



PENETRATION TEST  
REPORT - BYTEGUARD

Prepared By:

Iosif Castrucci

Donato Tralli

Gianpaolo Miliccia Mendoza

[www.byteguard.com](http://www.byteguard.com)

[info@byteguard.com](mailto:info@byteguard.com)

+123-456-7890

# TABLE OF CONTENTS

Executive Summary	3
Penetration Test Estimate	4
Pentest	5
Conclusion	8

# EXECUTIVE SUMMARY

Welcome to ByteGuard, your trusted partner in cybersecurity and programming consulting. At ByteGuard, we specialize in protecting your digital assets and enhancing your technological capabilities with cutting-edge solutions. Our expert team delivers comprehensive services, from threat assessment and incident response to custom software development and system integration. Secure your future with ByteGuard – where technology meets trust.

Byteguard (CLIENT) engaged IOSINT, LLC to conduct penetration testing against the security controls within their information environment to provide a practical demonstration of those controls' effectiveness as well as to provide an estimate of their susceptibility to exploitation and/or data breaches. The test was performed in accordance with IOSINT Information Security Penetration Testing Method.

IOSINT's Information Security Analyst (ISA) conducted all testing in coordination with CLIENTs Information Technology (IT) staff members to ensure safe, orderly, and complete testing within the approved scope.

CLIENT's information environment is NOT protected by endpoint antivirus and administrative, putting the CLIENT at great risk to compliance violation and potentially subject to large fines and/or loss of business reputation.

**This report presents the findings of an exercise conducted to evaluate the impact of firewall activation on a Windows XP machine with respect to external service scans in a LAN network. The primary objective was to understand how enabling the firewall influences the visibility and accessibility of network services from an external perspective.**

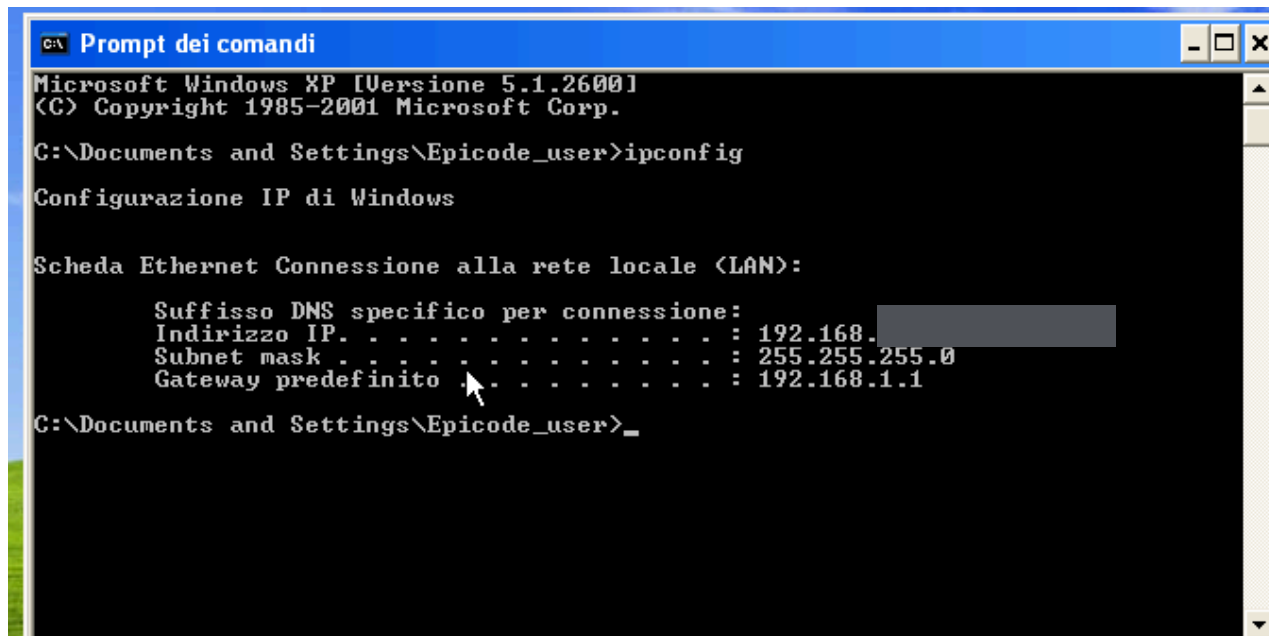
# Penetration Test Estimate

Project Duration: 1 week (5 working days)
Team: 3 people
Hourly Rate: 100 euros/hour
Work Hours:
Each team member: 40 hours
Total team hours: 120 hours
Labor Cost: 12,000 euros
Tools Used:
Total tool cost: 450 euros/10 days
Total Project Cost: 12,450 euros
-----
Cost Breakdown:
1. Labor Cost: 12,000 euros
2. Tool Costs: 450 euros
-----
<b>Total Estimate: 12,450 euros</b>

# PENTEST - LOCAL AREA NETWORK

## LAN NETWORK

Windows XP address byteguard host:



```
C:\> Prompt dei comandi
Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Epicode_user>ipconfig

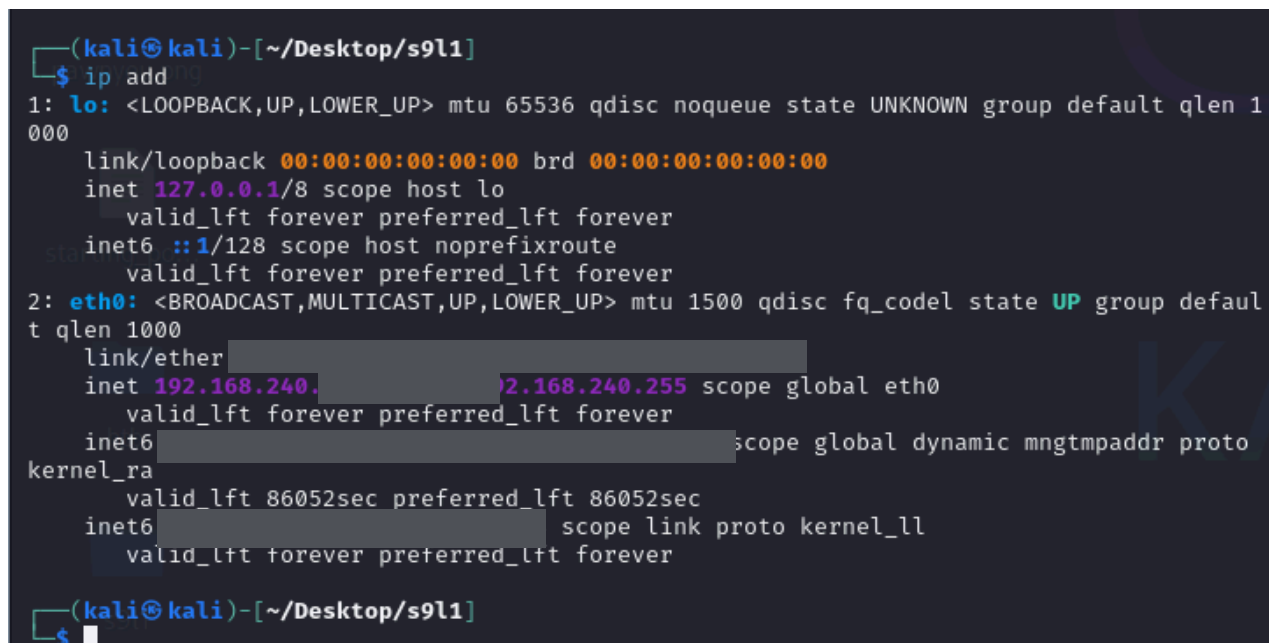
Configurazione IP di Windows

Scheda Ethernet Connessione alla rete locale (LAN):

    Suffisso DNS specifico per connessione:
    Indirizzo IP. . . . . : 192.168.1.1
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.1.1

C:\Documents and Settings\Epicode_user>_
```

IOSINT host attacker

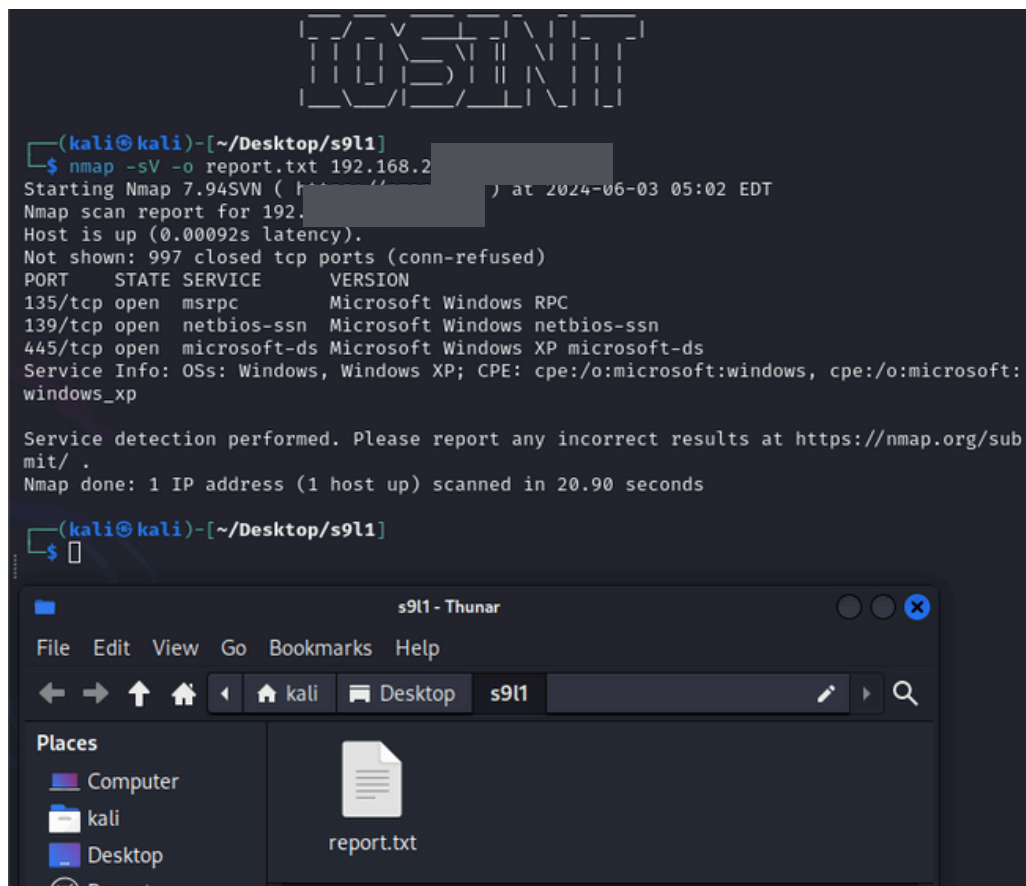
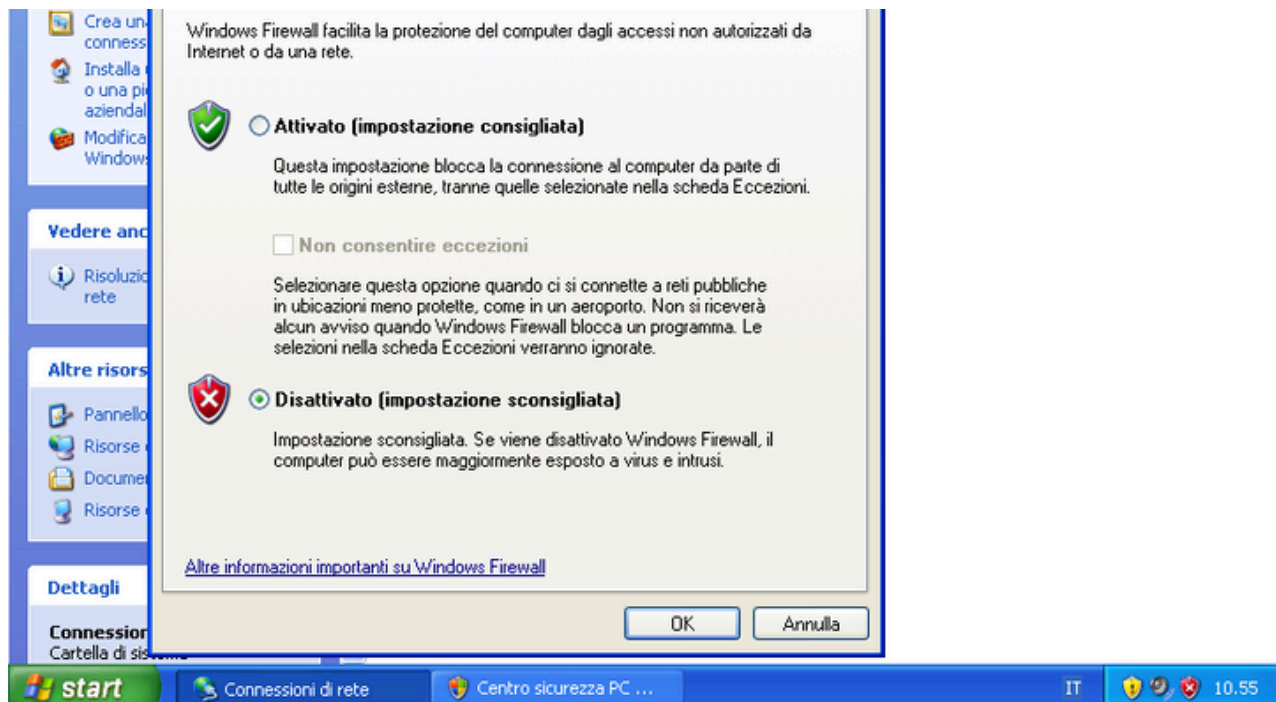


```
(kali@kali)-[~/Desktop/s9l1]
$ ip netns exec lo <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:14:00:00 brd ff:ff:ff:ff:ff:ff
    inet 192.168.240.1/24 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe14:0000/64 scope global dynamic mngtproto kernel_r
        valid_lft 86052sec preferred_lft 86052sec
    inet6 fe80::20c:29ff:fe14:0000/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever

(kali@kali)-[~/Desktop/s9l1]
$
```

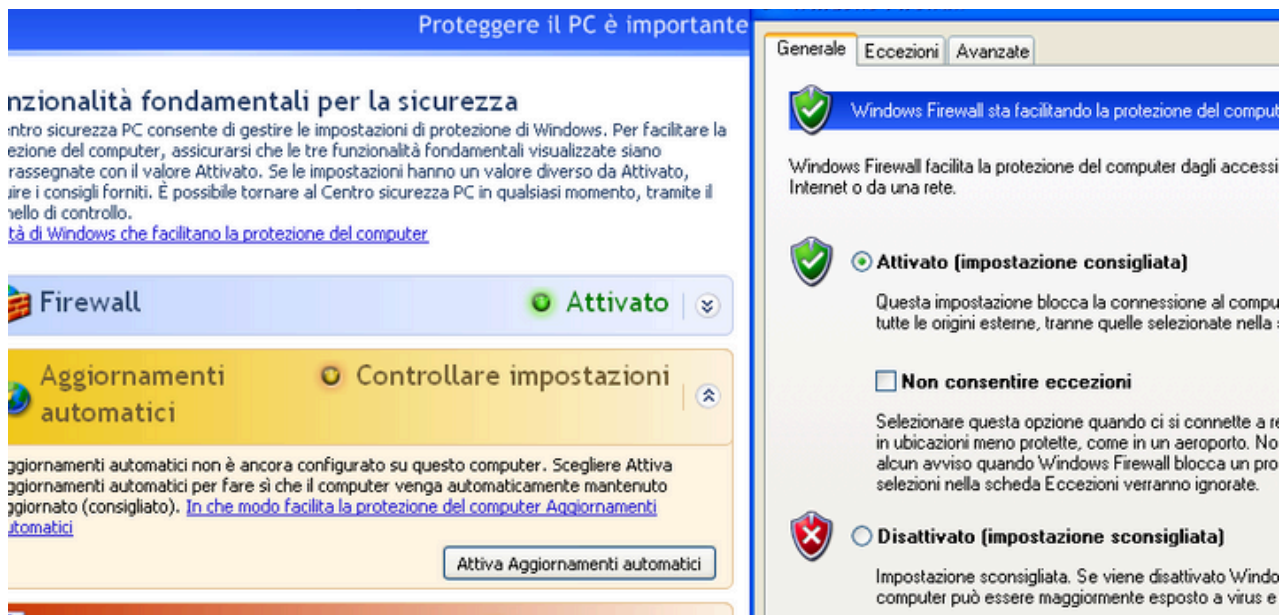
# PENTEST

## WINDOWS FIREWALL DISABLE

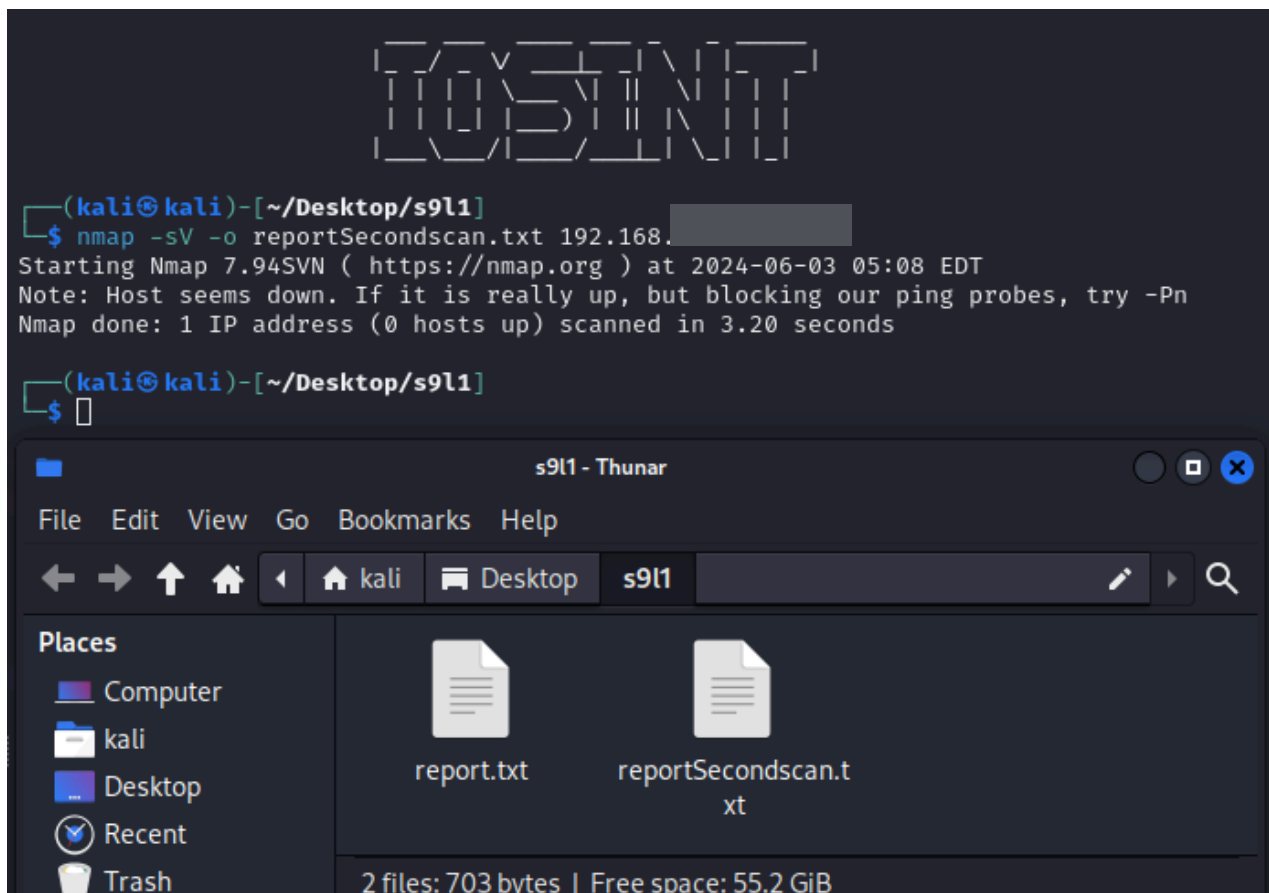


# PENTEST

## WINDOWS FIREWALL ENABLE



5. Perform a second scan - `nmap -sV -o reportSecondscan.txt <target ip>`



# PENTEST

Identify differences of reports:

Closed Ports: Ports that were previously open may now be closed.

Filtered Ports: Some ports may now appear as "filtered," meaning the firewall is blocking the scan attempts.

Service Inaccessibility: Certain services that were accessible before may now be inaccessible due to firewall rules.

## report.txt

```
# Nmap 7.94SVN scan initiated Mon Jun  3 04:21:55 2024 as: nmap -sV -o scanRep 192.168.1.100
Nmap scan report for 192.168.1.100
Host is up (0.0018s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Jun  3 04:22:15 2024 -- 1 IP address (1 host up) scanned in 19.89 seconds
```

## reportSecondscan.txt

```
# Nmap 7.94SVN scan initiated Mon Jun  3 04:27:55 2024 as: nmap -sV -o scanRepFirewallOn 192.168.1.100
# Nmap done at Mon Jun  3 04:27:58 2024 -- 1 IP address (0 hosts up) scanned in 3.42 seconds
```

## Results

### report.txt scan (Firewall Disabled)

- The initial scan detected several open ports and associated services, indicating that these services were accessible from an external network when the firewall was disabled.
- Example findings from report.txt:
  - Port 135/tcp (msrpc) - Microsoft Windows RPC
  - Port 139/tcp (NetBIOS-SSN) - Microsoft Windows netbios-scan
  - Port 445/tcp (microsoft-ds) - Microsoft Windows XP microsoft-ds

### reportSecondscan.txt (Firewall Enabled)

- The secondary scan suggests that the firewall is likely blocking ICMP echo requests (pings) and possibly other probes from Nmap. This can make the host appear offline or unreachable, even if it is actually up and running.



# PENTEST - BEST PRACTICE

The activation of the firewall on the Windows XP machine had a pronounced impact on the visibility and accessibility of network services. The initial scan with the firewall disabled revealed multiple open ports and services, which were subsequently blocked when the firewall was enabled. This exercise demonstrates the critical role of firewalls in network security, effectively preventing unauthorized access and potential attacks by controlling inbound and outbound traffic.

By leveraging firewall configurations, organizations can safeguard their networks against external threats, ensuring that only essential services are exposed while minimizing the risk of exploitation.

## Recommendations

- **Regular Firewall Audits:** Periodically review and update firewall rules to ensure optimal security configurations.
- **Service Minimization:** Disable or restrict access to non-essential services to reduce the attack surface.
- **Continuous Monitoring:** Implement continuous monitoring and logging to detect and respond to suspicious activities promptly.

By following these recommendations, organizations can enhance their network security and protect against evolving cyber threats.

# DISASTER IMPACT ANALYSIS REPORT

ByteGuard has undertaken a quantitative evaluation of the impact of specific disasters on its assets. This report calculates the annual loss the company would suffer in the event of:

Earthquake, fire and flood on the asset "primary building"

Earthquake, fire and flood on the asset "secondary building"

Earthquake, fire and flood on the asset "datacenter"

## Business Continuity and Disaster Recovery

Business continuity refers to the strategies and planning used by an organization to ensure that essential business functions can continue during and after a disaster. It involves proactive planning to avoid and mitigate risks associated with a disruption of operations.

Disaster recovery is a subset of business continuity focusing on the recovery of IT systems and data after a disaster. It involves specific steps and processes to restore normal operations as quickly as possible after an event that causes significant disruption.

## Calculating Annual Losses

To calculate the annual loss (ALE - Annualized Loss Expectancy), we use the formula:

$$ALE = SLE \times ARO$$

Where:

$$SLE \text{ (Single Loss Expectancy)} = AV \text{ (Asset Value)} \times EF \text{ (Exposure Factor)}$$

$$ARO \text{ (Annual Rate of Occurrence)} = 1 / \text{Expected number of years between occurrences}$$

	Primary Building	Single Loss Expectancy	Annualized Loss Expectancy
Earthquake	350000	280000	8400
Fire	350000	210000	10500
Flood	350000	192500	3850

	Secondary Building	Single Loss Expectancy	Annualized Loss Expectancy
Earthquake	150000	120000	3600
Fire	150000	75000	3750
Flood	150000	60000	1200

	Datacenter	Single Loss Expectancy	Annualized Loss Expectancy
Earthquake	100000	95000	2850
Fire	100000	60000	3000
Flood	100000	35000	700

# SUMMARY OF ANNUAL LOSSES

Earthquake on "primary building": €**8400**/year

Fire on "primary building": €**10500**/year

Flood on "primary building": €**3850**/year

Earthquake on "secondary building": €**3600**/year

Fire on "secondary building": €**3750**/year

Flood on "secondary building": €**1200**/year

Earthquake on "datacenter": €**2850**/year

Fire on "datacenter": €**3000**/year

Flood on "datacenter": €**700**/year