

# Cloud Security - Attacks

## AWS

### Privilege Escalation to SYSTEM in AWS VPN Client

- <https://rhinosecuritylabs.com/aws/cve-2022-25165-aws-vpn-client/> (<https://rhinosecuritylabs.com/aws/cve-2022-25165-aws-vpn-client/>).

### AWS WorkSpaces Remote Code Execution

- <https://rhinosecuritylabs.com/aws/cve-2021-38112-aws-workspaces-rce/> (<https://rhinosecuritylabs.com/aws/cve-2021-38112-aws-workspaces-rce/>).

### Resource Injection in CloudFormation Templates

- <https://rhinosecuritylabs.com/aws/cloud-malware-cloudformation-injection/> (<https://rhinosecuritylabs.com/aws/cloud-malware-cloudformation-injection/>).

### Downloading and Exploring AWS EBS Snapshots

- <https://rhinosecuritylabs.com/aws/exploring-aws-ebs-snapshots/> (<https://rhinosecuritylabs.com/aws/exploring-aws-ebs-snapshots/>).

### CloudGoat ECS\_EFS\_Attack Walkthrough

- [https://rhinosecuritylabs.com/cloud-security/cloudgoat-aws-ecs\\_efs\\_attack/](https://rhinosecuritylabs.com/cloud-security/cloudgoat-aws-ecs_efs_attack/) ([https://rhinosecuritylabs.com/cloud-security/cloudgoat-aws-ecs\\_efs\\_attack/](https://rhinosecuritylabs.com/cloud-security/cloudgoat-aws-ecs_efs_attack/)).

### GKE Kubelet TLS Bootstrap Privilege Escalation

- <https://rhinosecuritylabs.com/cloud-security/kubelet-tls-bootstrap-privilege-escalation/> (<https://rhinosecuritylabs.com/cloud-security/kubelet-tls-bootstrap-privilege-escalation/>).

### Weaponizing AWS ECS Task Definitions to Steal Credentials From Running Containers

- <https://rhinosecuritylabs.com/aws/weaponizing-ecs-task-definitions-steal-credentials-running-containers/> (<https://rhinosecuritylabs.com/aws/weaponizing-ecs-task-definitions-steal-credentials-running-containers/>).

### CloudGoat AWS Scenario Walkthrough: "EC2\_SSRF"

- [https://rhinosecuritylabs.com/cloud-security/cloudgoat-aws-scenario-ec2\\_ssrf/](https://rhinosecuritylabs.com/cloud-security/cloudgoat-aws-scenario-ec2_ssrf/) ([https://rhinosecuritylabs.com/cloud-security/cloudgoat-aws-scenario-ec2\\_ssrf/](https://rhinosecuritylabs.com/cloud-security/cloudgoat-aws-scenario-ec2_ssrf/))

## Pillaging AWS ECS Task Definitions for Hardcoded Secrets

- <https://rhinosecuritylabs.com/aws/pillaging-ecs-task-definitions-two-new-pacu-modules/> (<https://rhinosecuritylabs.com/aws/pillaging-ecs-task-definitions-two-new-pacu-modules/>)

## Abusing VPC Traffic Mirroring in AWS

- <https://rhinosecuritylabs.com/aws/abusing-vpc-traffic-mirroring-in-aws/> (<https://rhinosecuritylabs.com/aws/abusing-vpc-traffic-mirroring-in-aws/>)

## Exploiting AWS ECR and ECS with the Cloud Container Attack Tool (CCAT)

- <https://rhinosecuritylabs.com/aws/cloud-container-attack-tool/> (<https://rhinosecuritylabs.com/aws/cloud-container-attack-tool/>)

## Bypassing IP Based Blocking with AWS API Gateway

- <https://rhinosecuritylabs.com/aws/bypassing-ip-based-blocking-aws/> (<https://rhinosecuritylabs.com/aws/bypassing-ip-based-blocking-aws/>)

## Phishing Users with MFA on AWS

- <https://rhinosecuritylabs.com/aws/mfa-phishing-on-aws/> (<https://rhinosecuritylabs.com/aws/mfa-phishing-on-aws/>)

## AWS IAM Privilege Escalation – Methods and Mitigation

- <https://rhinosecuritylabs.com/aws/aws-privilege-escalation-methods-mitigation/> (<https://rhinosecuritylabs.com/aws/aws-privilege-escalation-methods-mitigation/>)

## Penetration Testing AWS Storage: Kicking the S3 Bucket

- <https://rhinosecuritylabs.com/penetration-testing/penetration-testing-aws-storage/> (<https://rhinosecuritylabs.com/penetration-testing/penetration-testing-aws-storage/>)

## Cloud Security Risks (P2): CSV Injection in AWS CloudTrail

- <https://rhinosecuritylabs.com/aws/cloud-security-csv-injection-aws-cloudtrail/> (<https://rhinosecuritylabs.com/aws/cloud-security-csv-injection-aws-cloudtrail/>)

# Amazon's AWS Misconfiguration: Arbitrary Files Upload in Amazon Go

- <https://rhinosecuritylabs.com/aws/amazon-aws-misconfiguration-amazon-go/>  
(<https://rhinosecuritylabs.com/aws/amazon-aws-misconfiguration-amazon-go/>).

## Privilege Escalation Attack : Attacking AWS IAM permission misconfigurations

- [https://payatu.com/blog/mayank.arora/iam\\_privilege\\_escalation\\_attack](https://payatu.com/blog/mayank.arora/iam_privilege_escalation_attack)  
([https://payatu.com/blog/mayank.arora/iam\\_privilege\\_escalation\\_attack](https://payatu.com/blog/mayank.arora/iam_privilege_escalation_attack)).

## IAM Vulnerable - An AWS IAM Privilege Escalation Playground

- <https://bishopfox.com/blog/aws-iam-privilege-escalation-playground> (<https://bishopfox.com/blog/aws-iam-privilege-escalation-playground>).

## Escalator to the Cloud: 5 Privesc Attack Vectors in AWS

- <https://bishopfox.com/blog/5-privesc-attack-vectors-in-aws> (<https://bishopfox.com/blog/5-privesc-attack-vectors-in-aws>).

## Vulnerable AWS Lambda function – Initial access in cloud attacks

- <https://sysdig.com/blog/exploit-mitigate-aws-lambdas-mitre/> (<https://sysdig.com/blog/exploit-mitigate-aws-lambdas-mitre/>).

## Inside a Privilege Escalation Attack via Amazon Web Services' EC2

- <https://thenewstack.io/inside-a-privilege-escalation-attack-via-amazon-web-services-ec2/>  
(<https://thenewstack.io/inside-a-privilege-escalation-attack-via-amazon-web-services-ec2/>).

## AWS Attacks

- <https://pentestbook.six2dez.com/enumeration/cloud/aws> (<https://pentestbook.six2dez.com/enumeration/cloud/aws>).

## AWS Shadow Admin

- <https://www.admin-magazine.com/Archive/2021/63/Shadow-admin-permissions-and-your-AWS-account>  
(<https://www.admin-magazine.com/Archive/2021/63/Shadow-admin-permissions-and-your-AWS-account>).

## Gaining AWS Console Access via API Keys

- <https://www.netspi.com/blog/technical/gaining-aws-console-access-via-api-keys/>  
(<https://www.netspi.com/blog/technical/gaining-aws-console-access-via-api-keys/>)

## Automate AWS AMI Creation For EC2 And Copy to Other Region

- <https://dheeraj3choudhary.com/automate-aws-ami-creation-for-ec2-and-copy-to-other-region-or-disaster-recovery>  
(<https://dheeraj3choudhary.com/automate-aws-ami-creation-for-ec2-and-copy-to-other-region-or-disaster-recovery>)

## Instance Connect - Push an SSH key to EC2 instance

- <https://cloudonaut.io/connect-to-your-ec2-instance-using-ssh-the-modern-way/> (<https://cloudonaut.io/connect-to-your-ec2-instance-using-ssh-the-modern-way/>)

## Golden SAML Attack

- <https://www.cyberark.com/resources/threat-research-blog/golden-saml-newly-discovered-attack-technique-forges-authentication-to-cloud-apps> (<https://www.cyberark.com/resources/threat-research-blog/golden-saml-newly-discovered-attack-technique-forges-authentication-to-cloud-apps>)
- <https://blog.sygnia.co/detection-and-hunting-of-golden-saml-attack> (<https://blog.sygnia.co/detection-and-hunting-of-golden-saml-attack>)

## Stealing hashes from Domain Controllers in the Cloud

- [https://medium.com/@\\_StaticFlow\\_/cloudcopy-stealing-hashes-from-domain-controllers-in-the-cloud-c55747f0913](https://medium.com/@_StaticFlow_/cloudcopy-stealing-hashes-from-domain-controllers-in-the-cloud-c55747f0913)  
([https://medium.com/@\\_StaticFlow\\_/cloudcopy-stealing-hashes-from-domain-controllers-in-the-cloud-c55747f0913](https://medium.com/@_StaticFlow_/cloudcopy-stealing-hashes-from-domain-controllers-in-the-cloud-c55747f0913))

## AWS PenTest Methodology

- <https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Cloud%20-%20AWS%20Pentest.md>  
(<https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Cloud%20-%20AWS%20Pentest.md>)

## CloudGoat Official Walkthrough Series: “rce\_web\_app”

- [https://rhinosecuritylabs.com/aws/cloudgoat-walkthrough-rce\\_web\\_app/](https://rhinosecuritylabs.com/aws/cloudgoat-walkthrough-rce_web_app/)  
([https://rhinosecuritylabs.com/aws/cloudgoat-walkthrough-rce\\_web\\_app/](https://rhinosecuritylabs.com/aws/cloudgoat-walkthrough-rce_web_app/))

## Azure

# GKE Kubelet TLS Bootstrap Privilege Escalation

- <https://rhinosecuritylabs.com/cloud-security/kubelet-tls-bootstrap-privilege-escalation/>  
(<https://rhinosecuritylabs.com/cloud-security/kubelet-tls-bootstrap-privilege-escalation/>).

## Cloud Security Risks (Part 1): Azure CSV Injection Vulnerability

- <https://rhinosecuritylabs.com/azure/cloud-security-risks-part-1-azure-csv-injection-vulnerability/>  
(<https://rhinosecuritylabs.com/azure/cloud-security-risks-part-1-azure-csv-injection-vulnerability/>).

## Security for SaaS Companies: Leveraging Infosec for Business Value

- <https://rhinosecuritylabs.com/cloud-security/security-saas-companies-leveraging-infosec-business-value/>  
(<https://rhinosecuritylabs.com/cloud-security/security-saas-companies-leveraging-infosec-business-value/>).

## Common Azure Security Vulnerabilities and Misconfigurations

- <https://rhinosecuritylabs.com/cloud-security/common-azure-security-vulnerabilities/>  
(<https://rhinosecuritylabs.com/cloud-security/common-azure-security-vulnerabilities/>).

## Enumerate valid emails

- <https://zigmax.net/enumerate-valid-emails-accounts%EF%BF%BC/> (<https://zigmax.net/enumerate-valid-emails-accounts%EF%BF%BC/>).

## Enumerate Azure Subdomains

- <https://www.netspi.com/blog/technical/cloud-penetration-testing/enumerating-azure-services/>  
(<https://www.netspi.com/blog/technical/cloud-penetration-testing/enumerating-azure-services/>).
- <https://m0chan.github.io/2019/12/16/Subdomain-Takeover-Azure-CDN.html>  
(<https://m0chan.github.io/2019/12/16/Subdomain-Takeover-Azure-CDN.html>).

## Azure Attacks

- <https://pentestbook.six2dez.com/enumeration/cloud/azure>  
(<https://pentestbook.six2dez.com/enumeration/cloud/azure>).

## Azure Active Directory Account Enumeration

- <https://helloitsliam.com/2021/11/18/azure-active-directory-account-enumeration/>  
(<https://helloitsliam.com/2021/11/18/azure-active-directory-account-enumeration/>).

# Abusing Microsoft's Azure domains to host phishing attacks

- <https://www.zscaler.fr/blogs/security-research/abusing-microsofts-azure-domains-host-phishing-attacks>  
(<https://www.zscaler.fr/blogs/security-research/abusing-microsofts-azure-domains-host-phishing-attacks>)

## Defending against the EvilGinx2 MFA Bypass

- <https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad/defending-against-the-evilginx2-mfa-bypass/m-p/501719> (<https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad/defending-against-the-evilginx2-mfa-bypass/m-p/501719>)
- <https://thecloudtechnologist.com/2019/04/29/defending-against-evilginx2-in-office-365/>  
(<https://thecloudtechnologist.com/2019/04/29/defending-against-evilginx2-in-office-365/>)

## Introduction To 365-Stealer - Understanding and Executing the Illicit Consent Grant Attack

- <https://www.alteredsecurity.com/post/introduction-to-365-stealer> (<https://www.alteredsecurity.com/post/introduction-to-365-stealer>)
- <https://www.cloud-architekt.net/detection-and-mitigation-consent-grant-attacks-azuread/> (<https://www.cloud-architekt.net/detection-and-mitigation-consent-grant-attacks-azuread/>)

## Azure AD Password spray; from attack to detection (and prevention).

- <https://derkvanderwoude.medium.com/password-spray-from-attack-to-detection-and-prevention-87c48cede0c0>  
(<https://derkvanderwoude.medium.com/password-spray-from-attack-to-detection-and-prevention-87c48cede0c0>)
- <https://jeffreypappel.nl/protecting-against-password-spray-attacks-with-azure-sentinel-and-azure-ad/>  
(<https://jeffreypappel.nl/protecting-against-password-spray-attacks-with-azure-sentinel-and-azure-ad/>)

## LATERAL MOVEMENT TO THE CLOUD WITH PASS-THE-PRT

- <https://stealthbits.com/blog/lateral-movement-to-the-cloud-pass-the-prt/> (<https://stealthbits.com/blog/lateral-movement-to-the-cloud-pass-the-prt/>)
- <https://derkvanderwoude.medium.com/pass-the-prt-attack-and-detection-by-microsoft-defender-for-afd7dbe83c94>  
(<https://derkvanderwoude.medium.com/pass-the-prt-attack-and-detection-by-microsoft-defender-for-afd7dbe83c94>)

## Azure AD Pass The Certificate

- <https://medium.com/@mor2464/azure-ad-pass-the-certificate-d0c5de624597>  
(<https://medium.com/@mor2464/azure-ad-pass-the-certificate-d0c5de624597>)

## How to SSH into specific Azure Web App instance

- <https://codez.deedx.cz/posts/how-to-ssh-into-web-app-instance/> (<https://codez.deedx.cz/posts/how-to-ssh-into-web-app-instance/>)

## Attacking Azure, Azure AD, and Introducing PowerZure

- <https://posts.specterops.io/attacking-azure-azure-ad-and-introducing-powerzure-ca70b330511a> (<https://posts.specterops.io/attacking-azure-azure-ad-and-introducing-powerzure-ca70b330511a>)

## Undetected Azure Active Directory Brute-Force Attacks

- <https://www.secureworks.com/research/undetected-azure-active-directory-brute-force-attacks> (<https://www.secureworks.com/research/undetected-azure-active-directory-brute-force-attacks>)

## How Azure AD Could Be Vulnerable to Brute-Force and DOS Attacks

- <https://medium.com/hackernoon/azure-brute-force-17e27dc05f85> (<https://medium.com/hackernoon/azure-brute-force-17e27dc05f85>)

## How to bypass MFA in Azure and O365

- <https://secwise.be/how-to-bypass-mfa-in-azure-and-o365-part-1/> (<https://secwise.be/how-to-bypass-mfa-in-azure-and-o365-part-1/>)

## AWS Security Tools

- <https://github.com/toniblyx/my-arsenal-of-aws-security-tools> (<https://github.com/toniblyx/my-arsenal-of-aws-security-tools>)
- <https://github.com/blackbotsecurity/AWS-Attack> (<https://github.com/blackbotsecurity/AWS-Attack>)
- <https://github.com/aws-labs/aws-cloudsaga> (<https://github.com/aws-labs/aws-cloudsaga>)
- <https://github.com/aws-labs/aws-support-tools> (<https://github.com/aws-labs/aws-support-tools>)
- <https://github.com/0xVariable/AWS-Security-Tools> (<https://github.com/0xVariable/AWS-Security-Tools>)
- <https://cybersecurityup.github.io/awstrm/index.html> (<https://cybersecurityup.github.io/awstrm/index.html>)
- <https://github.com/daft-hack/CloudPentestCheatsheets/blob/master/cheatsheets/AWS.md> (<https://github.com/daft-hack/CloudPentestCheatsheets/blob/master/cheatsheets/AWS.md>)
- <https://github.com/RhinoSecurityLabs/cloudgoat> (<https://github.com/RhinoSecurityLabs/cloudgoat>)

## Azure Security Tools

- <https://github.com/NetSPI/MicroBurst/blob/master/Misc/Invoke-EnumerateAzureBlobs.ps1>  
(<https://github.com/NetSPI/MicroBurst/blob/master/Misc/Invoke-EnumerateAzureBlobs.ps1>).
- <https://microsoft.github.io/Azure-Threat-Research-Matrix/> (<https://microsoft.github.io/Azure-Threat-Research-Matrix/>).
- <https://github.com/Cloud-Architekt/AzureAD-Attack-Defense> (<https://github.com/Cloud-Architekt/AzureAD-Attack-Defense>).
- <https://github.com/daftack/CloudPentestCheatsheets/blob/master/cheatsheets/Azure.md>  
(<https://github.com/daftack/CloudPentestCheatsheets/blob/master/cheatsheets/Azure.md>).
- <https://github.com/Kyuu-Ji/Awesome-Azure-Pentest/blob/main/README.md> (<https://github.com/Kyuu-Ji/Awesome-Azure-Pentest/blob/main/README.md>).
- <https://github.com/ine-labs/AzureGoat> (<https://github.com/ine-labs/AzureGoat>).
- <https://github.com/kmcquade/awesome-azure-security> (<https://github.com/kmcquade/awesome-azure-security>).
- <https://github.com/nccgroup/azucar> (<https://github.com/nccgroup/azucar>).