Cloud Security Suite
One stop tool for AWS/GCP/Azure security audit
https://github.com/SecurityFTW/cs-suite

Shivankar Madaan
@shivankarmadaan
whoami

• Senior Security Engineer
• Conferences – BH Asia, BH EU, c0c0n
• Active Member of Null Bangalore Chapter
• Researcher at heart
Why AWS/GCP/Azure Audit?

• Misconfigured Access (IAM, root, policy/Service Accounts)
• Vulnerable services in use
• Public Access (Ports)
• Exposed Data (S3/Cloud Storage/Blobs)
• And many more..
How?

• Third Party Audit
  • You get a third party to do your dirty work
  • Lot of money involved
  • Giving access to the infrastructure
How…

• Open Source tools
  • Scout2
  • Prowler
  • Lunar
  • G-Scout
  • Azucar
• Local Auditing tools
• Other scripts on Github and Bitbucket
Cloud Security Suite

- Takes the “open source setup” pain away from you
- Compiles all the Audit checks
- Custom Audit checks
- Runs all in one go
- Centralized Portable Reports
- Audits the Servers Instances
- GCP Audit Capabilities
- Integration of AWS Trusted Advisor
- JSON Output (Have fun!)
Introducing Azure Support in CS-Suite
Cloud Security Suite (Azure)

$ git clone https://github.com/SecurityFTW/cs-suite.git
$ cd cs-suite/
$ sudo python setup.py
$ python cs.py -env azure
Demo – Azure Audit
Cloud Security Suite (AWS)

$ git clone https://github.com/SecurityFTW/cs-suite.git
$ cd cs-suite/
$ sudo python setup.py
$ python cs.py -env aws
Cloud Security Suite (GCP)

```bash
$ git clone https://github.com/SecurityFTW/cs-suite.git
$ cd cs-suite/
$ sudo python setup.py
$
$ python cs.py -env gcp -pId bhasia-arsenal
```

The following entities were found to be in violation of this rule: All Ports Open to All

```
default-allow-icmp


sourceRanges: [
  "0.0.0.0/0"
]

direction: "INGRESS"

destinationRanges:

allowed: [
  
  "IPProtocol": "icmp"
]

description: "Allow ICMP from source IP""
```
Demo – AWS Audit
{  
  "account": "<ID>",
  "check_no": "<check_type>",
  "aws-cli_profile": "default",
  "region": "us-east-1",
  "level": "null",
  "value": "Cloudfront <ID> is not WAF integration enabled",
  "score": "Scored",
  "type": "WARNING",
  "check": "CDN_AUDIT"
}

Path - cs-suite/reports/AWS/aws_audit/<account_name>/<time_stamp>/final_report/final_json
Server Audit

• IP based auditing – Public and Private
• Runs the audit on the remote machine
• Report copied back to main machine
• Portable HTML report
• Region independent Audit, in case of public IP Address
Demo – Server Audit (Linux)
Demo – Server Audit (Windows)
References

- https://github.com/nccgroup/Scout2
- https://github.com/Alfresco/prowler
- https://aws.amazon.com/security/
- https://github.com/nccgroup/G-Scout/
- https://github.com/CISOfy/lynis
Feedback / Suggestions / Queries?

@shivankarmadaan  
shivankarmadaan@gmail.com  
https://github.com/shivankar-madaan