0yO1NDTD02
X-Microsoft-Antispam-Message-Info:
=?utf-8?B?Z0UvaE13aHBEaHowQ2lwZ3lrMFBhbmxjbE1EcG1ia0FmWGFCT212SFpSVkFv?=
=?utf-8?B?QmtLTk1WRDBZK1g2VFB1enBiS3Q5T05DU21IaHhOaUFtMllVemFDekpaOUh1?=
=?utf-8?B?WE5sSFQyNDl6Z0Y2akpEU3RVcVNiMUVEaUZ6NGV5a0pHT0k0a2J6SkFlU3JI?=
=?utf-8?B?dSt3TVdzTTlSY0VXZ1pCM2lPQzY4aWhYYWM3Qk1CR0lpWmM0Mlh4aHI3dTBP?=
=?utf-8?B?MDhoc0hiOFFQR29Cb1VNZWY5bmFGQ0V6Ynh2b3BNbWVPdWZ5SWR1bjJQamll?=

=?utf-8?B?MG5wRCthWWRYanE0RjlCU3grOGt0RFhBN1FTSFk4Y2lCdk5UbXBFRFA4ODBD?=
=?utf-8?B?UXdLdC9mTWFNaG9FbUhrWTJSTE1WN21Ka0twdWEwOVUrbWRlV2d2bE1neTlX?=
=?utf-8?B?T1Nyc1BvMGx3R0h1VlFxRjNTRjN4RDZlVXJUSDRZV21tcklqK1lvWjE3UDJz?=
=?utf-8?B?b0lRV1JTbnRRb2t2QUVvTVB2Vnp5RDNEbk5VTDd4SjZib1ExSEJRaGJqTXNO?=
=?utf-8?B?NS83cHJseUpJWTQzbE1pU21MQWYvNFR2dnVMWHNXSG1KZFU1S2F6S2xlNDVC?=
=?utf-8?B?Qm9XUm83SWdYams0Y0hSdXpSYUovcFBXTUNBeUNMVHdDZ0hCRVU0Y3NqUVVC?=
=?utf-8?B?b0EzTVpSbE1GcVBsSkNMZjZ0N2lISG12Z0h1RU5tODR3WHl0dkM0YTZ2OE1J?=
=?utf-8?B?VjlIU3MwWjFiQTg0Vkp4RWhENTNiS0oyTjBuODZSeXhwR0lFYjVsNlJCSVY3?=
=?utf-8?B?ZGlreHV3ZUZhM2J1bjFGdCtiaGJxWktjY0t4dUlWQ1hyVTdlalIDWC9ZT3dj?=
=?utf-8?B?WlpiTkpoWVBSZklYTzlCY1NkZnpmc1cvdXRXL2Z0M21vNkNycnJlRjNNNXdE?=
=?utf-8?B?YWJYSUhmU0VjMmRnVXRkbjFaazlNcnNnQ1YwKytGTTdkK0Zwd1dnMlVDenEx?=
=?utf-8?B?NVNNN2c2MnJGemhnS2F4azFTOXRGdldVWllhTzBOVUZYYkxVMlgrc1RYQTdk?=
=?utf-8?B?ajQ5SHYxNmZDZFpseTlPcENBVVpsWDFGVDRzQ29kRmxkWmdRQmtURzUvbDhG?=
=?utf-8?B?REswUHhkeU9VblN1TjEvQUFZemNuUFZwWVo3TnFyVkh4aFBmc1IvK2R0d1Nm?=
=?utf-8?B?SFNUQm0xK1lydlFlZ0tBTVJBRmFReTRLdDd6YXM5MS9FRGVnejFVaE1QYm9n?=
=?utf-8?B?UG4yRnJrRXczY3ZjVzZIMHVVclFFUmJZMEwxWEZUcFZiRmdPaGt0ZWJLYWlL?=
=?utf-8?B?WEJvUGZyd3ZDNUJiSzNscEpScUY2OFRNWkw5a3FOT05aazF0NitHaHVWNkVt?=
=?utf-8?B?c2lSaFdGc3I1WjA5MzhCUnlreWxPZmJ2NS9qdG5EMFNCN1RtcjdxR2ZKelFu?=
=?utf-8?B?MEhHdjZCU3FnV1hzMkxuejM3WGw4VG1lakxSZnlLRmJYMGYrTGpNVHhtaFUy?=
=?utf-8?B?cjJLL2MrV1pvWlNSeEgrTzRmakVrYnU3aHFlUWRBN3JtN1FYZVVMcEJ1M1VE?=
=?utf-8?B?NXlEUXNDekVESGtrelp1VWtsTXJFcE0wTHdXZ0t1YXZibFBhclNid2pFZ0k0?=
=?utf-8?B?M2s4R1BPL3NRYnJvTVFUZERvQjZzc1AzTHB3dzgvOUVTVi85RTg3a0RBUkhy?=
=?utf-8?B?WkpBS2VZWUdRdHRlVEVxS1JNcVo4TUludkhKSjlhQUwyUmJtTWpsaks5UXJr?=
=?utf-8?B?SlhzOU9rcGRtaFR2djh1cFFtaWZnZXpYMHUrV1diRG9mN2w3UUM0QXNlL09D?=
=?utf-8?B?WWxsUkhiSUpkeTVEMTJEL1Z1dDBFNmpjckJrRHFWQUtZdmlFeVh1OGVXNnZW?=
=?utf-8?B?d3dSV0lZakhia2F6THdKenhOMGtRbS85NjEyNFczN2RTdkFWWFJaNHlOdEZt?=
=?utf-8?B?NzFSaUtManphMUFIVGIraUQvcjhlMzIyazZEV0lzMDRabUVocnduVTdGOHRp?=
=?utf-8?B?QTNKNTVnYy9ybFc4dTJhYWN6T09oTVVTMmxkODV3V292WHVsS2M4dDd4VnNJ?=
=?utf-8?B?S29KK0lBb0dseFg0cW1iN2ZOYytmRkRiMnYyUDN3ZnNYVWtaZFkyZ1liMlJL?=
=?utf-8?B?YnJsdGJsWlJ5ZWFNUG4rTmJoaUZ4THNuS0pCL2NhYUhMc2MzdXdKU2FtaFgx?=
=?utf-8?B?OVhwTXZNdDk1bitmZDVsU2lIZDR3b3FaQ3Bqam1TRGRwWjhzUWJZbkZ3RHJr?=
=?utf-8?B?SUNaV29ESUFya3ZKdnlJTVhMQzh2TXVYdlFEeWN0eUU5d281V1JLZWtUaUNJ?=
=?utf-8?B?T05Oc3RaU1pIK0xKQzdCT3ZJZWsvVjdnSzNqSTFHeDNCSVZCRElkQTdJekhK?=
=?utf-8?B?eUxvbktFYU5ZRmYvS2dwTm1LamlZZngxd2szTEFhUFJQdjZocFl0emJnQzJ5?=
=?utf-8?B?Q0E5QlV0Sy96VDZEcEt1emQzT2piNk5SQkNDRldraUlHNUtwS0REZ3hlY3NF?=
=?utf-8?B?N2ZncjVCOEkxT1F4LzlLOWFYTXBZdUxOUDQzT1NtTkJBcTZjUmRtMTRKcUQ1?=
=?utf-8?B?dWRPSzNuMXpPQ3kwS21JbENNSHRFeFlURnJ3SjRTSzJnVkdCMmQvNkxOend5?=
=?utf-8?B?OWJNVDVUOGpJTHp6Y1dBUVpCMGtrZlNhYkZBS3Y1eUxKSHY5dlJPM2I0Q2ZR?=
=?utf-8?B?TjFYUVZXZjA5NXZZaVZ6K2FDS3k5NTBmUHI1bmdTU0RqbjZEejhjamZ5bThK?=
=?utf-8?B?b1drc0ZwSWNkOThhYmVWQ2x4SDV5L0NTaS9RdE1Ja0c0WGV5THVxL0YrMXNo?=
=?utf-8?B?RFo5ajV4RXlDR1N3aWJmNjA1anord3g1aVU0aXBVeGhEUkNKWHVLTkphR3NP?=
=?utf-8?B?VXpnQURacmdRRUtxbnhFY2tGVm5BeEx0Nm9NcVl1eFIvYW5rSjFZM1BSTkRV?=
=?utf-8?B?aFQwSU0xSHQ5d1ArS0NwMXRRWWVLVVkrQWlNRlh0VjNXSU9xaFhJWlBlaHM1?=
=?utf-8?B?VVpyajdmZndkMDh5NU9YblZkRjhCKzIzZW5Ubi93MnNYN0lGOWRuSXlJNExD?=
=?utf-8?B?MGJ3TnZZMXEzTUhueVJpZzVaYzIyMUhobGczWGhVT2hrbmpRSlJkQTNNaHYy?=
=?utf-8?B?RnRWVVg5NTN4aE5hVjRobEZrU0UxcUJLQWpiS3RoYlRkOEVMNEwxaEh1Z2sw?=
=?utf-8?Q?Cw8S59Dmf?=
MIME-Version: 1.0

LOGIX ACADEMY

Solution

- **Confirm if the email is legitimate or not**

The email is spoofed and not legitimate, it has a spoofed reply email address which is different from the actual one. It appears to come from support@facebook.com but will actually be sent to secureinternationalalerts10@gmail.com

Headers Found

Header Name	Header Value
Authentication-Results	spf=none (sender IP is 89.144.21.170) smtp.mailfrom=facebook.com; dkim=none (message not signed) header.d=none;dmarc=none action=none header.from=;
Received-SPF	None (protection.outlook.com: facebook.com does not designate permitted sender hosts)
X-IncomingTopHeaderMarker	OriginalChecksum:9377C5A386D30792B842D1A9F38971885DE726853F37368B7234AA9A4F101D19;UpperCasedChecksum:F7E410CB226C6C2CEDECF4A46FC5B486B7C51D7A39B947271FBAFE69D465E90B;SizeAsReceived:326;Count:8
From	"Facebook" <support@facebook.com>
Subject	Someone tried to log in To Your Account, User ID : Victim 1001
Reply-To	secureinternationalalerts10@gmail.com
To	victim1001@hotmail.com
Content-Type	text/html; charset="UTF-8"
Content-Transfer-Encoding	quoted-printable
Date	Sun, 18 Sep 2022 19:13:32 +0000
X-IncomingHeaderCount	8
Return-Path	secureinternationalalerts10@gmail.com

- **Identify the IP address of the source SMTP server**

Source IP address of the origin server: 89.144.21.170

Relay (Seconds)

Hop	Delay	From	By	With	Time (UTC)	Black list
1	*	donmvfed.co.uk 89.144.21.170	BN1NAM02FT031.mail.protection.outlook.com 10.13.2.145	Microsoft SMTP Server	9/18/2022 7:13:37 PM	
2	0 seconds	BN1NAM02FT031.eop-nam02.prod.protection.outlook.com 2603:10b6:408:ac:cafe::87	BN8PR07CA0029.outlook.office365.com 2603:10b6:408:ac::42	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	9/18/2022 7:13:37 PM	
3	1 Second	BN8PR07CA0029.namprd07.prod.outlook.com 2603:10b6:408:ac::42	MW4PR19MB6746.namprd19.prod.outlook.com 2603:10b6:303:20b::9	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	9/18/2022 7:13:38 PM	
4	1 Second	MW4PR19MB6746.namprd19.prod.outlook.com ::1	CY8PR19MB6938.namprd19.prod.outlook.com	HTTPS	9/18/2022 7:13:39 PM	

- **Identify the specific country and city where the source SMTP server is located**

This email originated from Germany. Please note that based on IP reallocations, it may point to a different ISP/Country, which will be considered the latest info at that point in time and therefore correct.