
NT KONF
25. – 27.
SEPTEMBER
2023
PORTOROŽ
NT KONF
NT KONFERENCA

25. – 27.
SEPTEMBER
2023
PORTOROŽ

Pentesting in the Cloud

Saša Kranjac MVP, RD

Saša Kranjac

CEO @ Kloudatech

Microsoft Regional Director

Microsoft Security MVP | Microsoft Azure MVP

Microsoft Certified Trainer (MCT) | MCT Regional Lead

Certified EC-Council Instructor (CEI)

CompTIA Instructor

www.kloudatech.com

www.sasakranjac.com

X: @SasaKranjac

KLOUDATECH
www.kloudatech.com

CompTIA Authorized Partner | DELIVERY PARTNER

Microsoft REGIONAL DIRECTOR

MVP Microsoft® Most Valuable Professional

Microsoft MCT

C|EI Certified EC-Council Instructor

NT KONF NT KONFERENCA

#ntk23

The plan is to talk about:

- What's that?
- (Cloud) penetration testing authorization
- Threat actor types and attack vectors
- Steps and frameworks
- Discovery and exploits

What's that?

- **Penetration testing** or a **pentest** is a simulated cyber attack against a (computer) system to validate exploitable vulnerabilities
- **Pentesting** is a cybersecurity forensics technique that may discover vulnerabilities not found during the automated scanning and through other part of the overall risk assessment
- Penetration testing ≠ Vulnerability assessment
- Penetration testing **enables** (more complete) vulnerability assessment

(Cloud) Penetration Testing Authorization

Cloud penetration testing authorization

- What are you allowed to test?
- Most cloud providers allow pentesting **without** notifying and/or submitting a written request
- **Important!** Always check before performing a penetration test
- Usually, try to avoid extrecmes of (or completely avoid!):
  - **Fuzzing** (finding program failures (code errors) by supplying malformed input data to program interfaces (entry points) that parse and consume this data (e.g. file, network, registry, shared memory parsers)
  - **Phishing**
  - Assets **other than** yours
  - **Any** kind of **DoS** (Denial of Service attacks)
  - Port scanning

Azure pentesting

As of June 15, 2017, Microsoft no longer requires pre-approval to conduct a penetration test against Azure resources. This process is only related to Microsoft Azure, and not applicable to any other Microsoft Cloud Service.

> ⓘ **Important**
>
> While notifying Microsoft of pen testing activities is no longer required customers must still comply with the Microsoft Cloud Unified Penetration Testing Rules of Engagement.

- https://learn.microsoft.com/en-us/azure/security/fundamentals/pen-testing
- https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement
- https://learn.microsoft.com/en-us/security/benchmark/azure/security-control-penetration-tests-red-team-exercises

Azure pentesting

- Standard tests you can perform include:
  - Tests on your endpoints to uncover the Open Web Application Security Project (OWASP) top 10 vulnerabilities
  - Fuzz testing of your endpoints
  - Port scanning of your endpoints

One type of pen test that you **can't perform** is **any** kind of **Denial of Service (DoS) attack.**

You may only simulate attacks using Microsoft approved testing partners:

- **BreakingPoint Cloud**: A self-service traffic generator where your customers can generate traffic against DDoS Protection-enabled public endpoints for simulations.
- **Red Button**: Work with a dedicated team of experts to simulate real-world DDoS attack scenarios in a controlled environment.
- **RedWolf** a self-service or guided DDoS testing provider with real-time control.

Azure pentesting – Prohibited Actions

The following is **prohibited** by Microsoft:

- Scanning or conducting tests on **other** Azure customer assets
- Accessing data that is not **completely yours**
- Conducting **any** DDoS attacks
- Conducting **any intensive** network **fuzzing** against Azure virtual machines
- **Any** tests that generate a **huge amount of traffic** through automated testing methods
- Attempt **phishing** or any **social engineering attacks** on Microsoft's employees
- Utilizing **any** services that **violate** the **acceptable usage policies** as mentioned in the online usage terms

Azure pentesting – Allowed/Encouraged Actions

The following is **allowed/encouraged** by Microsoft:

- Create multiple test or trial accounts to test cross-account access vulnerabilities. Using these to access **other** customer's data is **prohibited**.
- Running vulnerability scanning tools, port scan, or fuzz on **your virtual machine**.
- Testing **your account** by generating traffic which is expected to match regular working periods and can also include surge capacity.
- Try to break out of Azure services to access **other** customer assets. If any vulnerability is found, inform Microsoft and **stop** any further tests.
- Test Microsoft Intune to ensure all restrictions function as expected.

Amazon Web Services (AWS) pentesting

- https://aws.amazon.com/security/penetration-testing/

AWS Customer Support Policy for Penetration Testing

AWS customers are welcome to carry out security assessments or penetration tests against their AWS infrastructure without prior approval for 8 services, listed in the next section under “Permitted Services.”

Please ensure that these activities are aligned with the policy set out below. Note: Customers are not permitted to conduct any security assessments of AWS infrastructure, or the AWS services themselves. If you discover a security issue within any AWS services in the course of your security assessment, please **contact AWS Security** immediately.

Amazon Web Services (AWS) pentesting

Permitted Services

- Amazon EC2 instances, NAT Gateways, and Elastic Load Balancers
- Amazon RDS
- Amazon CloudFront
- Amazon Aurora
- Amazon API Gateways
- AWS Fargate
- AWS Lambda and Lambda Edge functions
- Amazon Lightsail resources
- Amazon Elastic Beanstalk environments

Prohibited Activities

- DNS zone walking via Amazon Route 53 Hosted Zones
- Denial of Service (DoS), Distributed Denial of Service (DDoS), Simulated DoS, Simulated DDoS (These are subject to the DDoS Simulation Testing policy)
- Port flooding
- Protocol flooding
- Request flooding (login request flooding, API request flooding)

Google Cloud Platform (GCP) pentesting

- https://support.google.com/cloud/answer/6262505?hl=en

Cloud Security FAQ

Here you will find answers to some Frequently Asked Questions related to Security and Compliance on Google Cloud Platform.

For more information about security of the platform and its products, please see Google Cloud Platform Security and Compliance

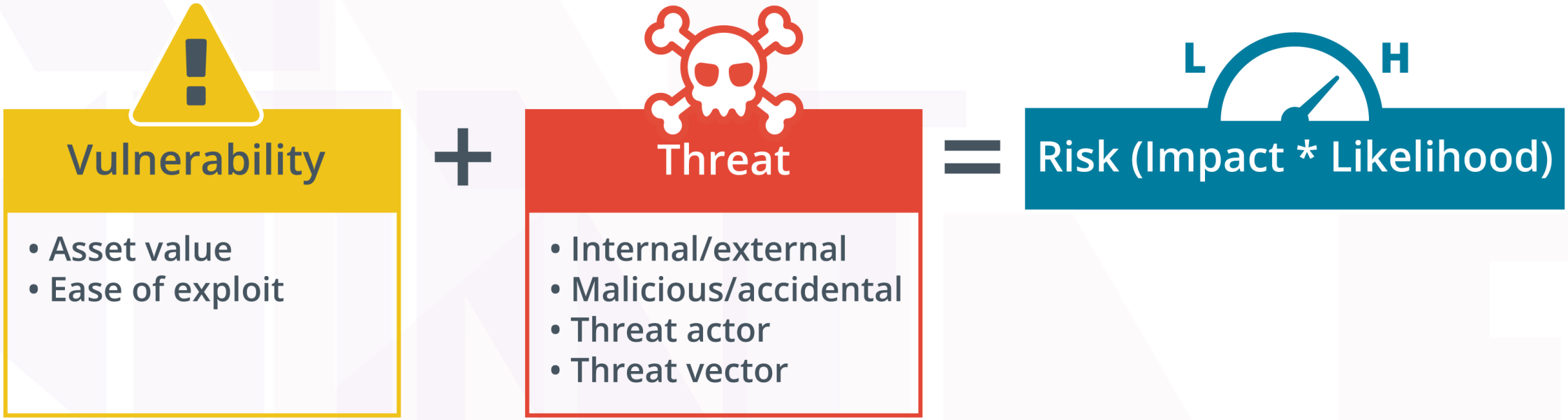
Penetration testing

Do I need to notify Google that I plan to do a penetration test on my project?

If you plan to evaluate the security of your Cloud Platform infrastructure with penetration testing, you are not required to contact us. You will have to abide by the Cloud Platform Acceptable Use Policy and Terms of Service, and ensure that your tests only affect your projects (and not other customers' applications). If a vulnerability is found, please report it via the Vulnerability Reward Program.

Threat Actor Types And Attack Vectors

Vulnerability, Threat, and Risk



Attributes of Threat Actors

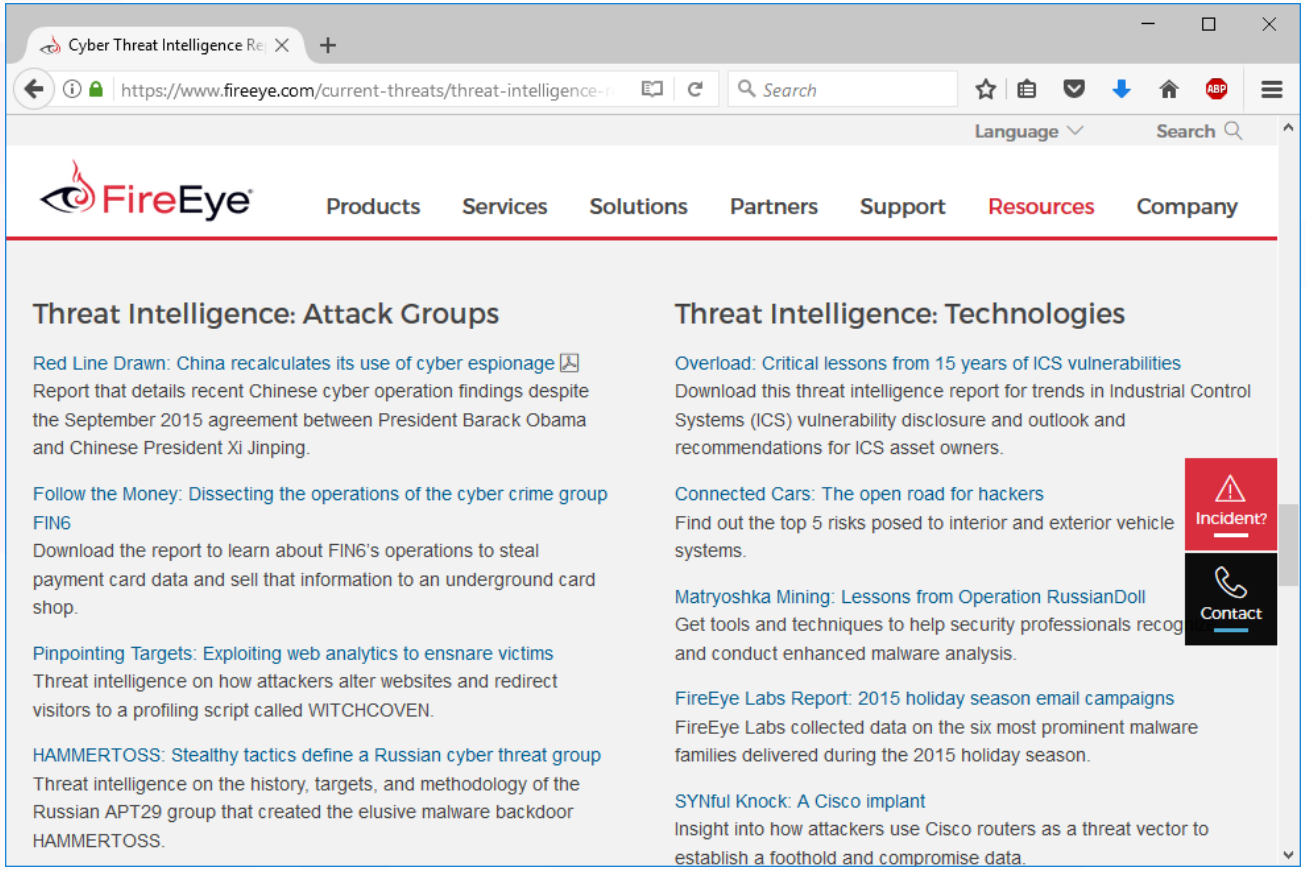
- Known threats versus adversary behaviors
- Internal/external
- Intent/motivation
  - Maliciously targeted versus opportunistic
  - Accidental/unintentional
- Level of sophistication
  - Resources/funding
  - Adversary capability levels

Hackers, Script Kiddies, and Hacktivists

- The "Lone Hacker"
  - White hats versus black hats versus gray hats
  - Authorized versus non-authorized versus semi-authorized
- Script kiddies
- Hacker teams and hacktivists

State Actors and Advanced Persistent Threats

- State-backed groups
  - Attached to military/secret services
  - Highly sophisticated
- Advanced Persistent Threat (APT)
- Espionage and strategic advantage
- Deniability
- False flag operations



NT KONF
NT KONFERENCA

Insider Threat Actors

- Malicious insider threat
  - Has or has had authorized access
  - Employees, contractors, partners
  - Sabotage, financial gain, business advantage
- Unintentional insider threat
  - Weak policies and procedures
  - Weak adherence to policies and procedures
  - Lack of training/security awareness
  - Shadow IT

Attack Surface and Vectors

- Attack surface
  - Points where an attacker can discover/exploit vulnerabilities in a network or application
- Vectors
  - Direct access
  - Removable media
  - Email
  - Remote and wireless
  - Supply chain
  - Web and social media
  - Cloud

TOP Attack vectors TODAY

- Compromised Credentials
- Weak and Stolen Credentials
- Malicious Insiders
- Missing or Poor Encryption
- Ransomware
- Misconfiguration
- Phishing

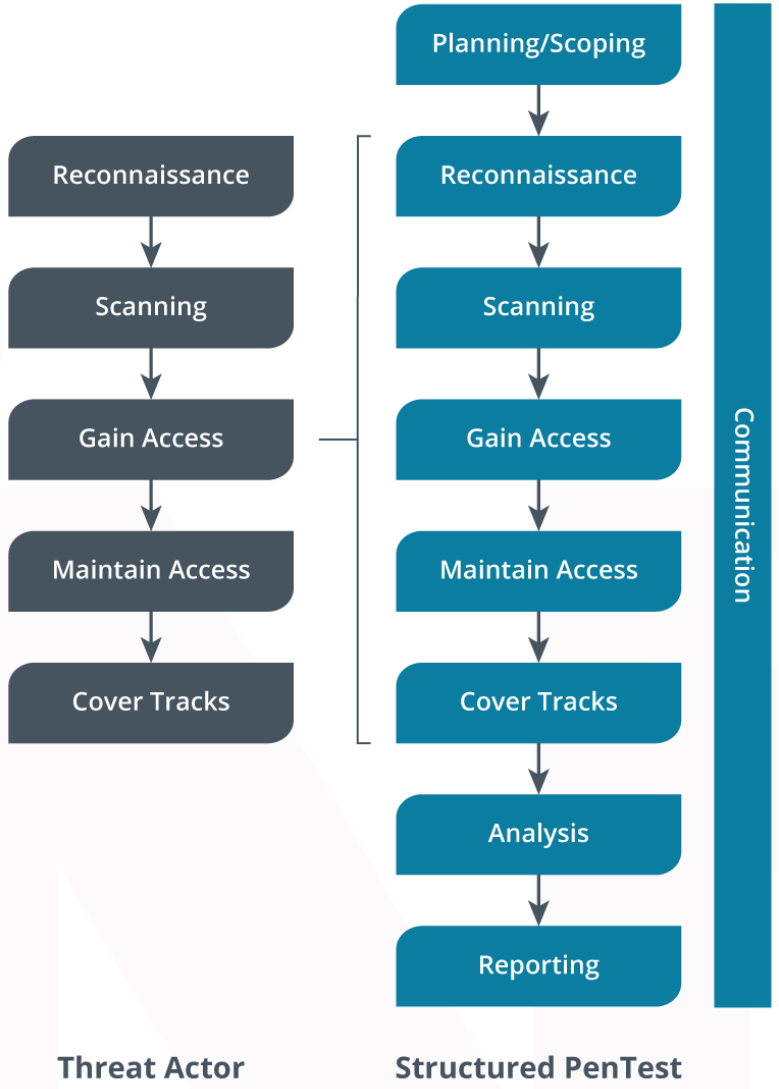
Steps and Frameworks

Pentesting steps

- **Planning and scoping** – outline a plan for the PenTest.
- **Reconnaissance** gather information about the target.
- **Scanning** – identify live hosts, listening ports, and running services.
- **Gaining access** – see how deep into the network they can travel.
- **Maintaining access** – maintain access undetected for as long as possible
- **Covering tracks** – removes any evidence that the team was in the system
- **Analysis** - analyze the findings and derive a summary of the risk rating
- **Reporting** – deliver the results

Pentesting steps

- Pentesting Team
  - Main goal – test infrastructure's defenses
- Threat Actor
  - Main goal - change the integrity of the system



Pentesting Frameworks

- A complete assessment will discover system weaknesses
- Many resources available that provide guidance on how to conduct an effective PenTesting exercise:
  - The Open Web Application Security Project (**OWASP**)
  - National Institute of Science and Technology (**NIST**)
  - Open-source Security Testing Methodology Manual (**OSSTMM**)

Structure and guidance

- Several organizations have developed structured guidelines and best practices to accomplish a PenTesting exercise.
  - **ISSAF** - open-source resource available to cybersecurity professionals.
  - **PTES** - provide a comprehensive overview of the proper structure of a complete PenTest.
  - **MITRE** provides research, publications, and tools at no charge for anyone who accesses the site.

MITRE ATT&CK

- ATT&CK - Adversarial Tactics, Techniques & Common Knowledge
- Provides tools and techniques specific to PenTesting.
- Contains categories that list tasks completed during a PenTest:
  - **Initial Access** lists attack vectors used to gain access to a network.
  - **Persistence** provides details on how to remain in a system.
  - **Credential access** provides solutions on how to obtain credentials

Investigating CVE and CWE

- **CVE** - Common Vulnerabilities and Exposures is a listing of all publicly disclosed vulnerabilities.
  - Each entry refers to specific vulnerability of a particular product
  - Is cataloged with the name and description of the vulnerability
- **CWE** - Common Weakness Enumeration is a database of software-related weaknesses maintained by the MITRE Corporation

Discovery and Exploits

Open-source Intelligence Tools (OSINT)

- Using **OSINT** is critical to the preliminary phases of a Pentest
- Used during the reconnaissance phase to gather information from freely and publicly available sources, for a more targeted discovery.
- Allows the team to discreetly gather information on the target without signaling any flags.

Searching Metadata

- Metadata is information stored or recorded as a property of an object, state of a system, or transaction.
  - Metadata entries can expose sensitive information!
- Two tools that aid in the discovery of metadata are **Metagoofil** and Fingerprinting Organizations with Collected Archives (**FOCA**).

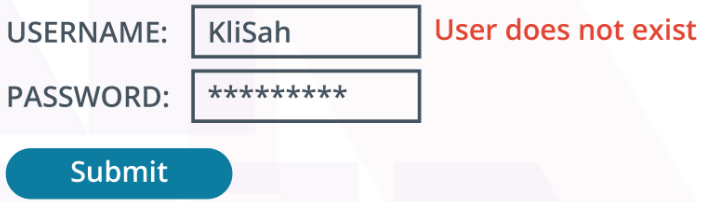
Searching Metadata with Metagoofil

- Metagoofil scrapes metadata, such as the author, company, title, and subject, from public documents on the target website(s)
- The output is then displayed in a standard browser using HTML
- When searching, commands will control the type of data:
  - Using **-d microsoft.com** will scan for documents on microsoft.com
  - Using **-t pdf** will scan for pdf documents
  - Using **-l 75** will search for 75 documents

Fingerprinting with FOCA

- A GUI tool used to discover metadata that may be hidden within documents, typically those downloaded from the web.
- Can work with a variety of document types
  - MS Office along with the OpenDocument format
  - PDFs and graphical design file types (SVG)
- Some of the useful metadata FOCA can extract includes:
  - User and people names, software and OS version information, printer information, and plaintext passwords

Monitoring Responses on a Login Page



If prompt returns "User does not exist," this verifies the username is not in the database

If prompt returns "Password is incorrect," this verifies the username is in the database

Collecting Data with theHarvester

- Can automate the information gathering tasks by using:
  - Google and Bing to gather information from public data sources.
  - Comodo's certificate search engine to obtain certificate information.
  - Social media sites like Twitter and LinkedIn.
  - Banner grabbing functionality using Shodan.
- theHarvester gathers information on the following:
  - Subdomain names, Employee names, Email addresses
  - PGP key entries, Open ports and service banners

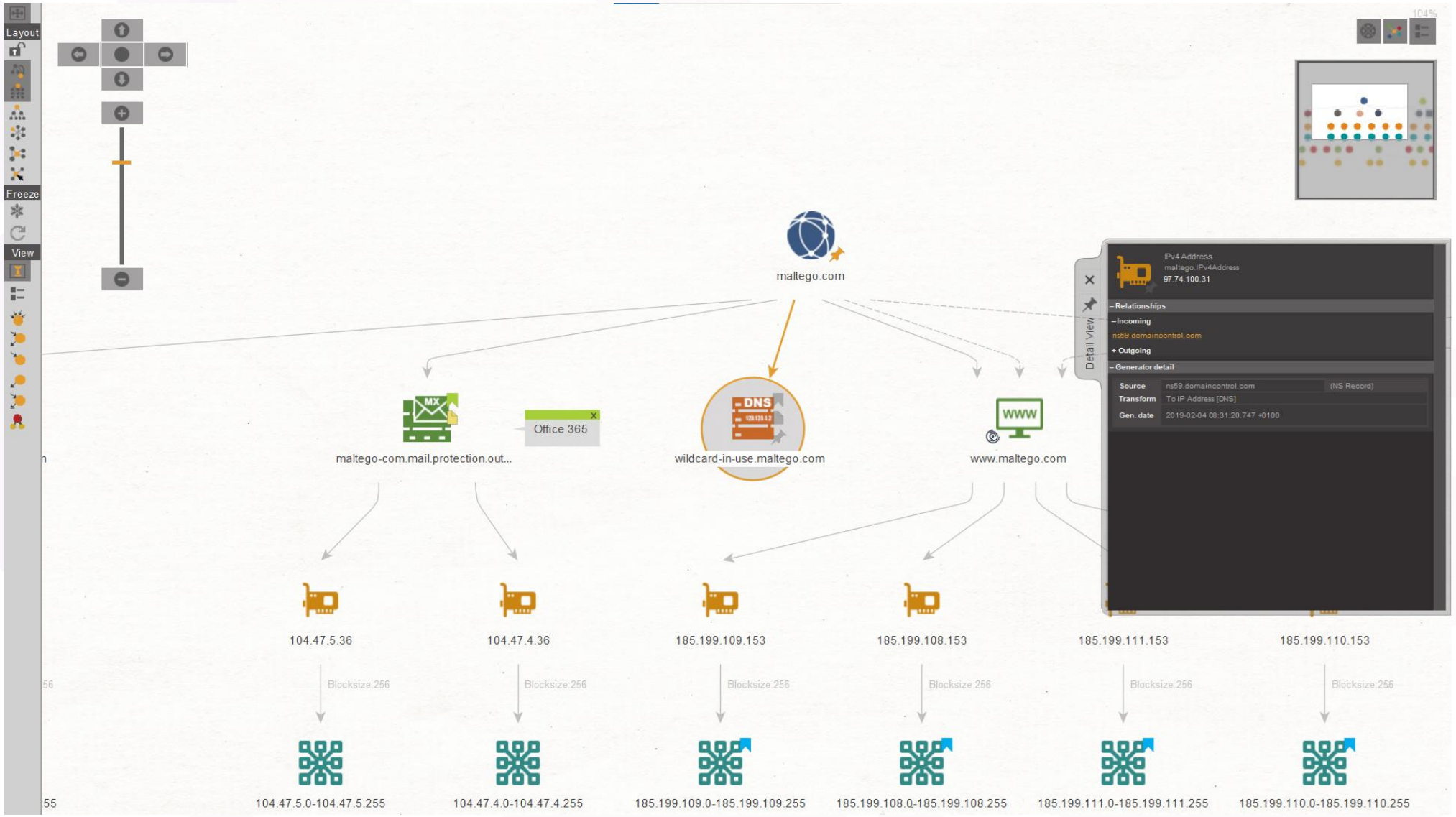
Collecting Data with theHarvester

- When using theHarvester, enter the target domain and the data source.
- The data can be used in an exploit, such as a Spearphishing attack.

Gathering with Recon-ng

- Recon-ng uses various modules to customize the search:
  - Whois query to identify points of contact
  - PGP key search
  - File crawler.
  - Social media profile associations.
  - DNS record enumerator
  - Check if the account has been associated with a breach.

Maltego and its Graph, and a lot more...



Searching with Shodan

- Shodan is a search engine designed to locate and index IoT devices that are connected to the Internet.
- Traffic lights, industrial control systems (ICSs), and other devices that have Internet connectivity and are part of the IoT.
- Shodan can be useful to the PenTest reconnaissance phase :
  - The team can locate the feed of a security camera outside the target organization's office to get a better picture of the premises and its defenses.
  - If the target organization employs control systems, the team may be able to manipulate these remotely as part of the attack phase.

Recon Tools

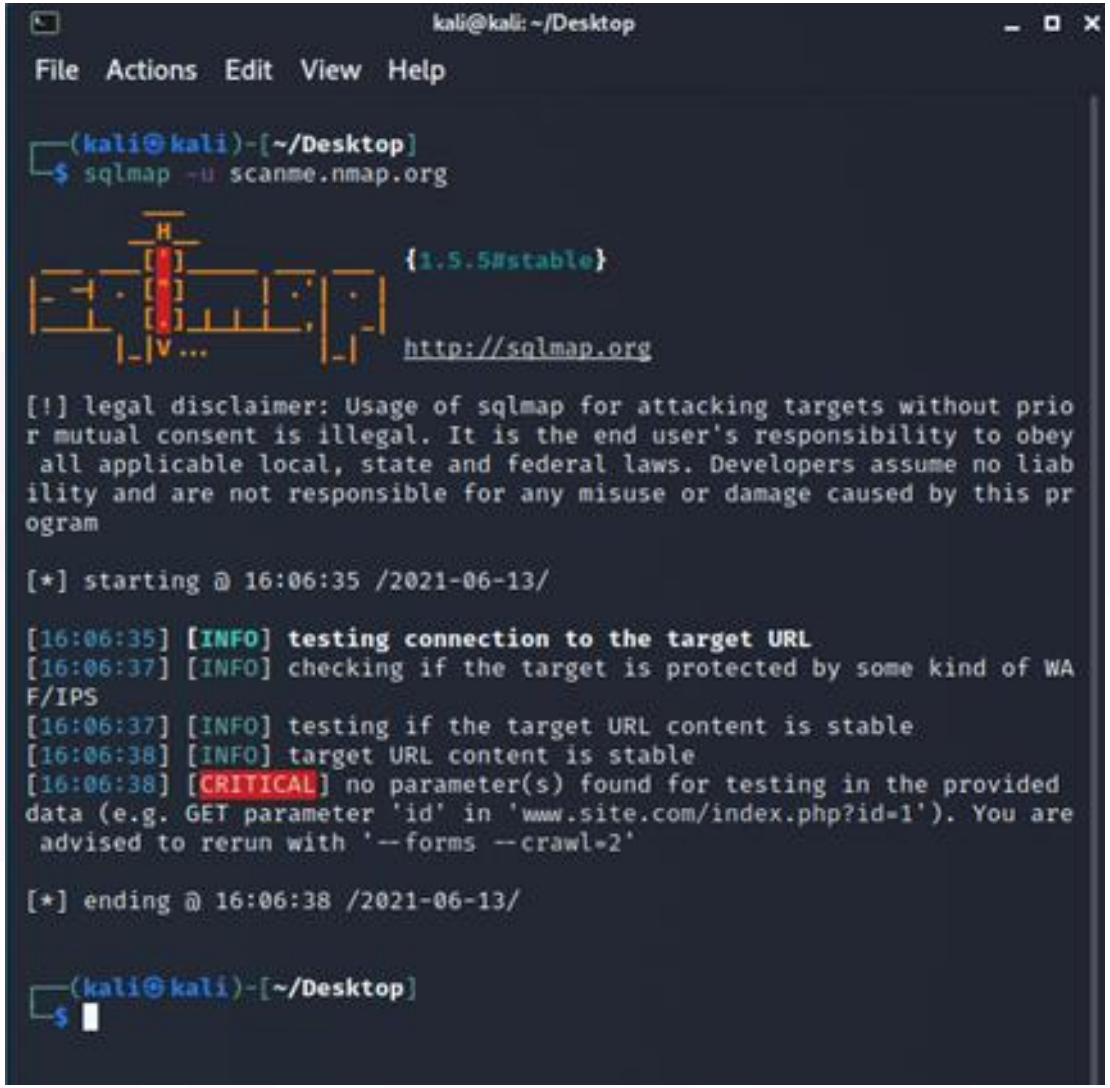
- Recon-NG | https://github.com/lanmaster53/recon-ng
- OWASP Amass | https://github.com/OWASP/Amass
- Spiderfoot | https://www.spiderfoot.net/
- Gobuster | https://github.com/OJ/gobuster
- Sublist3r | https://github.com/aboul3la/Sublist3r

Scanning the Web Server and Database

- Some possibilities for scanning include:
  - Web server on TCP 80 or 443 for server-specific vulnerabilities
  - Servers that run on nonstandard ports
  - Web applications for SQL-injection-related vulnerabilities
- There are many web application vulnerability scanners available:
  - Arachni, Skipfish, Grabber, Wapiti, OWASP ZAP, and Metasploit Pro.

SQLmap

- An open-source database scanner
- Locates and exploits SQL injection flaws.



Checking SSL/TLS Vulnerabilities

- Most websites today rely on cryptographic concepts such as SSL/TLS to protect data in transit from exposure.
- As a result, the team will also want to check for vulnerabilities:
  - **Logjam** vulnerability can weaken the encryption complexity
  - **Freak** vulnerability attacks the RSA-export keys and can allow a malicious actor to decrypt the communication stream
  - **Poodle** vulnerability alters the way SSL 3.0 handles block cipher mode padding to be able to select content within the SSL session

AWS S3 Buckets

- Amazon Simple Storage Service (S3)
- Storage service that is “secure by default”
- Configuration issues tend to unsecure buckets by making them publicly accessible
- Nslookup can help reveal region
- Use S3Scanner, lazys3, Bucket Finder, and s3-buckets-bruteforcer, to find the target AWS S3 buckets
    - S3 URL Format:
        - https://[bucketname].s3.amazonaws.com
        - https://s3-[region].amazonaws.com/[Org Name]
        - # aws s3 ls s3://<bucketname>/ --region <region>

AWS S3 Buckets

- Identify vulnerable S3 buckets

aws s3 ls s3://[bucket_name] aws s3 ls s3://[bucket_name] --no-sign-request

- Exploit S3 buckets

Reading Files ⟶ aws s3 ls s3://[bucket_name] --no-sign-request

Moving Files ⟶ aws s3 mv FileName s3://[bucket_name]/test-file.txt - -no-sign-request

Copying Files ⟶ aws s3 cp FileName s3://[bucket_name]/test-file.svg - -no-sign-request

Deleting Files ⟶ aws s3 rm s3://[bucket_name]/test-file.svg --no-sign-request

EBS Volumes

- Elastic Block Store (EBS)
- AWS virtual hard disks
- Can have similar issues to S3 being publicly available
- Dufflebag from Bishop Fox
  - https://github.com/bishopfox/dufflebag
- Difficult to target specific org but can find widespread leaks

Data in Public Azure Blobs

- Microburst
  - https://github.com/NetSPI/MicroBurst
- Invoke-EnumerateAzureBlobs
  - Brute forces storage account names, containers, and files
  - Uses permutations to discover storage accounts
- PS > Invoke-EnumerateAzureBlobs –Base <base name>

```
PS C:\Users\beau\Desktop\MicroBurst-master\MicroBurst-master> Invoke-EnumerateAzureBlobs -Base glitchcloud
Found Storage Account -  glitchcloud.blob.core.windows.net

Found Container - glitchcloud.blob.core.windows.net/confidential
       Public File Available: https://glitchcloud.blob.core.windows.net/confidential/secret.txt
```

Password Attacks

- Use MSOLSpray to do this:
  - https://github.com/dafthack/MSOLSpray
- The script logs if:
  - a user cred is valid
  - MFA is enabled on the account
  - a tenant doesn't exist
  - a user doesn't exist
  - the account is locked
  - the account is disabled
  - the password is expired

Create backdoor accounts in AWS

- **Endgame** - an exploitation framework that helps attackers gain control over an existing AWS cloud platform through a rogue account and create a backdoor account
- List the IAM resources with the user account:

  endgame list-resources -s iam
- List S3 buckets:

  endgame list-resources --service s3
- List resources across the services:

  endgame list-resources --service all
- Create a backdoor to a specific resource:

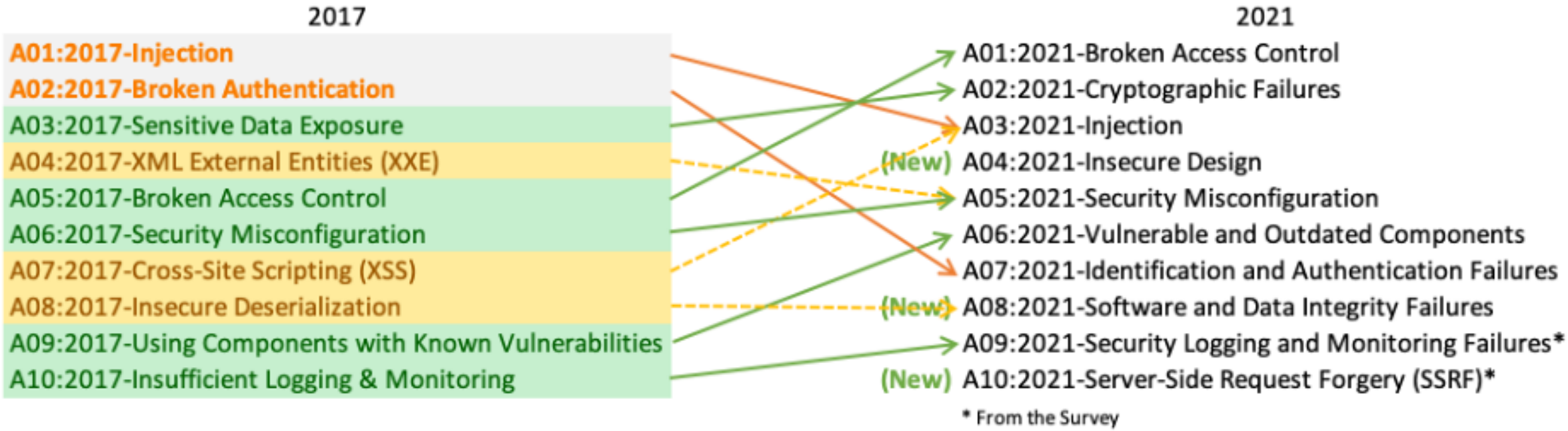
  endgame expose --service iam --name test-resource-exposure

Escalating Privileges of Google Storage Buckets using GCPBucketBrute

- Script-based tool
- Enumerate Google storage buckets and determine kind of access
- Check bucket policy to make direct HTTP request
- Attackers use Google storage "TestIamPermissions" API by providing a bucket name and list of Google storage permissions to retrieve list of permissions they have for that bucket
- If sufficient access -> Escalate privileges up to admin

```
root:~/example# python3 gcpbucketbrute.py -k testtest -u

Generated 1215 bucket permutations.

    EXISTS: testtest01
    EXISTS: testtest1
    EXISTS: testtest
    EXISTS: testtesttest
    EXISTS: testtest2
    EXISTS: mltesttest
    EXISTS: test-testtest
    EXISTS: testtestbucket

    UNAUTHENTICATED ACCESS ALLOWED: testtestgcp
        - UNAUTHENTICATED LISTABLE (storage.objects.list)
        - UNAUTHENTICATED READABLE (storage.objects.get)
        - ALL PERMISSIONS:
            [
                "storage.objects.get",
                "storage.objects.list"
            ]

    EXISTS: testtest0

    UNAUTHENTICATED ACCESS ALLOWED: testtestanalytics
        - VULNERABLE TO PRIVILEGE ESCALATION (storage.buckets.setIamPolicy)
        - ALL PERMISSIONS:
            [
                "storage.buckets.delete",
                "storage.buckets.setIamPolicy"
            ]

    EXISTS: testtestwebsite
    EXISTS: testtestimages

Scanned 1215 potential buckets in 35 second(s).

Gracefully exiting!
```

Top 10 Web Application Security Risks



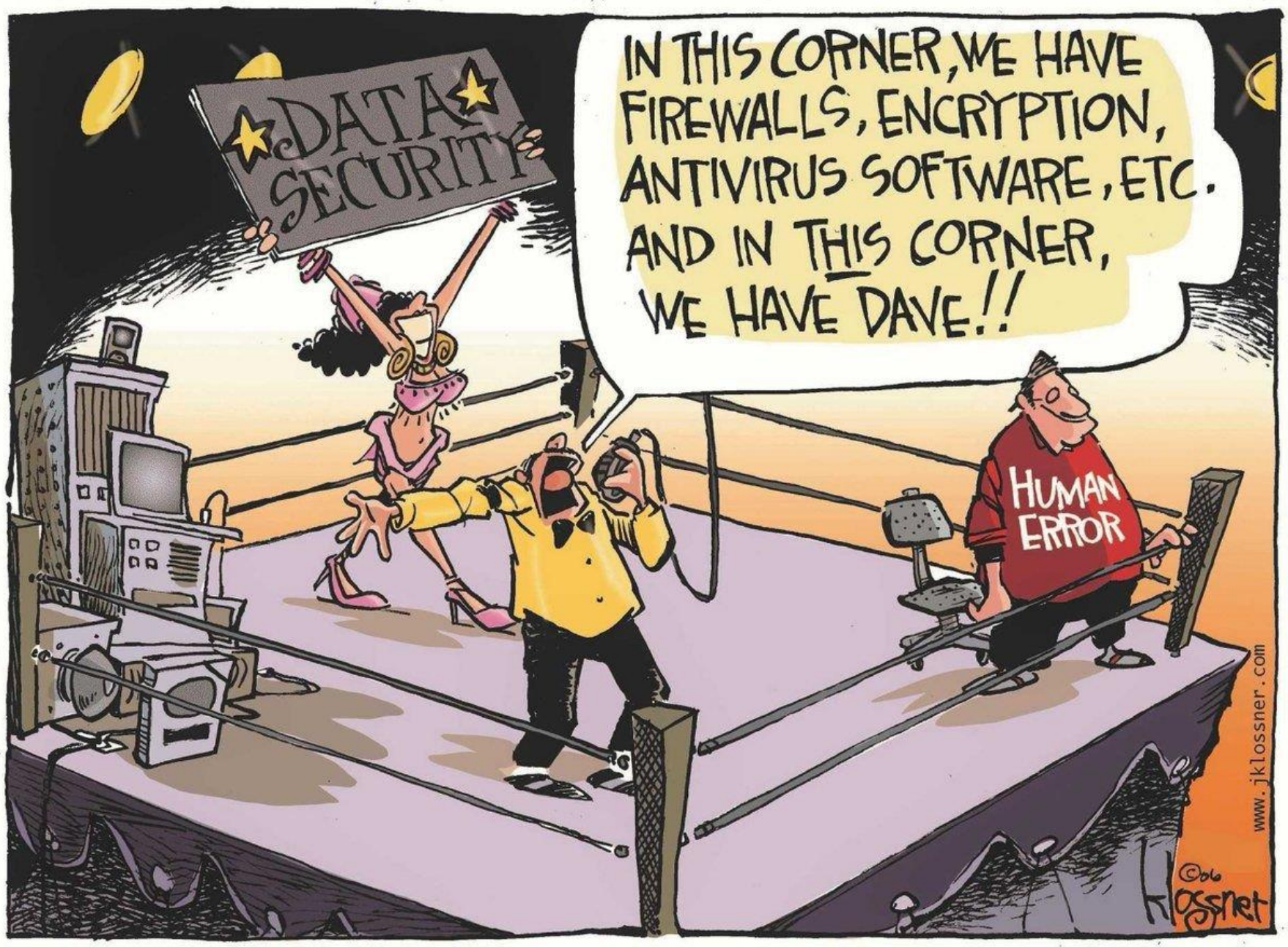
OWASP Top 10 Cloud Security Risks

Risks	Description
R1 - Accountability and Data Ownership	Using the public cloud for hosting business services can cause severe risk for the recoverability of data
R2 - User Identity Federation	Creating multiple user identities for different cloud providers makes it complex to manage multiple user IDs and credentials
R3 - Regulatory Compliance	There is a lack of transparency, and there are different regulatory laws in different countries
R4 - Business Continuity and Resiliency	There can be business risk or monetary loss if the cloud provider handles the business continuity improperly
R5 - User Privacy and Secondary Usage of Data	The default share feature in social web sites can jeopardize the privacy of user's personal data
R6 - Service and Data Integration	Unsecured data in transit is susceptible to eavesdropping and interception attacks
R7 - Multi Tenancy and Physical Security	Poor logical segregation may lead to tenants interfering with the security features of other tenants
R8 - Incidence Analysis and Forensic Support	Due to the distributed storage of logs across the cloud, law enforcement agencies may face problems in forensics recovery
R9 - Infrastructure Security	Misconfiguration of infrastructure may allow network scanning for vulnerable applications and services
R10 - Non-Production Environment Exposure	Using non-production environments increases the risk of unauthorized access, information disclosure, and information modification

Get started links

- https://github.com/azureandsecurityotaku/Awesome-Azure-Pentest
- https://github.com/azureandsecurityotaku/PayloadsAllTheThings
- https://github.com/azureandsecurityotaku/Awesome-Azure-Pentest
- https://github.com/azureandsecurityotaku/cloud-penetration-testing
- https://github.com/azureandsecurityotaku/WholePentesterGuides
- https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies
- https://github.com/Azure/Microsoft-Defender-for-Cloud

Do you know what THE biggest risk today is?



NT KONFERENCA

#ntk23

HVALA!

25. – 27.
SEPTEMBER
2023
PORTOROŽ

This is not school, but we love to get grades.
Please fill out our questoineers and leave us your feedback.
You may even win some cool rewards.

NT KONF

NT KONFERENCA

25. – 27.
SEPTEMBER
2023
PORTOROŽ