



Spring **2025** Edition

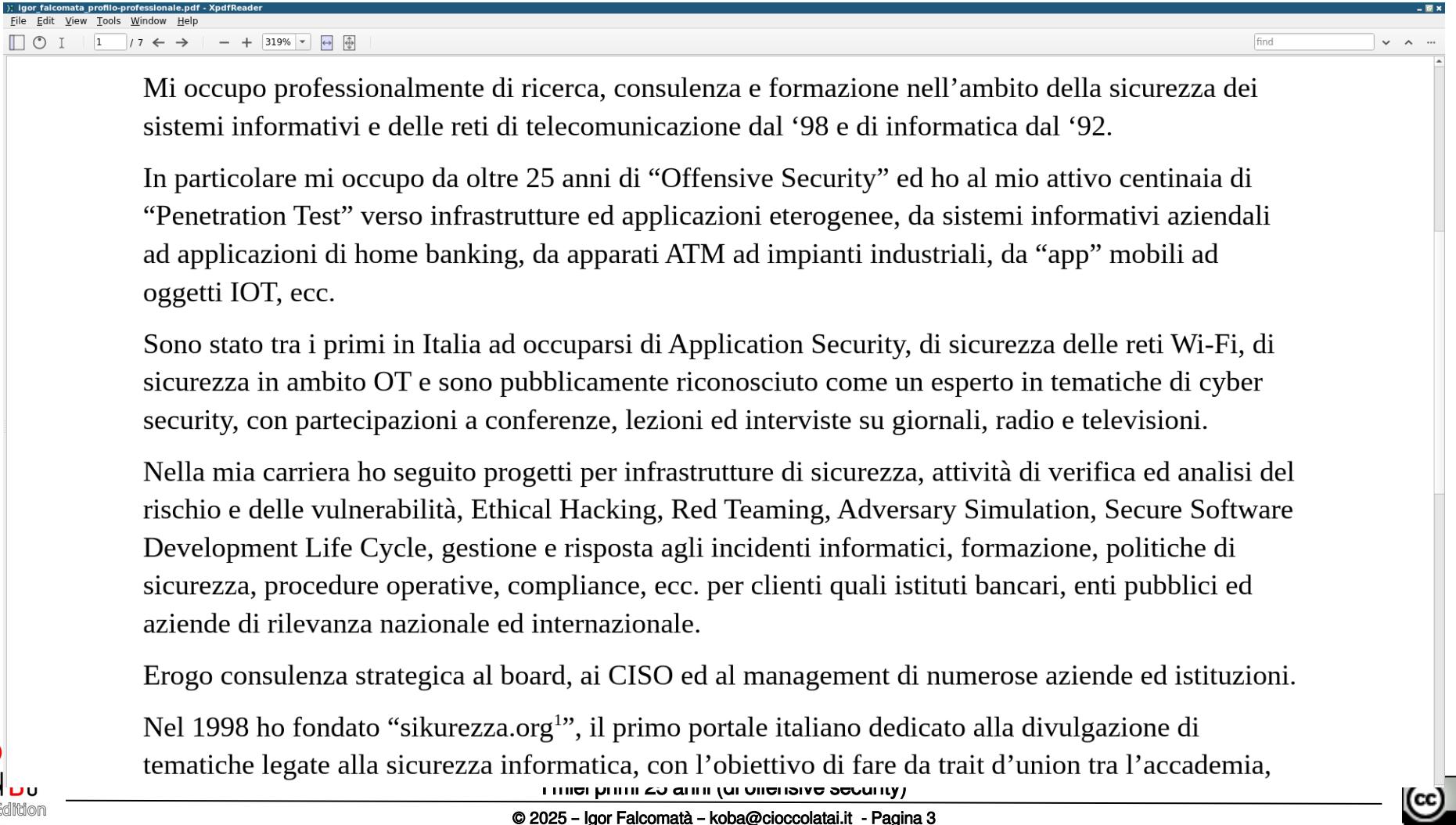
24^a EDIZIONE

I miei primi 25 anni
(di offensive security)

koba@cioccolatai.it

Chi sono

Chi sono



Igor falcomata profilo-professionale.pdf - XpdfReader
File Edit View Tools Window Help
1 / 7 319% find

Mi occupo professionalmente di ricerca, consulenza e formazione nell'ambito della sicurezza dei sistemi informativi e delle reti di telecomunicazione dal '98 e di informatica dal '92.

In particolare mi occupo da oltre 25 anni di "Offensive Security" ed ho al mio attivo centinaia di "Penetration Test" verso infrastrutture ed applicazioni eterogenee, da sistemi informativi aziendali ad applicazioni di home banking, da apparati ATM ad impianti industriali, da "app" mobili ad oggetti IOT, ecc.

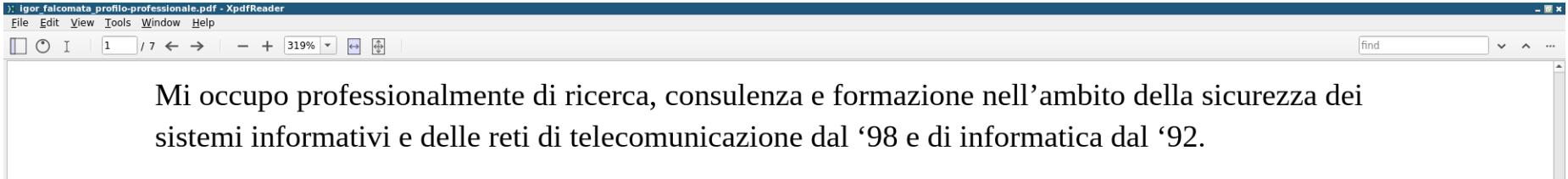
Sono stato tra i primi in Italia ad occuparsi di Application Security, di sicurezza delle reti Wi-Fi, di sicurezza in ambito OT e sono pubblicamente riconosciuto come un esperto in tematiche di cyber security, con partecipazioni a conferenze, lezioni ed interviste su giornali, radio e televisioni.

Nella mia carriera ho seguito progetti per infrastrutture di sicurezza, attività di verifica ed analisi del rischio e delle vulnerabilità, Ethical Hacking, Red Teaming, Adversary Simulation, Secure Software Development Life Cycle, gestione e risposta agli incidenti informatici, formazione, politiche di sicurezza, procedure operative, compliance, ecc. per clienti quali istituti bancari, enti pubblici ed aziende di rilevanza nazionale ed internazionale.

Erogo consulenza strategica al board, ai CISO ed al management di numerose aziende ed istituzioni.

Nel 1998 ho fondato "sikurezza.org¹", il primo portale italiano dedicato alla divulgazione di tematiche legate alla sicurezza informatica, con l'obiettivo di fare da trait d'union tra l'accademia,

Chi sono



Igor falcomata profilo-professionale.pdf - XpdfReader
File Edit View Tools Window Help
1 / 7 319% find
Mi occupo professionalmente di ricerca, consulenza e formazione nell'ambito della sicurezza dei sistemi informativi e delle reti di telecomunicazione dal '98 e di informatica dal '92.

In particolare mi occupo da oltre 25 anni di “Offensive Security” ed ho al mio attivo centinaia di “Penetration Test” verso infrastrutture ed applicazioni eterogenee, da sistemi informativi aziendali ad applicazioni di home banking, da apparati ATM ad impianti industriali, da “app” mobili ad oggetti IOT, ecc.

security, con partecipazioni a conferenze, lezioni ed interviste su giornali, radio e televisioni.

Nella mia carriera ho seguito progetti per infrastrutture di sicurezza, attività di verifica ed analisi del rischio e delle vulnerabilità, Ethical Hacking, Red Teaming, Adversary Simulation, Secure Software Development Life Cycle, gestione e risposta agli incidenti informatici, formazione, politiche di sicurezza, procedure operative, compliance, ecc. per clienti quali istituti bancari, enti pubblici ed aziende di rilevanza nazionale ed internazionale.

Erogo consulenza strategica al board, ai CISO ed al management di numerose aziende ed istituzioni.

Nel 1998 ho fondato “sikurezza.org¹”, il primo portale italiano dedicato alla divulgazione di tematiche legate alla sicurezza informatica, con l’obiettivo di fare da trait d’union tra l’accademia,

Chi sono

Igor Falcomata - Profilo professionale.pdf - XpdfReader
File Edit View Tools Window Help
Pashe x
Clipboard Fort Alignment Number ISst

Mi occupo professionalmente di sistemi informativi e

In particolare mi occuperò di "Penetration Test" verificando la sicurezza ad applicazioni di home automation, oggetti IOT, ecc.

Sono stato tra i primi a parlare di sicurezza in ambito Cloud Computing e Cyber security, con partecipazioni a diversi convegni.

Nella mia carriera ho lavorato per diversi clienti nel campo del rischio e delle vulnerabilità, sia in ambito Development Life Cycle che in campo della sicurezza, procedure aziende di rilevanza internazionale.

Ero consulente strutturale per diversi progetti.

Nel 1998 ho fondato l'associazione HackInU, con le tematiche legate alla



A screenshot of a Microsoft Excel spreadsheet titled "Cyber Security Checklist". The spreadsheet has two columns: "Checklist Item" and "Check". The items listed are:

Checklist Item	Check
Install and update antivirus software	✓
Enable firewall protection	✓
Use strong, unique passwords	✓
Implement multi-factor authentication	✓
Keep software up to date	✓
Encrypt sensitive data	✓
Backup data regularly	✓
Restrict user access to sensitive information	✓
Conduct security awareness training	✓
Perform periodic security audits	✓

The background of the slide features a photograph of a man from behind, wearing a cap and a dark jacket, looking at a computer screen displaying the Excel spreadsheet. The slide also includes a yellow and black striped barrier tape at the bottom.

Agenda

Agenda

*Si sa che la gente dà buoni consigli
sentendosi come Gesù nel tempio,
si sa che la gente dà buoni consigli
se non può più dare cattivo esempio.*

Bocca Di Rosa
F. De André

Offensive Security?

Offensive Security?

STORIA DELL'OFFENSIVE SECURITY

ANNI '60-80

- Prime analisi sulla sicurezza informatica in ambito militare e accademico

90s

Affermarsi del concetto di penetrazione attacco

2000-2010

Prime analizz sulla Peneterpot test prove servici estructurai com

2020-PcC

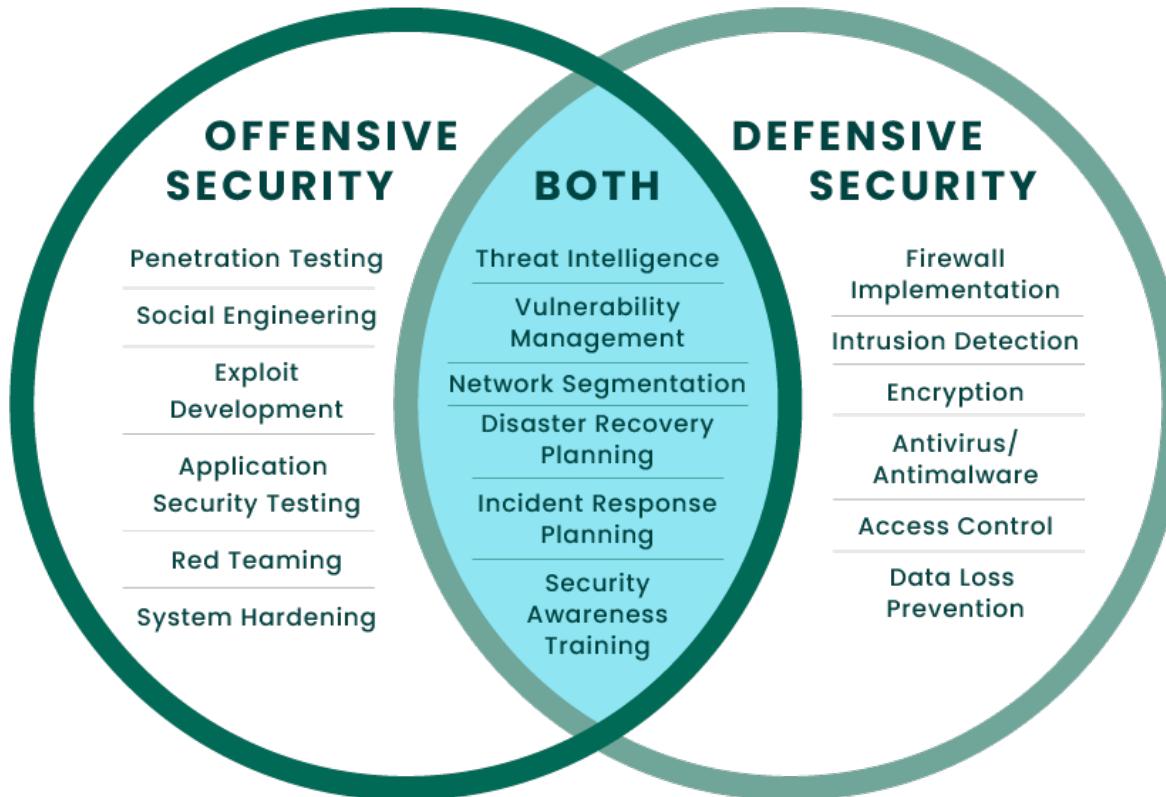
Prime a service estructuai com



ATTIVITÀ PRINCIPALI IN OFFENSIVE SECURITY

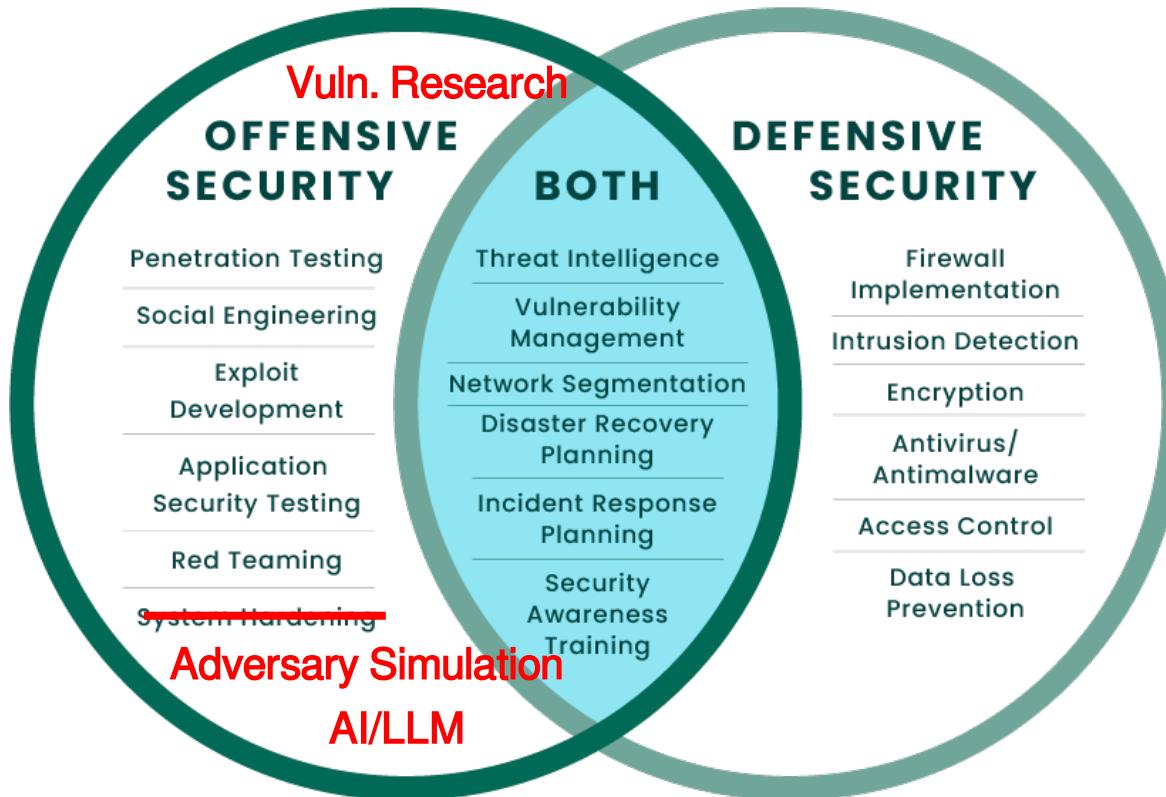
- | | |
|-------------------------|----------------------|
| • Vulnerabilit Assisent | Red Teaming Testrise |
| • Prenetation Testing | Red Teaming Testrise |
| • Exploitging Testing | Protrusion Testing |

Offensive Security?



Source: <https://www.coresecurity.com/offensive-security>

Offensive Security?



Source: <https://www.coresecurity.com/offensive-security>

Offensive Security?

Vulnerability Assessment != Penetration Test

Penetration Test != Red Teaming

Red Teaming != Social Engineering

Social Engineering != Adversary Simulation

Adversary Simulation != Exploit Development

Exploit Development != Vulnerability Research

Offensive

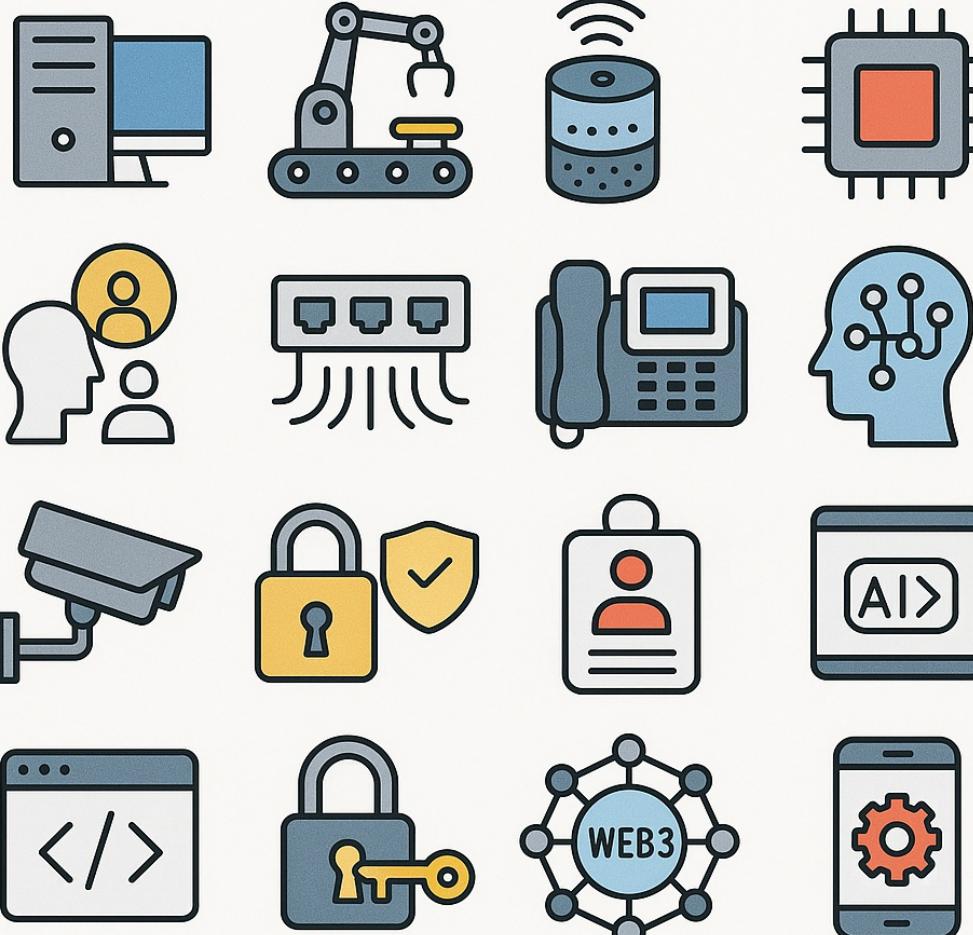
Vulnerab

Pe
Red

Social E

Adversar

Exploit De



tion Test
ng
ring
mulation
elopment
Research

Vulnerability Scanning

Cos'è il Vulnerability Scanning?

Il **Vulnerability Scanning** è un processo automatizzato di identificazione delle vulnerabilità di sicurezza in un sistema, rete o applicazione. Si avvale di strumenti specifici (scanner di vulnerabilità) per analizzare configurazioni, software e servizi alla ricerca di debolezze note che potrebbero essere sfruttate da attaccanti.

Caratteristiche del Vulnerability Scanning:

- **Automazione:** utilizza software dedicati per eseguire scansioni su larga scala.
- **Identificazione delle vulnerabilità note:** confronta il sistema con database di vulnerabilità (es. CVE, NVD).
- **Non intrusivo (o poco intrusivo):** a differenza del penetration test, non sfrutta attivamente le vulnerabilità ma le rileva.
- **Rapporto sui rischi:** fornisce una valutazione del rischio associato a ogni vulnerabilità rilevata.

Subject: system administrators guide to cracking
Date: 2 Dec 1993 03:36:16 GMT
From: zen@death.Sun.COM (d ... 415-336-0742)
Followup-To: comp.security.unix
Lines: 1106

Improving the Security of Your Site by Breaking Into it

Dan Farmer
Sun Microsystems
zen@sun.com

Wietse Venema
Eindhoven University of Technology
wietse@wzv.win.tue.nl

Introduction

Every day, all over the world, computer networks and hosts are broken into. The level of sophistication of these attacks varies greatly. It is generally believed that most break-ins succeed due to weaknesses in the systems. There are still a large number of intrusions that use more advanced techniques to break in. Less is known about the latter types of break-ins because, by their very nature they are much harder to detect.

CERT. SRI. The Nic. NCSC. RSA. NASA. MIT. Universities. Sun. You name it, we've seen it broken into. Anything that can be broken (and many that isn't) seems to be fairly easy game. Are things getting better? What happened?

Fade to...

A young boy, with greasy blonde hair, sitting in a dark room illuminated only by the glowing screen of the C64's 40 characters. He has just taken another long drag from his Ben and Hedges cigarette. He cracks a telnet to the next "faceless" "mil" site on his hit list. "root", "root", and "sys" -- all "nger" all fail. No matter. He pencils the host off of his list, and tiredly types in the next one.

1993

The end.

HACK

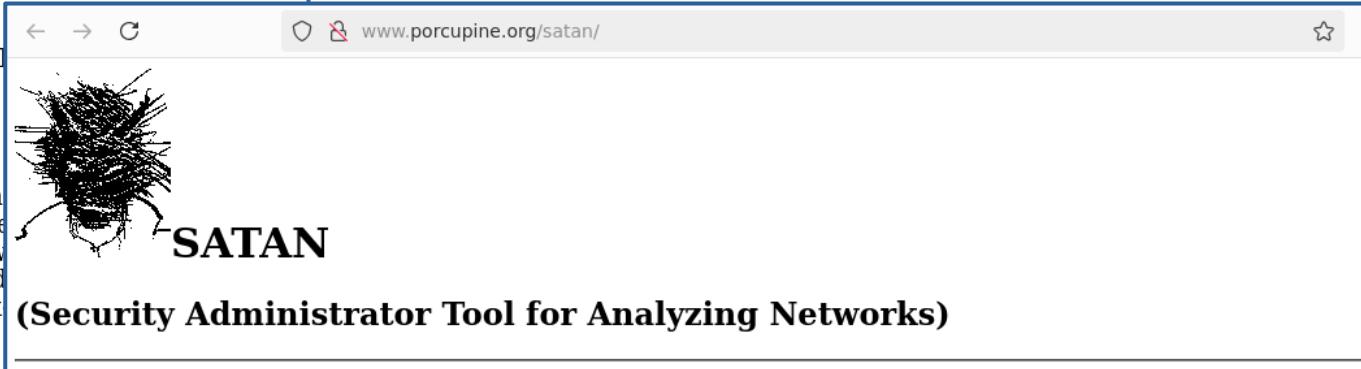
Spring 2022

24^ EDIZIONE

g

Cos'è il Vulnerability Scanning?

automatizzato di identificazione delle



The screenshot shows a web browser window with the URL www.porcupine.org/satan/. The page features a black and white illustration of a satanic figure with a large head and a skull-like face. Below the illustration, the word "SATAN" is written in large, bold, capital letters. Underneath "SATAN", the text "(Security Administrator Tool for Analyzing Networks)" is displayed. The page is titled "SATAN Information". A bulleted list of links includes: "What SATAN is about", "SATAN updates", "Bulletins from vendors etc.", "A SATAN demo with all documentation", "What you need in order to run SATAN", and "Downloading your own SATAN copy". Another section titled "SATAN Hints and tips" contains links to "Workaround for Netscape" and "Hints and tips for LINUX users". Large red numbers "1993" and "1995" are overlaid on the bottom left and right corners of the screenshot respectively.

SATAN Information

- [What SATAN is about](#)
- [SATAN updates](#)
- [Bulletins from vendors etc.](#)
- [A SATAN demo with all documentation](#)
- [What you need in order to run SATAN](#)
- [Downloading your own SATAN copy](#)

SATAN Hints and tips

- [Workaround for Netscape](#)
- [Hints and tips for LINUX users](#)

1995

Subject: system administrators guide to cracking
Date: 2 Dec 1993 03:36:16 GMT
From: zen@death.Sun.COM (d ... 415-33
Followup-To: comp.security.unix
Lines: 1106

Improving the Security of Your System

Dan Farmer
Sun Microsystems
zen@sun.com

Wietse Venema
Eindhoven University of Technology
wietse@cs.tue.nl

Introduction

Every day, all over the world, computers break into. The level of sophistication of these break-ins varies greatly. It is generally believed that most break-ins are carried out by amateurs, while a large number of intrusions are carried out by professionals who break in. Less is known about the latter, because the nature of their work is very nature they are much harder to detect.

CERT. SRI. The Nic. NCSC. RSA. NIST. Sun. You name it, we've seen it broken into. (and many that isn't) seems to be fairly common. What happened?

Fade to...

A young boy, with greasy blonde hair, illuminated only by the luminescence of another long strand from his Benji, cracked telnets to the next faceless machine, "root" and "sys" -- 1, "sys" -- 2, "sys" -- 3, he pencils the host off of his list, and times out.

HACK

Spring 2002

24° EDIZIONE



• Hints and tips for LINUX users

ity Scanning?

elle

works)

1995

Penetration testing

The UK [National Cyber Security Center](#) describes penetration testing as: "A method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the same tools and techniques as an adversary might."^[9]

The goals of a penetration test vary depending on the type of approved activity for any given engagement, with the primary goal focused on finding vulnerabilities that could be exploited by a nefarious actor, and informing the client of those vulnerabilities along with recommended mitigation strategies.^[10]

Penetration tests are a component of a full [security audit](#). For example, the [Payment Card Industry Data Security Standard](#) requires penetration testing on a regular schedule, and after system changes.^[11] Penetration testing also can support risk assessments as outlined in the NIST Risk Management Framework SP 800-53.^[12]

~~Penetration testing~~

The UK National Cyber Security Center describes penetration testing as gaining assurance in the security of an IT system by attempting to compromise the system's security, using the same tools and techniques as an attacker.

The goals of a penetration test vary depending on the type of engagement, with the primary goal focused on finding vulnerabilities that could be exploited by a nefarious actor, and informing the client of those vulnerabilities and recommended mitigation strategies.^[10]

Penetration tests are a component of a full security audit. For example, the ISO 27001 Industry Data Security Standard requires penetration testing on a regular basis to detect changes in the system environment. Penetration testing also can support risk assessment and compliance with the NIST Risk Management Framework SP 800-53.^[12]



Top 10 High Vulnerabilities: (CVSS v3.0)						
Plugin ID	Plugin Name	Plugin Family	CVSS v3.0	Known Exploit?	Publication Date	Count
42873	SSL Medium Strength Cipher Suites Supported (SWEET32)	General	7.5	Yes	2016/08/24	24



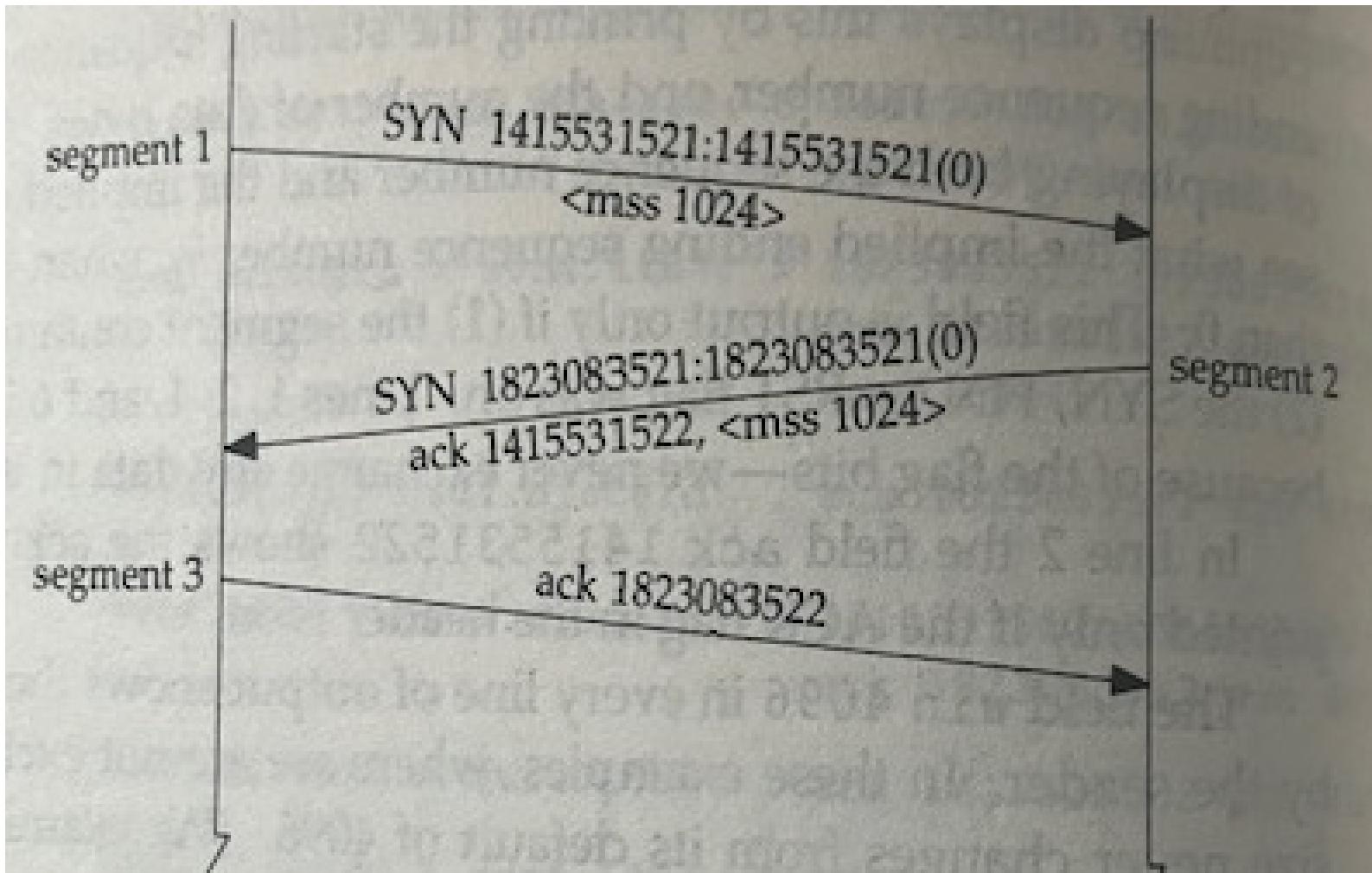
Top 10 Critical Vulnerabilities: (VPR)						
Top 10 most prevalent critical vulnerabilities						
Plugin ID	Plugin Name	Plugin Family	VPR	Known Exploit?	Publication Date	Count
146825	VMware vCenter Server RCE (direct check)	Misc.	9.8	Yes	2021/02/23	3
146826	VMware vCenter Server 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2021-0002)	Misc.	9.8	Yes	2021/02/23	3
97833	MS17-10: Security Update for Microsoft Windows SMB Server (60000000000000000000) (BLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNTHESIS) (WannaCry) (EternalRocks) (Petya) (unauthenticated check)	Windows	9.5	Yes	2017/03/14	3
138554	Microsoft DNS Server Remote Code Execution (StigGuard)	DNS	10.0	Yes	2020/07/14	2
125313	Microsoft RDP RCE (CVE-2019-0708) BlueKeep (unauthenticated check)	Windows	9.8	Yes	2019/05/14	2
135411	VMware vCenter Server 6.7: Sensible Information Disclosure Vulnerability (VMSA-2020-0006)	Misc.	9.4	Yes	2020/04/09	2
56435	MS17-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (unauthenticated check)	Windows	9.0	Yes	2012/03/13	2
133845	Apache Tomcat 7.0.x < 7.0.100 / 8.5.x < 8.5.51 / 9.0.x < 9.0.31: Multiple Vulnerabilities	Web Servers	9.6	Yes	2020/02/20	1
136807	Apache Tomcat 8.5.x < 8.5.55: Remote Code Execution	Web Servers	9.5	Yes	2020/05/11	1

Top 10 Critical Vulnerabilities: (VPR)

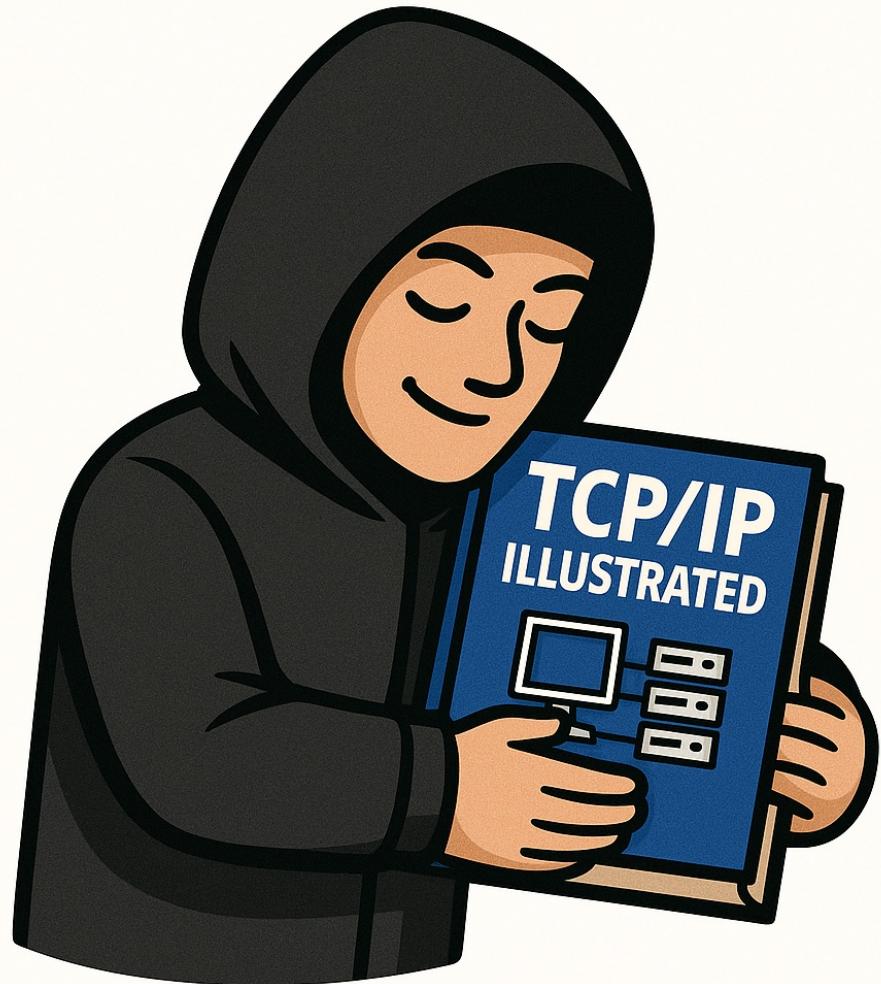
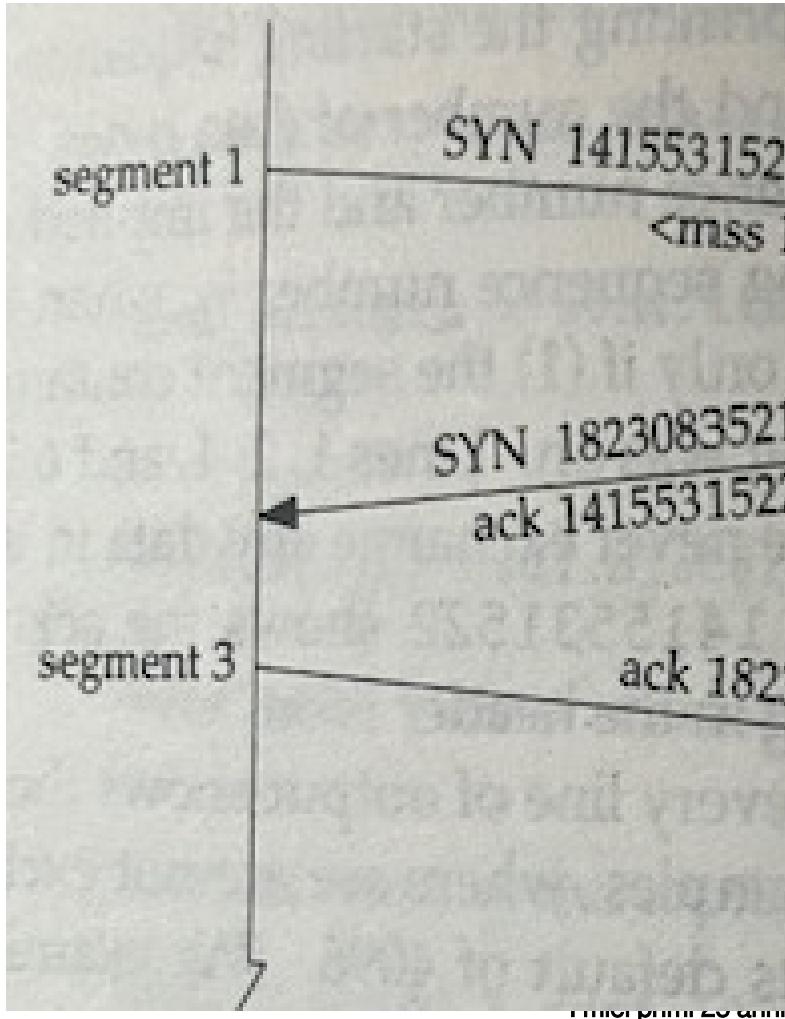


Come iniziare?

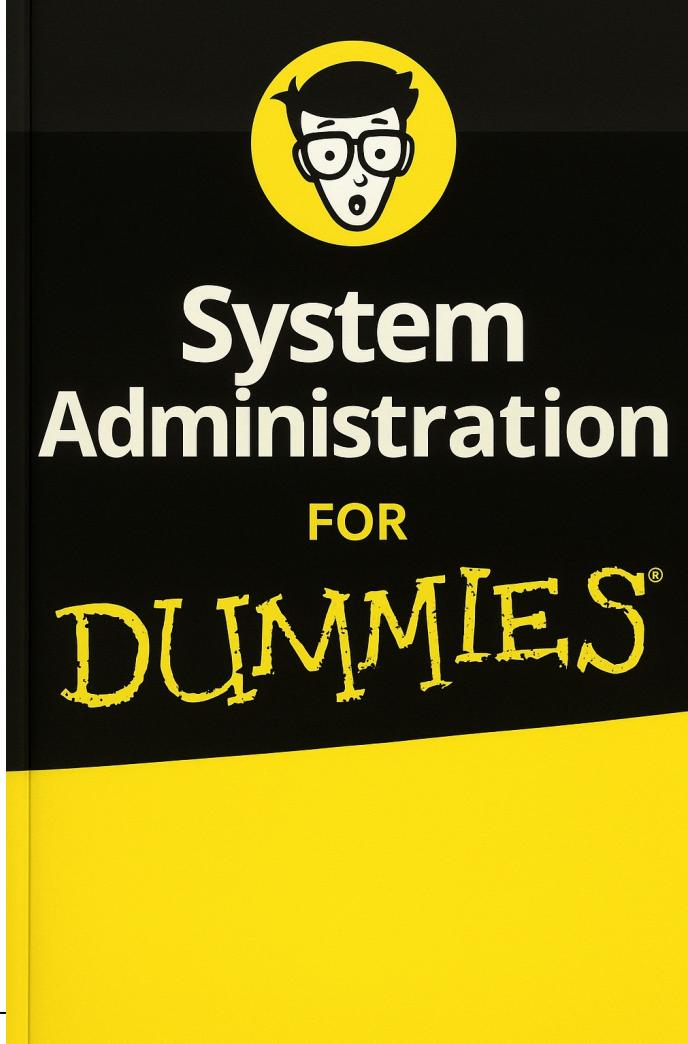
Conoscere “le basi” - networking



Conoscere “le basi” - networking



Conoscere “le basi” - informatica



Conoscere “le basi” - coding

It would be a pure function if not for the side effects on your sanity



Turning Coffee Into Code

The Definitive Guide

Conoscere le tecniche di attacco

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques	17 techniques	32 techniques	9 techniques	17 techniques	18 techniques	9 techniques	14 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (10)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Latent Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Browser Session Hijacking	Data Encoding (2)	Defacement (2)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Brower Extensions	Deobfuscate/Decode Files or Information	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Clipboard Data	Clipboard Data	Data Obfuscation (3)	Exfiltration Over C2 Channel	Disk Wipe (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Host Software Binary	Create or Modify System Process (5)	Deploy Container	Forge Web Credentials (2)	Cloud Service Discovery	Data from Cloud Storage	Data from Cloud Storage	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Endpoint Denial of Service (4)
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Native API	Create Account (3)	Domain or Tenant Policy Modification (2)	Direct Volume Access	Input Capture (4)	Cloud Storage Object Discovery	Data from Configuration Repository (2)	Data from Configuration Repository (2)	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Financial Theft
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (5)	Domain or Tenant Policy Modification (2)	Execution Guardrails (1)	Modify Authentication Process (9)	Container and Resource Discovery	Data from Fallback Channels	Data from Fallback Channels	Firmware Corruption	Inhibit System Recovery	Network Denial of Service (2)
Search Open Websites/Domains (3)	Trusted Relationship	Shared Modules	Serverless Execution	Event Triggered Execution (16)	Escape to Host	Execution for Defense Evasion	Multi-Factor Authentication Interception	Device Driver Discovery	Taint Shared Content	Taint Shared Content	Hide Infrastructure	Ingress Tool Transfer	Resource Hijacking
Search Victim-Owned Websites	Valid Accounts (4)	Software Deployment Tools	System Services (2)	External Remote Services	File and Directory Permissions Modification (2)	File and Directory Permissions Modification (2)	File and Directory Discovery	Domain Trust Discovery	Use Alternate Authentication Material (4)	Use Alternate Authentication Material (4)	Non-Application Layer Protocol	Non-Standard Port	Service Stop
			User Execution (3)	Hijack Execution Flow (13)	Hide Artifacts (12)	Hijack Execution Flow (13)	Group Policy Discovery	File Enumeration	Data from Local System	Data from Local System	Protocol Tunneling	Proxy (4)	System Shutdown/Reboot
			Windows Management Instrumentation	Implant Internal Image	Hijack Execution Flow (13)	Impair Defenses (11)	Log Enumeration	Network Service Discovery	Data from Network Shared Drive	Data from Network Shared Drive	Remote Access		
				Modify Authentication Process (9)	Process Injection (12)	Impersonation	Network Sniffing	Network Share Discovery	Data from Removable Media	Data from Removable Media			
				Office Application Startup (6)	Scheduled Task/Job (5)	Indicator Removal (9)	OS Credential Dumping (8)	Network Sniffing	Data Staged (2)	Email Collection (3)			
				Power Settings	Valid Accounts (4)	Indirect Command Execution	Steal Application Access Token	Protocol Tunneling	Input Capture (4)				
						Masquerading (9)	Steal or Forge Authentication Certificates	Proxy (4)					
						Modify Authentication	Peripherals Device						

Conoscere la storia

Title : Smashing The Stack For Fun And Profit

Author : Aleph1

.00 Phrack 49 00.

Volume Seven, Issue Forty-Nine

File 14 of 16

BugTraq, r00t, and Underground.org
bring you

XXXXXXXXXXXXXXXXXXXXXXXXXXXX
Smashing The Stack For Fun And Profit
XXXXXXXXXXXXXXXXXXXXXXXXXXXX

by Aleph One
aleph1@underground.org

`smash the stack` [C programming] n. On many C implementations it is possible to corrupt the execution stack by writing past the end of an array declared auto in a routine. Code that does this is said to smash the stack, and can cause return from the routine to jump to a random address. This can produce some of the most insidious data-dependent bugs known to mankind. Variants include trash the stack, scribble the stack, mangle the stack; the term mung the stack is not used, as this is never done intentionally. See spam; see also alias bug, fandango on core, memory leak, precedence lossage, overrun screw.

Introduction

~~~~~

Over the last few months there has been a large increase of buffer overflow vulnerabilities being both discovered and exploited. Examples of these are syslog, splitvt, sendmail 8.7.5, Linux/FreeBSD mount, Xt

**Title** : Introduction

**Author** : Phrack Staff

---[ Phrack Magazine Volume 8, Issue 53 July 8, 1998, article 01 of 15

-----[ P H R A C K 5 3 I N D E X

-----[ Rumble in the Mumble

More than 6 months have passed since our last offering. My most humble, sincere and heartfelt apologies. At long last, here we are. Better late than never, that's what I always say. Unless of course, the late version sucks, then I just like to disavow it entirely. Well, here we go again. Another Phrack issue to glorify behavior which would otherwise be classified as sociopathic or frankly psychotic (according to Mich Kabay). More of what you want, more of what you need. Technical articles on fanatically enticing topics, lines and lines of glorious source, another gut-busting installment of Loopback, and of course, the News. Mammas, don't let your babies grow up to be hackers. Or hookers for that matter.

Alright. Let's get down to business. Let's talk remote attack paradigms. Remote attack paradigms can fall into one of two types, based off of the standard client/server communication paradigm (we are glossing over any extensions to the model like client to client or server to server stuff). The two attack types are client to server (server-centric) and server to client (client-centric). Server-centric attacks are well known, understand and documented. Client-centric attacks are an area that is often overlooked, but is definitely fertile ground for exploitation. Below we look at both.

----[ Server-Centricity

Historically, the vast majority of remote attacks have been server-centric. Server-centric, in this scope, refers to attacks that target server (or daemon) programs. A common (and frequently reoccurring) example is sendmail. The attack targets a server (the sendmail daemon) and approximates a client (the exploit program). There are several reasons why this has been the trend:



# Conoscere la storia

**Title :** NT Web Technology Vulnerabilities

**Author :** rfp

---[ Phrack Magazine Volume 8, Issue 54 Dec 25th, 1998, article 08 of 12

-----[ NT Web Technology Vulnerabilities

-----[ rain.forest.puppy / [WT] <rfpuppy@iname.com>

\*Note: most of the vulnerabilities in this document have NOT been made public; they were discovered by rain.forest.puppy, or other members of WT. Lots of new toys out there on the Internet lately. Seems like the web is the way to go, and every software spigot is demanding they be 'web-enabled'. A lot are reinventing the wheel, bundling sub-standard web servers to serve up their HTML and Java interface.

But this article isn't about them. There's too many, and they're too easy to use as vulnerable targets. It's much more fun to find the needle in the haystack, so I'm going to focus on some more common setups. On to the show.

----[ IIS 4.0

IIS is not too bad as a web server. It still doesn't compare to Apache, but it has flexible scripting and server-side abilities. But, of course, everything has its price...

One interesting problem (and probably the only one that may be previously published at the time of this writing) is that appending an ".idc" extension to the end of a URL will cause IIS installations to try to run the so-called .IDC through the database connector .DLL. If the .IDC doesn't exist, than it returns a rather informative page stating that it can't open %documentroot%\<bogus name>.idc. For example:

"Cannot open c:\inetpub\wwwroot\index.html.idc"

Wow, absolute paths on the server. Very interesting. What good does this do? Well, it gives you some insight and hints. If you're trying to exploit CGI or other server-based programs, knowing what drive you're on when trying to

**Title :** PERL CGI Problems

**Author :** rfp

-----[ Phrack Magazine --- Vol. 9 | Issue 55 --- 09.09.99 --- 07 of 19 ]

-----[ Perl CGI problems ]

-----[ rain.forest.puppy / [ADM/Wiretrip] <rfp@wiretrip.net> ]

-----[ Intro

I guess I should have an intro as to what this is about. Mostly, I've been coding and auditing various CGIs, and was trying to figure out how to leverage a few problems I thought were holes. So whatever, I'll shutup and get onto the holes.

-----[ The Beef

----[ Poison NULL byte

Note: The name 'Poison NULL byte' was originally used by Olaf Kirch in a Bugtraq post. I liked it, and it fit... So I used. Greetings to Olaf.

When does "root" != "root", but at the same time, "root" == "root" (Confused yet)? When you co-mingle programming languages.

One night I got to wondering, exactly what would Perl allow, and could I get anything to blow up in unexpected ways. So I started piping very weird data out to various system calls and functions. Nothing spectacular, except for one that was quite notable...

You see, I wanted to open a particular file, "rfp.db". I used a fake web scenario to get an incoming value "rfp", tacked on a ".db", and then opened the file. In Perl, the functional part of the script was something like:

```
# parse $user_input
$database="$user_input.db";
open(FILE "<$database");
```

# DIY (provare, scrivere codice, tool, exploit, write-up, ..)



# Ma NON “bucare” (vedi Bug Bounty, CTF, ecc.)



# Percorso accademico

In Italia, diverse università offrono percorsi di studio dedicati alla **cybersecurity**, sia a livello di laurea triennale che magistrale. Ecco alcune delle principali:

## 1. Politecnico di Milano

Il Politecnico di Milano offre vari corsi incentrati sulla cybersecurity, sia a livello di laurea che di master. Ha un Master in "Cybersecurity Management" e diversi corsi di laurea triennale e magistrale in Ingegneria Informatica che includono moduli specifici sulla sicurezza informatica.

## 2. Università di Bologna

L'Università di Bologna offre una laurea magistrale in "Ingegneria Informatica" con specializzazioni in cybersecurity. Ha anche un programma di dottorato in sicurezza informatica.

## 3. Università di Roma La Sapienza

La Sapienza di Roma è una delle università più prestigiose in Italia e offre corsi di laurea e master in ingegneria informatica, con opzioni che riguardano la cybersecurity e la protezione delle informazioni.

## 4. Politecnico di Torino

Anche il Politecnico di Torino propone corsi di laurea e master in cybersecurity, tra cui un master in "Cybersecurity e Data Protection", rivolto a chi desidera specializzarsi in protezione dei dati e sicurezza informatica.

# Percorso accademico

## 5. Università Cattolica del Sacro Cuore di Milano

Questa università ha un programma di master in "Cybersecurity and Digital Trust" che offre una formazione completa sulla protezione dei sistemi informatici e sulla gestione del rischio digitale.

## 6. Università degli Studi di Napoli Federico II

L'Università di Napoli offre un Master in "Cybersecurity e Data Protection" e diversi corsi di laurea in Ingegneria Informatica con focus sulla sicurezza.

## 7. Università di Trento

L'Università di Trento ha un programma di Master in "Cybersecurity" che copre vari aspetti della sicurezza digitale, dalla protezione delle reti alla gestione dei rischi informatici.

## 8. Università di Pisa

Pisa offre sia corsi di laurea che di master in sicurezza informatica. Ha anche un programma di dottorato con focus su ricerca avanzata in cybersecurity.

## 9. Università di Milano-Bicocca

Milano-Bicocca ha un Master in "Cybersecurity" con focus su aspetti tecnici e di gestione della sicurezza delle informazioni e dei sistemi.

## 10. Università di Padova

L'Università di Padova offre un corso di laurea magistrale in "Ingegneria Informatica" con moduli specifici sulla sicurezza dei sistemi informatici.



# ITS

In Italia, diversi Istituti Tecnici Superiori (ITS) offrono percorsi formativi specifici nel campo della cybersecurity, rispondendo alla crescente domanda di professionisti specializzati nella protezione delle infrastrutture digitali. Ecco alcuni degli ITS che propongono corsi in questo ambito: [itsprodigi.it +2](http://itsprodigi.it)



# Corsi / Piattaforme di e-learning

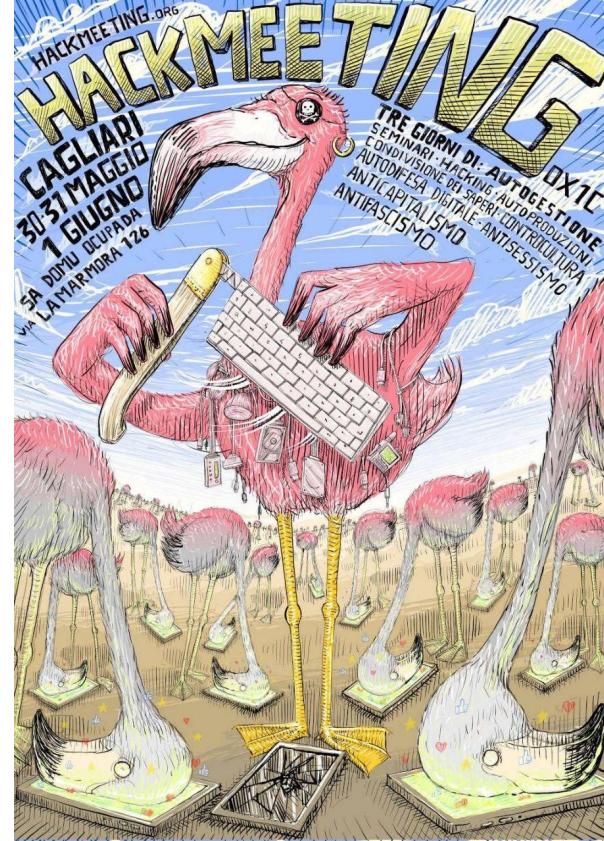
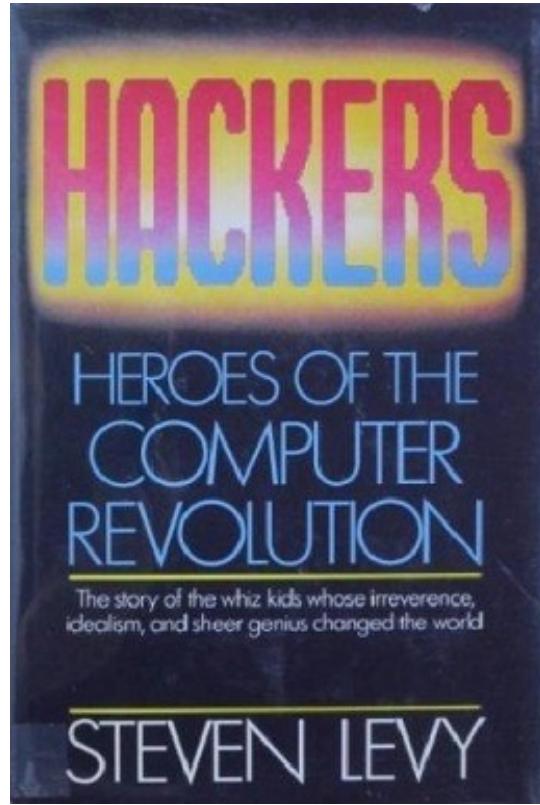


# Conoscere standard e framework

Several standard frameworks and methodologies exist for conducting penetration tests. These include the Open Source Security Testing Methodology Manual (OSSTMM), the Penetration Testing Execution Standard (PTES), the [NIST](#) Special Publication 800-115, the Information System Security Assessment Framework (ISSAF) and the [OWASP](#) Testing Guide. CREST, a not for profit professional body for the technical cyber security industry, provides its CREST Defensible Penetration Test standard that provides the industry with guidance for commercially reasonable assurance activity when carrying out penetration tests.<sup>[13]</sup>



# Hacking != Cyber Security



I miei primi 25 anni (di offensive secur

© 2025 – Igor Falcomatà – koba@cioccolatai.it - Pagina 34

Log in

```
ssh root@segfault.net # The password is 'segfault'
```

NEW: Start a Remote Desktop inside your Browser.

```
root@de.segfault.net:~$ password: TimeMerry..... [OK]
Your Server : TimeMerry..... [OK]
Your workstation : 213.202.239.83 (Germany)
Exit: cryptostorm : 185.117.118.23 (Switzerland)
Exit: Multivad : 185.204.1.224 (Helsinki/Finland)
Exit: NordVPN : 82.102.16.222 (Frankfurt/Germany)
TOR Proxy : 172.20.0.111:9050
Reverse Port : 185.117.118.23:34868
Shared storage : /everyone (encrypted)
Your storage : /sec (encrypted)
Your Onion WWW : /onion (encrypted)
Your Web Page : http://da75bdyvrt5n52xnf6oo0g1qgyvz6qf475pcwzilh1c1c5c6y5ofd.onion/timemerry/
SSH : ssh -o "SetEnv SECRET=KTMelDRNyhRVYTyZTeBzsxo" \
      root@de.segfault.net
SSH (TOR) : torsocks ssh -o "SetEnv SECRET=KTMelDRNyhRVYTyZTeBzsxo" \
      root@es.jtjwrb77k3dgjdgsbeaz6ennt1abzgdy375ndw6gzzmzwvqqd.onion
SSH (gsocket) : gosock -s KochzamQz ssh -o "SetEnv SECRET=KTMelDRNyhRVYTyZTeBzsxo" \
      root@de.segfault.gosocket
root@sf-TimeMerry:~$
```

What it does

**Segfault** offers free unlimited Root Servers. A new server (inside a Virtual Machine) is created for every SSH connection.

- Dedicated Root Server for every user.



Camp Contenuti FAQ Wiki Telegram



End Summer Camp  
[21]

2-7 Settembre 2025  
Parco della Scultura in Architettura  
San Donà di Piave (VE)

Tickets

Call for Papers

87 21 26

DAYS HOURS MINUTES



ESC è un incontro non-profit di persone interessate all'[Hacking](#),  
al [Software Libero](#) e al [DIY](#). Il contenuto dell'evento è in continua  
evoluzione e viene creato dai suoi partecipanti.

# Come continuare?

# Rimanere aggiornati

- **Social Networks (X, mastodon, Linked-In, ...)**
- **Conferenze (+ slide, video, ...)**
- **Community (OWASP, ISACA, ...)**
- **Mailing list**
- **Articoli (e-zine, blog, news, ...)**
- **Piattaforme di e-learning**

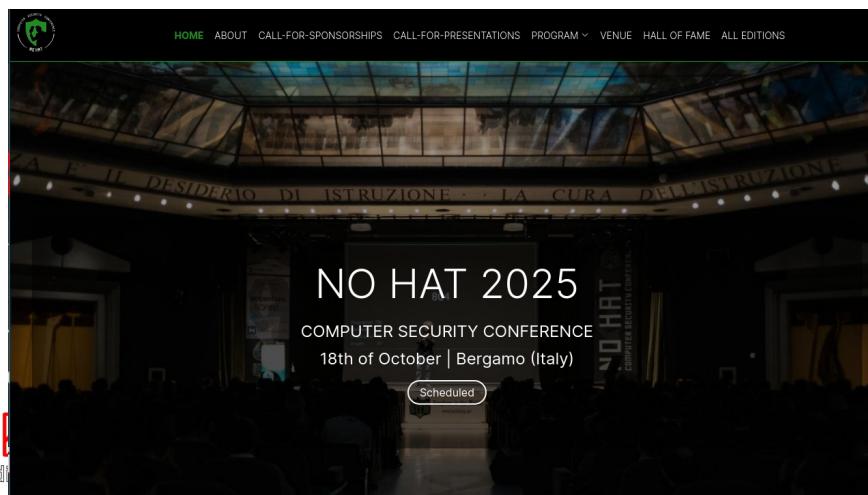
# Conferenze, camp, ..



The HackInBo website features a dark background with a world map. The title "HACKINBO" is prominently displayed in large red letters, with a small sound icon above the "I". Below it, the text "Bologna 07 giugno 2025" is shown in red, followed by a timer: "00 09 50 16 Giorni Ore Minuti Secondi". A blue button at the bottom left says "PRONTI PER LO STREAMING?".



The ROMHACK website has a pink header with the text "ROMHACK CONFERENCE TRAINING CAMP". The main content area is divided into two sections: "CONFERENCE 2025" (September 27, 2025) and "TRAINING 2025" (September 23-26, 2025). Both sections mention Salone delle Fontane as the venue. The conference section notes that early bird tickets sold out in 30 hours, while the training section says full price tickets are available at the beginning of July. A sidebar on the right contains various icons related to the event.



The NO HAT 2025 website shows a large image of a modern building at night. Overlaid text reads "NO HAT 2025 COMPUTER SECURITY CONFERENCE 18th of October | Bergamo (Italy)". A "Scheduled" button is visible at the bottom. The footer includes a small logo and the text "Spring 2025 Ed" and "24° EDIZIONE".



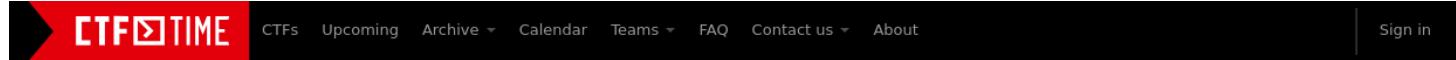
The WHAT HACKERS YEARN website has a dark background with a central neon-style graphic featuring the text "WHY WHY2025". Below it is a large glowing text box containing "What Hackers Yearn". The top navigation bar includes links for NEWS, WHYCST, SPONSORS, BUY TICKETS & MERCH!, and WIKI.



# ... anche locali

- **Bsides**
- **Hacklab**
- **Gruppi CTF universitari**
- **LUG**
- **Gruppi di studio/amici/ecc informali**
- **...**

# Capture The Flag



Home / CTFs / Events / Upcoming

## CTF Events

All Now running Upcoming Archive Format Location Restrictions 2025

| Name                                             | Date                                         | Format   | Location                 | Weight | Notes                             |
|--------------------------------------------------|----------------------------------------------|----------|--------------------------|--------|-----------------------------------|
| MindBreak 2025 by ESGI                           | 06 Giu., 21:00 UTC — 07 Giu. 2025, 06:00 UTC | Jeopardy | Paris, France            | 0,00   | <b>13</b> teams will participate  |
| Season V, US Cyber Open Beginner's Game Room CTF | 06 Giu., 21:30 UTC — 19 Giu. 2025, 23:59 UTC | Jeopardy | On-line                  | 0      | <b>Individual</b>                 |
| DIVER OSINT CTF 2025                             | 07 Giu., 03:00 UTC — 08 Giu. 2025, 03:00 UTC | Jeopardy | On-line                  | 0,00   | <b>88</b> teams will participate  |
| bi0sCTF 2025                                     | 07 Giu., 05:30 UTC — 08 Giu. 2025, 17:30 UTC | Jeopardy | On-line                  | 95,79  | <b>240</b> teams will participate |
| Goldrush Gauntlet 2025                           | 07 Giu., 13:00 UTC — 08 Giu. 2025, 21:00 UTC | Jeopardy | United States, Dahloenga | 0,00   | <b>4</b> teams will participate   |
| DFIR Labs CTF by The DFIR Report                 | 07 Giu., 16:30 UTC — 07 Giu. 2025, 20:30 UTC | Jeopardy | On-line                  | 0      | <b>Individual</b>                 |
| Season V, US Cyber Open Competitive CTF          | 09 Giu., 20:00 UTC — 19 Giu. 2025, 23:59 UTC | Jeopardy | On-line                  | 0      | <b>Individual</b>                 |
| AMSI CTF 2025                                    | 13 Giu., 20:00 UTC — 14 Giu. 2025, 18:00 UTC | Jeopardy | Paris                    | 0,00   | <b>3</b> teams will participate   |
| smileyCTF 2025                                   | 14 Giu., 00:00 UTC — 16 Giu. 2025, 00:00 UTC | Jeopardy | On-line                  | 48,61  | <b>35</b> teams will participate  |
| Crypto CTF 2025                                  | 14 Giu., 06:00 UTC — 15 Giu. 2025, 06:00 UTC | Jeopardy | On-line                  | 88,25  | <b>72</b> teams will participate  |
| Midnight Sun CTF 2025 Finals                     | 14 Giu., 10:00 UTC — 15 Giu. 2025, 10:00 UTC | Jeopardy | Sweden, Stockholm        | 100,00 | <b>2</b> teams will participate   |

# I tool..



Foto: Metal Hammer

I miei primi 25 anni (di offensive security)

© 2025 – Igor Falcomatà – koba@cioccolatai.it - Pagina 41

# ..sono indispensabili, ma..



SECTOOLS.ORG Site Search

[Home](#) [About/Help](#) [Suggest a new tool](#)

## Top 50 Security Tools

**Note:** These are archived 2000 survey results. For the latest survey, visit <http://SecTools.Org>.

In May/June of 2000, we conducted a survey of 1200 [Nmap](#) users from the [nmap-hackers](#) mailing list to determine their favorite security tools. Each respondent could list up to 5.

I was so impressed by the list they created that I am putting the top 50 up here where everyone can benefit from them. I think anyone in the security field would be well advised to go over the list and investigate any tools that are unfamiliar with. I also plan to point newbies to this page whenever they write me saying "I do not know where to start".

Respondents were allowed to list open source or commercial tools on any platform. Commercial tools are included as such in the list below.

Note that many of the descriptions in this list were taken from the [Debian](#) package descriptions, the [FreeBSD](#) descriptions, or from the home pages of the application. I didn't count any votes for [Nmap](#) because the survey was taken on an Nmap mailing list.

Without further ado, here is the list (starting with the most popular):

**Nessus** <http://www.nessus.org>

**Description:** Remote network security auditor, the client The Nessus Security Scanner is a security audit tool. It makes possible to test security modules in an attempt to find vulnerable spots that should be fixed. It is made up of two parts: a server, and a client. The server/daemon, nessusd, is in charge of the attacks, while the client, nessus, interferes with the user through nice X11/GTK+ interface. This package contains the 1.2 client, which exists in other forms and on other platforms, too.

**Netcat** <http://www.atstake.com/research/tools/index.html>

**Note:** This is an unofficial site

**Description:** TCP/IP swiss army knife A simple Unix utility which reads and writes data across network



KALI

GET KALI BLOG DOCUMENTATION COMMUNITY COURSES DEVELOPERS ABOUT

## Kali Tools

Tool Documentation

Want to learn more about a tool? Search for it here!

LIGHT  DARK

Didn't find the tool?

[CHECK REQUESTED TOOLS](#)

[SUBMIT NEW TOOL](#)

[:: Source](#) | [:: Package](#) | [\\$ :: Command](#)

[List all tools](#)



\$ dpl4hydra  
\$ hydra  
\$ hydra-wizard  
\$ pw-inspector



\$ restfulHarvest  
\$ theHarvester  
\$ theharvester



\$ appid\_detector\_...  
\$ snort  
\$ snort2lua



\$ steghide  
\$ steghide  
\$ steghide-doc



\$ captiveflask  
\$ eviltq3  
\$ phishkin3  
\$ ssstrip3



Mai Dire  
@maidireofficial

...

tool

Nel mondo ci sono milioni di ~~videocamere~~, ma ancora più numerosi sono gli ~~st~~ che le manovrano! 😂 #MaiDireStory



11:17 AM · 1 apr 2018

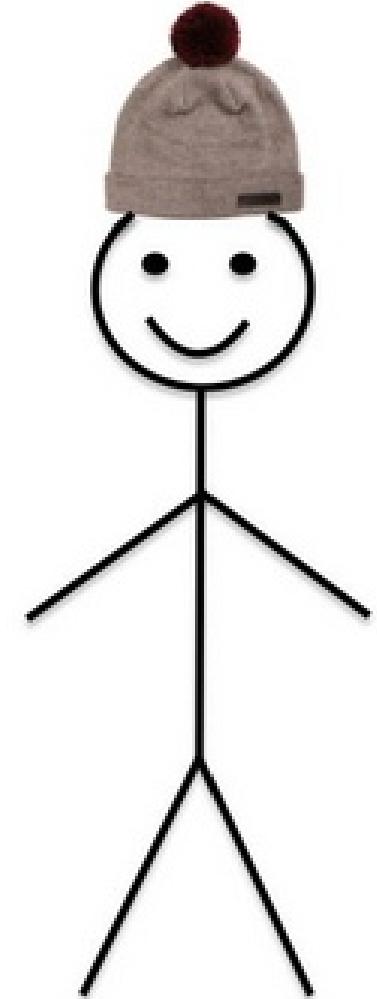


1

10

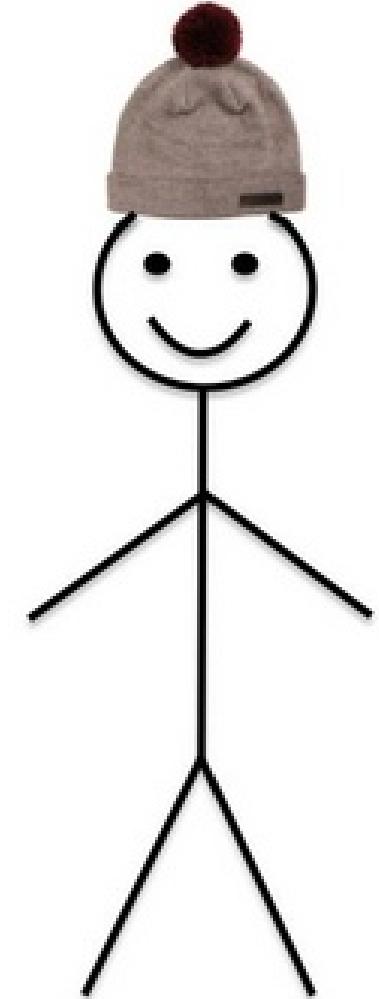


# This is Bob..



# This is Bob..

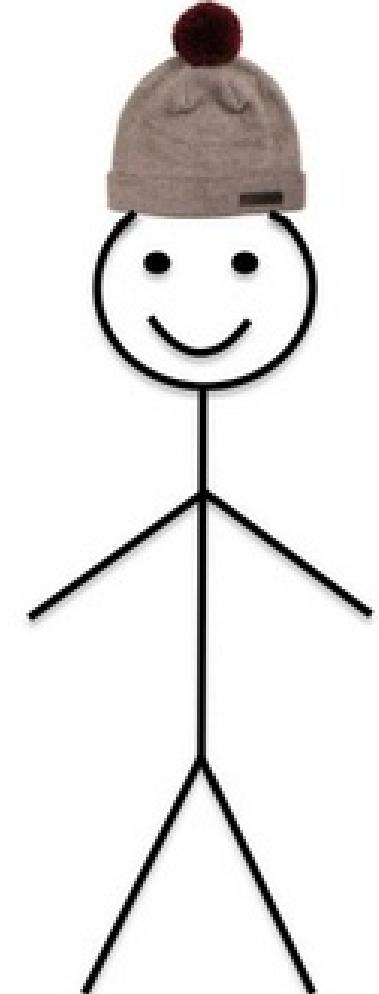
## .. Bob usa i tool, molti tool ..



# This is Bob..

**.. Bob usa i tool, molti tool ..**

- **sa come funzionano**
- **sa leggere il manuale**
- **sa guardare il traffico di rete**
- **sa interpretare il debug**
- **capisce il codice sorgente**

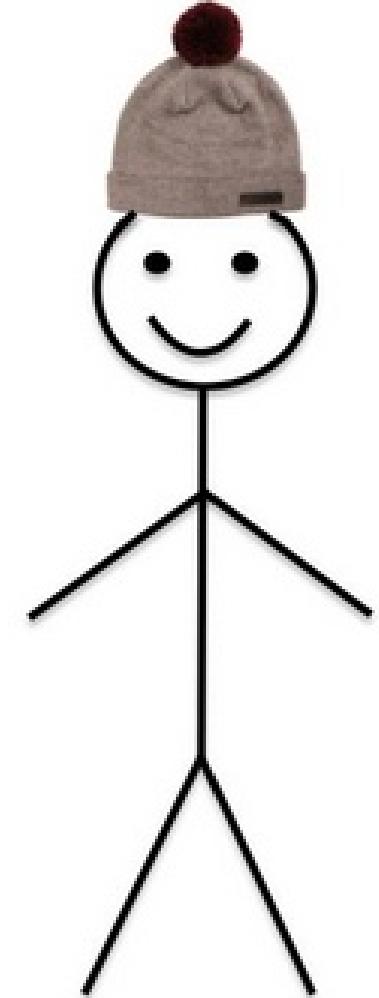


# This is Bob..

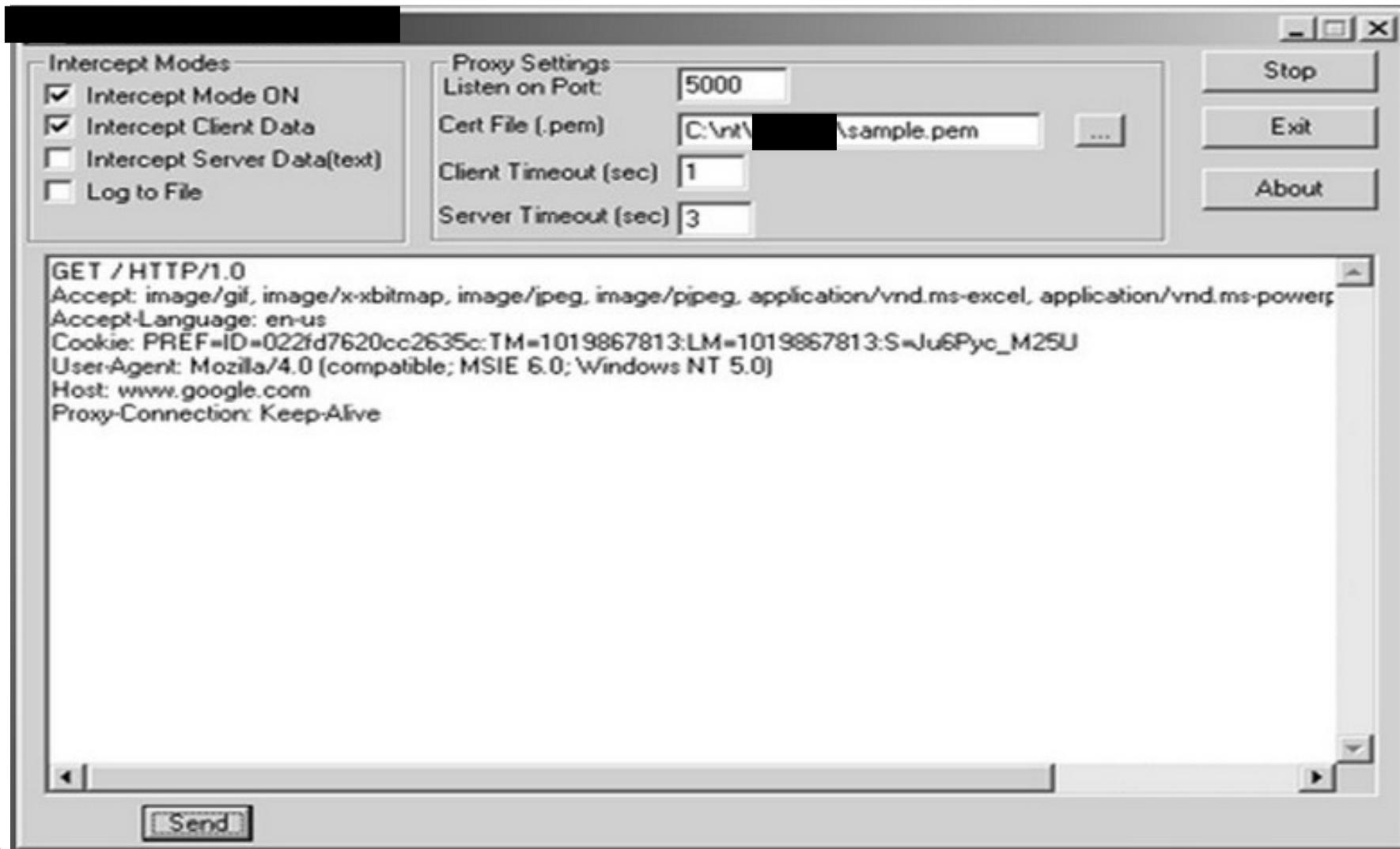
**.. Bob usa i tool, molti tool ..**

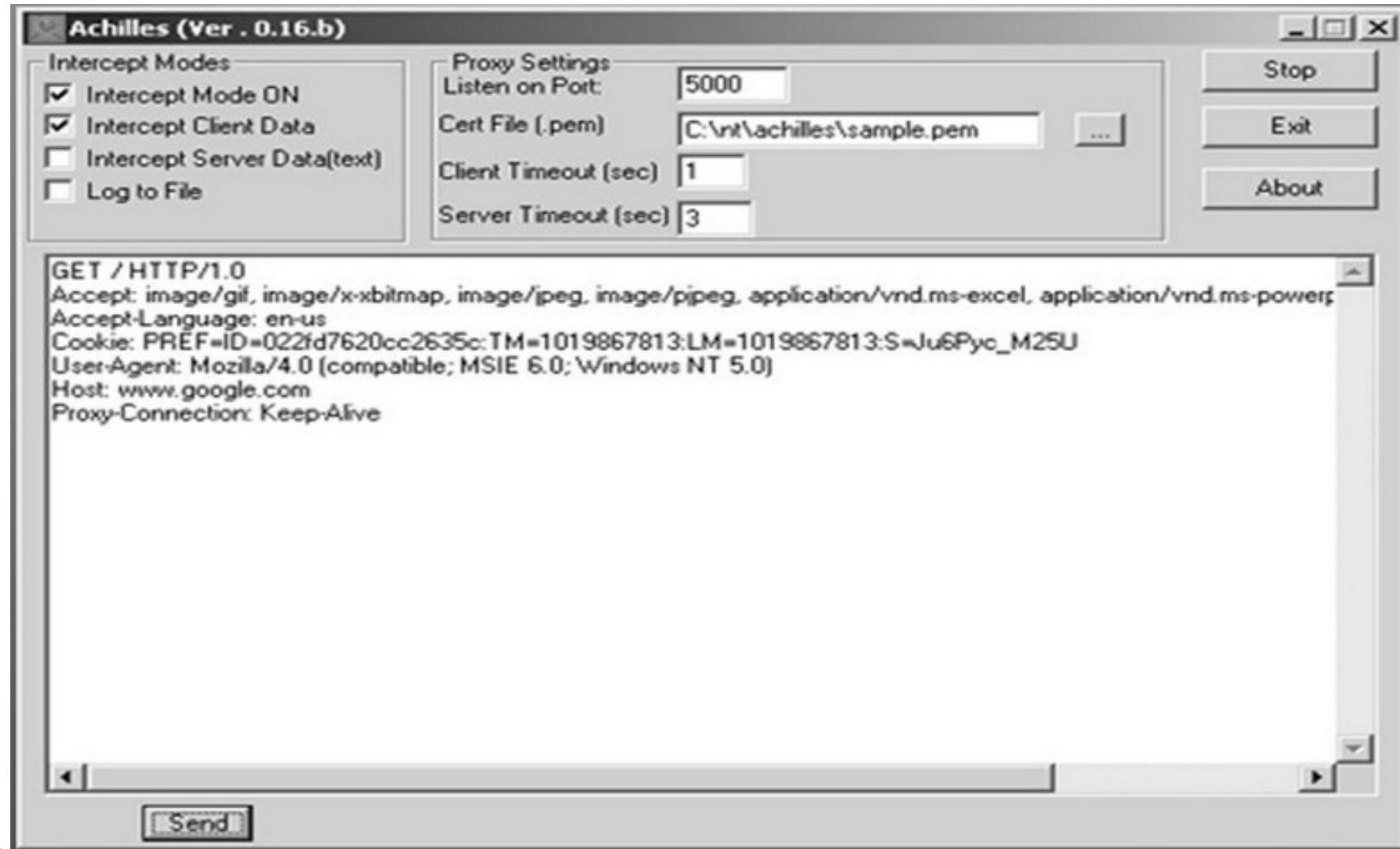
- **sa come funzionano**
- **sa leggere il manuale**
- **sa guardare il traffico di rete**
- **sa interpretare il debug**
- **capisce il codice sorgente**

**Be like Bob**



> Terminal - root@vlinux: ~





# Il mindset

# Workflow



# Log, log, log, ...



# Knowledge base

## Knowledge Base

Search the knowledge base...

### Frequently Asked Questions

- Tecniche di Attacco
- Simulazione di Minacce
- Valutazione delle Vulnerabilità
- Analisi dei Rischi
- Gestione degli Incidenti

### Recent Articles

- Gestione degli Incidenti  
Lorem ipsum dolor sit amet.
- Post-Exploitation  
Lorem ipsum dolor sit amet.
- Tattiche di Evasione  
Lorem ipsum dolor sit amet.



# Repository

The screenshot shows a GitHub repository page for the user 'octocat' named 'my-project'. The repository is public. The main navigation bar includes 'Explore', 'Issues', 'Pull Requests', a search bar, and a profile icon. Below the header, the repository name 'octocat / my-project' and its status ('public') are displayed, along with dropdown menus for 'Code', 'Issues', 'Pull Requests', and 'Actions'. A summary section shows '1 branch', '1 main', and '0 tags', with buttons for 'Branch' (set to 'main') and 'New Pull Request'. The main content area displays a list of recent commits:

| Commit  | Author  | Message          | Date                  |             |
|---------|---------|------------------|-----------------------|-------------|
| 582feb0 | octocat | Update README.md | 2 hours ago           |             |
|         |         | README.md        | Update README.md      | 2 hours ago |
|         |         | src/             | Add source code files | 3 days ago  |
|         |         | Dockerfile       | Create Dockerfile     | 6 days ago  |
|         |         | index.js         | Initial commit        | 6 days ago  |

At the bottom, there is a link to 'View all commits'.

# La potenza è nulla.. senza report

## Penetration Test Report

Tizio Caio

Pippotronic Inc.

April 2024

of a penetration test con-  
target system.

evaluation of the sparing  
and evidence examining

ologies used during these  
ommendations for impos-  
target system against thre-

ferred to ethical hacking)  
k on a computer system,  
nesses that could exploit  
prove insight into existing

security measures, and to provide recommendations for addressing identified issues.

In the presence of cyber attack, especially, under intu-  
ced rise, regular assessments and proactive security measures  
to reduce the risk of breaches and maintain the integrity and  
confidentiality of sensitive data.



# PENETRATION TEST REPORT

TIZIO CAIO

 PIPPOTRONIC



## INTRODUCTION

This report presents the results of a penetration test conducted to assess the security posture of the target organization's information systems. The primary objective of the test was to identify vulnerabilities, evaluate the effectiveness of existing security measures, and provide recommendations for improving the organization's security posture.

The penetration test was carried out over a period of five days and included both external and internal assessments. Testing methodologies included automated scanning, manual inspection, and exploitation of identified vulnerabilities. The scope and limitations of the test are outlined below.

# Bug Bounties

# Bug Bounties



# Vibe Coding..

# Per Eliza

Conosci il chatbot eliza? vorrei fare per il classico scherzo del primo aprile di sikurezza.org un chatbot utilizzabile via web, probabilmente solo javascript senza componenti server side, che intrattenga il visitatore su tematiche di cyber security utilizzando gli stessi principi di eliza

## Aggiornamento della memoria salvata completato

Ottima idea! Un chatbot in puro JavaScript senza componenti server-side è fattibile usando il modello di ELIZA, che si basa su pattern matching e trasformazioni di testo per simulare una conversazione. Posso sviluppare una versione che risponda con frasi ironiche o "da psicologo" su tematiche di cybersecurity. Ti serve solo il codice o anche una pagina HTML pronta all'uso?



grazie, ottimo. anche la pagina html per favore.

Ecco una versione del chatbot basato su ELIZA, con risposte a tema cybersecurity. Il codice è completamente client-side, senza necessità di server.

[Eliza Cyber Chatbot](#)

Ecco il codice HTML con il chatbot basato su E ↓ A per tematiche di cybersecurity. Si basa su

# Per Eliza

Conosci il chatbot eliza? vorrei fare per il classico scherzo del primo aprile di sikurezza.org un chatbot utilizzabile via web, probabilmente solo javascript senza componenti server side, che intrattenga il visitatore su tematiche di cyber security utilizzando gli stessi principi di eliza

## Aggiornamento della memoria salvata completato

Ottima idea! Un chatbot in puro JavaScript senza componenti server-side è fattibile usando il modello di ELIZA, che si basa su pattern matching e trasformazioni di testo per simulare una conversazione. Posso sviluppare una versione che risponde con frasi ironiche o "da psicologo" su tematiche di cybersecurity. Serve solo il codice, anche una pagina HTML per la prova?

# Bad Vibes

grazie, ottimo. anche la pagina html per favore.

Ecco una versione del chatbot basato su ELIZA, con risposte a tema cybersecurity. Il codice è completamente client-side, senza necessità di server.

[Eliza Cyber Chatbot](#)

Ecco il codice HTML con il chatbot basato su Eliza per tematiche di cybersecurity. Si basa su

# Per Eliza

ehm.. potresti sanitizzare l'input passato dall'utente prima di utilizzarlo per aggiornare la pagina, contro xss & co?

Certo! È molto importante sanitizzare l'input per evitare vulnerabilità come **XSS** (Cross-Site Scripting). Per proteggere il tuo chatbot da attacchi XSS, puoi fare in modo che l'input dell'utente venga **sanitizzato** prima di essere visualizzato sulla pagina.

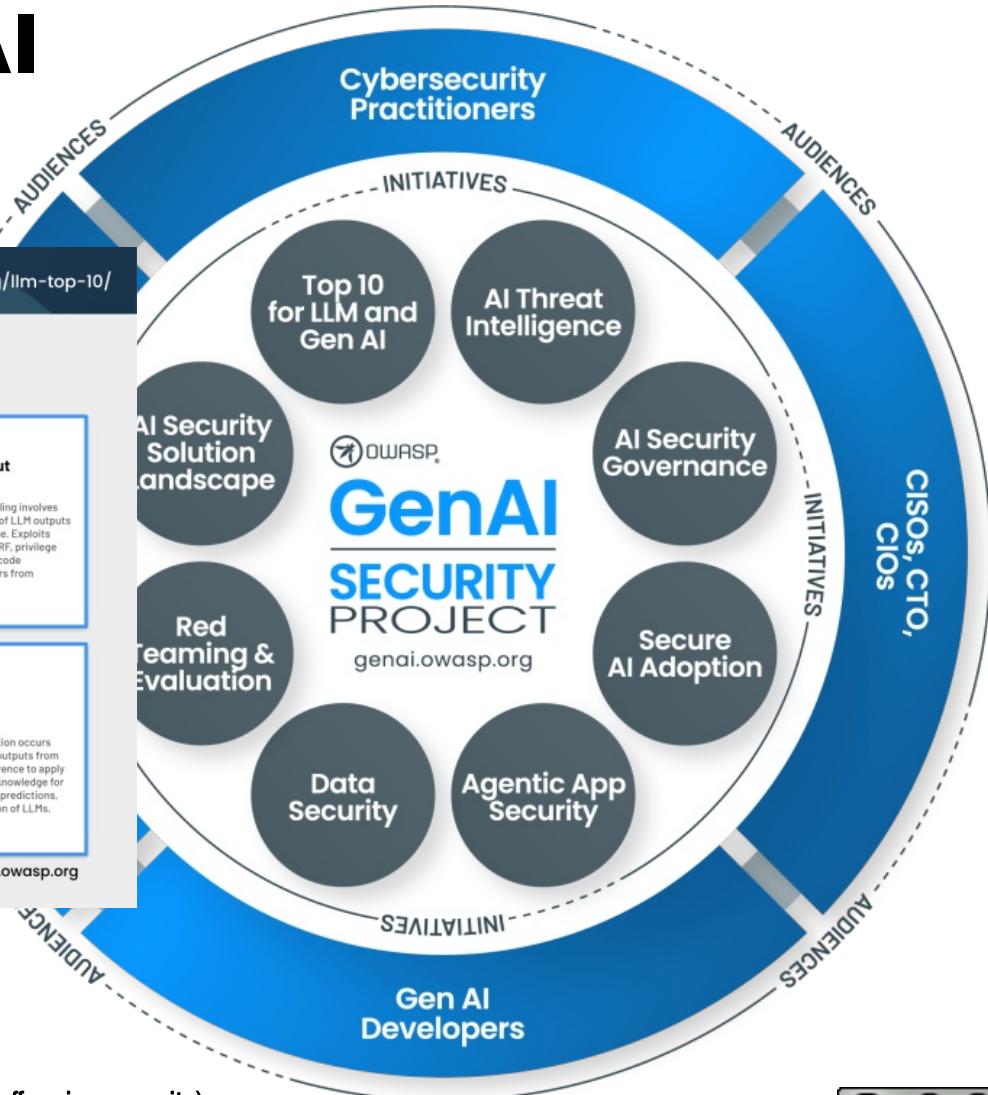
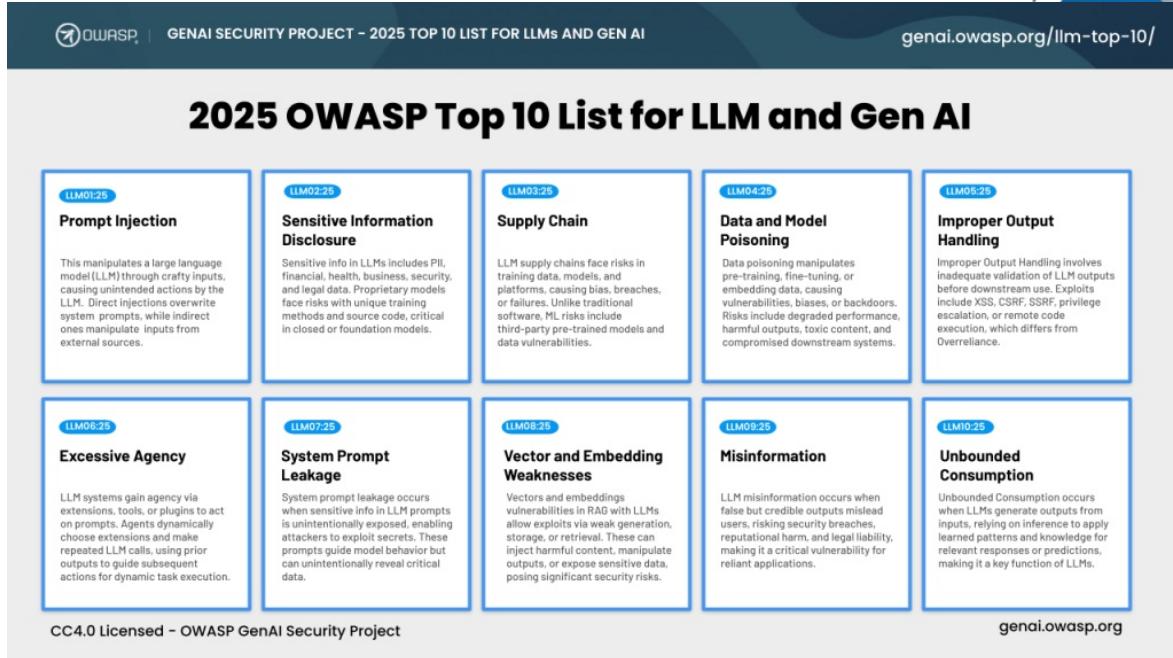
Puoi farlo utilizzando una funzione che converte i caratteri speciali in entità HTML, impedendo l'esecuzione di codice malicioso. Ecco come puoi fare:

1. Creiamo una funzione per sanitizzare l'input.
2. La utilizziamo prima di aggiornare la pagina con il testo dell'utente.

Ecco il codice aggiornato con la sanitizzazione dell'input:

# AI, AI, AI, ...

# Offensive Security vs AI



# AI for Offensive Security

[LOGIN](#)[Products](#) | [Solutions](#) | [Research](#) | [Academy](#) | [Support](#) | [≡](#)

## Using AI to find web app vulnerabilities: hacking expert John Hammond takes Burp AI for a spin

Amelia Coen | 30 April 2025 at 13:23 UTC



The screenshot shows the Burp Suite Pro interface with the "Burp AI" tab selected. A large magnifying glass highlights a red and blue bug icon, symbolizing a found vulnerability. The interface displays a list of audit items, including tasks like "Crawl and audit of ghandulice.shop" and "Live audit from...". The "Issues" section shows several findings, such as "Broken access control" with a severity of "High" and a confidence of "Medium". The URL for this issue is <https://ghandulice.shop/orders/detail>. The overall theme is dark with purple and blue highlights.

The S in MCP  
stands for  
**Security**

The "S" in MCP stands for "Security," referring to the Model Context Protocol, which is a standard for how Large Language Models (LLMs) interact with tools and data. However, it is important to note that MCP is not secure by default, which raises potential security concerns.

 conffab.com  Y Combinator

Generato automaticamente in base alle fonti elencate. Può contenere imprecisioni.

Chiedi un approfondimento

chat

Ti è stato utile?  

 Medium · Elena Cross  
Oltre 290 Mi piace · 2 mesi fa

## The "S" in MCP Stands for Security | by Elena Cross | Medium

MCP, short for Model Context Protocol, is the hot new standard behind how Large Language Models (LLMs) like Claude, GPT, or Cursor integrate with tools and ...

 Hacker News  
<https://news.ycombinator.com> · ... · Traduci questa pagina

## The "S" in MCP Stands for Security

7 apr 2025 — Do you know what it's called when data is treated as code when it's not supposed to be? It's called a "**security** vulnerability." Untrusted data ...

 LinkedIn · Luc van Donkersgoed  
Oltre 170 reazioni · 1 mese fa

## The "S" in MCP Stands for Security | Luc van Donkersgoed

If you run local **MCP** servers (and most of you are), you're literally allowing an unknown author to execute code on your machine with every prompt.

 Reddit · r/ClaudeAI  
4 commenti · 1 mese fa

## The "S" in MCP Stands for Security - ClaudeAI

Auth is baked into the protocols, this is why Anthropic didn't support it yet in Claude desktop. So the experts demonstrate only how he's ...

**The "S" in MCP Stands for Security** : r/programming 50 post 7 apr 2025  
**The "S" in MCP Stands for Security** 11 post 6 apr 2025

Altri risultati in [www.reddit.com](http://www.reddit.com)

Le persone hanno chiesto anche :

What is MCP in security?

What is MCP in cyber security?



# I got a job!

# Dress code



# Cercare lavoro



# Siate soffici



# Attenti al lato oscuro..



# In conclusione

# Give Back: Condividere per Crescere

The collage consists of several screenshots:

- A large group photo of the ParrotSec community at a conference.
- The official Parrot Security website homepage, featuring the tagline "The operating system for Hackers!" and a "Tools for every operation" section.
- A GitHub repository page for `byt3bl33d3r / CrackMapExec`, showing a list of commits and repository details.
- A GitHub repository page for `bettercap / bettercap`, showing a list of commits and repository details.
- The `sqlmap` project page on GitHub, featuring the tool's logo and download links.

I miei primi 25 anni (di offensive security)

# In conclusione

*[..] leave the game better than  
you found it so this game can  
continue to go on forever*

Larry Bird

# References

NB: all previous slides already have links pointing to the relative references

**Understanding Hackers' Work: An Empirical Study of Offensive Security Practitioners**

<https://arxiv.org/abs/2308.07057> (Andreas Happe, Jürgen Cito, 2023)

**A Modern History of Offensive Security Research** (Dino Dai Zovi, 2018)

<https://docs.google.com/presentation/d/19HfklojyLE8L8X8aZT-IJont96Jqlg4PqEhb2juIK2c/mobilepresent?slide=id.p>

**A brief history of security testing** (Tyler Bohlmann, 2022-2024)

<https://redcanary.com/blog/testing-and-validation/security-testing/>

**Pen Testing: Past, Present, and Future: An Inside Look Through Decades Of Security** (Joel Scambray, 2022)

<https://www.nccgroup.com/us/pen-testing-past-present-future/>

**Assumed Breach: The Evolution of Offensive Security Testing** (Jason Lang, 2024)

<https://trustedsec.com/blog/assumed-breach-the-evolution-of-offensive-security-testing>

**Marco `Raptor` Ivaldi - Hacking degli anni '90 tra IRC, Linux&C e Mitnick** (Podcast interview, italian)

<https://www.youtube.com/watch?v=nLH731xkftg>

**Stefano Chiccarelli - Hacking made in Italy dagli anni '80 ad oggi** (Podcast interview, italian)

<https://www.youtube.com/watch?v=nUpZs6Kvlwg>

**The ENISA Threat Landscape (ETL) report** (AAVV, ENISA)

<https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends>



# There Can Be Only One