ROMHACK

RED TEAMING

I LOVE IT WHEN A PLAN COMES TOGETHER

DISCLAIMER

Le azioni illustrate durante l'intervento, se effettuate nei confronti di un target reale, senza le opportune e adeguate autorizzazioni, costituiscono una serie di reati perseguibili sia penalmente che civilmente

Le tesi, le opinioni e le posizioni espresse in questo talk sono intime e personali, non necessariamente rappresentano le opinioni e le posizioni dell'azienda per cui lavoro

Nessun amministratore di sistema è stato maltrattato durante la realizzazione di questo talk

CHI SIAMO

Francesco «RageMan» Perna

- Sono socio e CSO di Quantum Leap (oggi parte del network Deloitte)

- Sono un ricercatore indipendente
  - Web Ecosystem
  - Operating System
  - Network Protocols
  - Embedded devices
  - ICS/SCADA

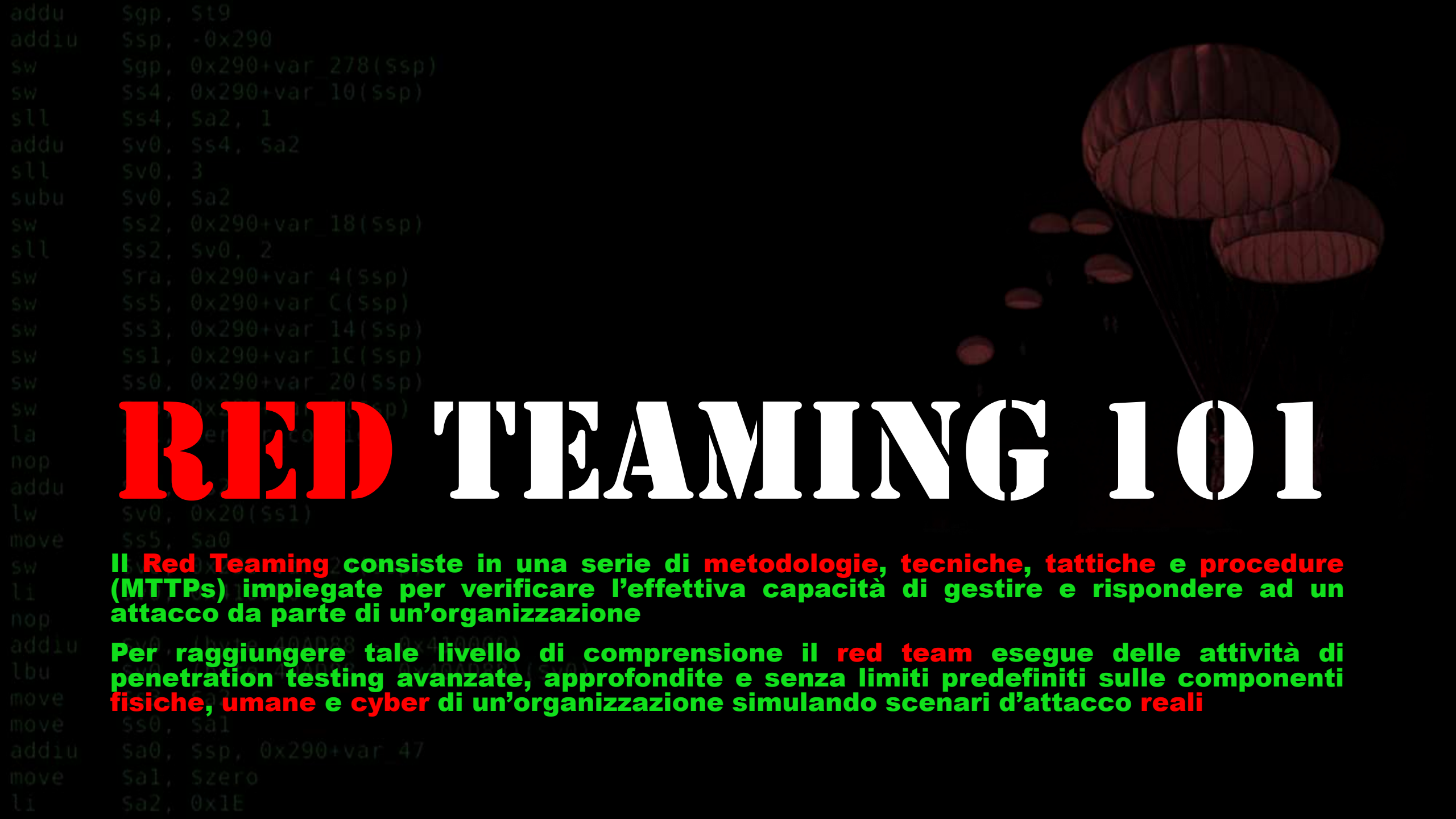
- Contribuisco alla scena Hacker italiana
  - Membro del direttivo Metro Olografix
  - Organizzatore del MOCA
  - Organizzatore del BSides
  - Membro di Sikurezza.org

- Contatti
  - fp@quantumleap.it
  - PGP Key ID – 0xACFD2B83
  - Key Fingerprint – DEC2 732D 0EB9 68DC FFAF FCF1 F04B 3B5D ACFD 2B83

CHI SIAMO

Lorenzo «illordlo» Nicolodi

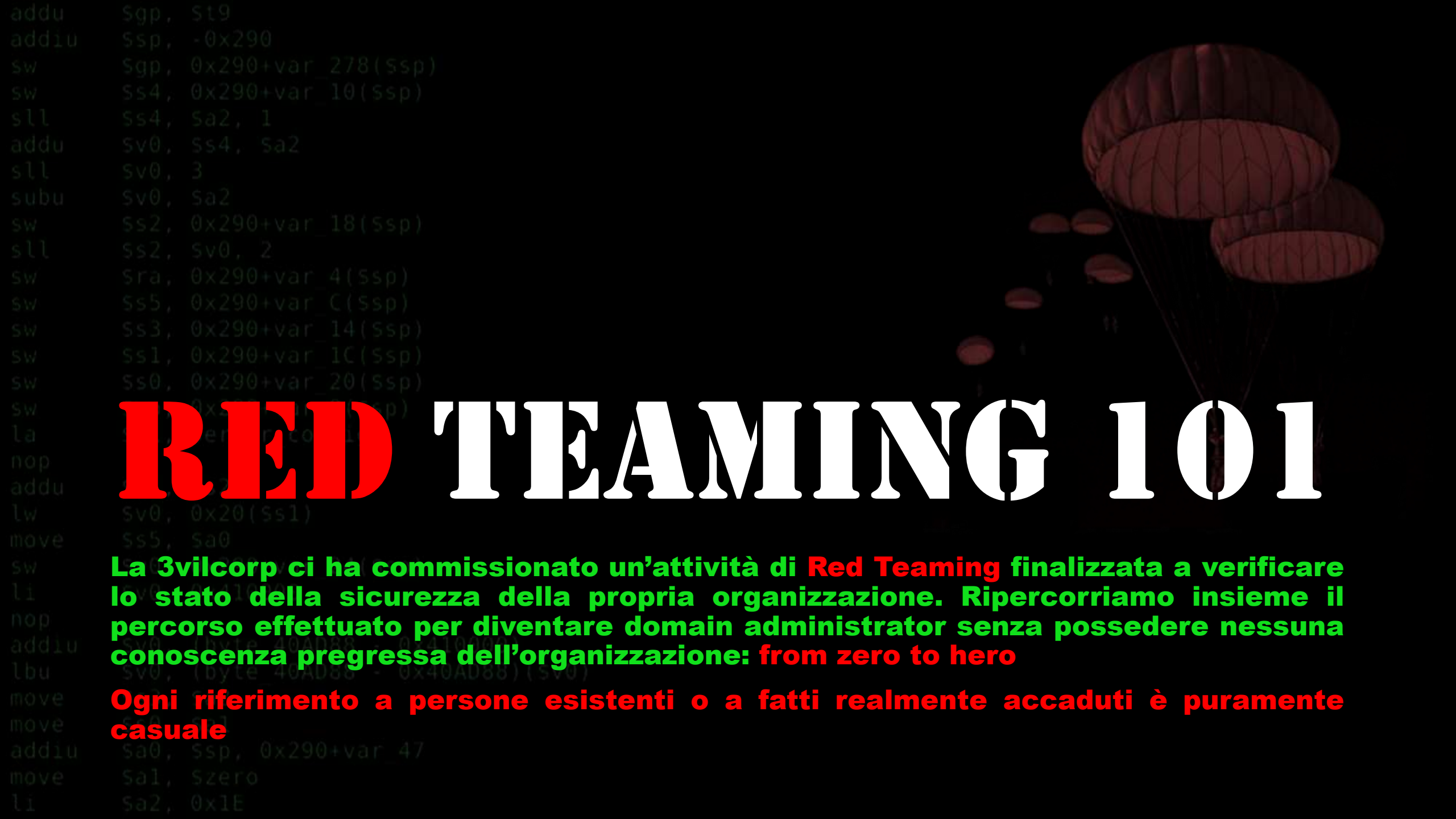
- Sono l'unico ad aver passato le selezioni di Microlab.red
  - Fornire esclusivamente attività «offensive»
  - Supporto con Quantum Leap nelle mission impossible
  - Supporto Rage nei suoi deliri e condivido con lui i miei
- Adoro fare ricerca in merito ad:
  - Assunzioni errate (a.k.a. nessuno lo farà mai)
  - Roba embedded, IoT o in genere che si rompe a guardarla
  - Implementazioni di protocolli di rete
- Approccio DIY per qualsiasi cosa o quasi
- Contatti
  - lo@microlab.red
  - PGP Key ID – 0xC33B1AC7
  - Key Fingerprint – FD5A B51C 8FA1 03AB 6560 7C27 6B8B FFFF C33B 1AC7



RED TEAMING 101

Il Red Teaming consiste in una serie di metodologie, tecniche, tattiche e procedure (MTTPs) impiegate per verificare l'effettiva capacità di gestire e rispondere ad un attacco da parte di un'organizzazione

Per raggiungere tale livello di comprensione il red team esegue delle attività di penetration testing avanzate, approfondite e senza limiti predefiniti sulle componenti fisiche, umane e cyber di un'organizzazione simulando scenari d'attacco reali



RED TEAMING 101

La 3vilcorp ci ha commissionato un'attività di Red Teaming finalizzata a verificare lo stato della sicurezza della propria organizzazione. Ripercorriamo insieme il percorso effettuato per diventare domain administrator senza possedere nessuna conoscenza pregressa dell'organizzazione: from zero to hero

Ogni riferimento a persone esistenti o a fatti realmente accaduti è puramente casuale

RED TEAMING

Differenze tra Vulnerability Assessment, Penetration Test e Red Teaming

	Vulnerability Assessment	Penetration Test	Red Teaming
Perimetro	I test sono effettuati in maniera massiva su **quanti più sistemi possibili** alla ricerca del maggior numero possibile di **vulnerabilità tecnologiche**. Il VA **non considera** le componenti **fisiche** e **umane**	I test sono effettuati in maniera **puntuale** sui sistemi e sulle applicazioni in perimetro alla ricerca di vulnerabilità **tecnologiche**, **logiche** e di **processo**. Si esplorano i vettori d'attacco in maniera accurata e approfondita	Sono considerate **tutte le componenti** (fisica, umana, cyber) di una organizzazione ma si esplorano i soli vettori d'attacco necessari a raggiungere gli obiettivi prefissati. Si utilizza un **approccio basato sugli scenari**
Exploitation	Capacità di exploiting **ridotta**: Sono sfruttate **automaticamente** solo le vulnerabilità senza impatto, **potenziale**, sui sistemi. Non vengono effettuati attacchi, il VA si limita ad identificare la presenza della vulnerabilità	Vengono sfruttate le vulnerabilità in funzione della **capacità di realizzare un attacco nel perimetro di analisi**. I movimenti laterali sono limitati ai soli sistemi in scope. Si usano spesso exploit/tools free e commerciali	Vengono sfruttate le vulnerabilità afferenti ai domini **fisico**, **umano** e **cyber** utilizzando tecniche e strumenti **pubblici** e **privati**. Sono implementati numerosi controlli per **ridurre** gli **impatti** potenziali sull'**operatività**
Obiettivi	Cerca di fornire un'indicazione circa il livello di **esposizione al rischio** dell'intero sistema informativo. L'esposizione viene valutata rispetto a **vulnerabilità tecnologiche note** e **misconfigurazioni** evidenti dei sistemi e delle infrastrutture analizzate	Viene **valutato puntualmente** il livello di rischio dei sistemi e delle applicazioni in perimetro **esponendo** chiaramente le **modalità di exploiting** delle vulnerabilità individuate e **suggerendo** le possibili contromisure da adottare.	Si tenta di **compromettere** l'organizzazione attraverso il raggiungimento degli **obiettivi** prefissati durante il kick-off dell'attività. Viene valutata la capacità dell'organizzazione di gestire e rispondere ad un attacco cyber mirato e di alto profilo

RED TEAMING
Verifiche preliminari

Le attività di Red Teaming **devono** essere effettuate solo a seguito di **un'attenta** verifica di tutti i prerequisiti (tecnici, organizzativi, legali). Questa fase è **delicatissima**, non sono ammesse leggerezze. In particolare bisogna:

- Effettuare le verifiche **contrattuali** e **normative** propedeutiche all'avvio delle attività (es. accordi sindacali, policy di gruppo, leggi locali, etc.) con l'ausilio di legali (sia penalisti che giuslavoristi) con competenze in ambito cyber security. I medesimi legali dovranno predisporre una manleva **adeguata**

- Ingaggiare gli **stakeholder** da coinvolgere o informare rispetto alle attività

- Definire chiaramente gli **obiettivi** da raggiungere, gli **scenari** che saranno realizzati, il **perimetro** dell'attività e la finestra temporale in cui saranno effettuate le operazioni tecniche. È auspicabile che gli accordi presi in tal senso vengano documentati

PARATEVI IL CULO
COVER YOUR ASS
蓋住你的屁股
ПОКРЫТЬ ВАШУ ЗАД
تغطية مؤخرتك

In estrema sintesi, dovete assicurarvi, nel limite della ragionevolezza, che se l'attività dovesse andare in maniera differente da come programmato, non siate voi a subirne le conseguenze dal punto di vista penale e/o civile

RED TEAMING
Pianificazione e preparazione

L'esecuzione delle attività di red teaming richiede un'attenta **preparazione** e **pianificazione**. Per completare questa fase si fa affidamento sulle informazioni acquisite tramite tecniche di **open source intelligence** (OSINT) e attraverso la **ricognizione fisica**. Nel corso di questa fase si procede a

- Identificare le **modalità di attacco** più efficaci per il raggiungimento degli obiettivi prefissati. Durante un'attività di red teaming bisogna fare poco rumore. Tools, tecniche e tattiche devono essere impiegati in funzione dei target ad adattati rispetto alla capacità di reazione dell'organizzazione

- Preparare e testare tutto il necessario per l'operazione (tools, hardware backdoor, VPN, strumenti a supporto dell'incursione fisica). Durante le attività, in genere, le **finestre temporali** in cui operare sono **ridotte**, dunque bisogna avere i tools pronti per poter gestire sia quanto pianificato che gli imprevisti

RED TEAMING
Esecuzione delle attività

- Utilizzando le medesime **metodologie**, **tecniche**, **tattiche** e **procedure** (MTTPs) utilizzate da un agente di minaccia reale, vengono individuate e sfruttate le vulnerabilità sulle componenti **fisiche**, **umane** e **cyber** dell'organizzazione

- Dopo aver guadagnato l'accesso iniziale, si attuano gli appropriati meccanismi di **persistenza** all'interno del perimetro aziendale

- Si procede dunque nella realizzazione dello scenario tentando di effettuare una serie di **movimenti laterali** che consentano di ottenere maggiori privilegi

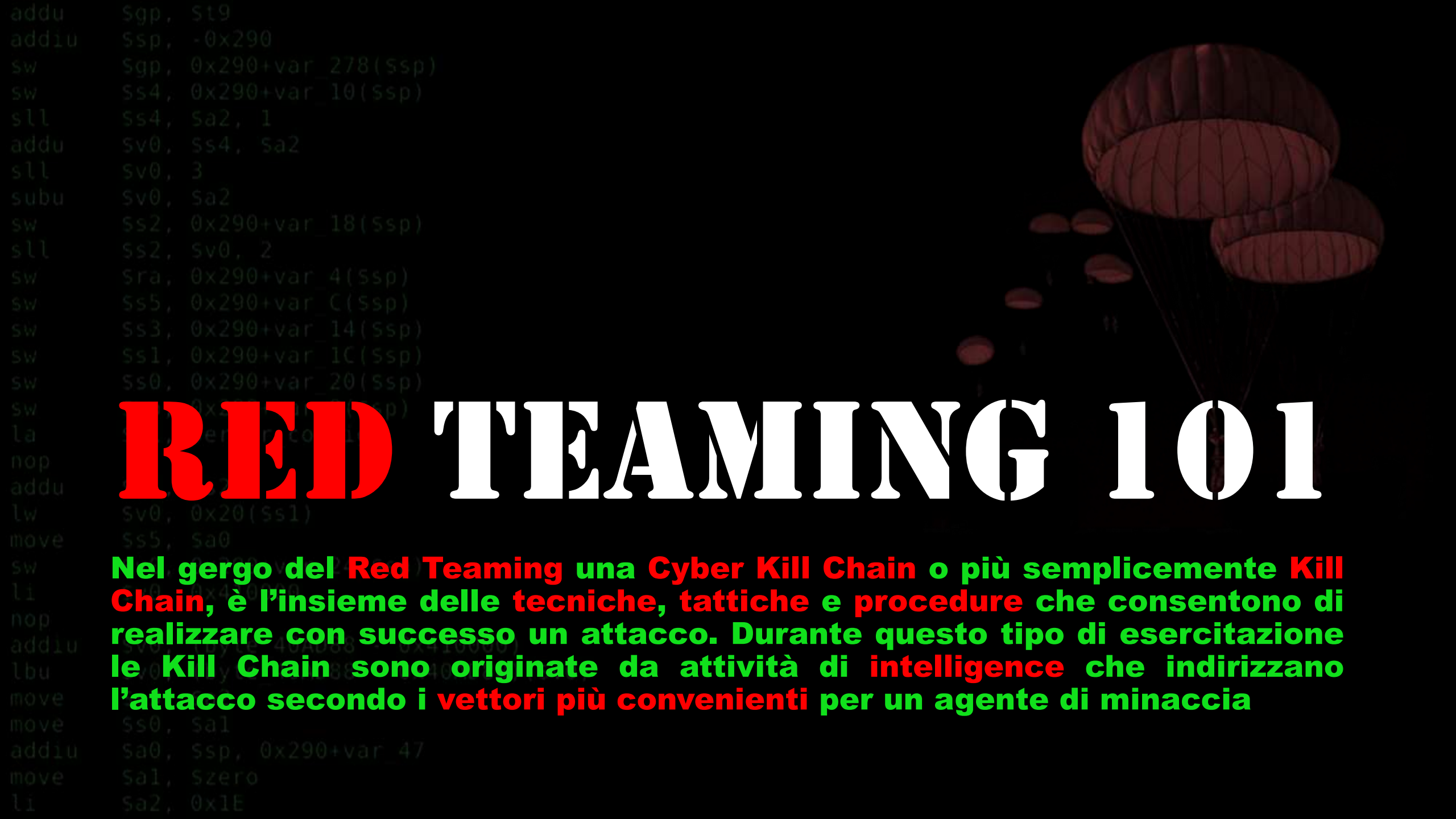
N.B. durante un'attività di red teaming, ottenere i privilegi amministrativi su un sistema o su un'infrastruttura non sempre coincide con il raggiungimento degli obiettivi prefissati. La **sicurezza informatica** non è data soltanto **sicurezza del sistema informativo**

RED TEAMING
Esfiltrazione informazioni e collazionamento delle evidenze

- In genere durante le attività di red teaming si ricorre all'esfiltrazione di informazioni per documentare l'efficacia di un attacco. Tale pratica deve essere **concordata preventivamente** con il Cliente in quanto potrebbe avere delle ripercussioni sulla gestione dell'attività **ex post**

- La documentazione delle attività di red teaming deve essere «continua», gli screenshot potrebbero non esser sufficienti a rappresentare la complessità di quanto accade durante l'operazione sul campo. In genere si adottano le seguenti tecniche di documentazione

  - Cattura dello schermo (2 fps. Sono sufficienti per documentare la sequenza dei comandi e le azioni effettuate)
  - Cattura dei terminali (comodo per redigere il report e fare copia incolla)
  - Video, possibilmente in alta definizione, con action cam e telefoni per documentare le operazioni fisiche
  - Foto, possibilmente in alta definizione, per documentare lo stato dei luoghi



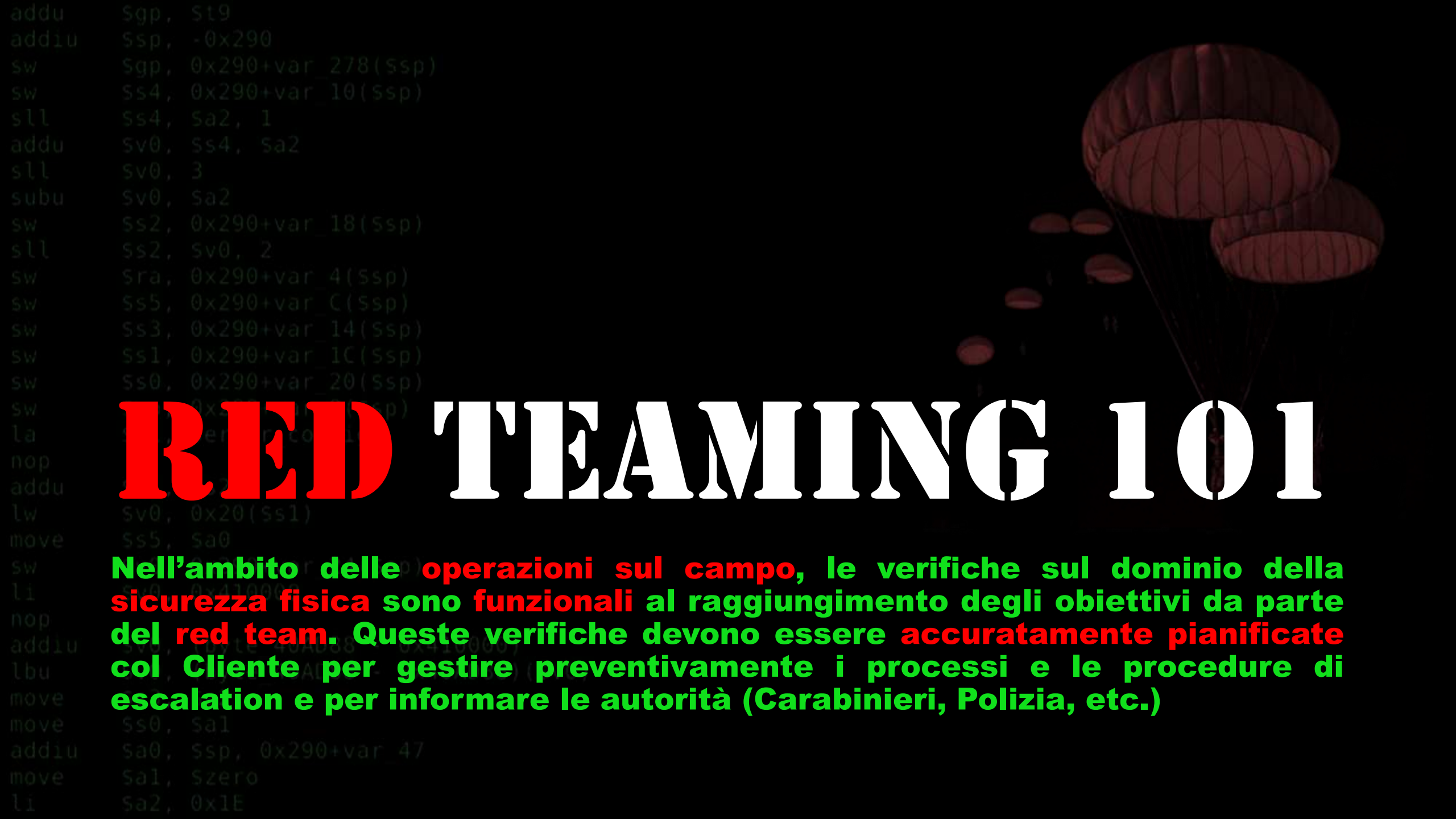
RED TEAMING 101

Nel gergo del Red Teaming una Cyber Kill Chain o più semplicemente Kill Chain, è l'insieme delle tecniche, tattiche e procedure che consentono di realizzare con successo un attacco. Durante questo tipo di esercitazione le Kill Chain sono originate da attività di intelligence che indirizzano l'attacco secondo i vettori più convenienti per un agente di minaccia

CYBER KILL CHAIN

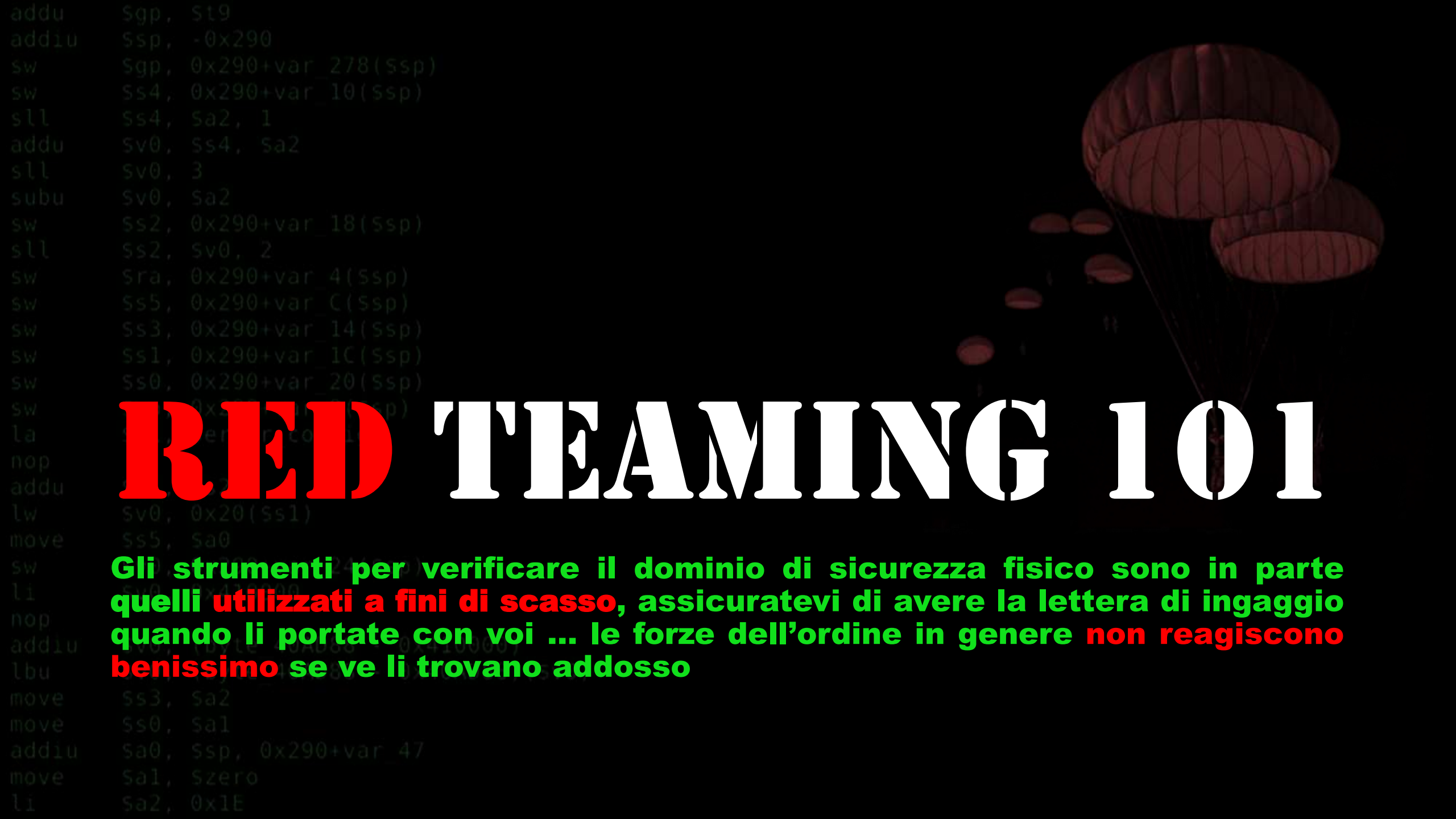
Esempi di Kill Chain in ambiente fisico, umano e cyber

	FISICO	UMANO	CYBER
1	Ricognizione fisica degli edifici dell'azienda ed individuazione delle vulnerabilità che consentono l'accesso fisico agli stabili	Acquisizione delle informazioni per creare uno scenario di spear phishing plausibile per il contesto dell'azienda	Ricognizione dei sistemi esposti sulla rete internet utilizzando delle tecniche di scansione a bassa interazione
2	Clonazione dei badge per l'accesso ai tornelli tramite remote badge sniffing. Accesso alla sede utilizzando i badge clonati	Invio dei messaggi di spear phishing attraverso la posta elettronica ed i servizi di instant messaging	Esecuzione delle tecniche, tattiche e procedure per sfruttare le vulnerabilità sui sistemi esposti
3	Installazione di backdoor hardware all'interno del perimetro di rete aziendale. Le backdoor possono essere connesse sia ai dispositivi di rete che ai computer	Acquisizione delle informazioni fornite dai target del phishing come ad esempio indirizzi IP, credenziali d'accesso, informazioni personali, etc.	Movimenti laterali sull'infrastruttura attaccata al fine di raggiungere gli obiettivi condivisi durante l'avvio delle attività
4	Attraverso le backdoor hardware il Red Team può eseguire gli attacchi sulla rete interna da remoto	Installazione di un backdoor sulla postazione di lavoro dell'utente per consentire gli attacchi di rete	Se necessario vengono effettuate attività a rumore crescente per testare la capacità di detection del blue team



RED TEAMING 101

Nell'ambito delle operazioni sul campo, le verifiche sul dominio della sicurezza fisica sono funzionali al raggiungimento degli obiettivi da parte del red team. Queste verifiche devono essere accuratamente pianificate col Cliente per gestire preventivamente i processi e le procedure di escalation e per informare le autorità (Carabinieri, Polizia, etc.)

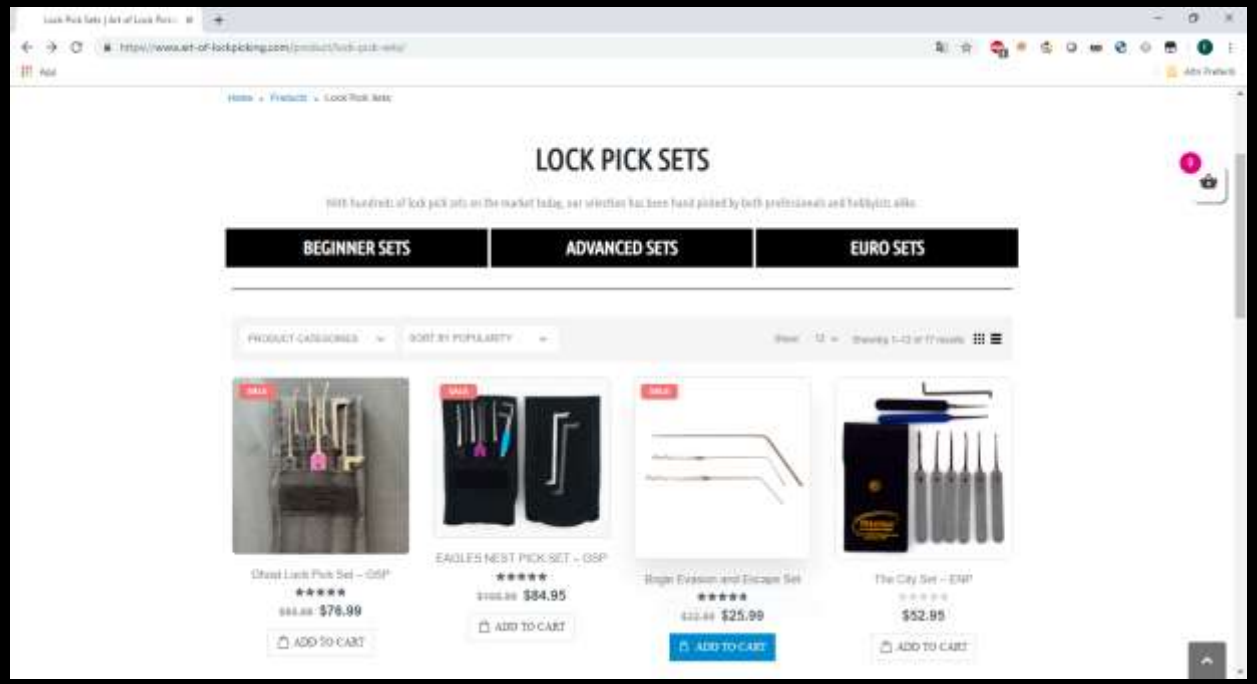


RED TEAMING 101

Gli strumenti per verificare il dominio di sicurezza fisico sono in parte quelli utilizzati a fini di scasso, assicuratevi di avere la lettera di ingaggio quando li portate con voi ... le forze dell'ordine in genere non reagiscono benissimo se ve li trovano addosso

RED TEAMING OPERATIONS

Verifica della sicurezza fisica – Grimaldelli



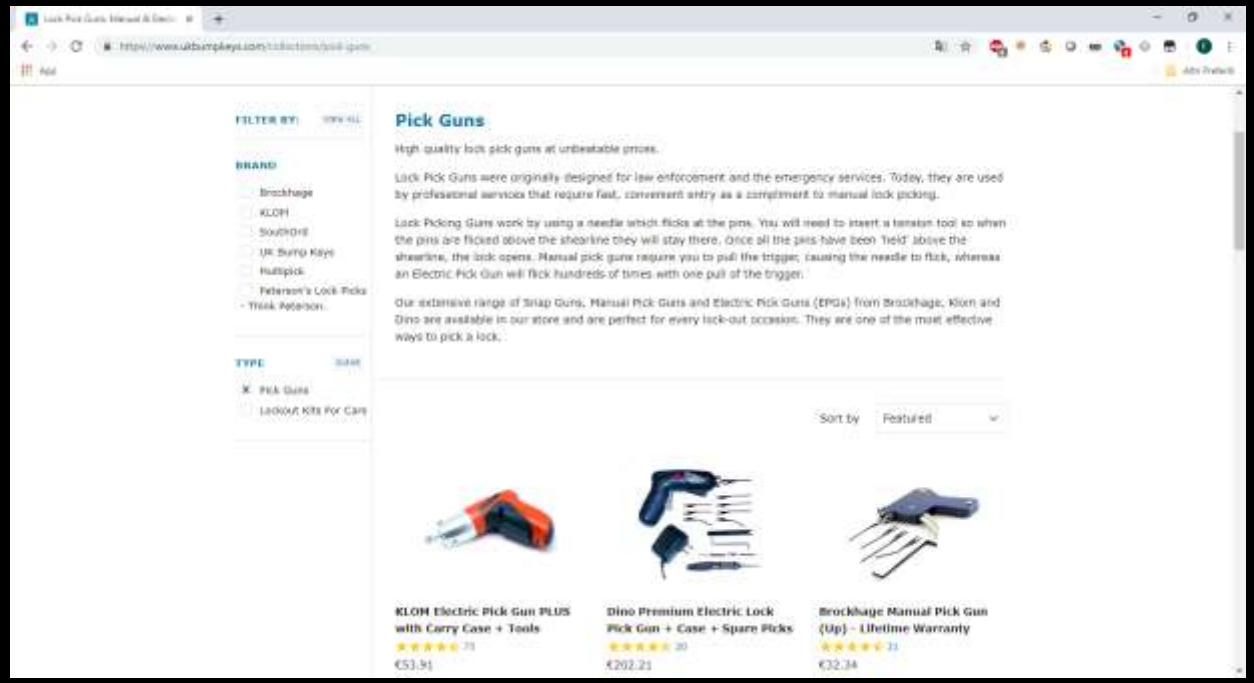
I set di grimaldelli possono essere acquistati online sui seguenti siti

- www.art-of-lockpicking.com
- www.lockpickshop.com
- www.sparrowslockpicks.ca
- www.ukbumpkeys.com

- I grimaldelli servono per **forzare** l'apertura delle serrature in maniera **non distruttiva** simulando l'azione meccanica della chiave. Facendo l'adeguata **pressione sui pistoncini** ed usando il **tensore** le serrature si aprono … it's a kind of magic!

RED TEAMING OPERATIONS

Verifica della sicurezza fisica – Bump keys & Lock Pick Guns



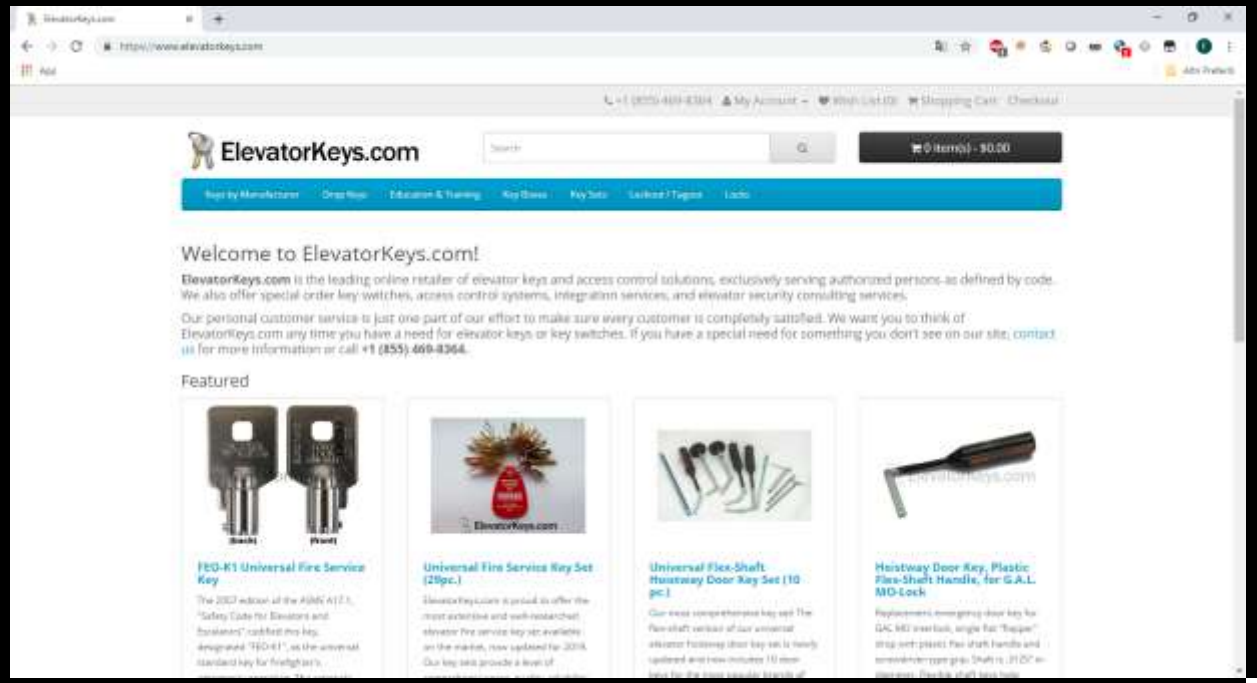
Bump keys, lock pick guns ed altri strumenti simili sono disponibili su

- www.art-of-lockpicking.com
- www.lockpickshop.com
- www.sparrowslockpicks.ca
- www.ukbumpkeys.com

- Le bump keys e le lock pick guns consentono l'apertura delle serrature utilizzando **la forza bruta**
- A seconda della serratura da aprire bisogna utilizzare lo **strumento corretto**: ad esempio, difficilmente sarà possibile aprire un cilindro europeo con una lock pick guns manuale (a meno che non abbiate un polso davvero molto allenato) e si dovrà usare una pistola elettrica

RED TEAMING OPERATIONS

Verifica della sicurezza fisica – Chiavi standard



- In determinate condizioni è possibile aprire le serrature utilizzando dei seti di **chiavi standard**
  - **Chiavi per ascensori**
  - **Chiavi per mobili ufficio**
  - **Chiave multifunzione 10 in 1**
    - **Valvole, pannelli, contatori, etc.**

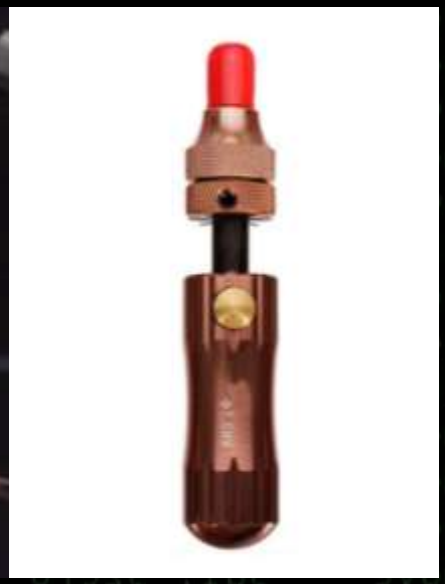
Le chiavi standard possono essere acquistate sui seguenti siti

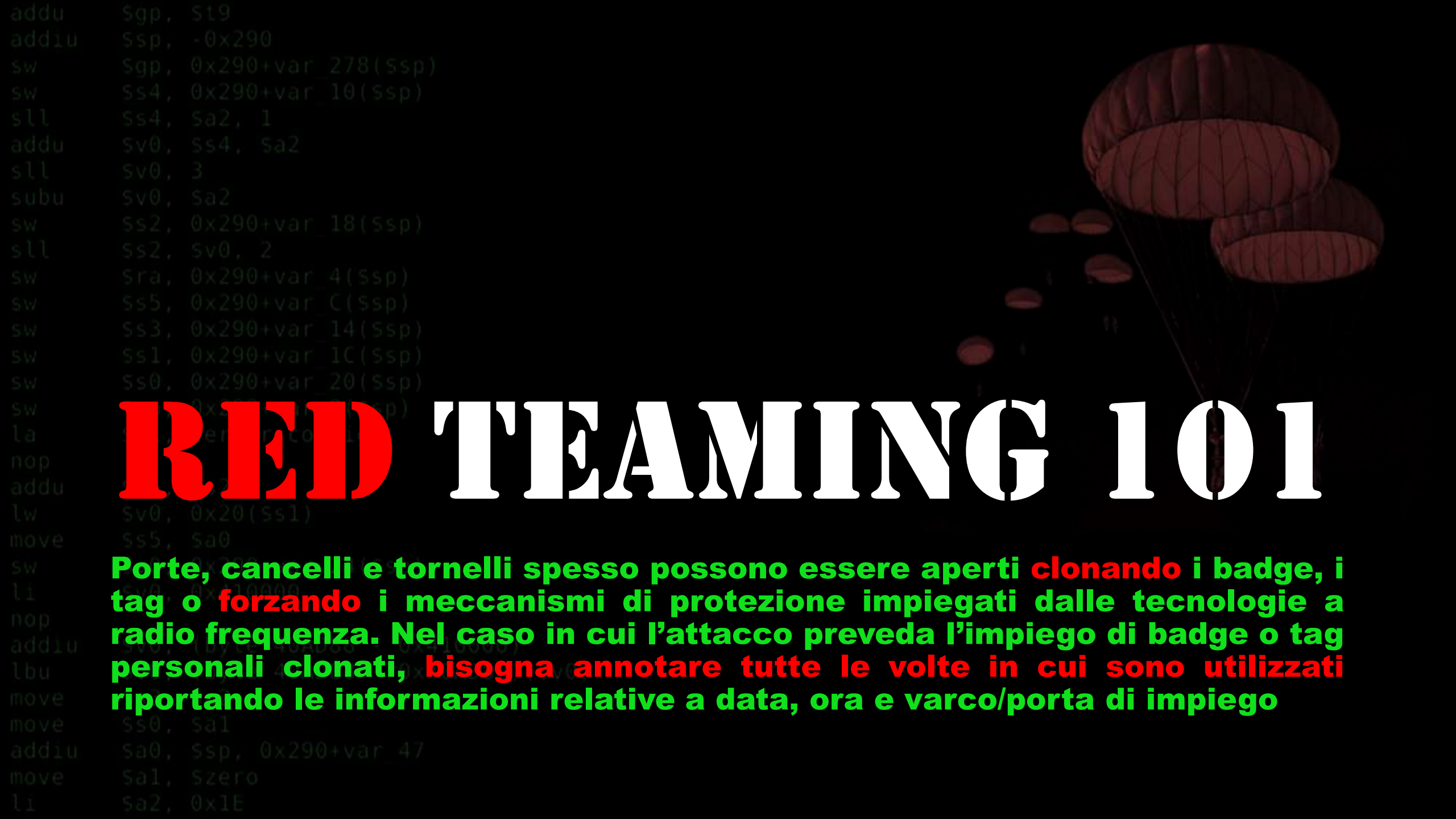
- www.elevatorkeys.com
- www.lockdoctor.biz
- www.easykeys.com
- www.keysplease.co.uk

RED TEAMING OPERATIONS

Verifica della sicurezza fisica – Altri strumenti

- Under the door tool
- Shove knife
- Tubolar lock pick tool
- Azoto liquido
- Fiamma ossidrica





RED TEAMING 101

Porte, cancelli e tornelli spesso possono essere aperti clonando i badge, i tag o forzando i meccanismi di protezione impiegati dalle tecnologie a radio frequenza. Nel caso in cui l'attacco preveda l'impiego di badge o tag personali clonati, bisogna annotare tutte le volte in cui sono utilizzati riportando le informazioni relative a data, ora e varco/porta di impiego

RED TEAMING OPERATIONS

Verifica della sicurezza fisica – 40, 315, 433 MHz

Amazon, Aliexpress ed eBay sono il paese dei balocchi per quanto riguarda questo genere di dispositivi

- https://www.amazon.it/Broadlink-telecomando-universale-domotica-intelligente/dp/B00W5BRY56
- https://it.aliexpress.com/item/Porta-del-garage-Copia-VENUTO-TOP432EE-contol-a-distanza-2-channel-Venuto-Top-432-EE-di/32837043418.html
- https://www.amazon.it/AZDelivery-433-MHz-Funk-trasmettitore/dp/B076KN7GNB

- 40, 315, 433 MHz sono frequenze utilizzate spesso per l'automazione casalinga (cancelli, serrande, tapparelle, luci)
- Spesso dispositivi molto economici e senza adeguata protezione (es. rolling code, che comunque possono essere bypassati via jam & forward) sono impiegati per proteggere edifici sensibili
- Utilizzando oggetti ready-made o progetti DIY basati su RPI/Arduino è possibile interagire con i ricevitori sul campo attraverso replay attack

RED TEAMING OPERATIONS

Verifica della sicurezza fisica – RFID 125KHZ/13.56MHZ made in PRC

Gli RFID RW made in PRC si possono trovare su Amazon e eBay

- www.amazon.it/gp/product/B07CLM7VK8
- www.amazon.it/gp/product/B07MBZ2793
- www.ebay.it/itm/Smart-RFID-Copier-ID-IC-Reader-Writer-Copy-with-13-56MHz-125KHz-Taglia-piccola

- Gli RFID RW servono per poter **clonare** una vasta gamma di schede e tag RFID in maniera molto semplice
- Le frequenze a cui operano sono 125KHZ, 250KHZ, 375KHZ, 500KHZ, 13.56MHZ.
- I formati supportati da questi lettori sono i seguenti
  - EM4305
  - EM5200
  - EM8800
  - T5577
  - ZX-F08 UID
  - ISO 14443 Tipo A e B.
- Funzionano bene ma alcuni formati popolari non sono supportati (es. HID ICLASS, HID Prox)

RED TEAMING OPERATIONS

Verifica della sicurezza fisica – RFID Hacking Swiss army knife

Il Proxmark può essere acquistato sul sito lab401.
MUST HAVE quando bisogna fare queste attività

› https://lab401.com/collections/rfid-tools

› Il proxmark è un tool versatile in grado di clonare quasi tutte le tipologie di RFID in commercio

› Ha numerose features, una delle più interessanti è quella che consente l'**emulazione** degli RFID

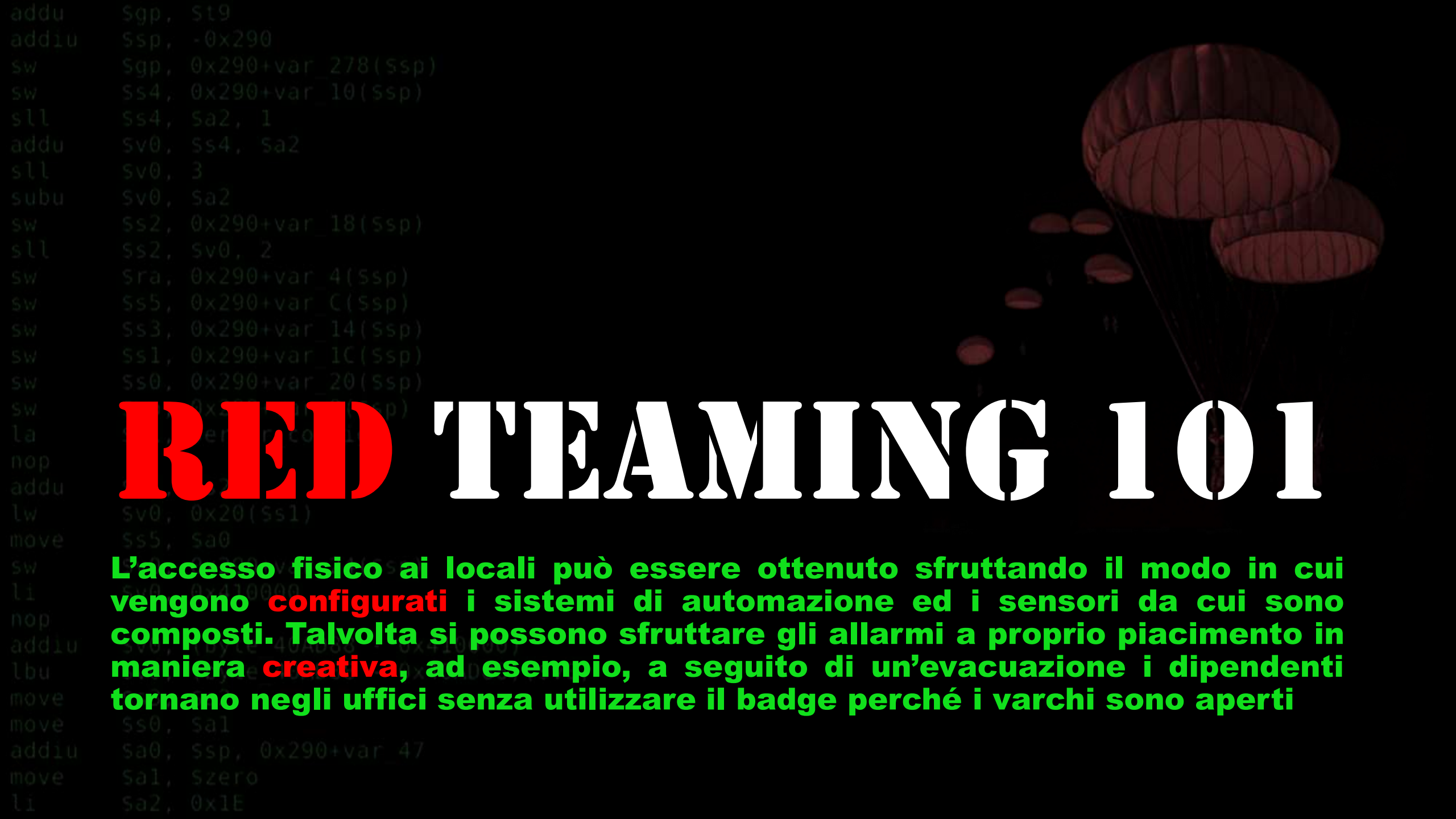
› Necessita di qualche modifica per estendere il campo d'azione se usato in maniera esclusiva durante le attività

RED TEAMING OPERATIONS

Verifica della sicurezza fisica – Long range sniffing

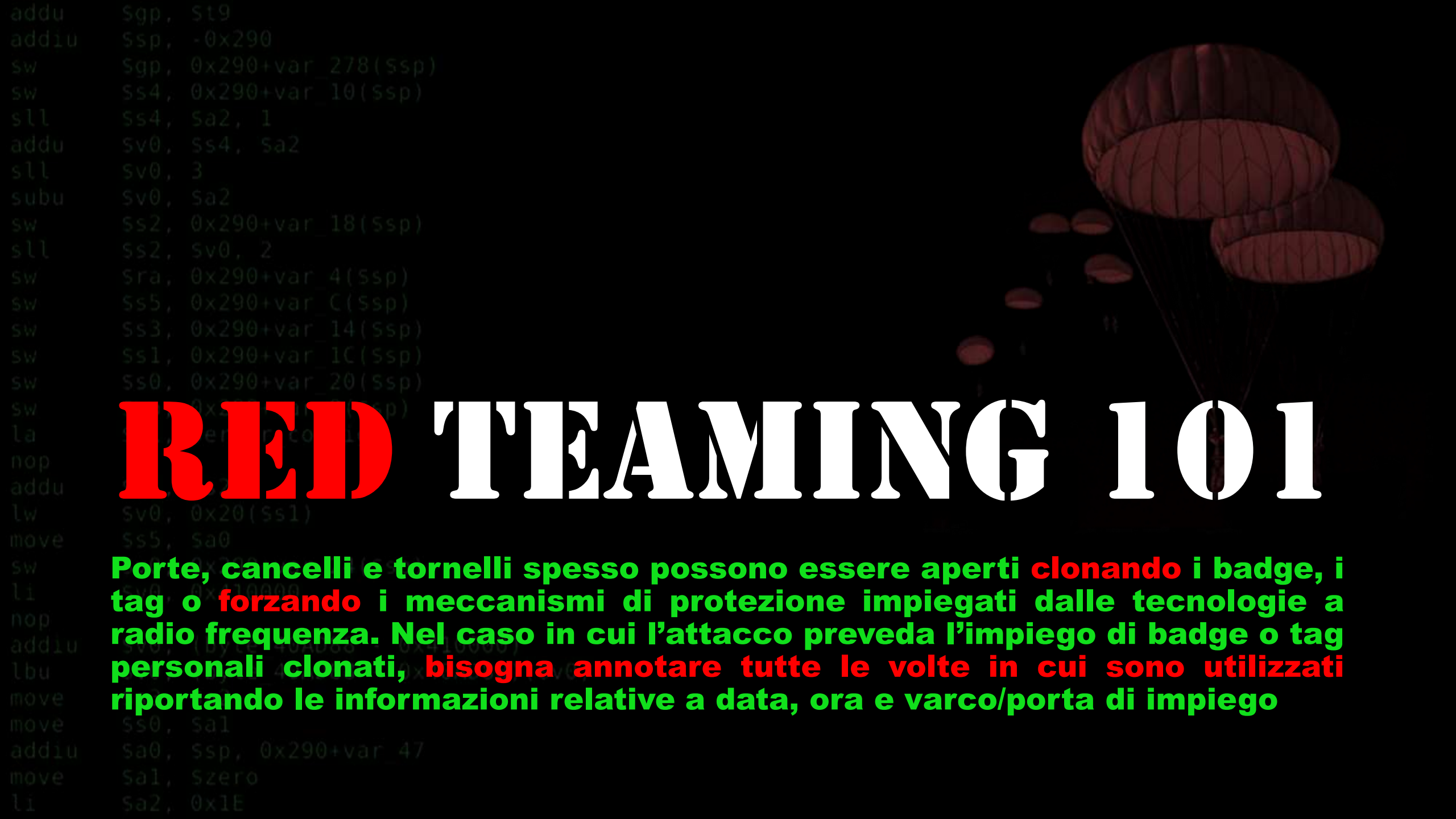
I lettori HID possono essere acquistati usati sia su Amazon che su eBay. Si suggerisce di sviluppare la soluzione utilizzando una board simile al Raspberry, più comoda durante le operazioni sul campo

- Poter clonare i badge a distanza incrementa la possibilità di poter accedere agli edifici senza che nessuno si accorga di noi
- Non esistono soluzioni standard, bisogna avere un po' di fantasia e modificare i lettori di badge a lunga distanza esistenti
- La chiave per leggere a distanza è fornire energia in maniera stabile al lettore
- Lettori che si prestano alle modifiche
  - HID – MaxiProx 5375
  - HID – Indala Long-Range Reader 620
  - HID – iCLASS – R90 Long Range Reader



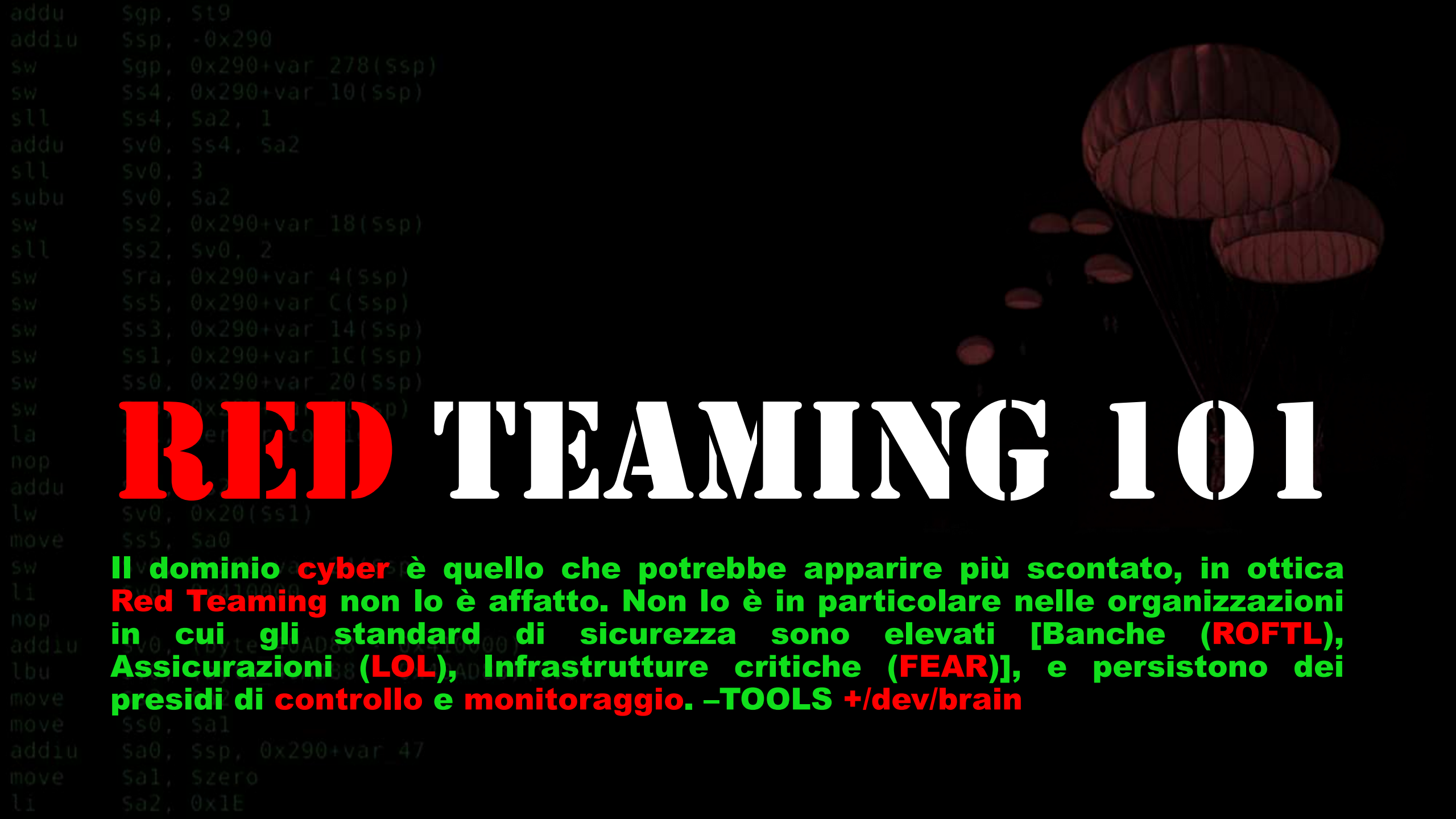
RED TEAMING 101

L’accesso fisico ai locali può essere ottenuto sfruttando il modo in cui vengono configurati i sistemi di automazione ed i sensori da cui sono composti. Talvolta si possono sfruttare gli allarmi a proprio piacimento in maniera creativa, ad esempio, a seguito di un’evacuazione i dipendenti tornano negli uffici senza utilizzare il badge perché i varchi sono aperti



RED TEAMING 101

Porte, cancelli e tornelli spesso possono essere aperti clonando i badge, i tag o forzando i meccanismi di protezione impiegati dalle tecnologie a radio frequenza. Nel caso in cui l'attacco preveda l'impiego di badge o tag personali clonati, bisogna annotare tutte le volte in cui sono utilizzati riportando le informazioni relative a data, ora e varco/porta di impiego



RED TEAMING 101

Il dominio cyber è quello che potrebbe apparire più scontato, in ottica Red Teaming non lo è affatto. Non lo è in particolare nelle organizzazioni in cui gli standard di sicurezza sono elevati [Banche (ROFTL), Assicurazioni (LOL), Infrastrutture critiche (FEAR)], e persistono dei presidi di controllo e monitoraggio. –TOOLS +/dev/brain

RED TEAMING OPERATIONS
Cyber Operations – Field Devices

I field devices sono da utilizzare coerentemente con la strategia di attacco e persistenza. Non è detto che debbano essere usati tutti

- Quando si fanno le operazioni sul campo bisogna essere preparati a tutto (o quasi ☺). Hak5, Great Scott Gadget, e altri vendor forniscono una serie di strumenti pronti per essere usati
- Le soluzioni DIY non sono da sottovalutare
- Non dimenticate cavi, adattatori, spine, prese, seriali, nastro isolante
- Cifratura, esfiltrazione, wiping

RED TEAMING OPERATIONS

Cyber Operations – Insecure Defaults + Fake AP + Responder = PW3D

RED TEAMING OPERATIONS

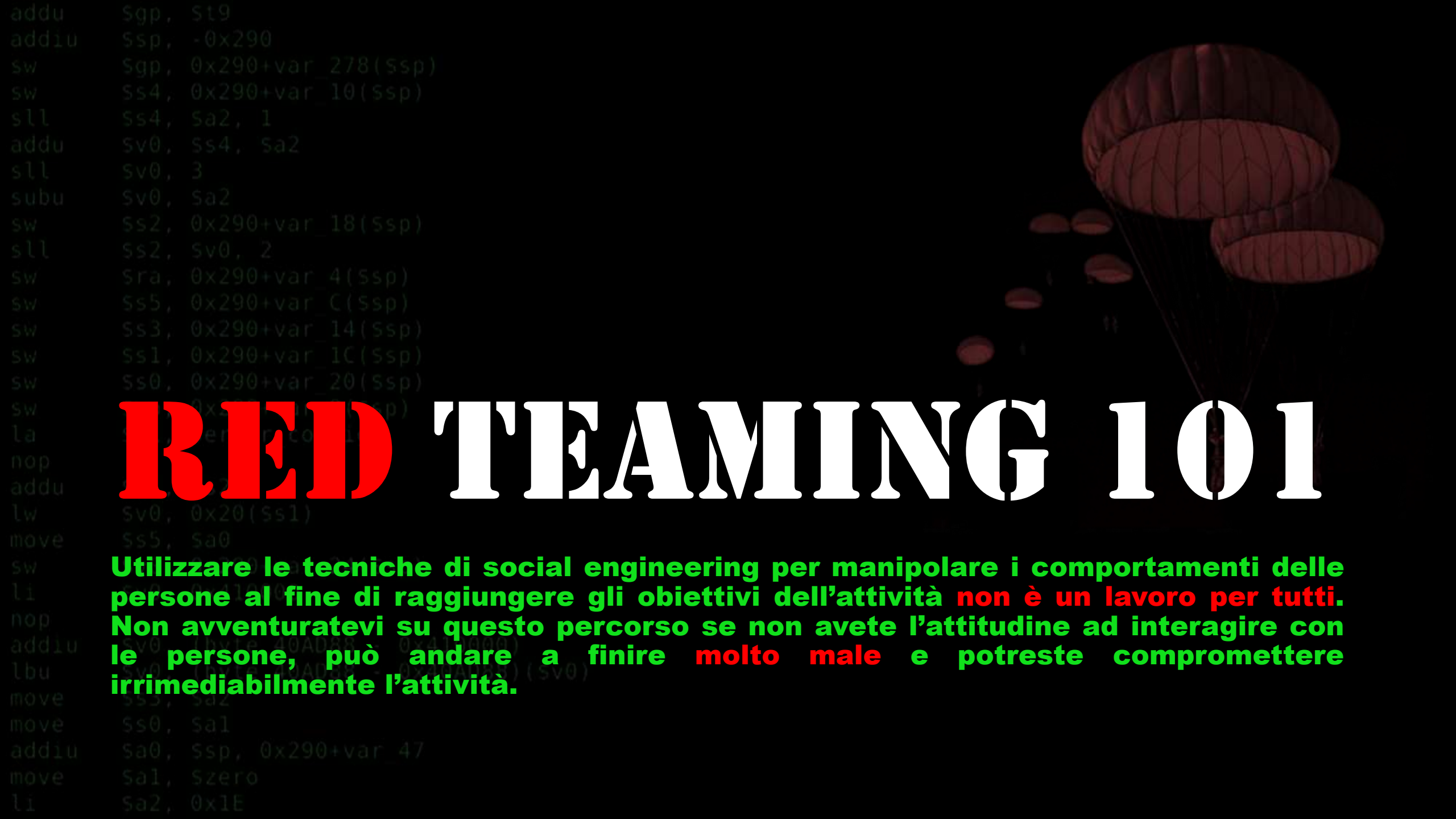
Cyber Operations – Command and control

- I sistemi di comando e controllo (C&C) sono utilizzati per interagire con i field devices, soprattutto quando esposti devono essere configurati per essere poco visibili

- Non esiste il sistema C&C adatto ad ogni esigenza, che sia P2P, Statico, DGA Based, bisogna valutare lo scenario in cui si effettuano le operazioni ed identificare quello più adatto

- I sistemi di monitoraggio aziendale diventano sempre più sofisticati, bisogna prevedere sistemi di C&C che facciano affidamento su canali di comunicazione out of band

- Bisogna prevedere dei meccanismi (ad esempio dei watchdog) per evitare di perdere l'accesso ai field devices



RED TEAMING 101

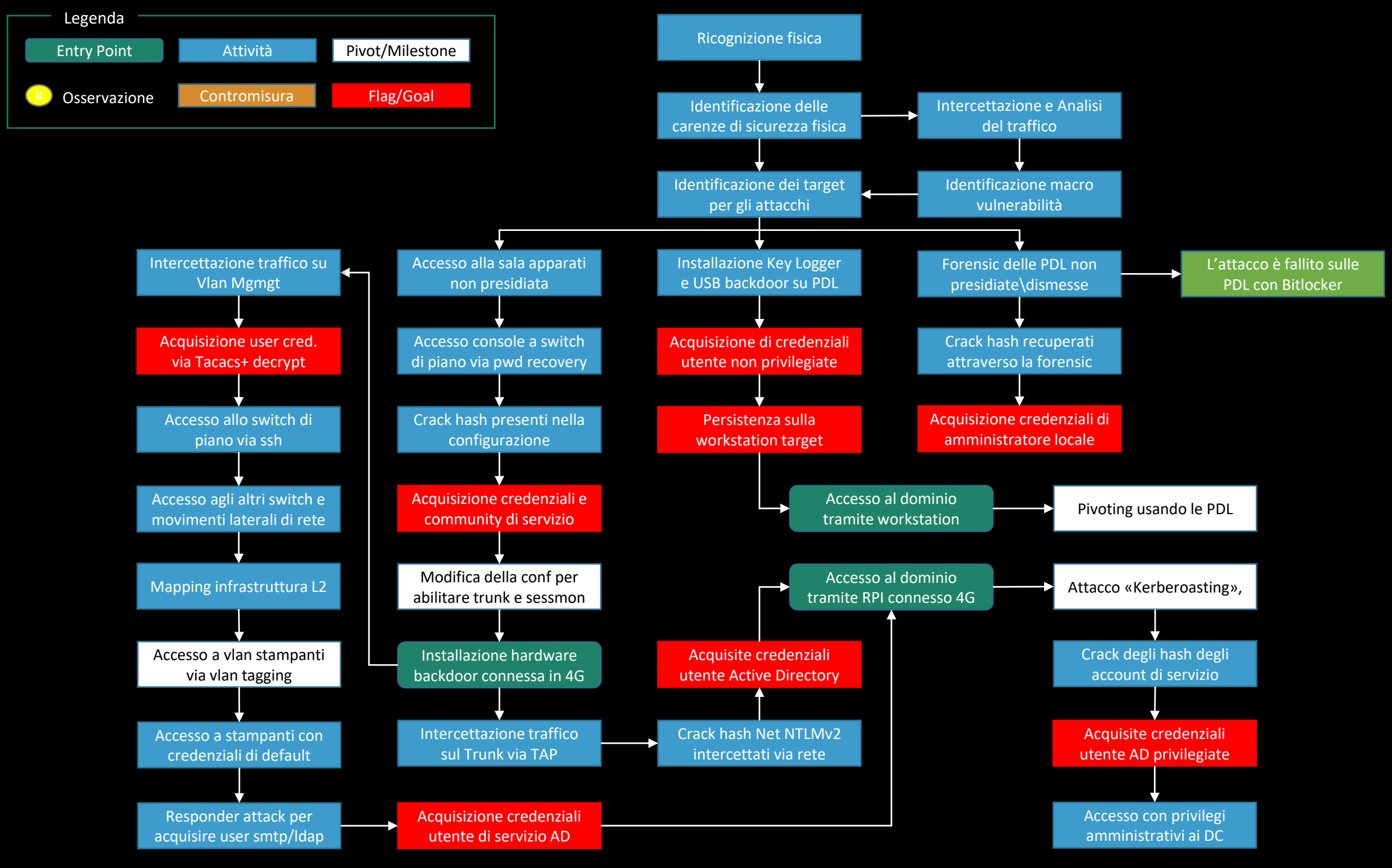
Utilizzare le tecniche di social engineering per manipolare i comportamenti delle persone al fine di raggiungere gli obiettivi dell'attività non è un lavoro per tutti. Non avventuratevi su questo percorso se non avete l'attitudine ad interagire con le persone, può andare a finire molto male e potreste compromettere irrimediabilmente l'attività.

RED TEAMING OPERATIONS

Verificare il fattore Umano

Le verifiche di sicurezza che si basano sull'interazione con le persone, devono essere valutate accuratamente in chiave legale, tattica e strategica.

- Non approcciare mai le persone senza aver compreso chi sono, cosa fanno e come operano all'interno dell'organizzazione
- Mantenete la calma, qualunque cosa succeda
- Utilizzare i playbook, le interazioni non si improvvisano, esistono pattern comportamentali ben codificati che si applicano a determinati profili di persone


Legenda
Entry Point
Attività
Pivot/Milestone
Osservazione
Contromisura
Flag/Goal
Ricognizione fisica
Identificazione delle carenze di sicurezza fisica
Intercettazione e Analisi del traffico
Identificazione dei target per gli attacchi
Identificazione macro vulnerabilità
Intercettazione traffico su Vlan Mgmgt
Accesso alla sala apparati non presidiata
Installazione Key Logger e USB backdoor su PDL
Forensic delle PDL non presidiate\dismesse
L'attacco è fallito sulle PDL con Bitlocker
Acquisizione user cred. via Tacacs+ decrypt
Accesso console a switch di piano via pwd recovery
Acquisizione di credenziali utente non privilegiate
Crack hash recuperati attraverso la forensic
Accesso allo switch di piano via ssh
Crack hash presenti nella configurazione
Persistenza sulla workstation target
Acquisizione credenziali di amministratore locale
Accesso agli altri switch e movimenti laterali di rete
Acquisizione credenziali e community di servizio
Accesso al dominio tramite workstation
Pivoting usando le PDL
Mapping infrastruttura L2
Modifica della conf per abilitare trunk e sessmon
Accesso al dominio tramite RPI connesso 4G
Attacco «Kerberoasting»,
Accesso a vlan stampanti via vlan tagging
Installazione hardware backdoor connessa in 4G
Acquisite credenziali utente Active Directory
Crack degli hash degli account di servizio
Accesso a stampanti con credenziali di default
Intercettazione traffico sul Trunk via TAP
Crack hash Net NTLMv2 intercettati via rete
Acquisite credenziali utente AD privilegiate
Responder attack per acquisire user smtp/ldap
Acquisizione credenziali utente di servizio AD
Accesso con privilegi amministrativi ai DC

```
addu    $gp, $t9
addiu   $sp, -0x290
sw      $gp, 0x290+var_278($sp)
sw      $s4, 0x290+var_10($sp)
sll     $s4, $a2, 1
addu    $v0, $s4, $a2
sll     $v0, 3
subu    $v0, $a2
sw      $s2, 0x290+var_18($sp)
sll     $s2, $v0, 2
sw      $ra, 0x290+var_4($sp)
sw      $s5, 0x290+var_C($sp)
sw      $s3, 0x290+var_14($sp)
sw      $s1, 0x290+var_1C($sp)
sw      $s0, 0x290+var_20($sp)
sw      $gp, 0x290+var_8($sp)
la      $s1, server_config
nop
addu    $s1, $s2
lw      $v0, 0x20($s1)
move    $s5, $a0
sw      $v0, 0x290+var_24($sp)
li      $v0, 0x410000
nop
addiu   $v0, (byte_40AD88 - 0x410000)
lbu     $v0, (byte_40AD88 - 0x40AD88)($v0)
move    $s0, $a1
addiu   $a0, $sp, 0x290+var_47
move    $a1, $zero
li      $a2, 0x1E
```

ROMHACK

GRAZIE!

@MetroOlografix

@illordlo