ABI OSSIF - Evoluzione di minacce e verifiche nella Cyber Physical Offense – F. Sensibile,

13/07/2022

RELATORE

Fabrizio Sensibile

Penetration tester dal 2000
Lead Auditor 27001
Offensive Security Certified Professional
OSSTTM Professional Security Tester
OSSTTM Professional Security Analyst
Contributore Metodologia OSSTMM
Docente accreditato. ISECOM mondo
Docenze svariati master di Cyber Security
Docenze in ambito NATO (NRDC)
Docenze in ambito governativo (C4, CII, CC, Interni ecc.)

HN SECURITY

UN NUOVO INIZIO

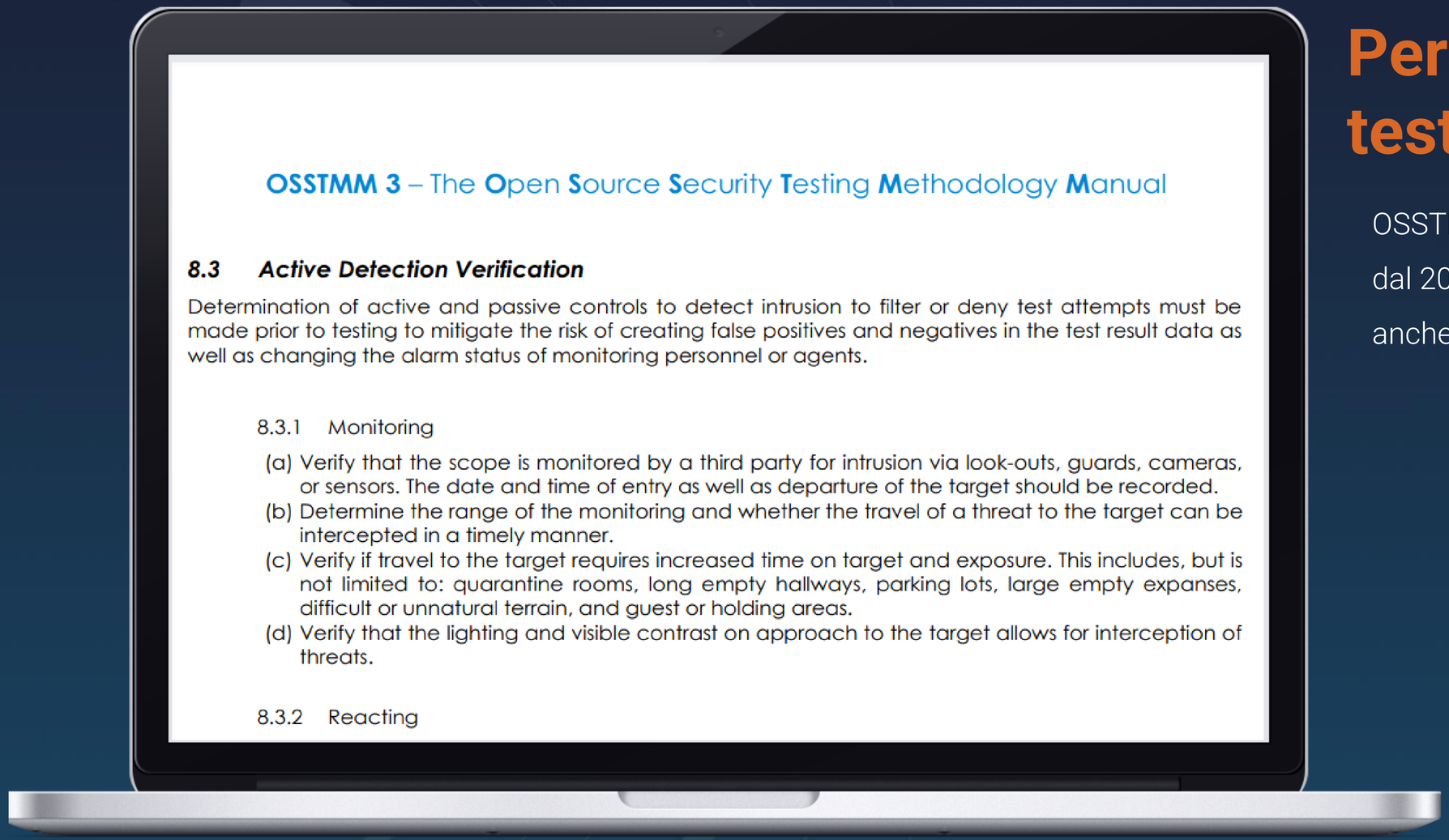
All’inizio del 2021 è nata HN Security, l’azienda del gruppo **Humanativa** specializzata nella sicurezza informatica.

Stiamo costruendo una realtà di eccellenza grazie ad un team coeso formato dai migliori talenti italiani, con l'obiettivo di diventare il punto di riferimento del settore.

HN SECURITY

Agenda

- Perché un Penetration Tester è qui?
- Ingegneria sociale iniziamo:
- *Sim Swap* e frodi finanziarie associate
- Case Study: ma che bel castello
- Case Study: Wardialing in an elevator
- Linea guida BCE/Banca d’Italia (TIBER-EU)
- Conclusioni



Perche un penetration tester è qui

OSSTMM e altri quadri di verifica prevedono già dal 2001 che la sicurezza fisica sia valutata anche in ottica di dato digitale.

H N S E C U R I T Y

Vettori multipli di attacco

Perché un Penetration Tester è qui?

Vediamo come alcune verifiche cyber fisiche siano già diffuse e in alcuni casi richieste da normative quali PCI-DSS.

Attacco ai badge di prossimità

Identificazione di reti abusive (rogue AP, HotSpot WiFi...)

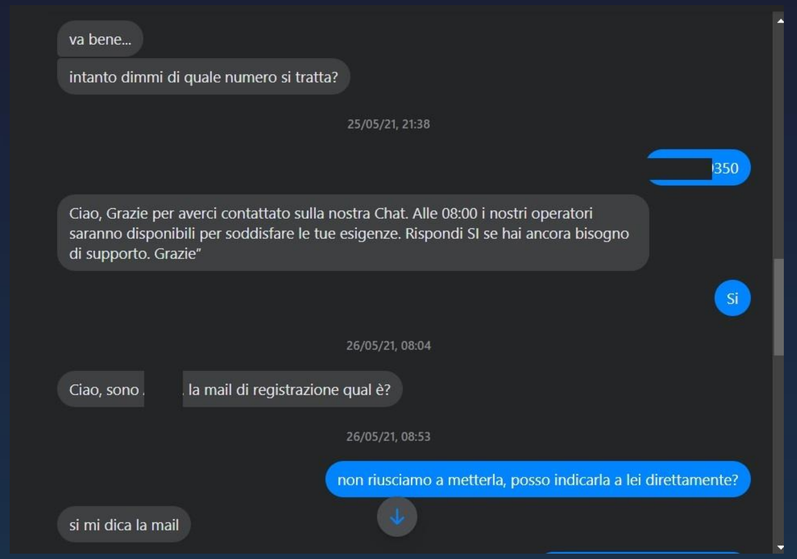
Ingegneria Sociale iniziamo

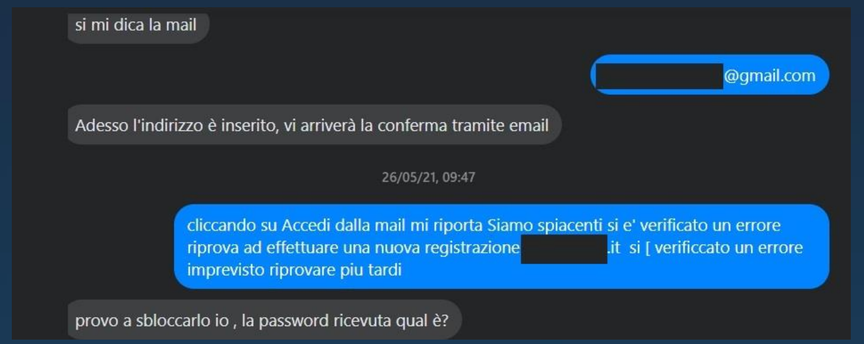
A maggio 2021 per un’esigenza personale contatto il servizio clienti di un noto operatore Mobile via Facebook, utilizzando un account decisamente poco attendibile.

Sfruttando alcune chiavi empatiche e fornendo unicamente il numero di telefono, mi viene creato e comunicato un account sul portale dove poter gestire dati e SIM dell'intestatario del numero.

A quel punto potrei richiedere **un invio di SIM sostitutiva ad un indirizzo arbitrariamente scelto da me**.

In questo caso la richiesta era valida e reale, e la persona un mio congiunto, ma questo dimostra come possa essere **realmente** semplice ottenere delle credenziali o addirittura la creazione stessa di un account per la gestione della SIM.





H N S E C U R I T Y

SIM Swapping

Fenomeno in grande aumento nel secondo semestre 2021

Uno degli attacchi ibridi maggiormente segnalato in questi ultimi mesi consiste nell’indurre un gestore telefonico ad emettere una nuova SIM associandola a un numero telefono e/o a account esistenti.

Per richiedere l’emissione di una nuova carta SIM i criminali fanno ricorso a tecniche di ingegneria sociale con i dipendenti dei gestori telefonici. (avete presente la slide precedente?).

Ripercussioni:

MFA basate su SMS/Chiamata

Furto di identità sociale

Sistemi OT con identificativo basato sul numero chiamante

Ingegneria Sociale Case Study: Ma che bel castello…

Una storica società italiana aveva sede in un fortino molto particolare con una valenza storica e artistica di rilievo.

Viene creato un falso libretto universitario di architettura per un nostro collega dall'aspetto giovanile.

Sfruttando il pensiero che l'imprenditore fosse molto orgoglioso di quella sede viene fatta richiesta di visitare la sede per la tesi di laurea.

Dopo aver recitato il ruolo assegnato il collega viene lasciato solo per il palazzo, installando una serie di device tra cui alcuni AP wireless minuscoli.

Mini Case Study: Wardialing in an elevator

WARDIALING: deriva il nome dal film War Games, consiste nella ricerca di apparati connessi ad una linea telefonica.

Normalmente in questo tipo di attività si ricercano apparati di rete, centralini, e altri asset tradizionalmente legati al mondo IT.

Ma durante una verifica in una grande azienda scopriamo qualcosa di quantomeno anomalo.

La numerazione rispondeva sempre, alle volte rimanendo in silenzio, altre volte si sentivano degli strani segnali acustici oppure un vociare di fondo.

Dopo un confronto con il committente abbiamo scoperto come funzionano i sistemi di telesoccorso degli ascensori, che con SIM, o via distribuzione PBX sono censiti nelle numerazioni aziendali

Di conseguenza un ascensore si trasforma in un punto di ascolto ambientale.
A dispetto di quanto proposto da un noto telefilm come ambiente riservatissimo….

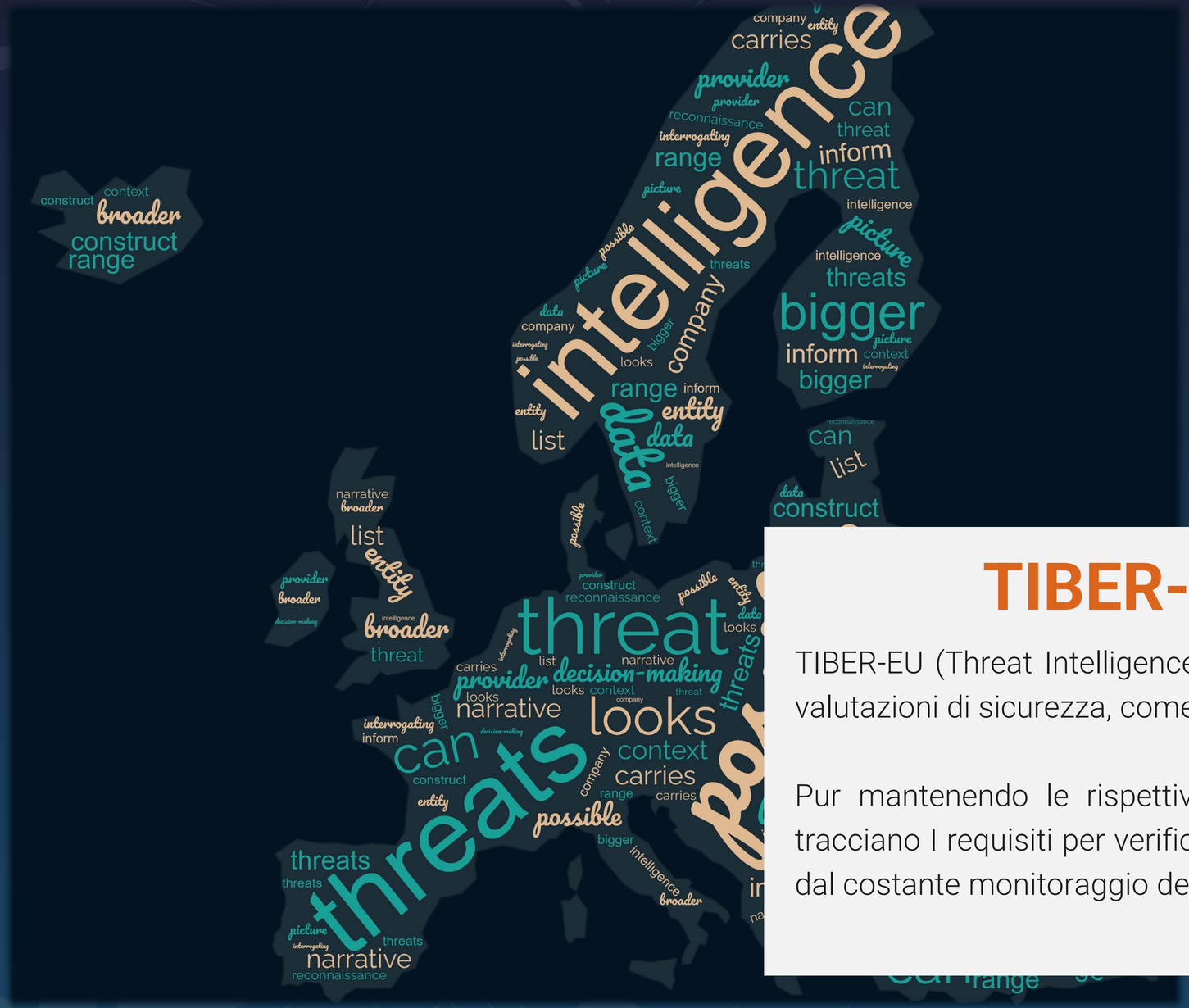
Approccio alla valutazione di sicurezza ibrido: Red Teaming

Naturale evoluzione degli approcci multicanale si pone come obbiettivo l’acquisizione di dati ritenuti e profilati come importanti. Tutti i mezzi **regolamentabili** sono validi (intrusione fisica, ingegneria sociale con attacchi "in presenza" o "da remoto ", hijacking della sorveglianza ecc…).

BCE e Banca di Italia verso TIBER-(EU)(IT)

Il panorama finora descritto chiaramente è noto alle istituzioni bancarie nazionali e comunitarie, che a fronte dell'incremento di frodi e attacchi agli istituti finanziari hanno iniziato a lavorare su un quadro di verifica comune agli stati membri, venendo poi richiamato ed inserito nel DORA (Digital Resilience Operation Act).

Vediamo come questo quadro potrà coadiuvare le azioni di monitoraggio e verifica della sicurezza in vari ambiti.



TIBER-EU approccio diverso

TIBER-EU (Threat Intelligence-based Ethical Red Teaming) definisce i requisiti per le valutazioni di sicurezza, come interoperabili tra cyber, physical e logical.

Pur mantenendo le rispettive competenze dei settori di sicurezza tradizionali, si tracciano I requisiti per verifiche di sicurezza con approccio Red Teaming, coadiuvata dal costante monitoraggio delle minacce verso l'istituzione finanziaria.

TIBER-EU: Ruoli e obbiettivi ben definiti

Threat Intelligence provider – l'azienda che esamina la gamma di possibili minacce e ne esegue una ricognizione sull'entità.

Red Team provider – l'azienda che esegue l'attacco simulato tentando di compromettere le funzioni critiche dell'entità imitando un cybercriminale

White Team – un piccolo team all'interno dell'entità target e unica entita a conoscenza che stia avvenendo un test, dando supporto in collaborazione con il cyber team TIBER

TIBER Cyber team – il team all'interno dell'autorità responsabile della supervisione del test e di assicurarsi che soddisfi i requisiti del quadro TIBER-EU, consentendo così il riconoscimento da parte delle autorità competenti

Conclusioni

- Come avrete avuto modo di intuire la complessità della sicurezza, specialmente in ambienti ibridi, non è una questione marginale.
- Anche le commissioni nazionali ed Europee si stanno preoccupando degli aspetti meno tradizionali della cyber security.
- Le verifiche in modalità Red Team possono aiutare ad avere una situazione più esaustiva della resilienza alle minacce.
- L'adozione del quadro TIBER-(EU-IT) permetterà di essere già in linea con i requisiti degli organi di controllo.
- Rivolgersi a fornitori affidabili e con un buon bagaglio di esperienza aiuta ad evitare ulteriore confusione in un mondo così in divenire.

Riferimenti

- Rapporto semestrale sicurezza Melani 2021/II: https://www.newsd.admin.ch/newsd/message/attachments/71411.pdf
- Panoramica TIBER-EU: https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html
- T-Mobile SIM fraud: https://www.bleepingcomputer.com/news/security/t-mobile-says-new-data-breach-caused-by-sim-swap-attacks/
- Approfondimento SIM swap: https://www.vice.com/en/article/5dmbjx/how-hackers-are-breaking-into-att-tmobile-sprint-to-sim-swap-yeh

HN Security S.r.l.

Viale Oceano Pacifico, 66 • 00144 Roma

Tel. +39.06.89161268 | Fax +39.06.89161316

www.humanativaspa.it - info@humanativaspa.it

Fabrizio Sensibile

Senior Security Analyst

fabrizio.sensibile@hnsecurity.it