Normative tecniche internazionali su testing e gestione di soluzioni IT

Relatore: Dott. Ing. Gianluca Golinelli

Gianluca Golinelli

g.golinelli@gianlucagolinelli.it

www.gianlucagolinelli.it

- Electronic Engineer, Laurea from University of Parma
- IT Security Specialist and Digital Forensics Consultant
- Board Member of C3I (Italian Commitee of Information Engineering)
- Technical Consultant of the Law Court of Parma
- Coordinator of the working group of Informatics, Electronics and Telecommunications of the Order of Parma Engineers from 2003 to 2017

Normative tecniche internazionali su testing e gestione di soluzioni IT

Agenda

1. Sistemi per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche (rif. Ethical Hacking)
2. Processi per il monitoraggio del rispetto degli adempimenti Privacy in tutto il ciclo di sviluppo dei sistemi informativi (rif. ISO27001 Annex A)
3. Processi per il monitoraggio dell'efficacia delle soluzioni tecniche ed organizzative in uso per la protezione dei dati (rif. ISO27002)

Normative tecniche internazionali su testing e gestione di soluzioni IT

Articolo 25

(continua) Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

3. Un **meccanismo di certificazione approvato** ai sensi dell'articolo 42 può essere utilizzato come elemento **per dimostrare la conformità ai requisiti** di cui ai paragrafi 1 e 2 del presente articolo.

Normative tecniche internazionali su testing e gestione di soluzioni IT

Articolo 32

(continua) Sicurezza del trattamento

….

d) una **procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche** e organizzative al fine di garantire la sicurezza del trattamento.

…..

3. L'adesione a un **codice di condotta** approvato di cui all'articolo 40 o a un **meccanismo di certificazione** approvato di cui all'articolo 42 **può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1** del presente articolo.

Come rilevare/scoprire vulnerabilità nei sistemi

- Vulnerability Assessment
- Ethical Hacking (PenTest)

- Code Review (Ispezione del codice)
- Testing funzionale (Black box, White box, fuzzing)

Gli asset da testare

- Server, Client
- Canali e protocolli trasmissivi
- Dispositivi di rete
- Applicazioni
- Sistemi operativi per la virtualizzazione
- Sistemi operativi mobile
- Hardware
- Sale server

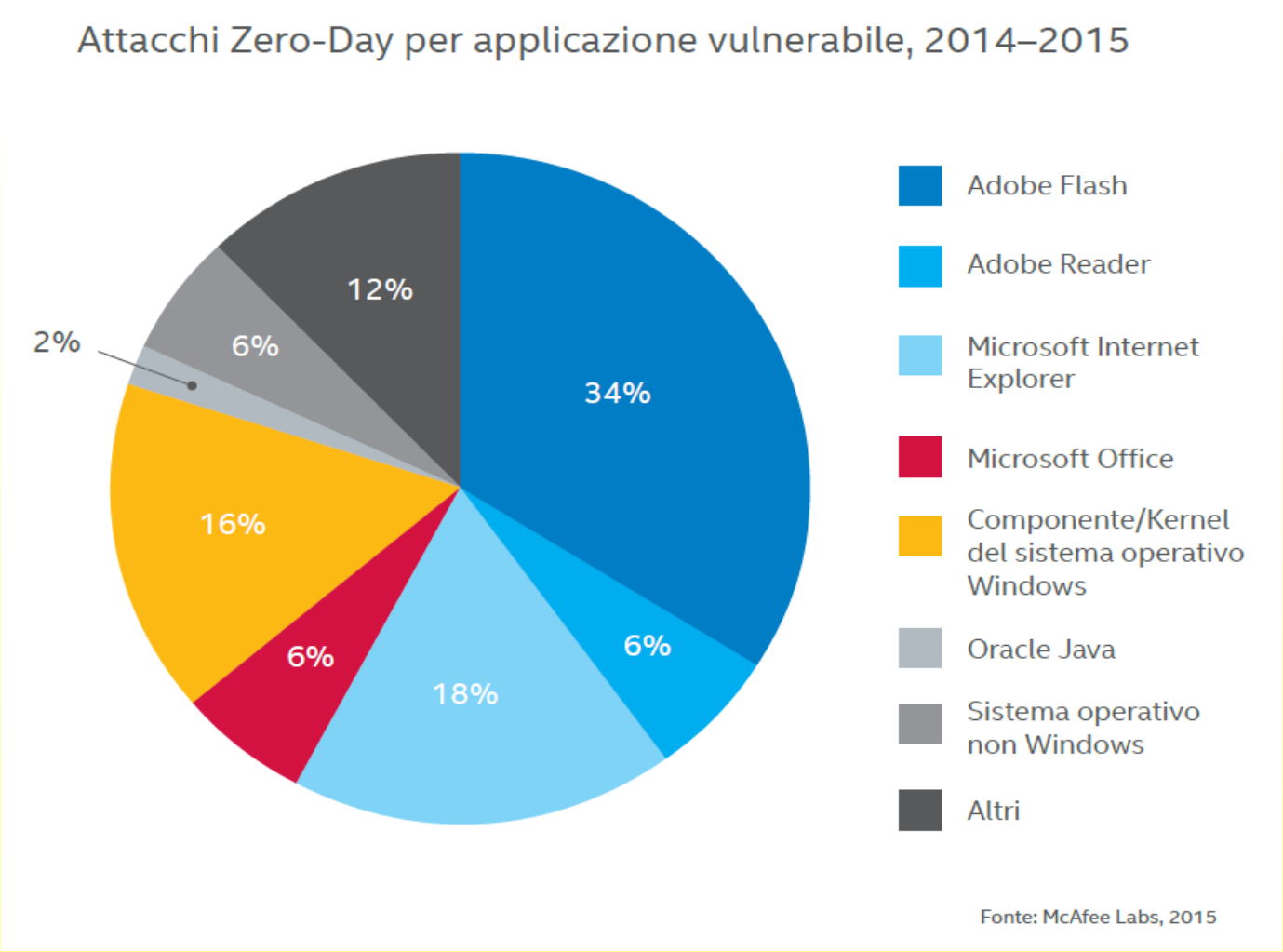
Le vulnerabilità IT

- Vulnerabilità dei sistemi operativi
- Vulnerabilità dei servizi del sistema operativo
- Vulnerabilità nelle applicazioni
- Vulnerabilità nei protocolli di comunicazione
- Vulnerabilità hardware
- Vulnerabilità nei dispositivi di networking
- Vulnerabilità delle risorse umane

Vulnerabilità: alcuni esempi recenti

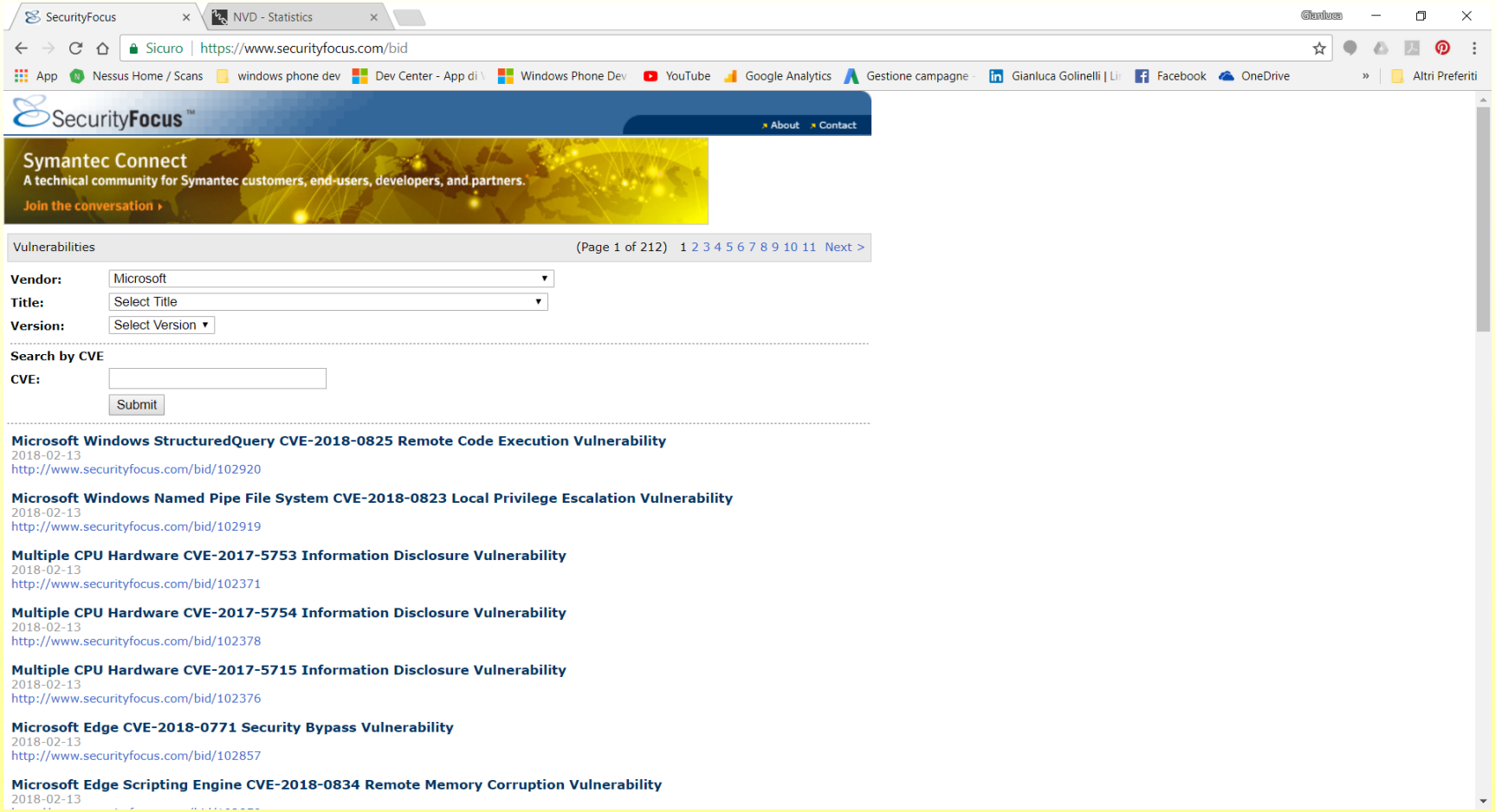
- **Windows SMB** Remote Code Execution Vulnerability (Microsoft Bulletin MS17-010) → WannaCry, Petya
- **Adobe Flash Player** versions 25.0.0.171 arbitrary code execution vulnerability (CVE-2017-3084)
- **Adobe Acrobat Reader** versions 15.020.20042 and earlier, arbitrary code execution vulnerability (CVE-2017-3010)
- **Microsoft Internet Explorer** 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability." (CVE-2016-7283)

Sistemi per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche (rif. Ethical Hacking)



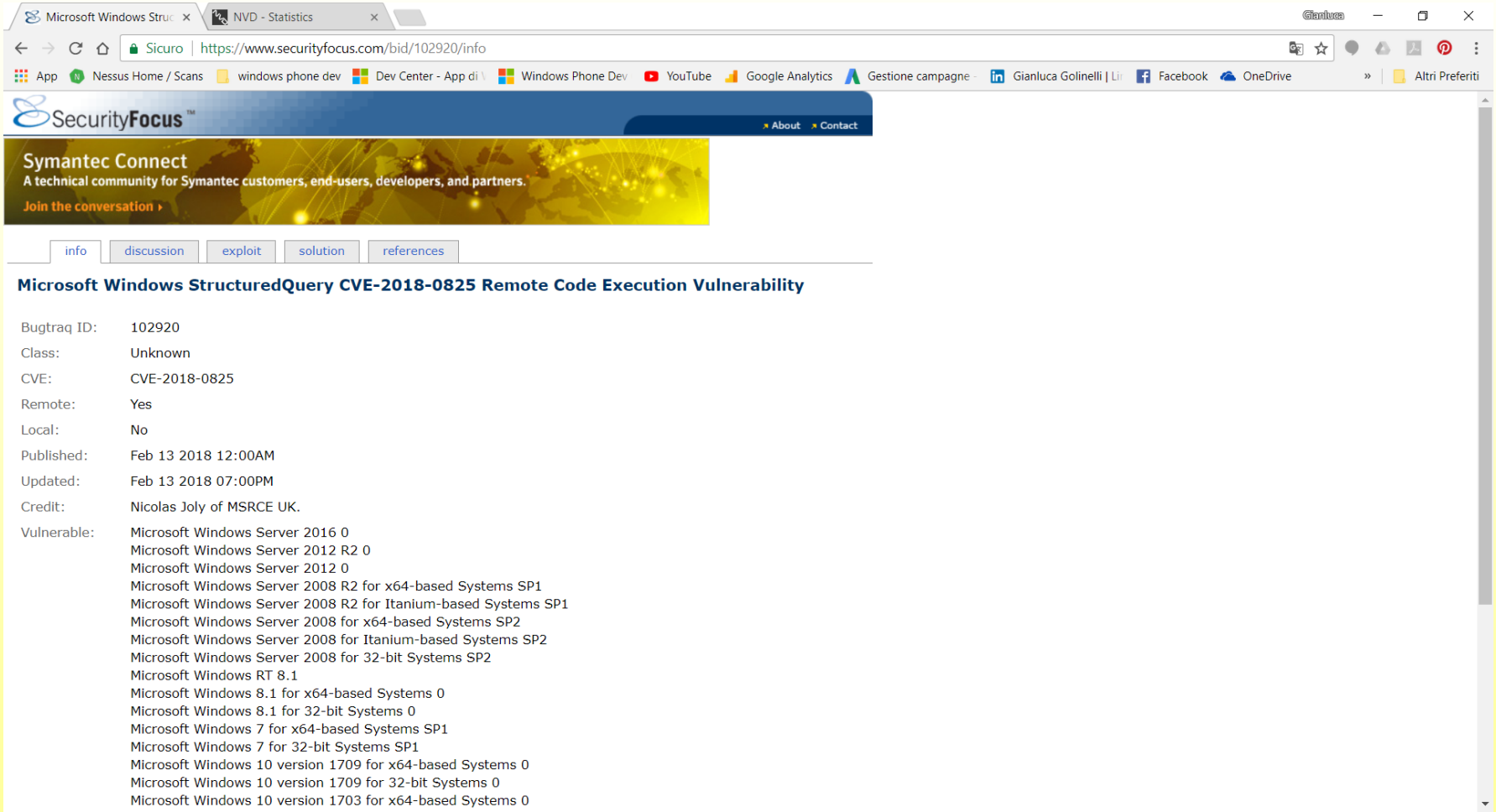
Sistemi per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche (rif. Ethical Hacking)

Ricercare vulnerabilità



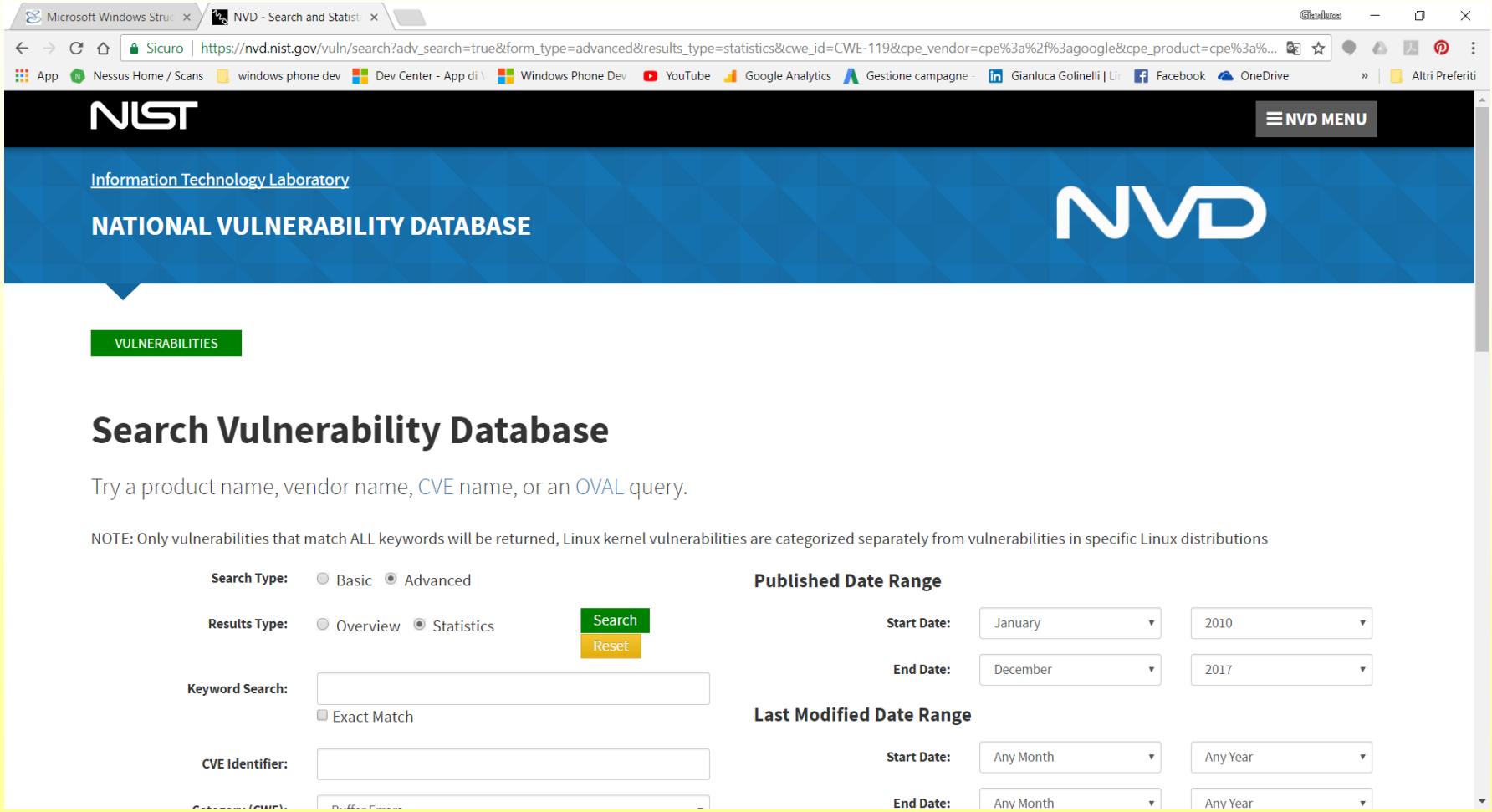
Sistemi per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche (rif. Ethical Hacking)

Ricercare vulnerabilità



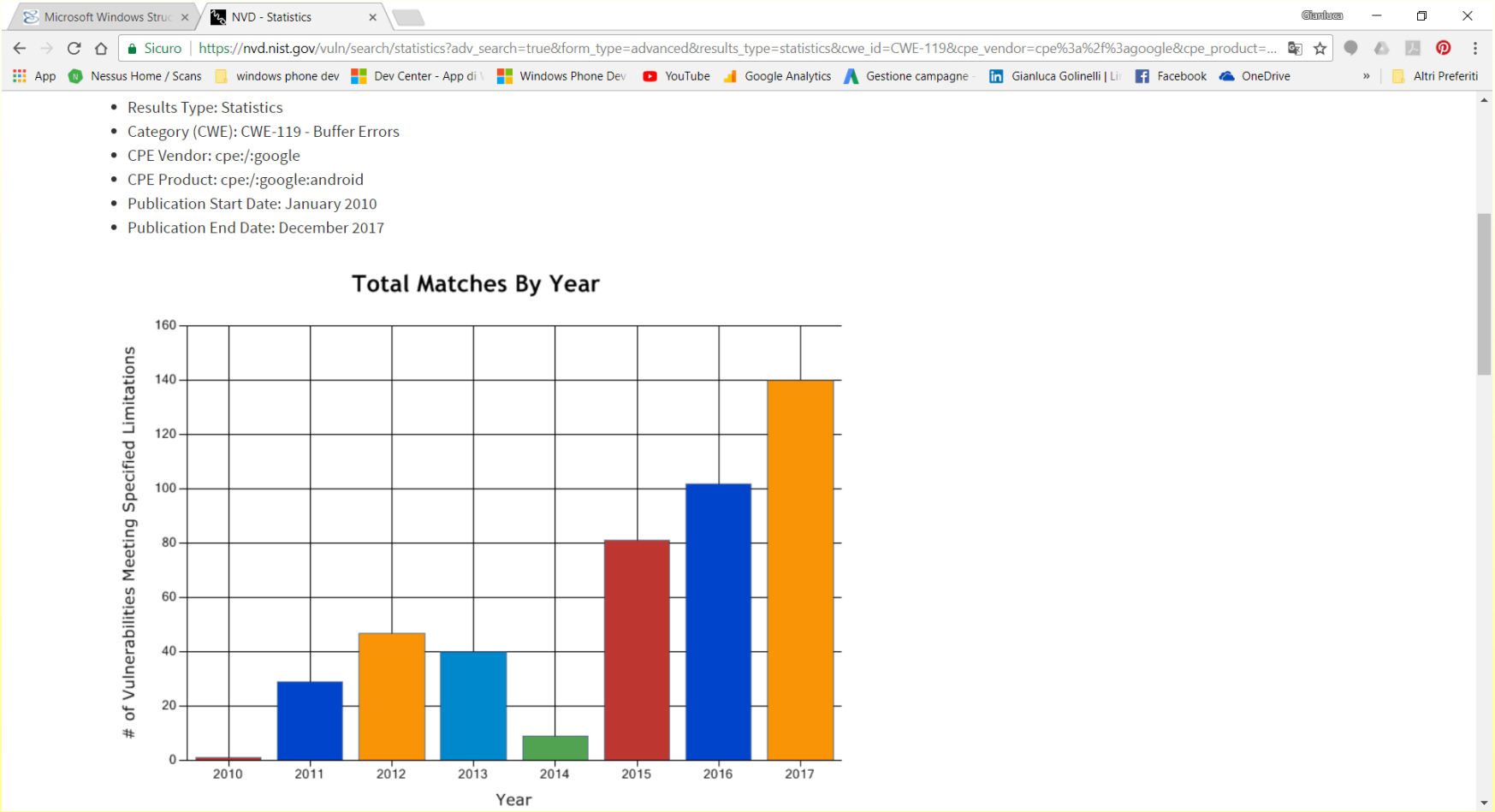
Sistemi per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche (rif. Ethical Hacking)

Ricercare vulnerabilità



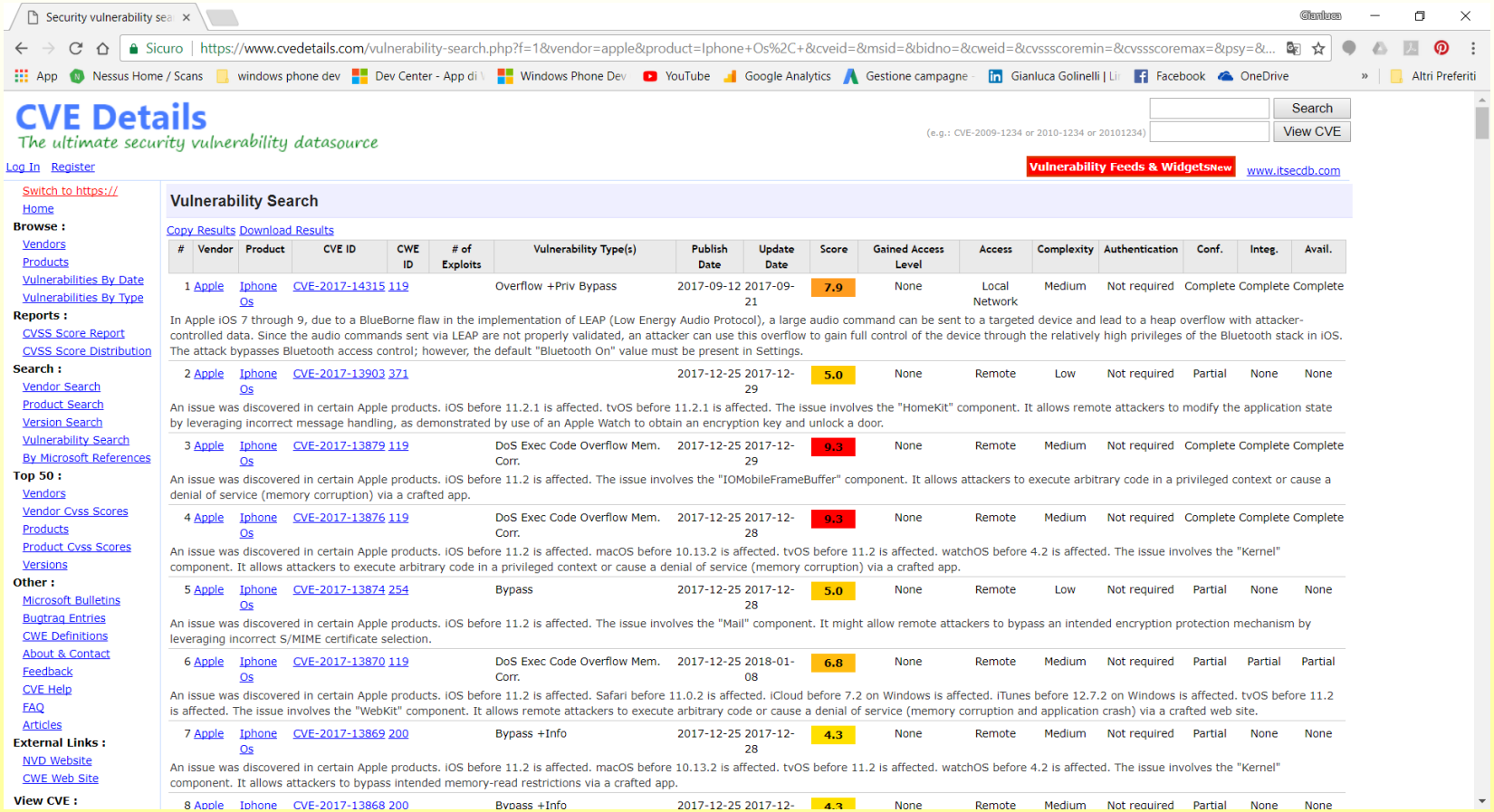
Sistemi per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche (rif. Ethical Hacking)

Ricercare vulnerabilità



Sistemi per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche (rif. Ethical Hacking)

Ricercare vulnerabilità



Security vulnerability sea

Sicuro | https://www.cvedetails.com/vulnerability-search.php?f=1&vendor=apple&product=Iphone+Os%2C+&cveid=&msid=&bidno=&cweid=&cvssscoremin=&cvssscoremax=&psy=&...

App | Nessus Home / Scans | windows phone dev | Dev Center - App di | Windows Phone Dev | YouTube | Google Analytics | Gestione campagne | Gianluca Golinelli | Li | Facebook | OneDrive | Altri Preferiti

CVE Details

The ultimate security vulnerability datasource

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234) Search | View CVE

Log In | Register

Vulnerability Feeds & Widgets New | www.itsecdb.com

Switch to https://
Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact
Feedback
CVE Help
FAQ
Articles
External Links :
NVD Website
CWE Web Site
View CVE :

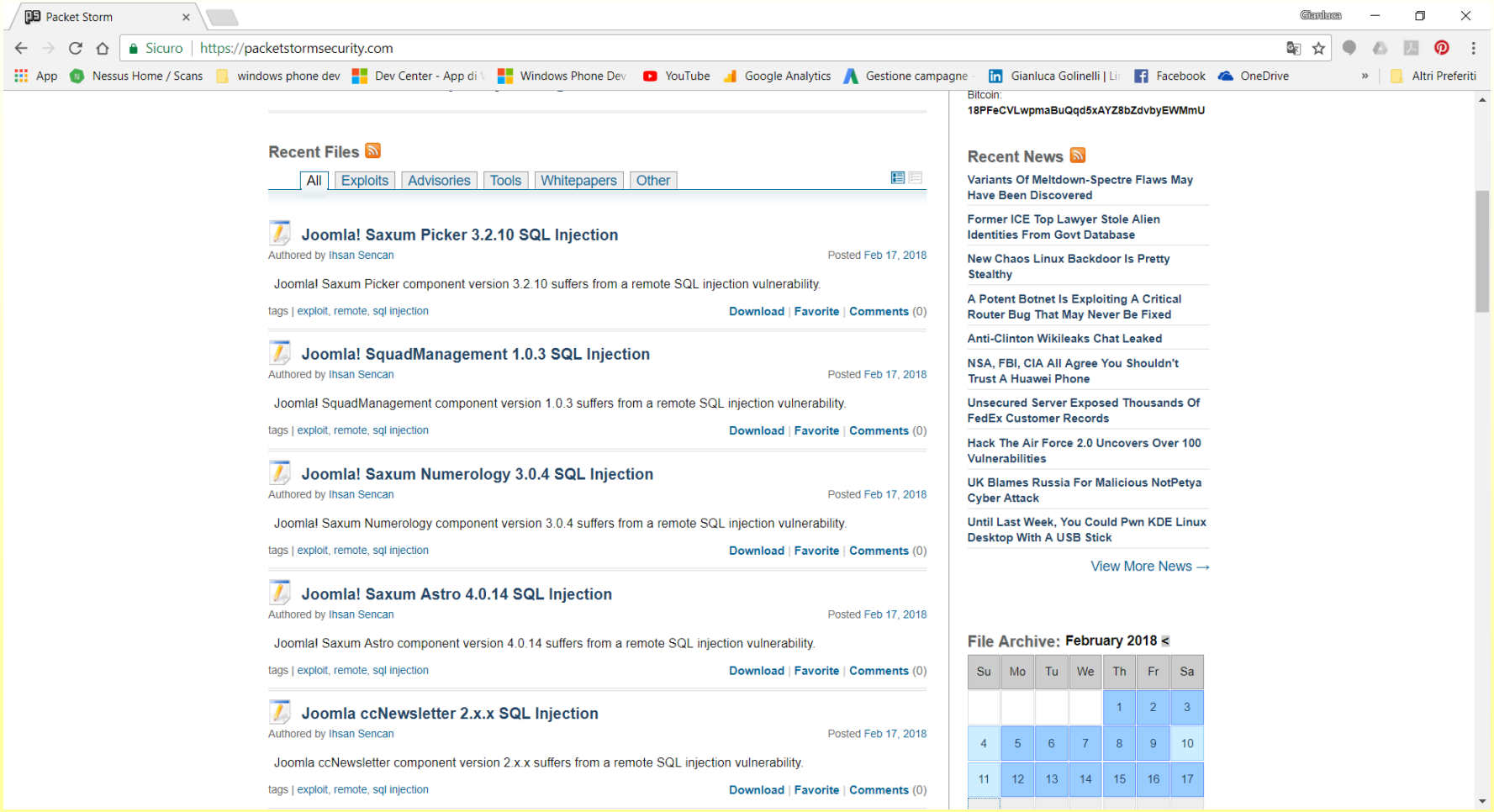
Vulnerability Search

Copy Results | Download Results

#	Vendor	Product	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	Apple	Iphone Os	CVE-2017-14315	119		Overflow +Priv Bypass	2017-09-12	2017-09-21	7.9	None	Local Network	Medium	Not required	Complete	Complete	Complete
In Apple iOS 7 through 9, due to a BlueBorne flaw in the implementation of LEAP (Low Energy Audio Protocol), a large audio command can be sent to a targeted device and lead to a heap overflow with attacker-controlled data. Since the audio commands sent via LEAP are not properly validated, an attacker can use this overflow to gain full control of the device through the relatively high privileges of the Bluetooth stack in iOS. The attack bypasses Bluetooth access control; however, the default "Bluetooth On" value must be present in Settings.																
2	Apple	Iphone Os	CVE-2017-13903	371			2017-12-25	2017-12-29	5.0	None	Remote	Low	Not required	Partial	None	None
An issue was discovered in certain Apple products. iOS before 11.2.1 is affected. tvOS before 11.2.1 is affected. The issue involves the "HomeKit" component. It allows remote attackers to modify the application state by leveraging incorrect message handling, as demonstrated by use of an Apple Watch to obtain an encryption key and unlock a door.																
3	Apple	Iphone Os	CVE-2017-13879	119		DoS Exec Code Overflow Mem. Corr.	2017-12-25	2017-12-29	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
An issue was discovered in certain Apple products. iOS before 11.2 is affected. The issue involves the "IOMobileFrameBuffer" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.																
4	Apple	Iphone Os	CVE-2017-13876	119		DoS Exec Code Overflow Mem. Corr.	2017-12-25	2017-12-28	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
An issue was discovered in certain Apple products. iOS before 11.2 is affected. macOS before 10.13.2 is affected. tvOS before 11.2 is affected. watchOS before 4.2 is affected. The issue involves the "Kernel" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.																
5	Apple	Iphone Os	CVE-2017-13874	254		Bypass	2017-12-25	2017-12-28	5.0	None	Remote	Low	Not required	Partial	None	None
An issue was discovered in certain Apple products. iOS before 11.2 is affected. The issue involves the "Mail" component. It might allow remote attackers to bypass an intended encryption protection mechanism by leveraging incorrect S/MIME certificate selection.																
6	Apple	Iphone Os	CVE-2017-13870	119		DoS Exec Code Overflow Mem. Corr.	2017-12-25	2018-01-08	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
An issue was discovered in certain Apple products. iOS before 11.2 is affected. Safari before 11.0.2 is affected. iCloud before 7.2 on Windows is affected. iTunes before 12.7.2 on Windows is affected. tvOS before 11.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.																
7	Apple	Iphone Os	CVE-2017-13869	200		Bypass +Info	2017-12-25	2017-12-28	4.3	None	Remote	Medium	Not required	Partial	None	None
An issue was discovered in certain Apple products. iOS before 11.2 is affected. macOS before 10.13.2 is affected. tvOS before 11.2 is affected. watchOS before 4.2 is affected. The issue involves the "Kernel" component. It allows attackers to bypass intended memory-read restrictions via a crafted app.																
8	Apple	Iphone	CVE-2017-13868	200		Bypass +Info	2017-12-25	2017-12-	4.3	None	Remote	Medium	Not required	Partial	None	None

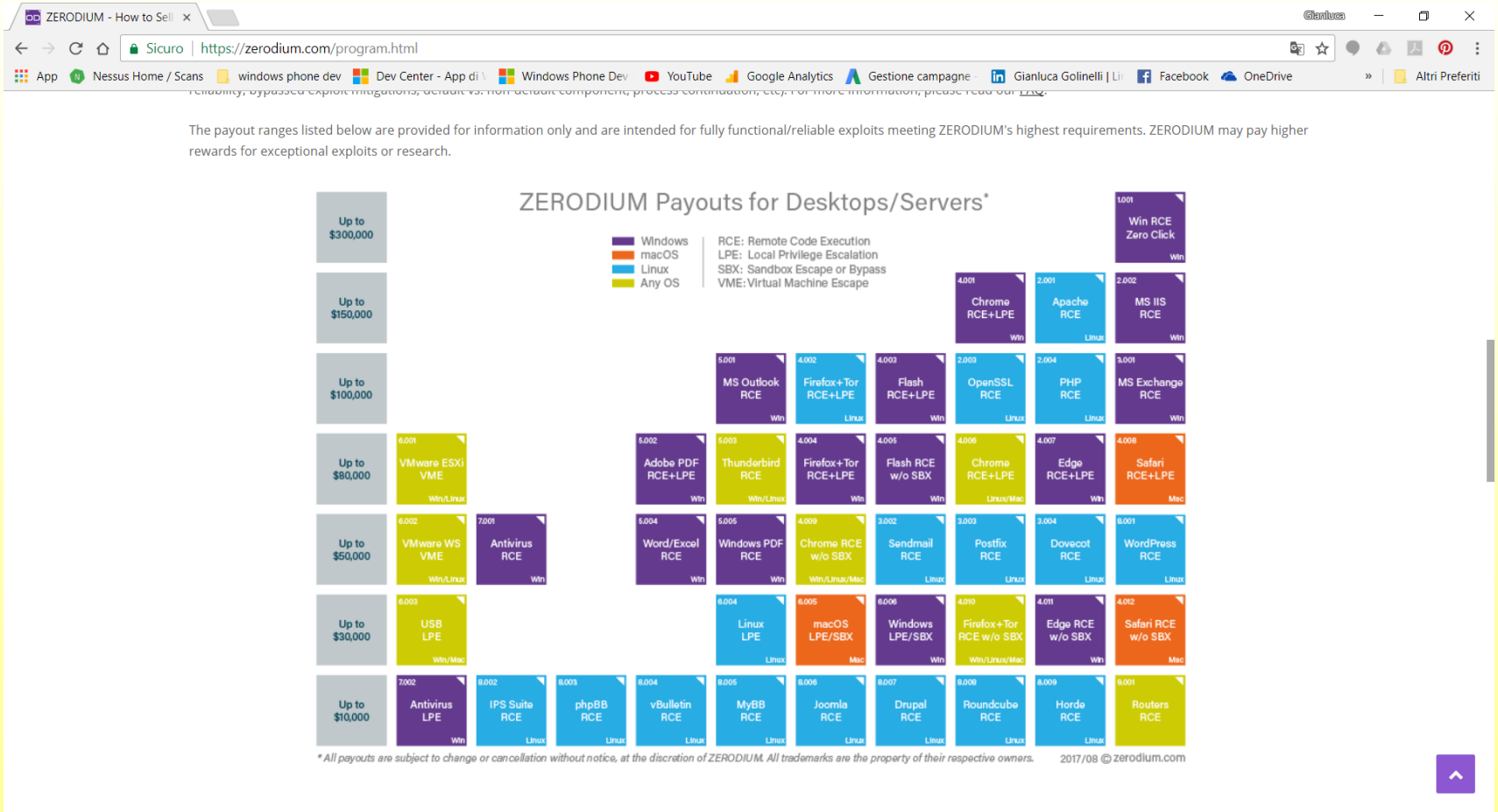
Sistemi per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche (rif. Ethical Hacking)

Ricercare vulnerabilità



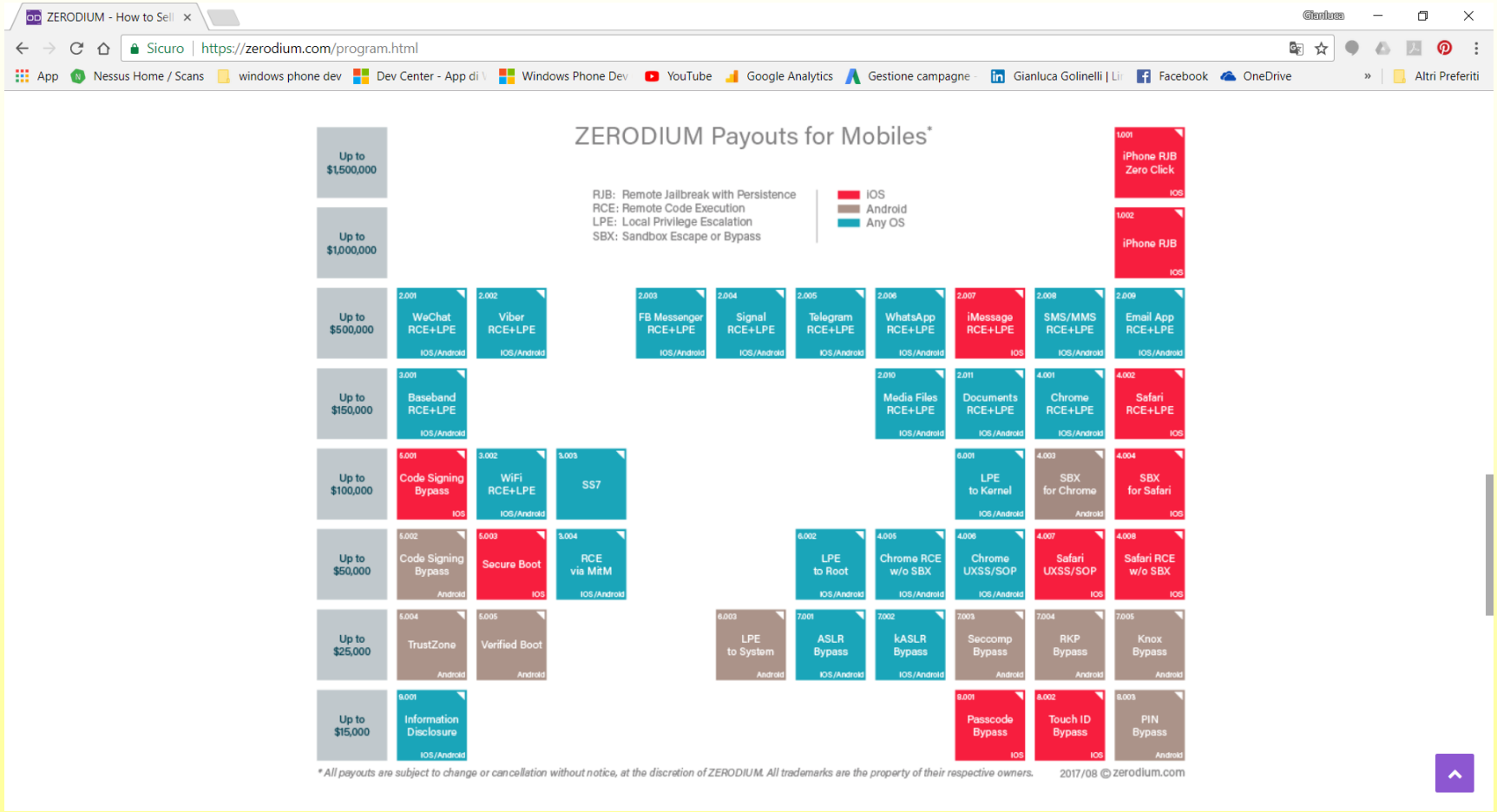
Sistemi per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche (rif. Ethical Hacking)

Il mercato delle vulnerabilità



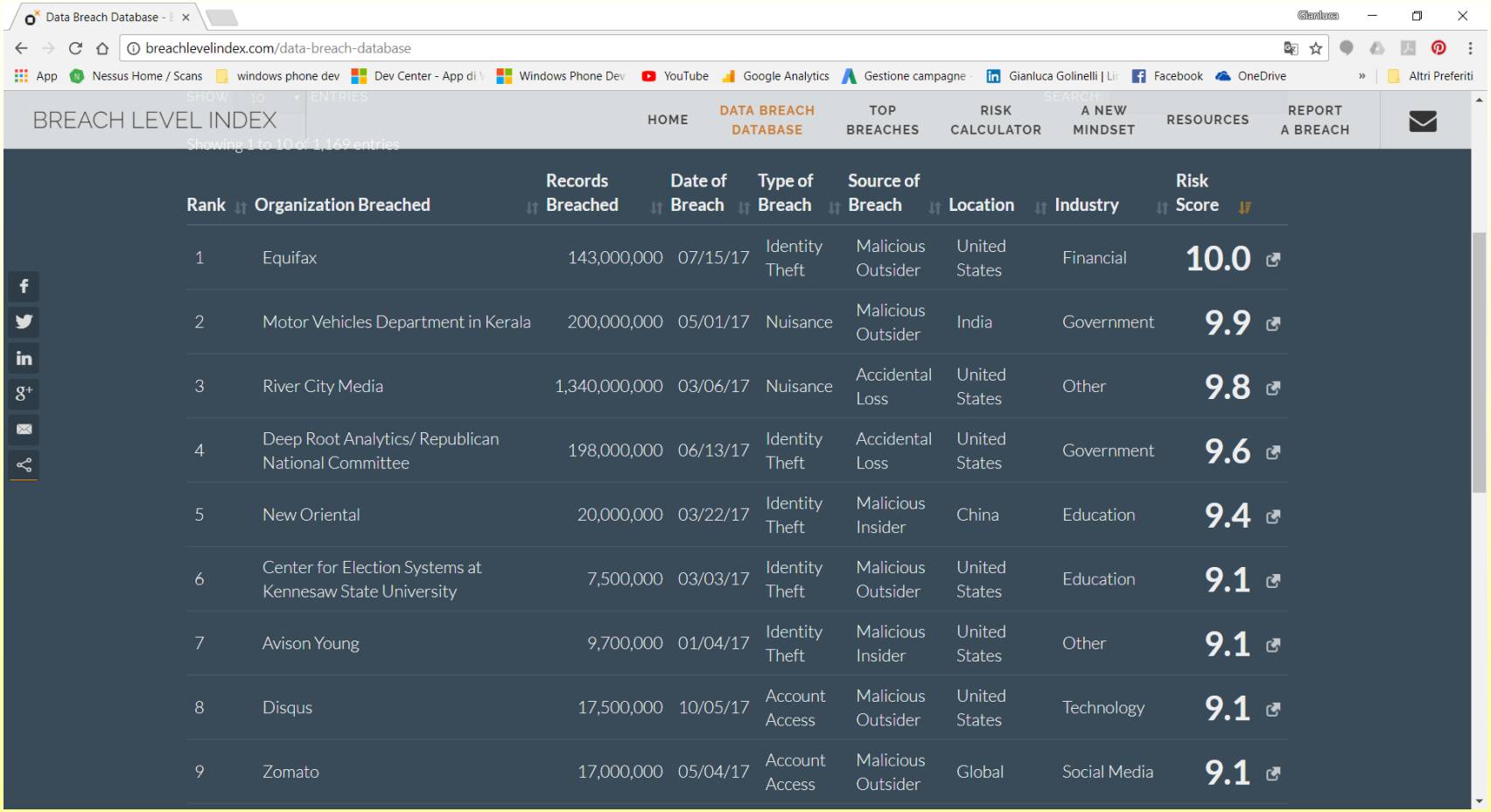
Sistemi per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche (rif. Ethical Hacking)

Il mercato delle vulnerabilità



Sistemi per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche (rif. Ethical Hacking)

Statistiche sui danni causati

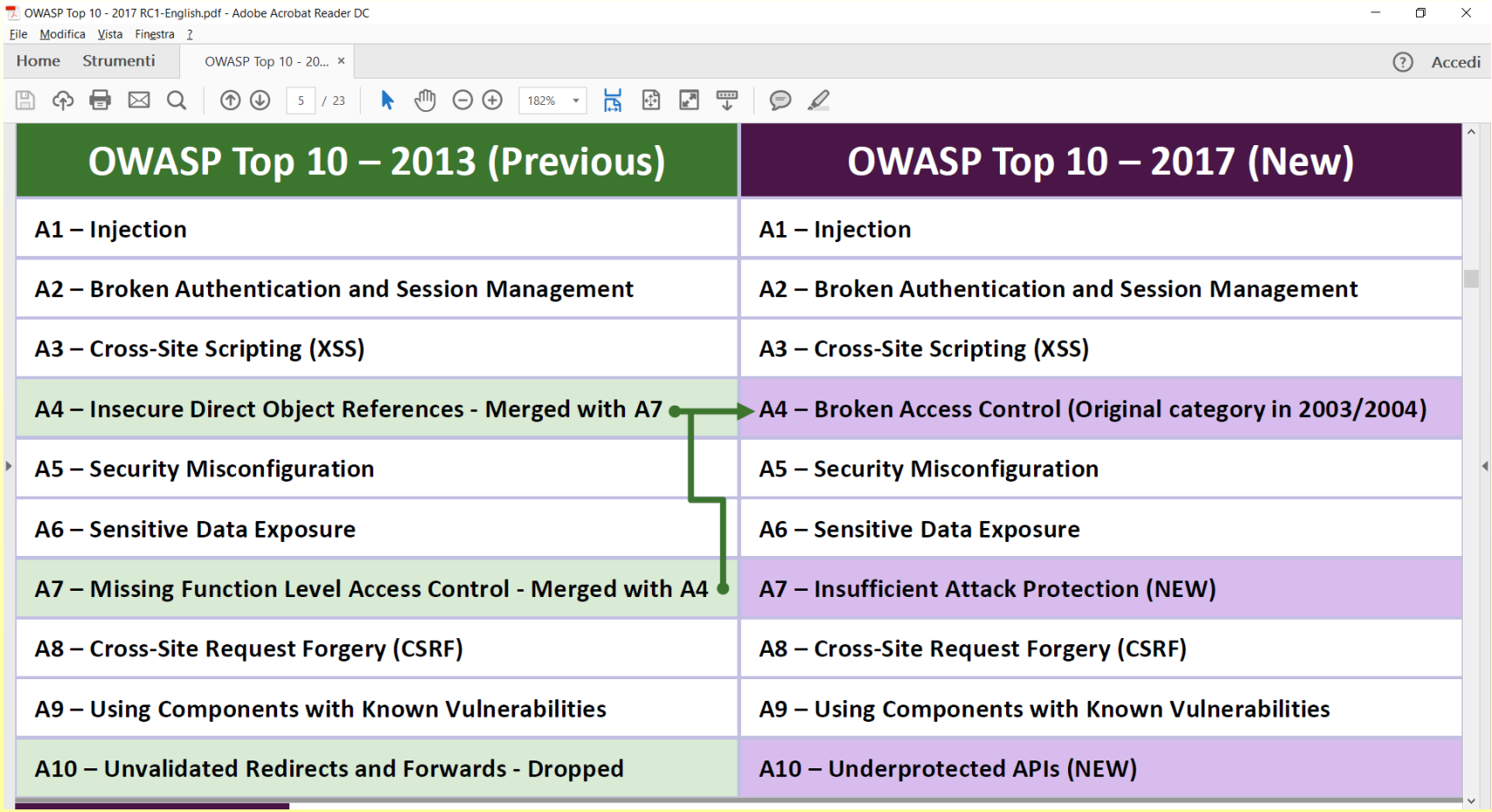


Showing 1 to 10 of 1,169 entries

Rank	Organization Breached	Records Breached	Date of Breach	Type of Breach	Source of Breach	Location	Industry	Risk Score
1	Equifax	143,000,000	07/15/17	Identity Theft	Malicious Outsider	United States	Financial	10.0
2	Motor Vehicles Department in Kerala	200,000,000	05/01/17	Nuisance	Malicious Outsider	India	Government	9.9
3	River City Media	1,340,000,000	03/06/17	Nuisance	Accidental Loss	United States	Other	9.8
4	Deep Root Analytics/ Republican National Committee	198,000,000	06/13/17	Identity Theft	Accidental Loss	United States	Government	9.6
5	New Oriental	20,000,000	03/22/17	Identity Theft	Malicious Insider	China	Education	9.4
6	Center for Election Systems at Kennesaw State University	7,500,000	03/03/17	Identity Theft	Malicious Outsider	United States	Education	9.1
7	Avison Young	9,700,000	01/04/17	Identity Theft	Malicious Insider	United States	Other	9.1
8	Disqus	17,500,000	10/05/17	Account Access	Malicious Outsider	United States	Technology	9.1
9	Zomato	17,000,000	05/04/17	Account Access	Malicious Outsider	Global	Social Media	9.1

Sistemi per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche (rif. Ethical Hacking)

VULNERABILITA' NELLE APPLICAZIONI WEB



OWASP Top 10 – 2013 (Previous)	OWASP Top 10 – 2017 (New)
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References - Merged with A7	A4 – Broken Access Control (Original category in 2003/2004)
A5 – Security Misconfiguration	A5 – Security Misconfiguration
A6 – Sensitive Data Exposure	A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control - Merged with A4	A7 – Insufficient Attack Protection (NEW)
A8 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards - Dropped	A10 – Underprotected APIs (NEW)

Ethical Hacking o Penetration Testing

Un **Penetration Test o Pen-Test** è un **metodo per valutare la sicurezza di una rete**, simulando un attacco di intrusione da parte di un hacker.

Il processo implica un'analisi approfondita del sistema target alla ricerca di punti deboli e vulnerabilità, **mettendosi dal punto di vista di un potenziale attaccante.**

Tutte le eventuali vulnerabilità riscontrate al termine del Pen-Test vengono relazionate al committente con indicazione della loro incidenza in termini di sicurezza e delle possibili contromisure.

IN BASE AL PUNTO INIZIALE DA CUI ATTACCARE

I Pen-Test si possono distinguere in base al punto di partenza da cui simulare l'attacco:

- Pen-Test condotti **dall'esterno della rete target**
- Pen-Test condotti **dall'interno della rete target**

IN BASE ALLA CONOSCENZA DEL SISTEMA TARGET

- **Black-Box Pen-Test**, implica una completa mancanza di informazioni sulla rete da testare
- **White-Box Pen-Test**, vengono fornite al tester tutte le informazioni più significative sulla rete target (inclusi digrammi della rete, indirizzi IP, informazioni sui sistemi operativi, etc)
- **Gray-Box Pen-Test**, condizione intermedia di conoscenza iniziale

IN BASE AL LIVELLO TECNICO DEL TEST

- **Low Level Pen-Test**, svolto generalmente esclusivamente con tool automatici e ricercando vulnerabilità note.
- **Medium Level Pen-Test**, svolto anche sfruttando tecniche di social-engineering.
- **High Level Pen-Test**, vengono ricercati anche bug e vulnerabilità meno note o recentissime.

ALL'INSAPUTA O MENO DELLO STAFF IT

- **Overt Pen-Test**, svolto con la consapevolezza dello staff IT.
- **Covert Pen-Test**, svolto all'insaputa dello staff IT, con lo scopo di testare anche le capacità degli addetti alla sicurezza.

ASPETTI LEGALI E CONTRATTUALISTICI DI UN PEN-TEST
Definizione delle ROE – Rules Of Engagement

Data la criticità dei Pen-Test, i contratti di commessa devono essere redatti opportunamente in modo da salvaguardare le parti in causa.

Gli aspetti più critici da regolamentare sono:

- disclosure su danni e/o malfunzionamenti eventuali prodotti in fase di testing (indemnification clause)
- privacy dei dati residenti sui sistemi target
- Etc

LE FASI DI UN PENETRATION TEST

- Footprinting della rete target
- Scansionamento della rete
- Enumerazione di account e risorse condivise (identificazione delle vulnerabilità)
- Hacking del sistema target identificato
- Redazione della reportistica

Sistemi per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche (rif. Ethical Hacking)

METODOLOGIE PER ETHICAL HACKING

Standard **OSSTMM** (Open Source Security Testing Methodology) di ISECOM (Institute for Security and Open Methodology).
www.isecom.org/research/osstmm.html

Standard **OWASP** (Open Web Application Security Project).
www.owasp.org/index.php/Category:OWASP_Testing_Project

Standard **NIST SP 800-115** (National Institute of Standards and Technology). csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

Penetration Testing Framework by Kevin Orrey
vulnerabilityassessment.co.uk/Penetration%20Test.html

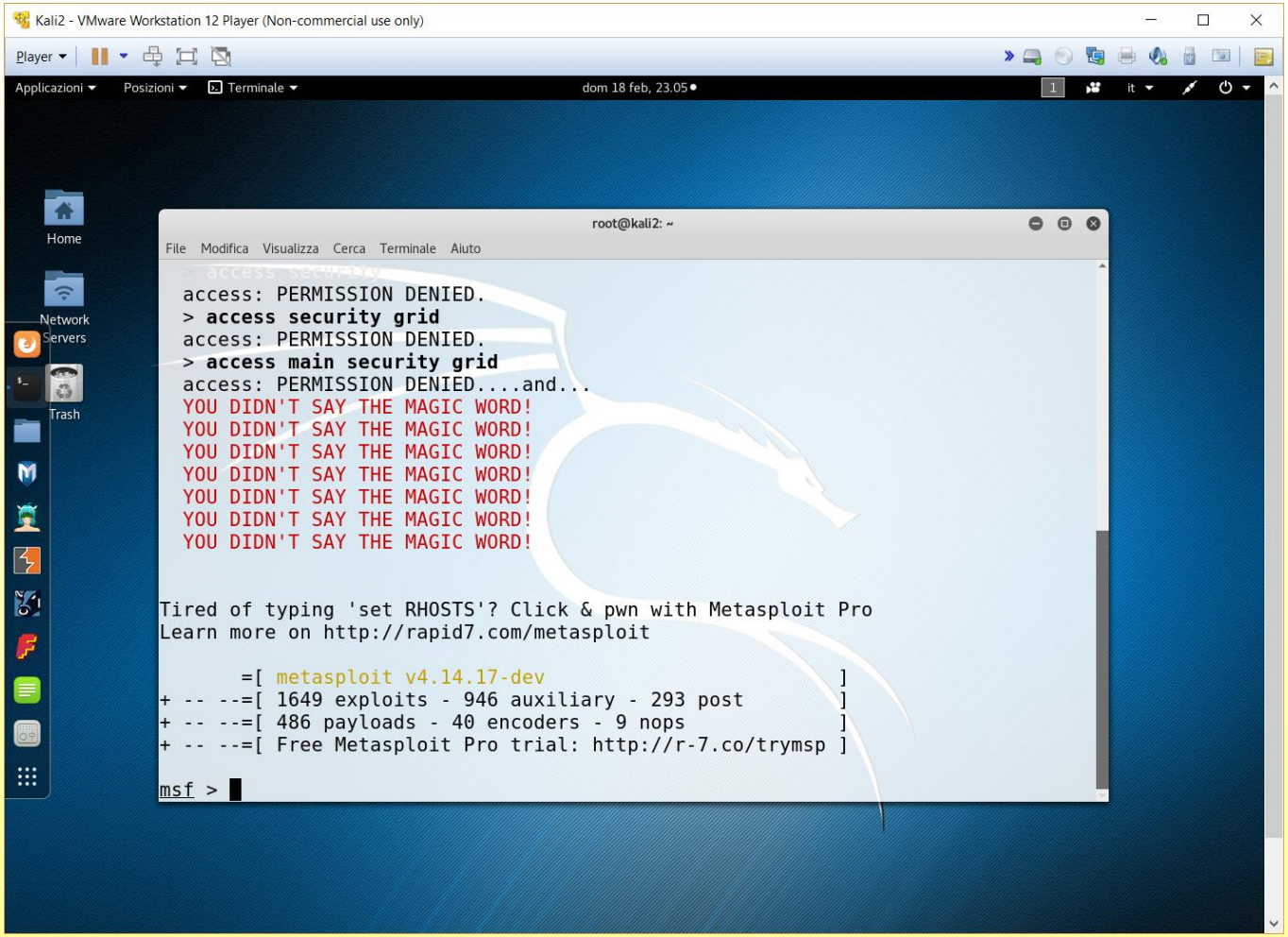
Standard **ISSAF** (Information Systems Security Assessment Framework) del OISSG (Open Information Systems Security Group)
oissg.org/files/issaf0.2.1B.pdf

Framework per l'esecuzione di PenTest

- Commerciali:
  - Metasploit (Rapid7)
  - Core Impact (Core Security)
  - …
- Distribuzioni Linux
  - Kali Linux
  - Parrot Security OS
  - Backbox
  - BlackArch
  - …

Sistemi per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche (rif. Ethical Hacking)

Kali Linux e Metasploit



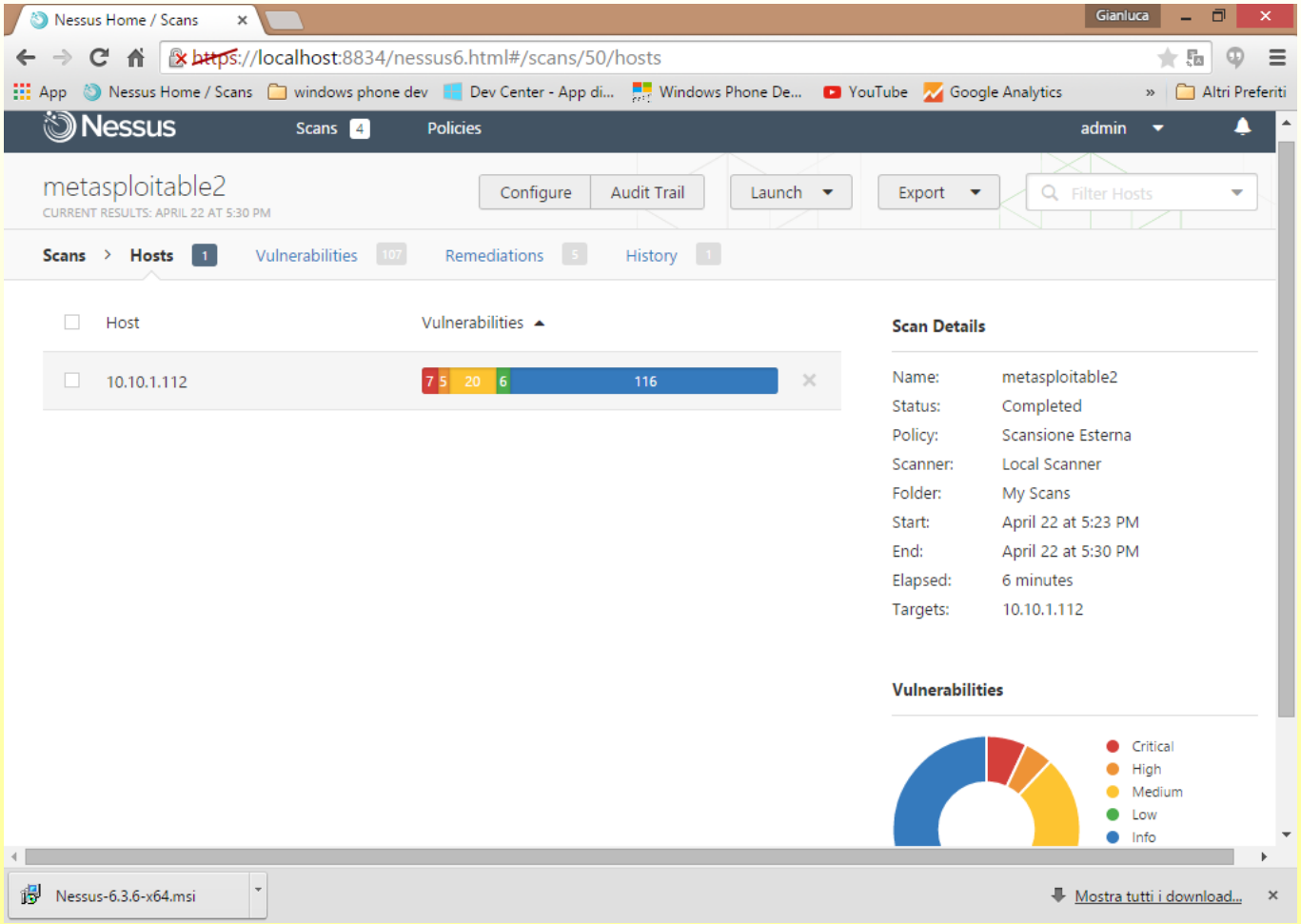
I Vulnerability Assessment

Si svolgono normalmente con l'ausilio di tool chiamati Vulnerability Scanner:

- General Purpose Vulnerability Scanner
  - Tenable Nessus
  - Rapid7 Nexpose
  - …
- Web Vulnerability Scanner
  - Acunetix Web Vulnerability Scanner
  - Burp Suite
  - Netsparker
  - …

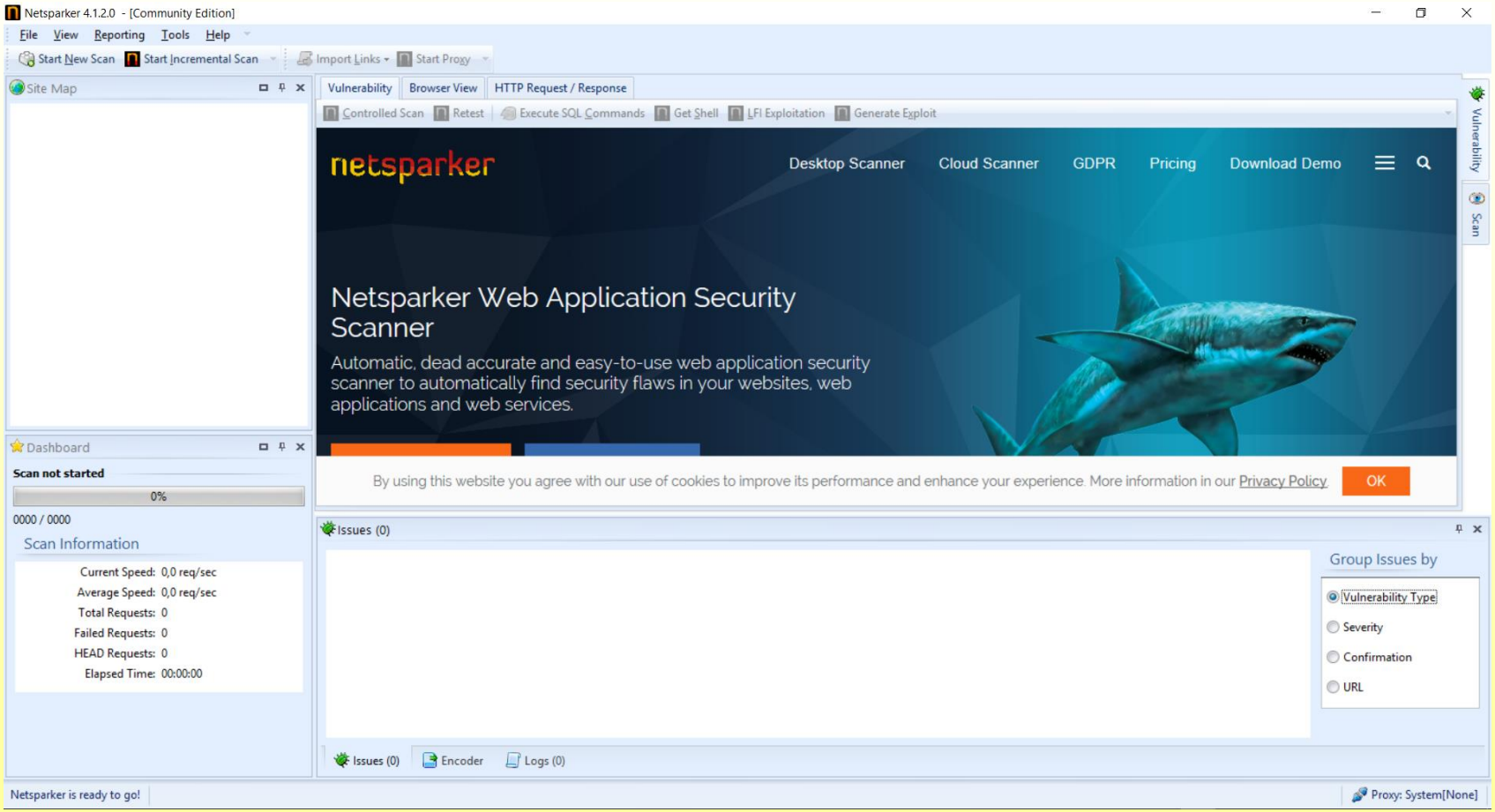
Sistemi per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche (rif. Ethical Hacking)

Tenable Nessus



Sistemi per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche (rif. Ethical Hacking)

Netsparker



Standard e Framework sulla gestione della sicurezza IT

- ISO/IEC 27001:2013, ISO/IEC 27002:2013
- NIST Cybersecurity Framework v1.1 draft (2017)
- NIST SP 800-53 rev.4 (2013) - Security and Privacy Controls for Federal Information Systems and Organizations

- COBIT-5 (2012)
- ITIL 2011
- …

ISO/IEC 27001: 2013
Information Security Management Systems: requirements
Sistemi di Gestione per la Sicurezza delle Informazioni: requisiti

Scopo di un ISMS:

Preservare la riservatezza, l'integrità e la disponibilità delle informazioni mediante l'applicazione di un processo di gestione del rischio.

ISO/IEC 27001: 2013
Information Security Management Systems: requirements
Sistemi di Gestione per la Sicurezza delle Informazioni: requisiti

Scopo della ISO/IEC 27001:

Fornire i **requisiti** per stabilire, attuare, mantenere e migliorare in modo continuo un Sistema di Gestione per la Sicurezza delle Informazioni (ISMS) nel contesto di un'organizzazione.

ISO 27001: sommario

4 Contesto dell'organizzazione

- 4.1 Comprendere l'organizzazione e il suo contesto

(fattori interni ed esterni che possono avere un impatto sull'ISMS)

- 4.2 Comprendere le necessità e le aspettative delle parti interessate alla gestione dell'ISMS
- 4.3 Determinare il campo di applicazione del ISMS (a quali servizi, processi, trattamenti di dati, etc si applica)
- 4.4 Sistema di gestione per la sicurezza delle informazioni (l'organizzazione deve gestire l'ISMS in conformità alla ISO 27001)

ISO 27001: sommario

5 Leadership

- 5.1 Leadership e impegno (Il top management deve garantire che gli obbiettivi e le politiche dell'ISMS siano stabiliti, le risorse siano disponibili, vi sia adeguata formazione, etc)
- 5.2 Politica (il top management stabilisce un'adeguata politica per la sicurezza delle informazioni: appropriata alle finalità aziendali, volta al miglioramento continuo, etc)
- 5.3 Ruoli, responsabilità e autorità nell'organizzazione (il top management garantisce l'assegnazione di autorità e responsabilità per i ruoli pertinenti la sicurezza delle informazioni)

ISO 27001: sommario

6 Pianificazione del ISMS

- 6.1 Azioni per affrontare rischi e opportunità
  - 6.1.1 Generalità
  - 6.1.2 Valutazione del Rischio relativo alla Sicurezza delle Informazioni
  - 6.1.3 **Trattamento del Rischio relativo alla Sicurezza delle Informazioni**
    - Determinare tutti i **controlli (disposizioni) necessari** per attuare le opzioni selezionate per il trattamento del rischio relativo alla sicurezza delle informazioni → **Annex A**
- 6.2 Obiettivi (coerenti, misurabili, aggiornati) per la sicurezza delle informazioni e pianificazione per conseguirli (cosa sarà fatto).

ISO 27001: sommario

7 Supporto – supporto fornito dall'organizzazione per ISMS

- 7.1 Determinare e mettere a disposizione le **risorse**
- 7.2 Determinare e garantire le necessarie **competenze**
- 7.3 Garantire la **consapevolezza** delle persone relativamente alle policy per l'ISMS
- 7.4 Garantire **comunicazioni** interne ed esterne in relazione a ISMS
- 7.5 L'ISMS deve comprendere **Informazioni Documentate**

ISO 27001: sommario

8 Attività operative

- 8.1 Pianificazione e controllo operativo su processi necessari per soddisfare i requisiti di sicurezza determinati ai punti 6.1 e 6.2

- 8.2 Valutazione del Rischio relativo alla Sicurezza delle Informazioni, ad intervalli pianificati o a fronte di cambiamenti

- 8.3 Attuazione del piano di Trattamento del Rischio relativo alla Sicurezza delle Informazioni

ISO 27001: sommario

9 Valutazione delle prestazioni

- 9.1 Monitoraggio, misurazione, analisi e valutazione della sicurezza delle informazioni ed efficacia dell'ISMS

- 9.2 L'organizzazione deve condurre Audit interni per verificare se l'ISMS è conforme ai requisiti dell'organizzaione e della ISO 27001

- 9.3 Riesame di direzione da parte del top management del ISMS per verificarne la continua adeguatezza, efficacia ed idoneità

ISO 27001: sommario

10 Miglioramento

- 10.1 Non conformità e azioni correttive (a fronte di esse l'organizzazione deve intraprendere azioni a mitigazione o correttive, fronteggiare le conseguenze, etc)

- 10.2 Miglioramento continuo dell'adegatezza, idoneità, efficacia dell'ISMS

Annex A (Appendice A)
Obiettivi di controllo e controlli di riferimento

ISO/IEC 27001 – Annex A (Appendice A)
Obiettivi di controllo e controlli di riferimento

L' Appendice A della ISO 27001 riprende esattamente gli obiettivi di controllo e i controlli indicati nella **ISO/IEC 27002:2013** dai **punti 5 a 18**.

Con la differenza che nella ISO/IEC 27002 per ogni controllo viene indicata anche una **guida dettagliata all'implementazione del controllo.**

ISO/IEC 27001 – Annex A (Appendice A)

Ambiti di controllo:

5. Politiche per la sicurezza delle informazioni
6. Organizzazione della sicurezza delle informazioni
7. Sicurezza delle risorse umane
8. Gestione degli asset
9. Controllo degli accessi
10. Crittografia
11. Sicurezza fisica e ambientale
12. Sicurezza delle attività operative
13. Sicurezza delle comunicazioni
14. Acquisizione, sviluppo e manutenzione dei sistemi
15. Relazioni con i fornitori
16. Gestione degli incidenti relativi alla sicurezza delle informazioni
17. Aspetti relativi alla sicurezza delle informazioni nella gestione della continuità operativa
18. Conformità

ISO/IEC 27001 – Annex A (Appendice A) esempio

A.8 Gestione degli asset		
A.8.1 Responsabilità per gli asset		
Obiettivo: Identificare gli asset dell'organizzazione e definire adeguate responsabilità per la loro protezione.		
A.8.1.1	Inventario degli asset	*Controllo* Tutti gli asset associati alle informazioni e alle strutture di elaborazione delle informazioni devono essere identificati; un inventario di questi asset deve essere compilato e mantenuto aggiornato.
A.8.1.2	Responsabilità degli asset	*Controllo* Gli asset censiti nell'inventario devono avere un responsabile.
A.8.1.3	Utilizzo accettabile degli asset	*Controllo* Le regole per l'utilizzo accettabile delle informazioni e degli asset associati alle strutture di elaborazione delle informazioni devono essere identificate, documentate e attuate.
A.8.1.4	Restituzione degli asset	*Controllo* Tutto il personale e gli utenti di parti esterne devono restituire tutti gli asset dell'organizzazione in loro possesso al termine del periodo di impiego, del contratto o dell'accordo stipulato.

ISO/IEC 27001 – Annex A (Appendice A)

Ambiti di controllo:

5. Politiche per la sicurezza delle informazioni

Controlli:

Verificare che esistano delle policies per la sicurezza delle informazioni, e che siano verificate e riesaminate ad intervalli regolari, etc.

6. Organizzazione della sicurezza delle informazioni

Controlli :

Verificare che siano definiti ruoli e responsabilità per la sicurezza delle informazioni, si adotti una politica di separazione dei compiti, siano adottati meccanismi di security by design nella gestione dei progetti, etc.

Siano presenti policy per la sicurezza di dispositivi mobili e per il telelavoro.

ISO/IEC 27001 – Annex A (Appendice A)

Ambiti di controllo:

7. Sicurezza delle risorse umane

Controlli :

Verificare prima dell'impiego che i candidati siano idonei per etica, leggi e regolamenti.

Durante l'impiego, verificare che la direzione promuova l'awareness di tutto il personale relativamente alle politiche e procedure sulla sicurezza delle informazioni, e che esistano dei processi disciplinari.

A fronte di cessazione verificare che i doveri che permangono siano definiti e comunicati

ISO/IEC 27001 – Annex A (Appendice A)

Ambiti di controllo:

8. Gestione degli asset

Controlli :

Identificare gli asset dell'organizzazione e definire idonee responsabilità per la loro protezione (inventario, utilizzo accettabile, responsabili degli asset, restituzione)

Verificare la presenza di Classificazione ed etichettatura delle informazioni al fine di garantire adeguata protezione in linea con l'importanza.

Verificare l'adeguatezza del Trattamento dei supporti di dati a fronte di operazioni di trasporto, dismissione per prevenire usi non autorizzati delle informazioni archiviate.

ISO/IEC 27001 – Annex A (Appendice A)

Ambiti di controllo:

9. Controllo degli accessi

Controlli :

Verificare che sia definita una politica di controllo degli accessi in linea con i requisiti di business e di sicurezza delle informazioni, sia presente un processo di registrazione / deregistrazione per l'abilitazione dei diritti degli utenti.

Verificare che gli utenti siano formati e consapevoli della esponsabilità nella custodia delle credenziali di autenticazione

Verificare l'adeguatezza delle misure adottate per prevenire accessi non autorizzati a sistemi ed applicazioni (robustezza password, procedure di log-on sicure, limitazione negli accessi ai codici sorgenti, etc)

ISO/IEC 27001 – Annex A (Appendice A)

Ambiti di controllo:

10. Crittografia

Controlli :

Verificare la corretta implementazione ed uso di meccanismi di crittografia a garanzia della riservatezza, autenticità e integrità delle informazioni (politica sul corretto uso, protezione e durata delle chiavi crittografiche).

ISO/IEC 27001 – Annex A (Appendice A)

Ambiti di controllo:

11. Sicurezza fisica e ambientale

Controlli :

Verificare che siano definiti dei perimetri di sicurezza a protezione delle aree che contengono informazioni critiche,

che siano presenti dei sistemi di controllo fisico degli accessi,

che siano presenti protezioni fisiche da calamità naturali, etc.

Verificare che le apparecchiature siano protette da pericoli ambientali, accessi non autorizzati, da malfunzionamenti alla rete elettrica, che siano mantenute correttamente, etc.

ISO/IEC 27001 – Annex A (Appendice A)

Ambiti di controllo:

12. Sicurezza delle attività operative

Controlli :

Verificare la presenza di procedure operative per gli utenti

Verificare la separazione tra l'ambiente di sviluppo e quello di produzione

Verificare le capacità operative delle risorse per far fronte a future esigenze

Verificare l'adeguata adozioni di policies e strumenti per prevenire, identificare e neutralizzare malware.

Verificare l'adozione di adeguate politiche di backup dei dati

Verificare l'adozione di adeguate politiche per la gestione dei log

Verificare la presenze di procedure per controllare l'installazione del software sui sistemi produzione

Verificare corretta politica di rilevazione e gestione delle vulnerabilità,

etc

ISO/IEC 27001 – Annex A (Appendice A)

Ambiti di controllo:

13. Sicurezza delle comunicazioni

Controlli :

Verificare che le reti siano gestite e controllate al fine di proteggere le informazioni

Verificare che a livello di rete vi sia segregazione di servizi, utenti, etc.

Verificare la presenza di opportune politiche e procedure per il trasferimento di informazioni tramite i vari meccanismi di comunicazione e relativi accordi tra parti interessate, inclusi accordi di riservatezza.

ISO/IEC 27001 – Annex A (Appendice A)

Ambiti di controllo:

14. Acquisizione, sviluppo e manutenzione dei sistemi

Controlli :

Verificare la presenza dei requisiti di sicurezza nei requisiti dei nuovi sistemi informativi o dell'aggiornamento di quelli esistenti

Verificare la presenza di adeguati meccanismi di protezione dei servizi applicativi su reti pubbliche e la presenza di meccanismi di gestione delle transazioni

Verificare la presenza di politiche per lo sviluppo sicuro del software

Verificare la presenza di procedure per il controllo dei cambiamenti dei sistemi

Verificare l'impatto sulle applicazioni di cambiamenti ai sistemi (piattaforme operative) prime di eseguirle in ambienti di produzione.

Verificare la presenza di principi per l'ingegnerizzazione sicura dei sistemi

Verificare la presenza di opportuni meccanismi di testing (test di sicurezza, test di accettazione, etc)

ISO/IEC 27001 – Annex A (Appendice A)

Ambiti di controllo:

15. Relazioni con i fornitori

Controlli :

Verificare la presenza di accordi e di adeguate politiche di sicurezza delle informazioni nell'accesso da parte di fornitori

Verificare la presenza di un monitoraggio e riesame costante dell'erogazione dei servizi da parte dei fornitori

Verificare che i cambiamenti dei servizi dei fornitori siano gestiti

ISO/IEC 27001 – Annex A (Appendice A)

Ambiti di controllo:

16. Gestione degli incidenti relativi alla sicurezza delle informazioni

Controlli :

Verificare che siano stabilite le procedure e le responsabilità in caso di incidenti di sicurezza che coinvolgano le informazioni

Verificare la presenza di opportuni canali per la segnalazione tempestiva degli incidenti di sicurezza

Verificare la presenza di procedure per valutare e classificare gli incidenti di sicurezza

Verificare la presenza di procedure documentate per la risposta agli incidenti

Verificare la presenza di procedure per migliorare la sicurezza dei sistemi facendo tesoro degli incidenti pegressi

Verificare la presenza di procedure per la raccolta di evidenze in caso di incidenti

ISO/IEC 27001 – Annex A (Appendice A)

Ambiti di controllo:

17. Aspetti relativi alla sicurezza delle informazioni nella gestione della continuità operativa

Controlli :

Verificare la presenza di requisiti e politiche per la continuità della sicurezza delle informazioni

Verificare e valuare periodicamente l'efficacia dei meccanismi di continuità della sicurezza delle informazioni

Verificare la presenza di adeguata ridondanza delle strutture di elaborazione delle informazioni al fine di garantire la disponibilità delle informazioni.

ISO/IEC 27001 – Annex A (Appendice A)

Ambiti di controllo:

18. Conformità

Controlli :

Verificare per ogni sistema informativo che siano stati identificati e definiti tutti i requisiti cogenti (di legge) e contrattuali

Verificare la conformità per la protezione delle registrazioni, dei meccanismi di crittografia, e per la protezione dei dati personali in ottemperanza alle legislazioni in vigore, agli accordi e ai regolamenti.

Verificare che la gestione della sicurezza delle informazioni sia riesaminata in modo indipendente ad intervalli regolari.

ISO/IEC 27002: 2013
Code of Practice for information security controls. (Codice di condotta per i controlli di sicurezza delle informazioni)

Costituisce una guida all'implementazione dei controlli dell'Annex A della ISO 27001

Processi per monitoraggio dell'efficacia delle soluzioni tecniche e organizzative in uso per la protezione dei dati (rif. ISO27002)

ISO/IEC 27002

Ambiti di controllo:

5. Politiche per la sicurezza delle informazioni
6. Organizzazione della sicurezza delle informazioni
7. Sicurezza delle risorse umane
8. Gestione degli asset
9. Controllo degli accessi
10. Crittografia
11. Sicurezza fisica e ambientale
12. Sicurezza delle attività operative
13. Sicurezza delle comunicazioni
14. Acquisizione, sviluppo e manutenzione dei sistemi
15. Relazioni con i fornitori
16. Gestione degli incidenti relativi alla sicurezza delle informazioni
17. Aspetti relativi alla sicurezza delle informazioni nella gestione della continuità operativa
18. Conformità

ISO/IEC 27002

Esempio:

9. Controllo degli accessi

…

9.4.3 Sistema di gestione delle password

Controllo:

I sistemi di gestione delle password devono essere interattivi e devono assicurare password di qualità.

Guida all'implementazione:

Un sistema di gestione delle password dovrebbe:

a) Imporre l'uso di ID utente e password individuali per mantenere le responsabilità
b) Consentire agli utenti di scegliere e modificare le proprie password e contemplare una procedura di conferma per rilevare errori di input
c) Imporre la scelta di password di qualità (robuste)
d) Imporre agli utenti di cambiare le proprie password al primo log-on

ISO/IEC 27002

e) Imporre un cambio delle password periodico e all'occorrenza

f) Mantenere uno storico delle password utilizzate e prevenirne il riuso

g) Non visualizzare le password a video quando vengono inserite

h) Archiviare i file delle password separatamente rispetto ai dati di sistema dell'applicazione

i) Archiviare e trasmettere le password in formato protetto

Altre informazioni:

Alcune applicazioni richiedono che le password degli utenti siano assegnate da un'autorità indipendente; in questi casi i punti b) d) e) non si applicano. Nella maggior parte dei casi le password vengono scelte e gestite dagli utenti.

Riferimenti utili

http://www.securityfocus.com/bid

http://www.kali.org

http://www.isecom.org/research/

https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents

https://www.iso.org/isoiec-27001-information-security.html

https://www.iso.org/standard/54533.html