MULTI-CLOUD RED TEAM – PT.1

JOAS ANTONIO

AWS RED TEAM

AWS – Enumerationg and Design

- https://rhinosecuritylabs.com/aws/aws-role-enumeration-iam-p2/
- https://securityonline.info/aws-enumerator-aws-service-enumeration/
- https://pentestbook.six2dez.com/enumeration/cloud/aws
- https://sidechannel.blog/en/enumerating-services-in-aws-accounts-in-an-anonymous-and-unauthenticated-manner/index.html
- https://www.youtube.com/watch?v=gNXXfNZp3ik
- https://book.hacktricks.xyz/pentesting/pentesting-web/buckets/aws-s3
- https://subscription.packtpub.com/book/security/9781839216923/5/ch05lvl1sec23/enumerating-and-understanding-aws-services
- https://www.virtuesecurity.com/aws-penetration-testing-part-2-s3-iam-ec2/

AWS – Exploit Lambda

- https://medium.com/r3d-buck3t/vulnerable-lambda-leaks-aws-account-information-c613837377ad
- https://security.snyk.io/vuln/SNYK-JS-AWSLAMBDA-540839
- https://docs.aws.amazon.com/lambda/latest/dg/security-configuration.html
- https://unit42.paloaltonetworks.com/gaining-persistency-vulnerable-lambdas/
- https://www.darkreading.com/cloud/securing-serverless-attacking-an-aws-account-via-a-lambda-function
- https://thetestlabs.io/code/exploiting-common-serverless-security-flaws-in-aws/
- https://github.com/torque59/AWS-Vulnerable-Lambda
- https://blog.aquasec.com/aws-lambda-security
- http://blog.blueinfy.com/2018/11/lambda-post-exploitation-devil-in.html
- https://www.trendmicro.com/en_be/devops/21/g/security-for-aws-lambda-serverless-applications.html

AWS – Pivoting and Lateral Movement

- https://www.youtube.com/watch?v=2NF4LjjwoZw
- https://twitter.com/andresriancho/status/1181360103213211648
- https://www.kentik.com/resources/aws-vpc-flow-logs-for-kentik/
- https://orca.security/solutions/threat/lateral-movement/
- https://www.chrisfarris.com/post/lateral-movement-aws/
- https://www.crowdstrike.com/resources/videos/aws-lateral-movement-attack/
- https://www.youtube.com/watch?v=V54lRz3YgBY
- https://sysdig.com/blog/lateral-movement-cloud-containers/
- https://orca.security/solutions/threat/lateral-movement/

Repositore Full

- https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Cloud%20-%20AWS%20Pentest.md
- https://github.com/CyberSecurityUP/Awesome-Cloud-PenTest
- https://github.com/jassics/awesome-aws-security
- https://buckets.grayhatwarfare.com/

AZURE RED TEAM

Azure - Enumeration

- https://github.com/chryzsh/DarthSidious/blob/master/enumeration/azure-enumeration.md
- https://adsecurity.org/?tag=azure-ad-account-enumeration
- https://pentestbook.six2dez.com/enumeration/cloud/azure
- https://www.netspi.com/blog/technical/cloud-penetration-testing/enumerating-azure-services/
- https://www.youtube.com/watch?v=8D3c70Yv4jo
- https://securityonline.info/azurite-enumeration-reconnaissance-microsoft-azure-cloud/
- https://www.pentestpartners.com/security-blog/azure-ad-attack-of-the-default-config/
- https://www.sandeepseeram.com/post/azure-pentesting
- https://www.youtube.com/watch?v=C_2Yfl8AMTY

Azure - Exploitation

- https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Cloud%20-%20Azure%20Pentest.md
- https://www.getastra.com/blog/security-audit/azure-penetration-testing/
- https://www.redteamsecure.com/penetration-testing/azure-penetration-testing

Azure – Lateral Movement and Pivoting

- https://www.xmcyber.com/privilege-escalation-and-lateral-movement-on-azure-part-1/
- https://www.xmcyber.com/privilege-escalation-and-lateral-movement-on-azure-part-2/
- https://posts.specterops.io/death-from-above-lateral-movement-from-azure-to-on-prem-ad-d18cb3959d4d
- https://www.netspi.com/blog/technical/cloud-penetration-testing/lateral-movement-azure-app-services/
- https://jeffreyappel.nl/protecting-against-lateral-movement-with-defender-for-identity-and-monitor-with-azure-sentinel/
- https://medium.com/@talthemaor/lateral-movement-graph-for-azure-ad-7c5e0136e2d8
- https://blog.ahasayen.com/azure-advanced-threat-protection-lateral-movement/
- https://stealthbits.com/blog/lateral-movement-to-the-cloud-pass-the-prt/
- https://azureinfohub.azurewebsites.net/ContentItems/Details/22484
- https://m365internals.com/2021/11/30/lateral-movement-with-managed-identities-of-azure-virtual-machines/
- https://www.linkedin.com/pulse/use-azure-sentinel-mitigate-lateral-movement-farhan-nadeem/
- https://btcyber.net/managing-inside-threats-azure-atp/

GCP RED TEAM

GCP – Enumeration

- https://notsosecure.com/cloud-services-enumeration-aws-azure-and-gcp
- https://rhinosecuritylabs.com/gcp/google-cloud-platform-gcp-bucket-enumeration/
- https://book.hacktricks.xyz/cloud-security/gcp-security/gcp-compute-enumeration
- https://cloud.google.com/dotnet/docs/reference/Google.Cloud.Metastore.V1Beta/latest/Google.Cloud.Metastore.V1Beta.Service.Types.State
- https://pentestbook.six2dez.com/enumeration/cloud/gcp
- https://medium.com/@tomaszwybraniec/google-cloud-platform-pentest-notes-service-accounts-b960dc59d93a
- https://github.com/RhinoSecurityLabs/GCPBucketBrute
- https://about.gitlab.com/blog/2020/02/12/plundering-gcp-escalating-privileges-in-google-cloud-platform/

GCP – Exploitation

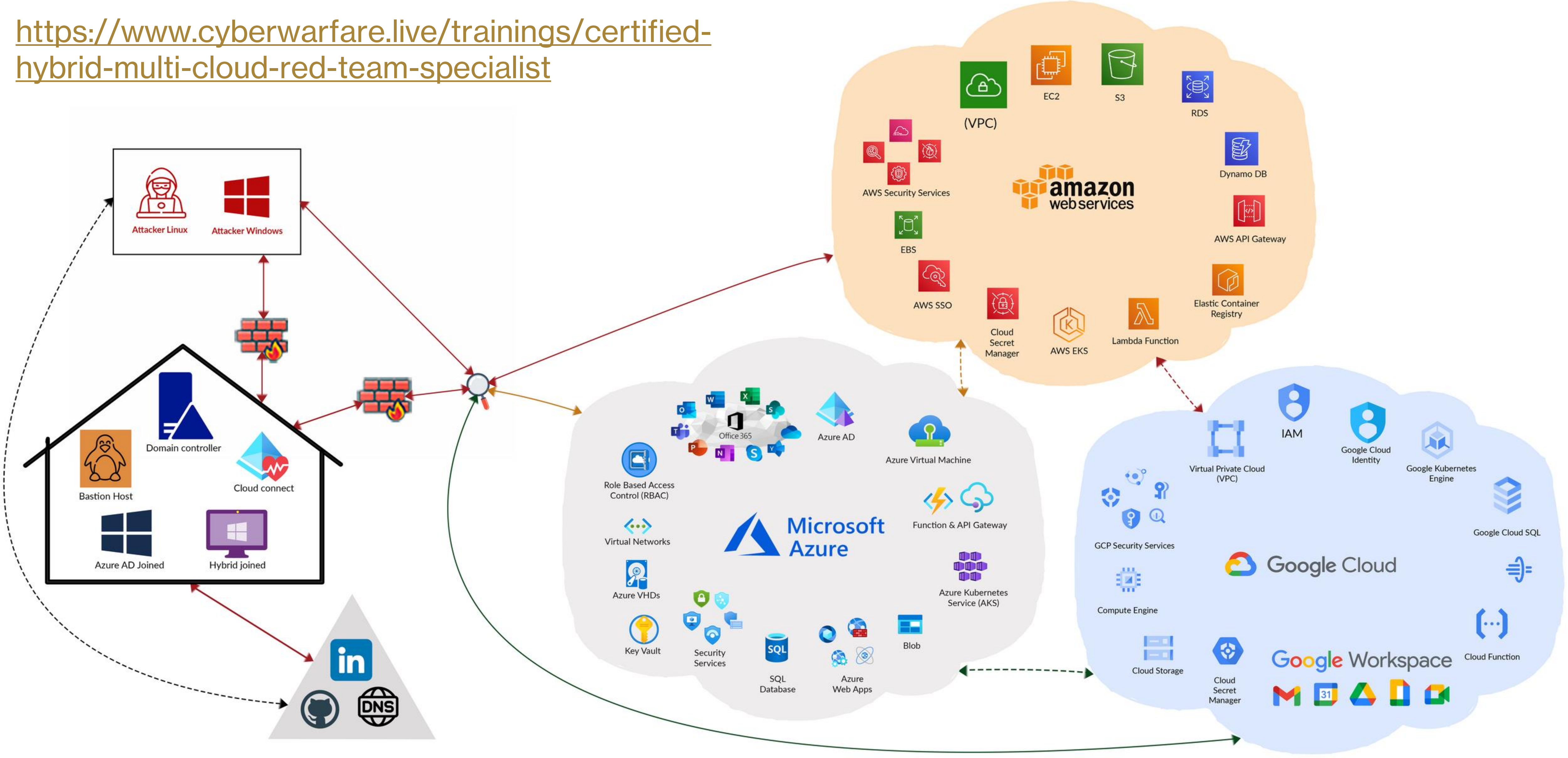
- https://www.4armed.com/blog/hacking-kubelet-on-gke/
- https://rhinosecuritylabs.com/cloud-security/kubelet-tls-bootstrap-privilege-escalation/
- https://security.googleblog.com/2020/05/expanding-our-work-with-open-source.html
- https://www.darknet.org.uk/2021/01/gke-auditor-detect-google-kubernetes-engine-misconfigurations/
- https://blog.appsecco.com/kubernetes-from-an-attackers-perspective-owasp-bay-area-meetup-c0c78a5bfb4e
- https://infosecwriteups.com/pentest-notes-google-cloud-edition-2e138bb0f504
- https://cobalt.io/blog/what-a-pentester-learned-from-becoming-google-cloud-architect-certified
- https://cloud.google.com/architecture/security-controls-and-forensic-analysis-for-GKE-apps
- https://rhinosecuritylabs.com/assessment-services/gcp-penetration-testing/
- https://securetriad.io/gcp-penetration-testing/

GCP – Lateral Movement and Pivoting

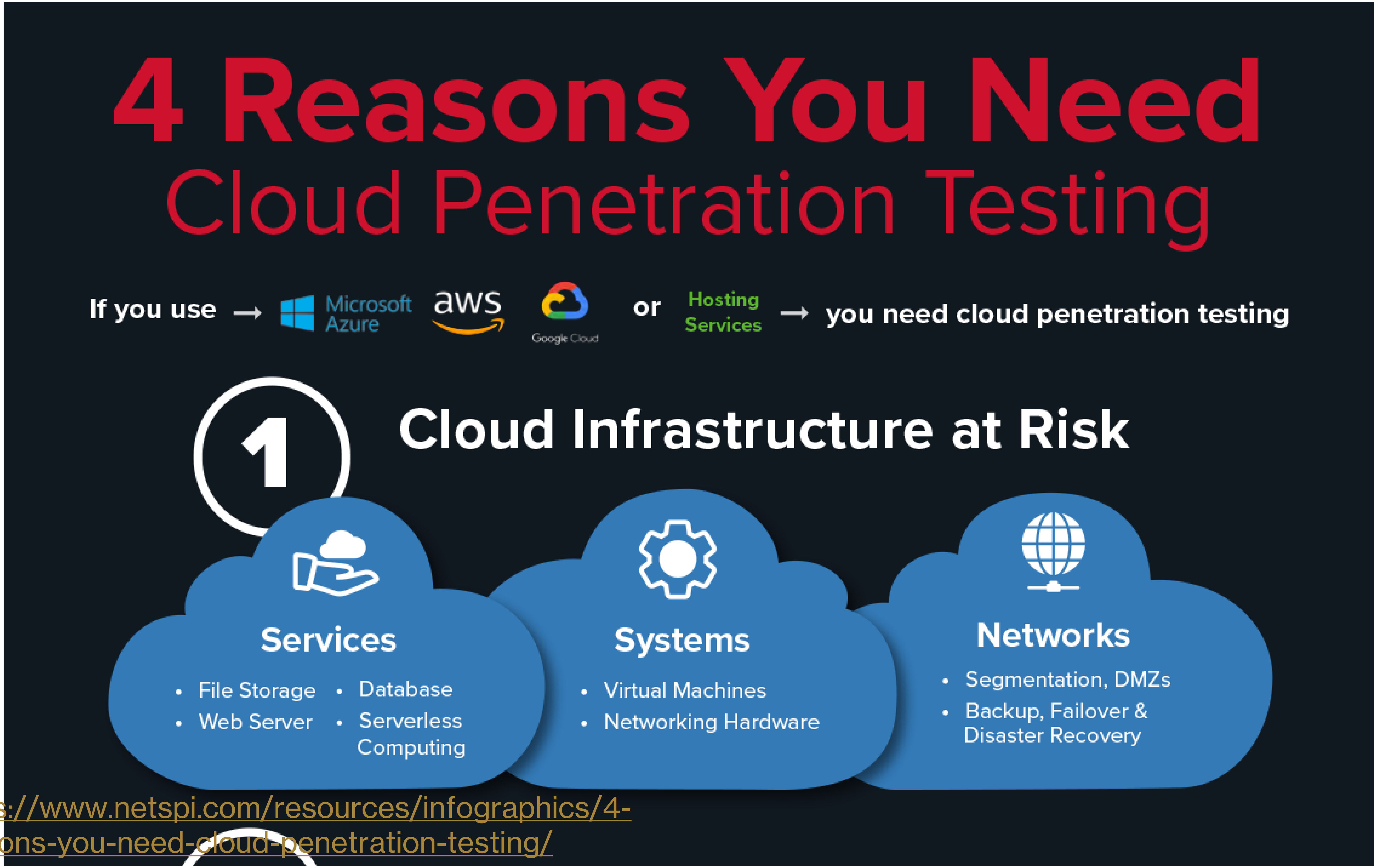
- https://rhinosecuritylabs.com/gcp/privilege-escalation-google-cloud-platform-part-1/
- https://rhinosecuritylabs.com/gcp/iam-privilege-escalation-gcp-cloudbuild/
- https://book.hacktricks.xyz/cloud-security/gcp-security
- https://github.com/RhinoSecurityLabs/GCP-IAM-Privilege-Escalation

RED TEAMING IN HYBRID MULTI CLOUD ENVIRONMENT

https://www.cyberwarfare.live/trainings/certified-hybrid-multi-cloud-red-team-specialist



REASONS AUDIT CLOUD



4 Reasons You Need Cloud Penetration Testing

If you use → Microsoft Azure aws Google Cloud or Hosting Services → you need cloud penetration testing

1 Cloud Infrastructure at Risk

Services

- File Storage
- Web Server
- Database
- Serverless Computing

Systems

- Virtual Machines
- Networking Hardware

Networks

- Segmentation, DMZs
- Backup, Failover & Disaster Recovery

https://www.netspi.com/resources/infographics/4-reasons-you-need-cloud-penetration-testing/

CLOUD PENTEST

- https://www.youtube.com/watch?v=aqumgrSBDM4
- https://www.youtube.com/watch?v=lOhvlooWzOg
- https://www.youtube.com/watch?v=fiSJQfiS21c
- https://www.youtube.com/watch?v=A7mZ6bJs7CY
- https://www.youtube.com/watch?v=pKpaXhsVMol
- https://www.youtube.com/watch?v=mRhJjdlR9Xk