PENTEST REPORT:BYTEGUARD

JUNE 3,2024

PENETRATION TEST REPORT - BYTEGUARD

Prepared By:
Iosif Castrucci
Donato Tralli
Gianpaolo Miliccia Mendoza
Danilo Malagoli

www.byteguard.com
info@byteguard.com
+123-456-7890

TABLE OF CONTENTS

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

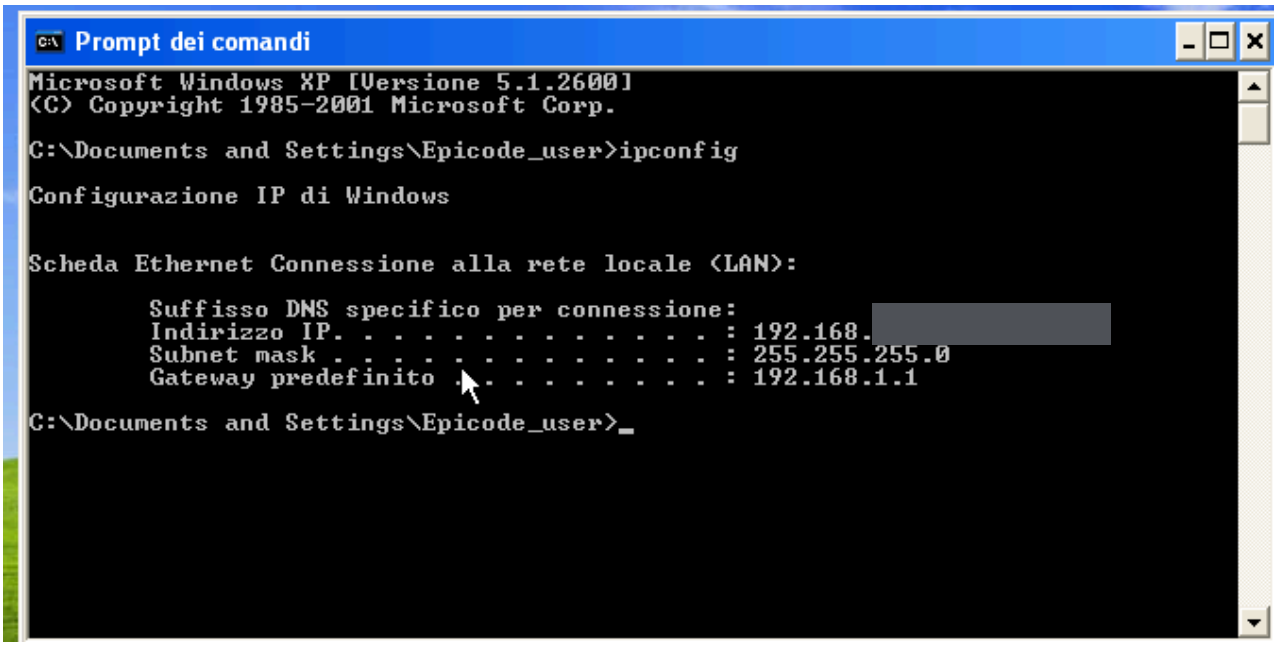
Cost Breakdown:
1. Labor Cost: 12,000 euros
2. Tool Costs: 450 euros

Total Estimate: 12,450 euros

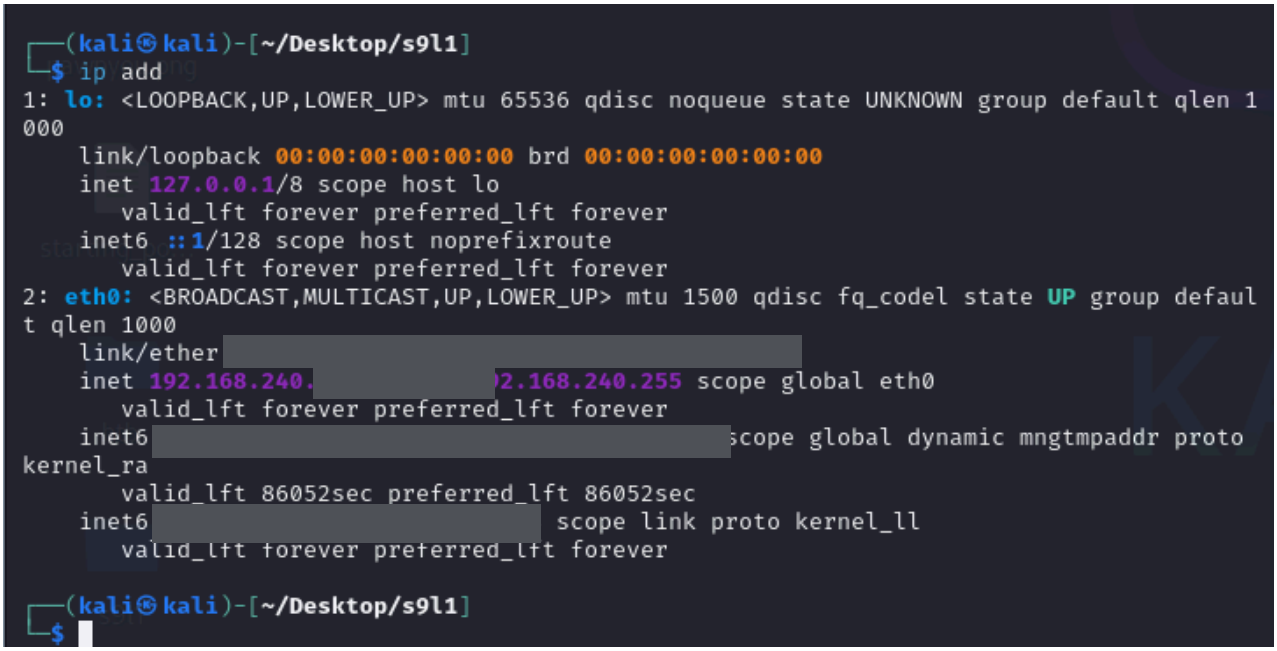
PENTEST - LOCAL AREA NETWORK

LAN NETWORK

Windows XP address byteguard host:

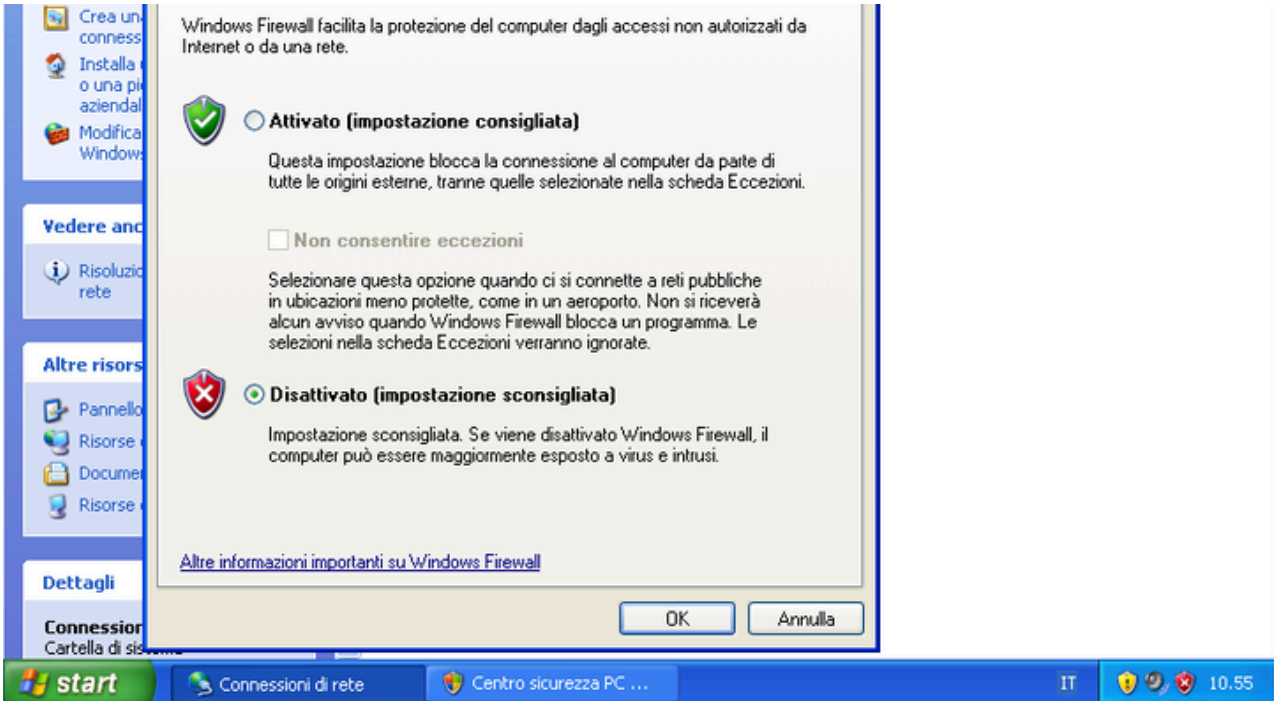


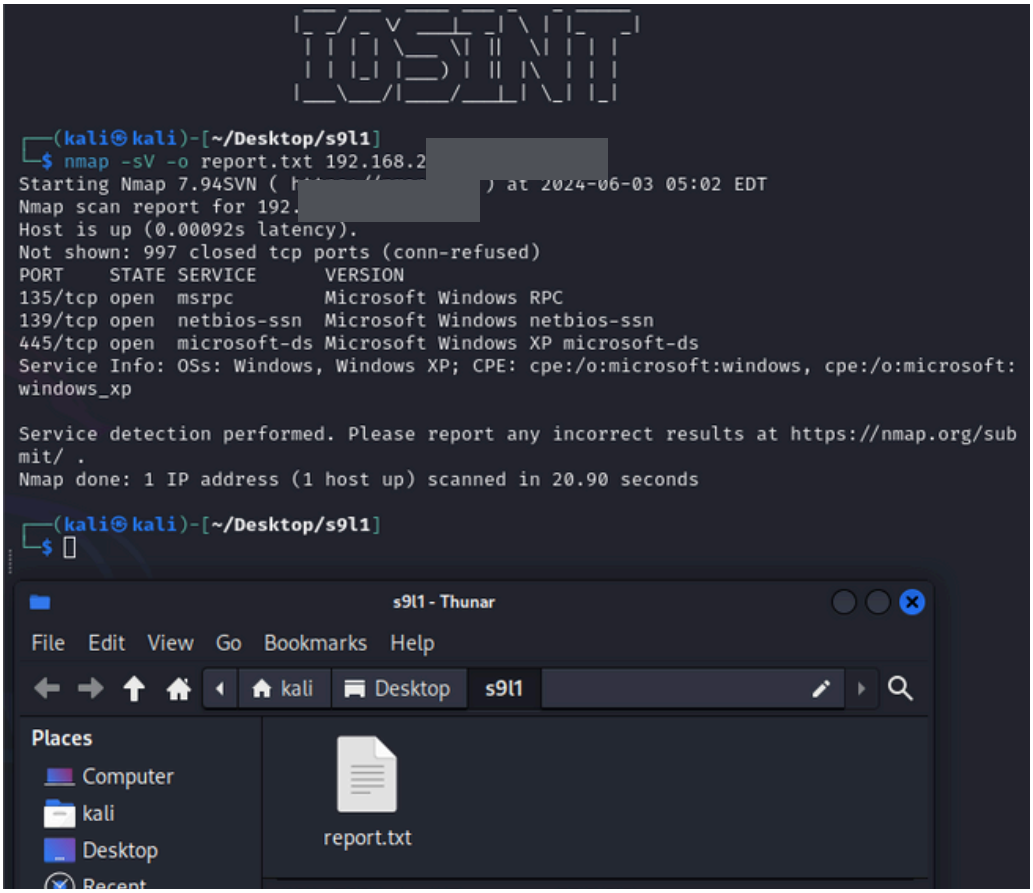
IOSINT host attacker



PENTEST

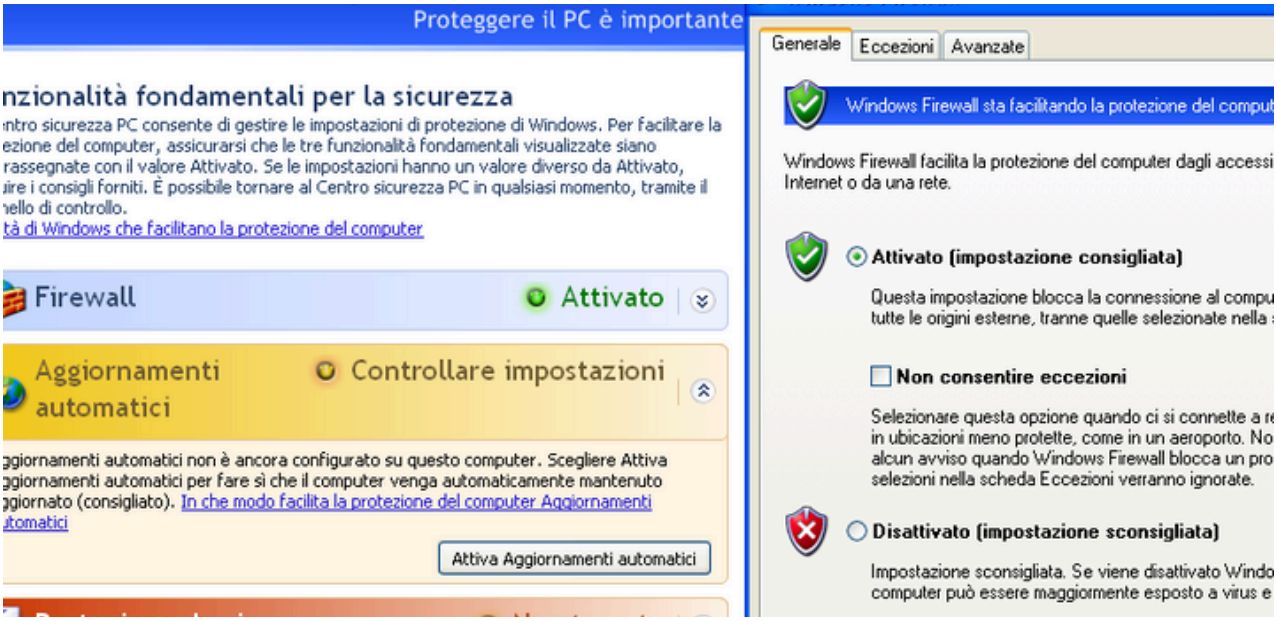
WINDOWS FIREWALL DISABLE



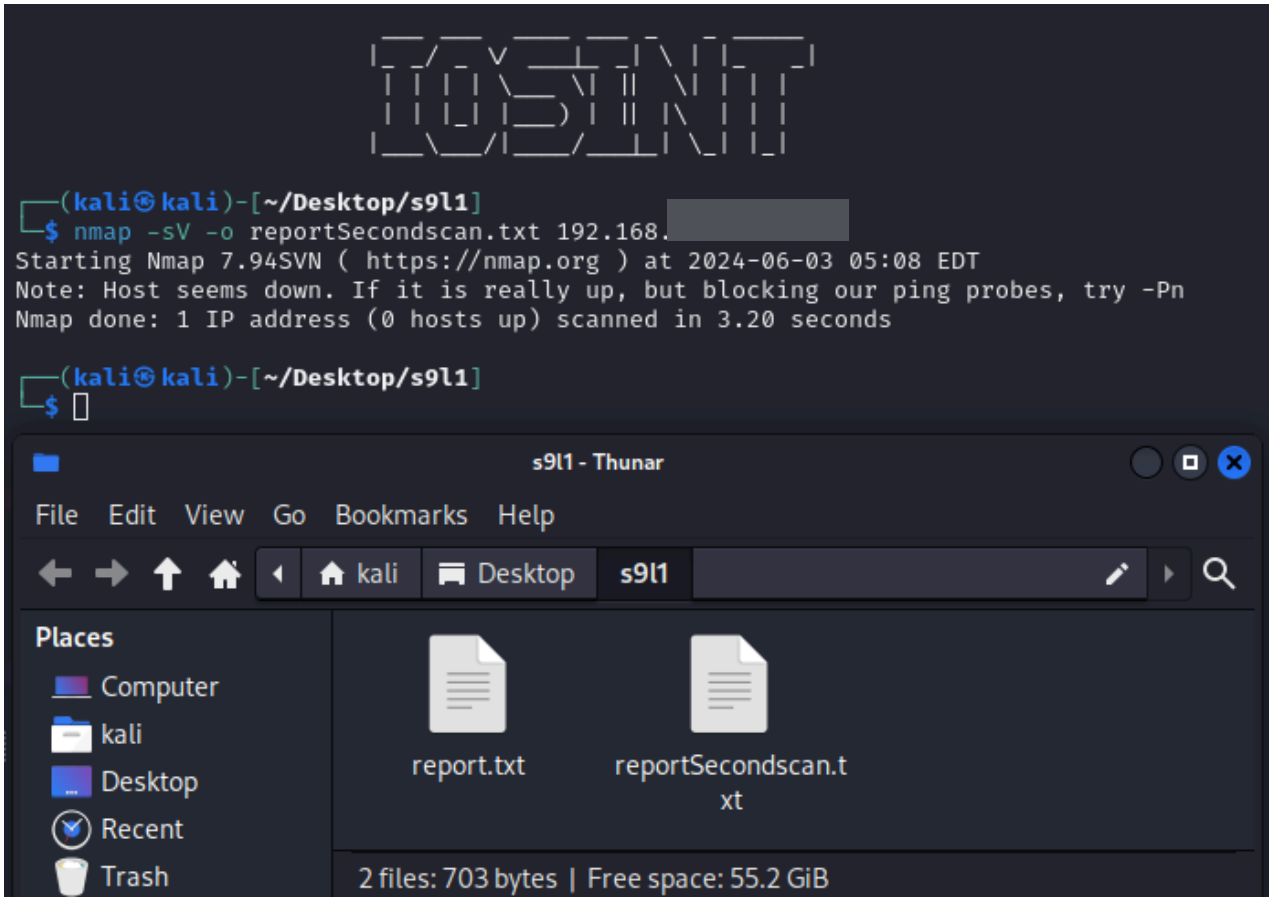


PENTEST

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[redacted]
Nmap scan report for 192.168[redacted]
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[redacted]
# 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 x ARO

Where:

SLE (Single Loss Expectancy) = AV (Asset Value) x EF (Exposure Factor)

ARO (Annual Rate of Occurrence) = 1 / 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

BC / DC BEST PRACTICE FOR BYTEGUARD

Business Continuity
- Hyperconvergence
- Multi-node Cluster
- Cold Site, Hot Site
- Dynamic Routing
- Multiple Internet Lines
- Clustered Firewall
- Asynchronous Replication
- Fault Tolerance
- HA (High Availability)
- VMware (example)

Disaster Recovery
- Backup NAS/Storage
- Cloud
- Offline Disks
- Remote Disks/NAS
- Veeam (example)

Best practices for Business Continuity (BC) and Disaster Recovery (DR) include regular data backups, maintaining redundant systems, using cloud solutions, implementing multi-node clusters, ensuring dynamic routing, and testing recovery procedures frequently. Utilize reliable tools like Veeam, and adhere to the 3-2-1 backup rule for optimal data protection.

WIRESHARK ANALYSIS

ByteGuard also requested us to analyze a Wireshark pcap file to understand if there are any specific activities or if there is an attacker present. Wireshark pcap files contain network traffic data, and analyzing them can reveal any suspicious or malicious activities occurring within the network. By examining the packet capture data, we can identify unusual patterns, unauthorized access attempts, or any other indicators of a potential security breach. This analysis helps us determine the presence of an attacker and take appropriate measures to safeguard the network and its assets.

To begin the intervention, we asked ourselves three main questions to conduct the analysis

1.- Identify eventually IOC:

TCP requests

2.- Based on the found IOC's, make hypotheses about the potential attack vectors used:

The attacker with the IP 192.168.200.100 is scanning the machine with IP address 192.168.200.150

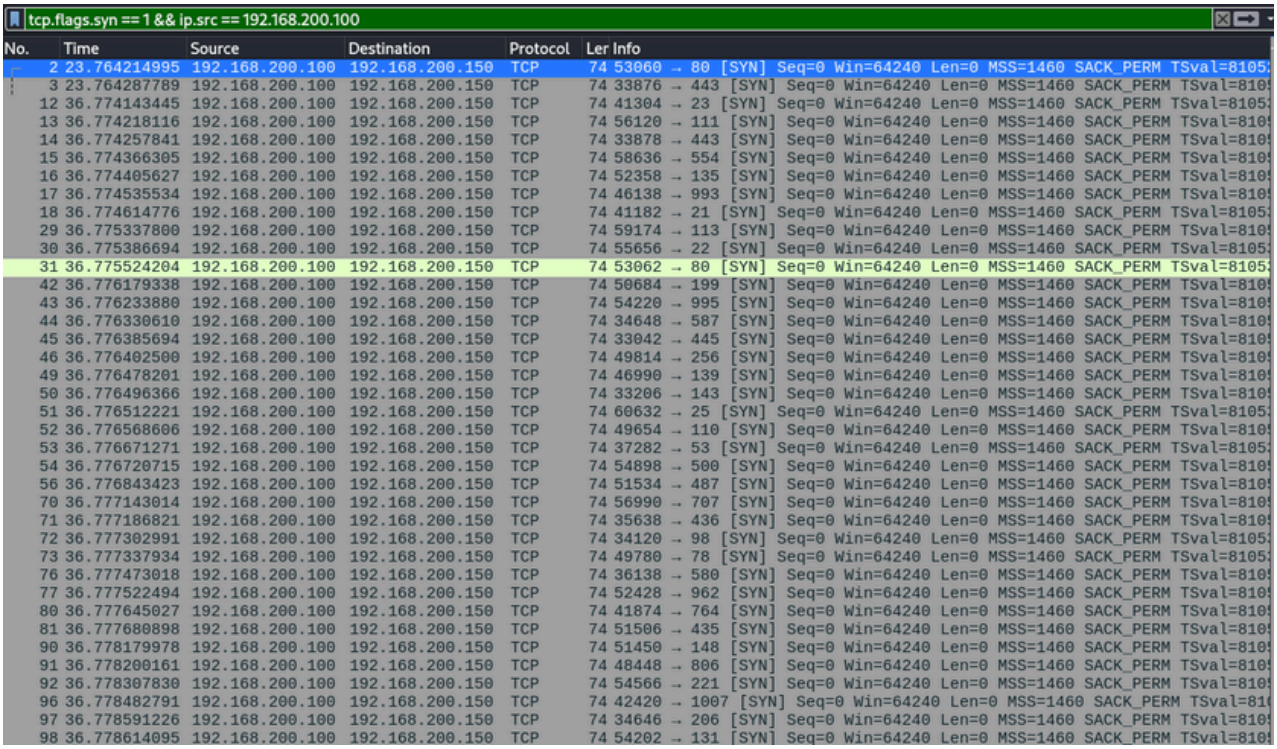
3.- Recommend an action to reduce impacts of the attack:

Change the firewall policy to block access to the machine with IP address 192.168.200.150 from the attacker with IP address 192.168.200.100

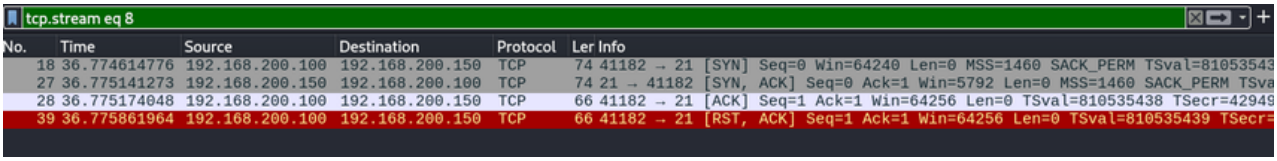
The capture reveals a high number of TCP (SYN) requests targeting various destination ports, suggesting that the host 192.168.200.100 might be scanning the host 192.168.200.150. This is evidenced by some lines in the capture showing [SYN+ACK] responses from the target, indicating open ports, and [RST+ACK] responses, indicating closed ports. To mitigate this, firewall rules could be implemented on the target host to block incoming requests from 192.168.200.100.

WIRESHARK PCAP FILE SCREENSHOTS

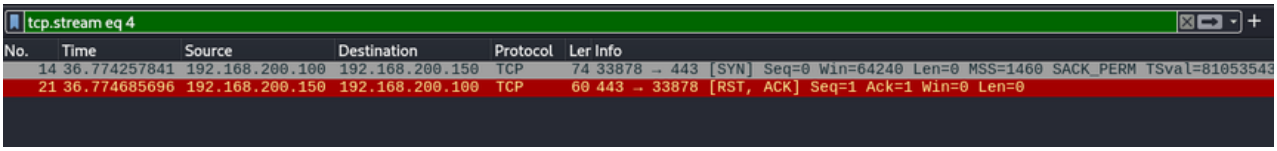
Example of the attackers ip 192.168.200.100 scanning differents ports of the target ip 192.168.200.150



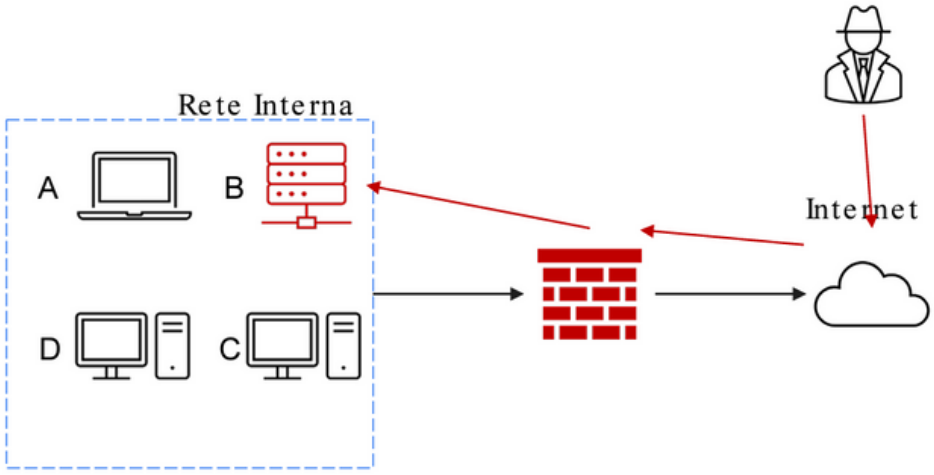
Example of an open port



Example of a closed door



ISOLATION TECHNIQUES

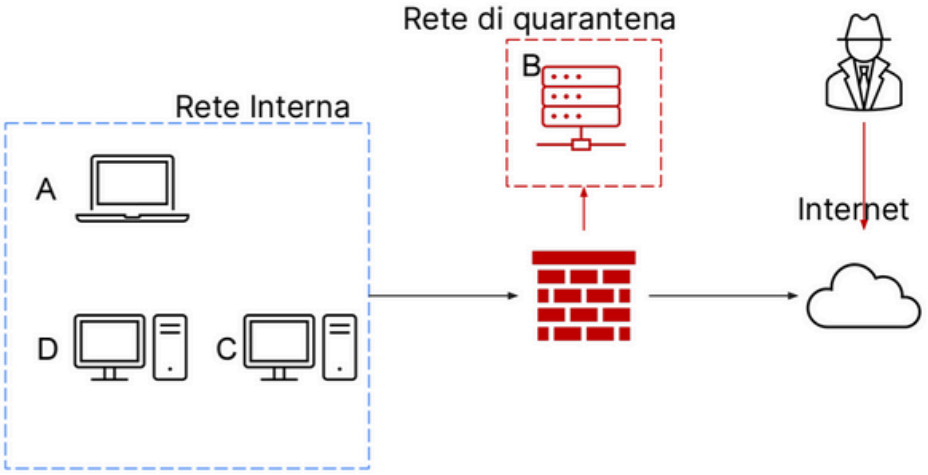


To isolate the compromised system B, the following techniques can be adopted:

1.- Network Disconnection: Immediately remove system B from the corporate network to prevent further lateral movement of the attacker and stop data exfiltration. This can be done physically or logically through network devices such as switches and routers.

2.- Creation of Isolated VLANs: Move system B to a separate VLAN that is not connected to the main network to isolate network traffic and contain the damage.

3.- Limited Physical Access: Restrict physical access to compromised servers to prevent further hardware tampering. This includes using physical locks and access controls to server rooms.

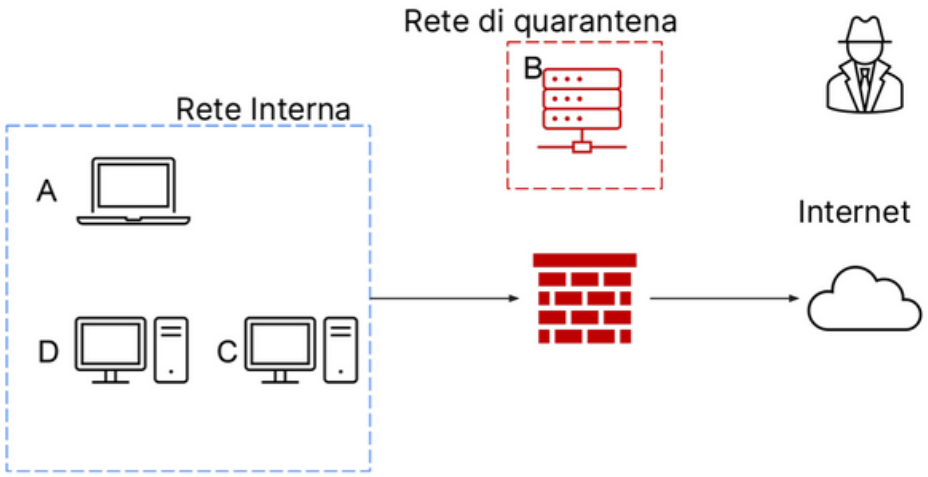


COMPLETE REMOVAL FROM NETWORK AND INTERNET:

1.- Shutdown System B: If all other methods fail to secure System B, the final step is to completely remove it from the network and internet. Shut down the system to ensure it no longer poses a threat.

2.- Remove Network Cables: Physically remove any network cables and disable wireless connections to prevent any accidental reconnection to the network.

3.- Power Down: Turn off System B entirely to halt any ongoing malicious activities and prevent further damage.



REMOVAL OF THE INFECTED SYSTEM B

To remove the infected system B, follow these steps:

1.- Data Backup: Perform a complete backup of non-infected and uncompromised data, following data security guidelines to ensure data is stored securely.

2.- System Cleaning: Use cleaning and malware removal software to eliminate any presence of malicious code. This may include the use of antivirus, anti-malware, and specialized removal tools.

3.- Restoration from Backup: Restore the system using backups taken before the compromise, ensuring that restored data is free from malware. Verify and secure backups before restoration.

4.- Patches and Updates: Apply all necessary patches and updates to address vulnerabilities that allowed the initial attack. Ensure the operating system and all applications are up to date.

ELIMINATION OF SENSITIVE INFORMATION

Before disposing of compromised disks, it is essential to securely eliminate sensitive information. The main techniques are:

1.- Clear: This process makes data unreadable through software means. It is usually performed by overwriting the data with zeros or random patterns. This method is recommended for less sensitive data where the media needs to be reused without the risk of simple recovery.

2.- Purge: This method goes beyond Clear and makes data unrecoverable even with advanced data recovery tools. Common techniques include degaussing for magnetic disks and specific sanitization commands for solid-state drives. This method is used for highly sensitive data where a higher level of security is required compared to Clear.

3.- Destroy: This is the most secure method and involves the physical destruction of storage media, making any form of data recovery impossible. Common techniques include shredding disks, hot fusion, or physical destruction using specialized machinery. This method is used when it is required that data can never be recovered in any way, and the media will not be reused.

DIFFERENCE BETWEEN PURGE AND DESTROY

1.- Purge: Eliminates data making it irrecoverable through advanced cleaning or sanitization techniques. The physical media remains intact and can be reused if procedures allow.

2.- Destroy: Involves the physical destruction of storage media, ensuring data cannot be recovered in any way. This method is definitive and does not allow for the reuse of the media.