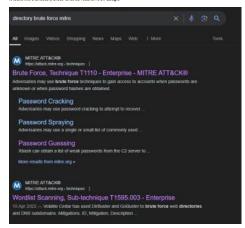
Heartbreaker-Denouement Challenge

Task 1: What type of scanning technique was used to discover the web path of the victim's web server? Specify the name of the corresponding MITRE sub-technique.

I checked the access.log inside the apache2 and looked at the logs

35.169.66.139 - [13/Mar/2004:13):95:29 40000] *GET /A37/ HITP/1.1" 604 397 ** "Morilla/5.0 [Mindows HT 10.0; Minds; x64] AppleWebEits/537.36 [DETMG, like Gacto) Chrome/97.0.4220.08 Safazi/537.36" [55.169.66.139 - [13/Mar/2004:13):95:129 40000] *GET /Assi HITP/1.1" 604 397 ** "Morilla/5.0 [Mindows HT 10.0; Minds; x64] AppleWebEits/537.36 [DETMG, like Gacto) Chrome/97.0.4220.08 Safazi/537.36" [55.169.66.139 - [13/Mar/2004:13):95:129 40000] *GET /Appl., Part Printla/1.5.0 [Mindows HT 10.0; Minds; x64] AppleWebEits/537.36 [DETMG, like Gacto) Chrome/97.0.4220.08 Safazi/537.36" [55.169.66.139 - [13/Mar/2004:13):95:129 40000] *GET /Appl., Part Printla/5.0 [Mindows HT 10.0; Minds; x64] AppleWebEits/537.36 [DETMG, like Gacto) Chrome/97.0.4220.08 Safazi/537.36" [35.169.66.139 - [13/Mar/2004:13):95:129 40000] *GET /Appl., Part Printla/5.0 [Mindows HT 10.0; Minds; x64] AppleWebEits/537.36 [DETMG, like Gacto) Chrome/97.0.4220.08 Safazi/537.36" [35.169.66.139 - [13/Mar/2004:13):95:129 40000] *GET /Appl., Mark [17/1.2" 404 384 ** "Morilla/5.0 [Mindows HT 10.0; Minds; x64] AppleWebEits/537.36 [DETMG, like Gacto) Chrome/97.0.4220.88 Safazi/537.46" [35.169.66.139 - [13/Mar/2004:13):95:129 40000] *GET /Appl., Mark [17/1.2" 404 384 ** "Morilla/5.0 [Mindows HT 10.0; Minds; x64] AppleWebEits/537.36 [DETMG, like Gacto) Chrome/97.0.4220.88 Safazi/537.46" [35.169.66.139 - [13/Mar/2004:13):95:129 40000] *GET /Appl., Mark [17/1.2" 404 384 ** "Morilla/5.0 [Mindows HT 10.0; Minds; x64] AppleWebEits/537.36 [DETMG, like Gacto) Chrome/97.0.4220.88 Safazi/537.36" [35.169.66.139 - [13/Mar/2004:13):95:129 40000] *GET /Appl., Mark [17/1.2" 404 384 ** "Morilla/5.0 [Mindows HT 10.0; Minds; x64] AppleWebEits/537.36 [DETMG, like Gacto) Chrome/97.0.4220.88 Safazi/537.36" [35.169.66.139 - [13/Mar/2004:13):95:129 40000] *GET /Appl., Mark [17/1.2" 404 384 ** "Morilla/5.0 [Mindows HT 10.0; Minds; x64] AppleWebEits/537.36 [DETMG, like Gacto) Chrome/97.0.4220.88 Safazi/537.36" [35.169.66.139 - [13/Mar/2004:13):95:129 40000] *GET /Appl., Mark [17/1.2" 404 38

It looks like a directory brute force so I search it on Google



Answer: Wordlist Scanning

1888.2: It seems a web request possibly could have been rerouted, potentially revealing the web server's web path to the Threat Actor. What specific HTML status code might have provided this information?

Answer: 301

Task 3: What was the initial payload submitted by the threat actor to exploit weakness of the web server?

| Food Name 13 4:002138.336007 2024 | [ppp?ressions | [pid 400] [claims 15.169.66.1309:35005] Request POOT /nd-lossapp-tracker.php Input: | [Ped Mars 13 4:002138.336007 2024] [ppp?ressions | [pid 400] [claims 15.169.66.1309:35005] Request POOT /nd-lossapp-tracker.php Input: | [Ped Mars 13 4:0016.58158 2024] [ppp?ressions | [pid 400] [claims 15.169.66.1309:35005] Request POOT /nd-lossapp-tracker.php Input: | [Ped Mars 13 4:0016.58158 2024] [ppp?ressions | [pid 400] [claims 15.169.66.1309:35005] Request POOT /nd-lossapp-tracker.php Input: | [Ped Mars 13 4:0016.58158 2024] [ppp?ressions | [pid 400] [claims 15.169.66.1309:35005] Request POOT /nd-lossapp-tracker.php Input: | [Ped Mars 13 4:0016.58158 2024] [ppp?ressions | [pid 400] [claims 15.169.66.1309:35005] Request POOT /nd-lossapp-tracker.php Input: | [Ped Mars 13 4:0016.46.1309:35005] [ppp?ressions | [pid 400] [claims 15.169.66.1309:35005] Request POOT /nd-lossapp-tracker.php Input: | [Ped Mars 13 4:0016.46.1309:35005] [ppp?ressions | [pid 400] [claims 15.169.66.1309:35005] [Ppd. mars 13 4:0016.46.1309:35005] [Ppd. mars 13 4:0016.46.1309:3500

Answer: file:///etc/passwd

Task 4: What is the name of the vulnerability exploited by the Threat Actor?

I took the logs from task 3 and asked the ChatGPT what could be the vulnerability

Task 5: At what time (UTC) did the Threat Actor first realize they could access the cloud metadata of the web server instance?

Found it inside the error.log

[Wed Mar 13 14]:06:21.655943 2024] [php7:motice] [pid 412] [client 35.169.66.138:52712] Request: NOST /wb-loanapp-tracker.php Input: http://leb.254.169.254, referen: http://leb.234.169.254, referen: http://leb.234.169.254

Task 6: For a clearer insight into the Database content that could have been exposed, could you provide the name of at least one of its possible tables?

Inside the \root\home\ubuntu\.mysql_history there is several tables

Inside the Yoothomelubuntul mysql_history there
| Fischery U.s.
| Fischery U.s

Answer: CustomerInfo

Task 7: Which AWS API call functions similarly to the 'whoami' command in Windows or Linux?

Task 8: It seems that the reported compromised AWS IAM credential has been exploited by the Threat Actor Can you identify the regions where these credentials were used successfully? Separate regions by comma and in ascending order.

Answer: us-east-1,us-east-2

Task 9: Discovering that the compromised IAM account was used prior to the web server attack, this suggests the threat actor might have obtained the public IP addresses of running instances. Could you specify the API call the could have exposed this information?

I asked the ChatGPT

Answer: DescribeInstances

Task 10: Looks like the Threat Actor didn't only use a single IP address. What is the total number of unsuccessful requests made by the Threat Actor?

I searched for "DescribeInstances"

line 41681 "errorifessage": Tou are not authorized to perform this operation. User: armiswists:194622803460:assumed-role/ECQDatabaseConnection/i-Obd5911685069996 is not authorized to perform ecd:_perciple_natances*, line 16021 "eventiment: "Oscillenatances", "oscillenatances", "oscillenatances", "oscillenatances", "errorifessage": Tou are not authorized to perform this operation. Disc: armiswists:194622803460:assumed-role/ECQDatabaseConnection/i-Obd5911685069996 is not authorized to perform ecd:_perciplenatances* because no identity-based policy allows the ecd:_perciplenatances* armiswists:194622803460:assumed-role/ECQDatabaseConnection/i-Obd5911685069996 is not authorized to perform ecd:_perciplenatances* because no identity-based policy allows the ecd:_perciplenatances* armiswists:194622803460:assumed-role/ECQDatabaseConnection/i-Obd5911685069996 is not authorized to perform ecd:_perciplenatances* because no identity-based policy allows the ecd:_perciplenatances* armiswists:194622803460:assumed-role/ECQDatabaseConnection/i-Obd5911685069996 is not authorized to perform ecd:_perciplenatances*.

"errorMessage": "Deers armswesses; 19962200460.assumed-role/ECDstabaseConnection/:-Dodf5169b06948: is not authorized to perform; lambdavlistFunctions on recourse: * because no identity-based policy allows the lambdavlistFunctions action,"
"errorMessage": "Deers armswesses; "Observations action a

Then I took the string "is not authorized to perform" and searched for it too

Fearch '%s not authorized to perform' [742 hits in 1 file of i searched] [Bornal Word]

Shared '%s not authorized to perform' [742 hits in 1 file of i searched] [Bornal Word]

Shared '%s not authorized to perform' [742 hits in 1 file of i searched] [Bornal Word]

Shared '%s not authorized to perform' [742 hits in 1 file of i searched] [Bornal Word]

Shared '%s not authorized to perform teacher the shared '%s not authorized to

Task 11:

Can you identify the Amazon Resource Names (ARNs) associated with successful API calls that might their revealed details about the victim's cloud infrastructure? Separate ARNs by comma and in successful apid calls the successful API calls that might the revealed details about the victim's cloud infrastructure? Separate ARNs by comma and in successful API calls the revealed of the revea

After I found the answer for task 10, I checked the ARNs and found only 2 ARNs

"errorMessage": "User: am:sams;sts::949622803460;assumed-role/EC2DatabaseConnection/i-Obdf91168b506436
"errorMessage": "User: am:sams;sts::949622803460;assumed-role/EC2DatabaseConnection/i-Obdf91168b506436

Answer: arn:aws:iam::949622803460:user/devops-ash,arn:aws:sts::949622803460:assumed-role/EC2DatabaseConnection/i-0bdf91168b50e943e

ndb-prod-2024-03-13-06-53,wb-customerdb-prod-2024-03-13-07-59

I searched for snapshotId and found several snapshots. Then I told chat to make me all combinations to

Answer: transactiondb-prod-2024-03-13-06-53,wb-customerdb-prod-2024-03-13-07-59

Task 13: The Threat Actor successfully exfiltrated the data to their account. Could you specify the account ID that was used?

renthusion' "1.0", serionalist" "Tage" ! Assemblish, "Tage" ! Assemblish, "Tage ! Tage),
"webldFederationData": [],
"attributes": [
"creationData": "2024-03-13T14:09:02Z*,
"mfaRuthenbicated": "false"), "ec2RoleDelivery": "1.0" onsellements": {
drapshotIdentifier": "wbroustomerdb-prod-2024-03-13-07-35",
drapshotAttributes": [

I told ChatGPT about the account ID from task 13, showed him part of the log and asked him about the MITRE Technique

The activity described involves exfiltrating data by modifying the attributes of an Amazon RDS snapshot to include an external account ID, which is a form of data exfiltration using cloud services. According to the MITRE ATT&CX framework, this activity can be mapped to the technique:

MITRE Technique ID: T1537 Technique Name: Exfiltration Over Web Service

This technique covers the exfiltration of data using cloud-based services, such as AWS, where attackers can exploit cloud storage and data management services to transfer data out of an organization's environment. In this specific case, modifying RDS snapshot attributes to include an external account ID to exfiltrate data fits this technique.

Answer: T1537