

# 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

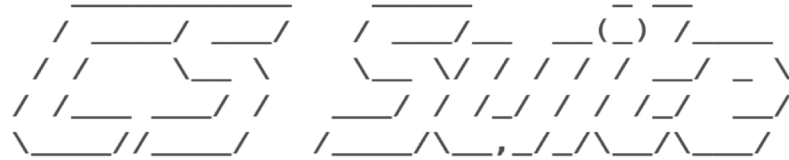
# Cloud Security Suite

- 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
```



## Security Center

Encryption,  
Firewall, Threat  
Detection

## Storage Accounts

File Service,  
Storage service

## Logging and Monitoring

Log retention  
policy, Alerts on  
Create/delete  
events

## Networking

Network  
Watcher,  
Network Rules

## Virtual Machines

Agents, Disk  
Encryption,  
Extensions

## Azure Vault

Keys, Secrets  
Retention

## SQL Databases

Audit, alerts,  
retention

# 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
```



## Scout2

First thing you  
should look at !

## Prowler

Second best  
thing !

## Web & Network

Info on: CDN,  
CERTS, DNS,  
ELB

## Data Stores

Info on: EC, ES,  
RDS, REDSHIFT

## Notification

More info on:  
CloudFormation,  
SES, SNS

## Configs

More info on:  
EC2, KEYS,  
AWS Config,  
VPC

## AWS Trusted Advisor

More info on:  
Checks from  
AWS Trusted  
Advisor

## IP Audit

Check IP Audit  
results

# Cloud Security Suite(GCP)

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

Network▼

Service Account▼

Firewall▼

Bucket▼

Role▼

SQL Instance▼

Compute Engine▼

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

**default-allow-icmp**

network: "https://www.googleapis.com/compute/v1/projects/bhasia-arsenal/global/networks/default"

sourceRanges: [  
 "0.0.0.0/0"  
]

direction: "INGRESS"

destinationRanges:

allowed: [  
 {  
 "IPProtocol": "icmp"  
 }  
]

description: "Allow ICMP from anywhere"

# Demo – AWS Audit

# JSON

---

```
{  
  "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>
- <https://github.com/alanrenouf/Windows-Workstation-and-Server-Audit>

# Feedback / Suggestions / Queries ?



@shivankarmadaan



shivankarmadaan@gmail.com



<https://github.com/shivankar-madaan>