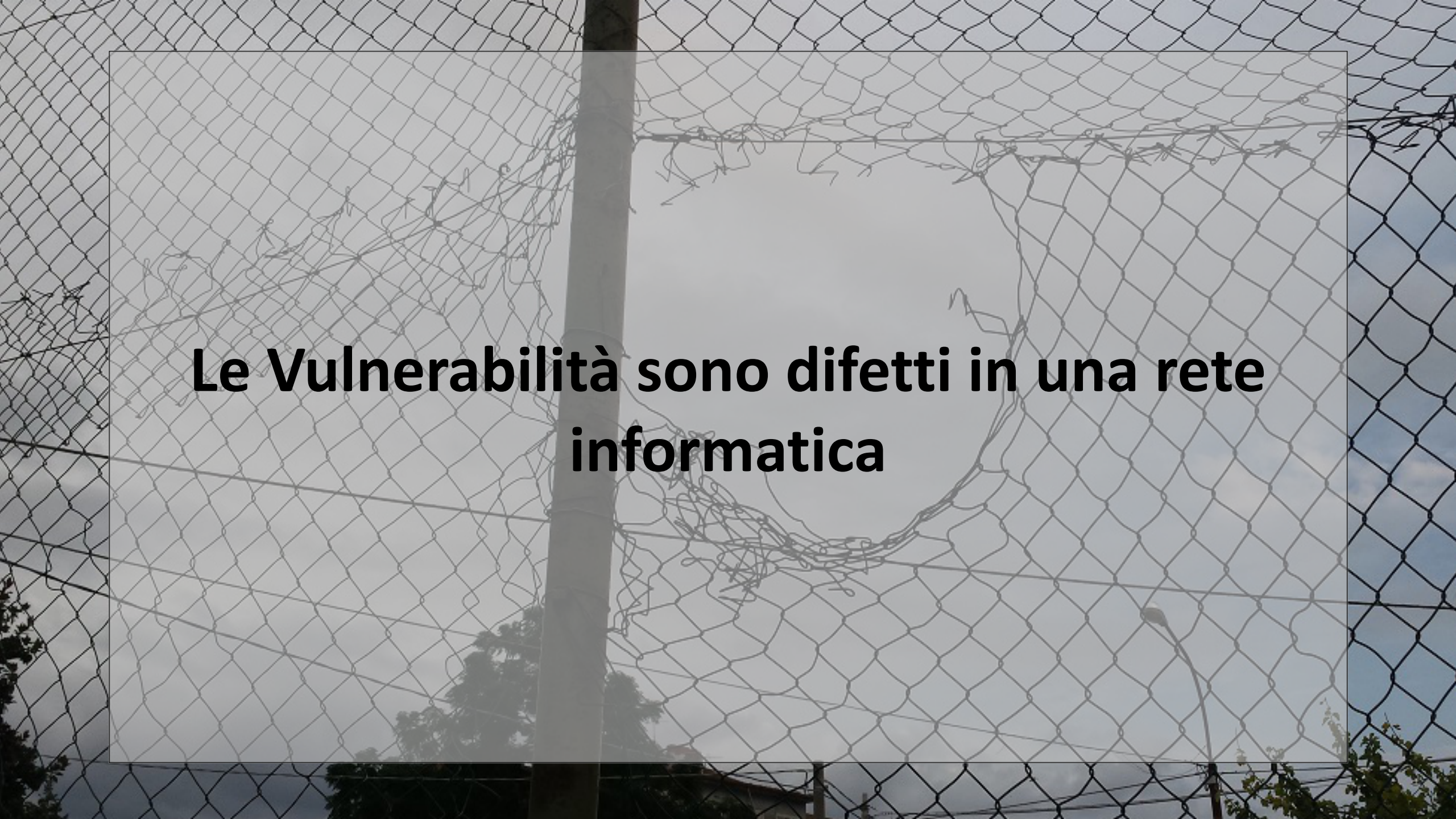
FRED
FOR SECURITY



Le Vulnerabilità sono difetti in una rete informatica

www.fredforsecurity.it

Fred for security è la soluzione “all in one”per effettuare penetration test con cadenza mensile, in modo automatizzato e guidato dall’ a.i., Fred permette di:

1) individuare le vulnerabilità;
2) intervenire sulla rete con un team di “cybersecurity manager as a service”;
3) risparmiare fino al 95% rispetto allo stesso lavoro eseguito da un cybersecurity manager.

www.fredforsecurity.it

CASE STUDY 1

Sistema Target: [redacted]

Vulnerabilità	Directory /nbproject/private/ Directory Traversal
Livello rischio	Medio
Porta	80/tcp
SPID	63410
Impatto	The identified directory found on the remote web server is subject to a remote directory traversal vulnerability. An attacker can exploit this vulnerability to access arbitrary files on the target system in the same permission content as of the web server is running with.
Soluzione	Please upgrade to the latest version of the identified software you are running with the found directory. And set correct permissions on the found directory.
Output della vulnerabilità / Evidenze	

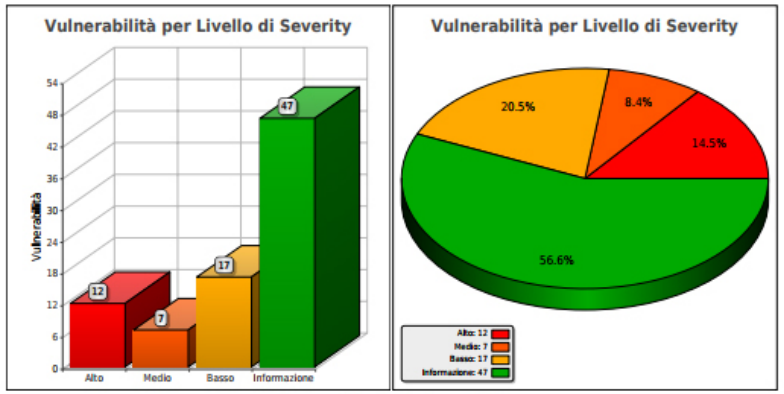
```
AttackString: GET http://www[redacted]project/private/ HTTP/1.0
AttackOutput: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final/
/EN">
<html>
<head>
<title>Index of /nbproject/private</title>
</head>
<body>
<h1>Index of /nbproject/private</h1>
<table>
```

Fred ha ispezionato un sito web e ha trovato una directory che doveva rimanere "privata", contenente un file di configurazione con informazioni riservate (credenziali di accesso FTP e del DB).

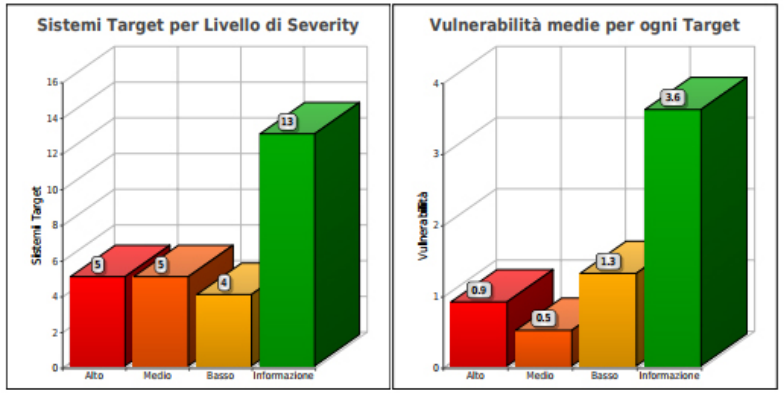
L'accesso FTP consentirebbe il "defacing" del sito, ovvero la sua riprogrammazione con pagine falsificate, mentre l'accesso al DB garantirebbe un data leack delle informazioni ivi contenute.

Analisi dei Risultati

Un totale di **83** potenziali vulnerabilità sono state individuate nei sistemi di destinazione, con un rapporto di **14.5%** di vulnerabilità di livello Alto. Le vulnerabilità di livello Alto sono state trovate in **5** Target. La vulnerabilità più frequente, con l'esclusione del livello di Severity Informazione, è '**Microsoft PrintNightmare Remote Code Execution**', con il livello di Severity 'Alto', trovata su 5 Target. Il sistema di destinazione con il maggior numero di vulnerabilità è '**192.168.2.229**', con un totale di **18** vulnerabilità. Sistemi Target privi di vulnerabilità: .



Numero totale di vulnerabilità



www.fredforsecurity.it

CASE STUDY 2

Vulnerabilità	Possible Anonymous FTP or NULL Backdoor Vulnerability
Livello rischio	Alto
Porta	21/tcp
	1736
Impatto	It is possible on the remote FTP Server to login with the following username "NULL" and the password "NULL". An old Linux FTP Server backdoor had this login name as well. An attacker can use this to compromise the system.
Output della vulnerabilità / Evidenze	
	AttackString: PASS NULL
	AttackOutput: 331 User ok
	230 User logged in successfully

Vulnerabilità	Passwordless FTP server Vulnerability
Livello rischio	Alto
Porta	21/tcp
	2688
BugtraqID	5200
Impatto	It is possible on the remote ftp server to login with the username root and no password at all. This can allow an attacker to gain full access over the FTP Server at administrative level.
Output della vulnerabilità / Evidenze	
	AttackString: PASS
	AttackOutput: 331 User ok
	230 User logged in successfully

Vulnerabilità	WFTP Login Vulnerability
Livello rischio	Alto
Porta	21/tcp
	1728

Fred ha trovato una backdoor presente in un vecchio server linux, via FTP, senza immettere alcuna credenziale, si può raggiungere il server con accesso ai files.

www.fredforsecurity.it

CASE STUDY 3

Sistema Target: 192.168.2.15

Vulnerabilità	Microsoft PrintNightmare Remote Code Execution
Livello rischio	Alto
Porta	0/tcp
SPID	64047
CVE	CVE-2021-1675
Impatto	The target is vulnerable to the PrintNightmare vulnerability. This can allow attackers to conduct remote command execution. Attackers are exploit the vulnerability with public exploits. It is due to a vulnerability in Windows Print Spooler.
Output della vulnerabilità / Evidenze	
	192.168.2.15 is Vulnerable to CVE-2021-1675

Vulnerabilità	DNS Recursion Allowed
Livello rischio	Medio
SPID	56963
Impatto	The target DNS service is subject to a remote DNS Recursion vulnerability. Attackers can exploit this in DDoS Attacks. Recursion is used to process a DNS request where the DNS server performs the request for the client. Recursion should only be allowed for trusted clients.
Output della vulnerabilità / Evidenze	
	yahoo.com mail is handled by 1 mta5.am0.yahoodns.net.

Vulnerabilità	It is possible to obtain remote NetBIOS name table
Livello rischio	Basso
SPID	1770
Impatto	Attackers can use this information to base other attacks on.
Output della vulnerabilità / Evidenze	
	Name Service Type ---------- SRVDC Workstation Service Domain Name Domain Controllers SRVDC File Server Service

Vulnerabilità	MAC address obtained via NetBIOS
Livello rischio	Basso
SPID	1771
Impatto	It is possible on the remote target via NetBIOS to retrieve the MAC address. The MAC address is the

Fred ha ispezionato ha individuato una fotocopiatrice vulnerabile, un hacker potrebbe attaccarla e si troverebbe gli all'interno della rete.

La fotocopiatrice risulta anche vulnerabile agli attacchi DDOS, inviando richieste multiple il sistema collasserebbe o stamperebbe fogli all'infinito.

www.fredforsecurity.it

CASE STUDY 4

Sistema Target: 192.168.2.5

Vulnerabilità	NB1300 Router Default FTP Account Vulnerability
Livello rischio	Alto
Porta	21/tcp
SPID	3615
Impatto	It is possible on the remote NB1300 router system to login to the ftp with a default administrative account Username: admin Password: password. This can allow an attacker to steal sensitive information from the device or change the configuration of the device.
Soluzione	It is recommended to immediately connect to the device and set another password. Further more it is recommended to block all incoming traffic to the identified port so that only trusted ip addresses can connect to it.
Output della vulnerabilità / Evidenze	
	AttackString: PASS password
	AttackOutput: 331 User ok
	230 User logged in successfully

Fred ha individuato un router (NB1300) con credenziali amministrative mai ancora di default:

Username: admin
Password: password

www.fredforsecurity.it

Grazie !