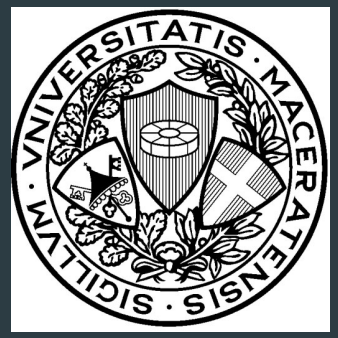


Il Penetration Testing quale metrica del grado di sicurezza di una rete

Università degli Studi di Macerata

2/11/2016

Alessandro Di Carlo

$WHOAMI

@samaritan_o

http://bit.ly/2fL3nM5

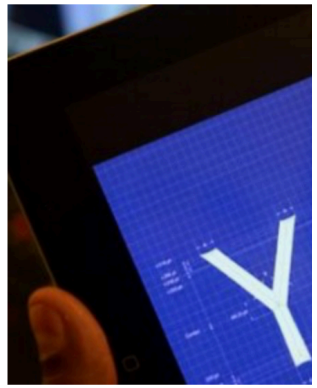
- 6+ years in InfoSec
- National and International speaker
- Master Degree in Computer Science
- Cyber Security Consultant at Tiger Security Srl
- IT Security Expert
- Digital Forensics maniac
- **eCPPT** – eLearnSecurity Certified Professional Penetration Tester
- **eWAPT** – eLearnSecurity Web Application Penetration Tester (next week)
- (ISC)2 – IISFA – ONIF Active Member

$Di cosa parleremo oggi?

- Che cos’è un Penetration Testing
- Aspetti legali del Penetration Testing
- Le fasi di un Penetration Testing
- Demo

$Un po’ di cronaca

Yahoo, violati account di 500 milioni di utenti. In rete Michelle Obar



MEDIA & REGIME

Hackerato anche il p
irruzione vi sarebber
servizi russi che avev
Stato Colin Powell. E
lavorando con le aut

di F. Q. | 22 settembre 2016

R.it | Sicurezza

Home | News | Speciali | Mobile | Soci

LinkedIn: rubati i dati 110 milioni di utenti

La piattaforma social avverte: "Cambiate le pas
data breach è avvenuto nel 2012 i profili in ques
rischio: si possono "craccare" in 72 ore

I DA
ven
hac
per
Bitc
nuo

Degli hacker hanno rubato oltre 60 milioni di password di Dropbox

31 August 2016 // 10:24 AM CET

Degli hacker hanno rubato i dati di oltre 60 milioni di account della piattaforma di cloud storage Dropbox. Benché gli account siano stati rubati durante una breccia precedentemente dichiarata, e benché Dropbox affermi di aver già forzato un reset delle password degli utenti, ancora non si sapeva quanti fossero gli utenti colpiti da questo hack, e solamente ora si riescono a capire le reali proporzioni del fenomeno.

Motherboard ha ottenuto una serie di file contenenti indirizzi email e password hashed degli utenti Dropbox attraverso alcune fonti del mercato per il commercio di database. In tutto, i quattro file si sommavano per un totale di 5GB, e contenevano i dettagli di 68.680.741 account. I dati sono reali, secondo un funzionario Dropbox che non è stato autorizzato a parlare a rilasciare dichiarazioni on the record.

All’inizio di questa settimana, Dropbox ha annunciato che avrebbe forzato un reset delle password per alcuni utenti dopo aver scoperto un pacchetto di dati di account risalenti a una breccia databile al 2012. L’azienda non ha reso pubblico l’esatto

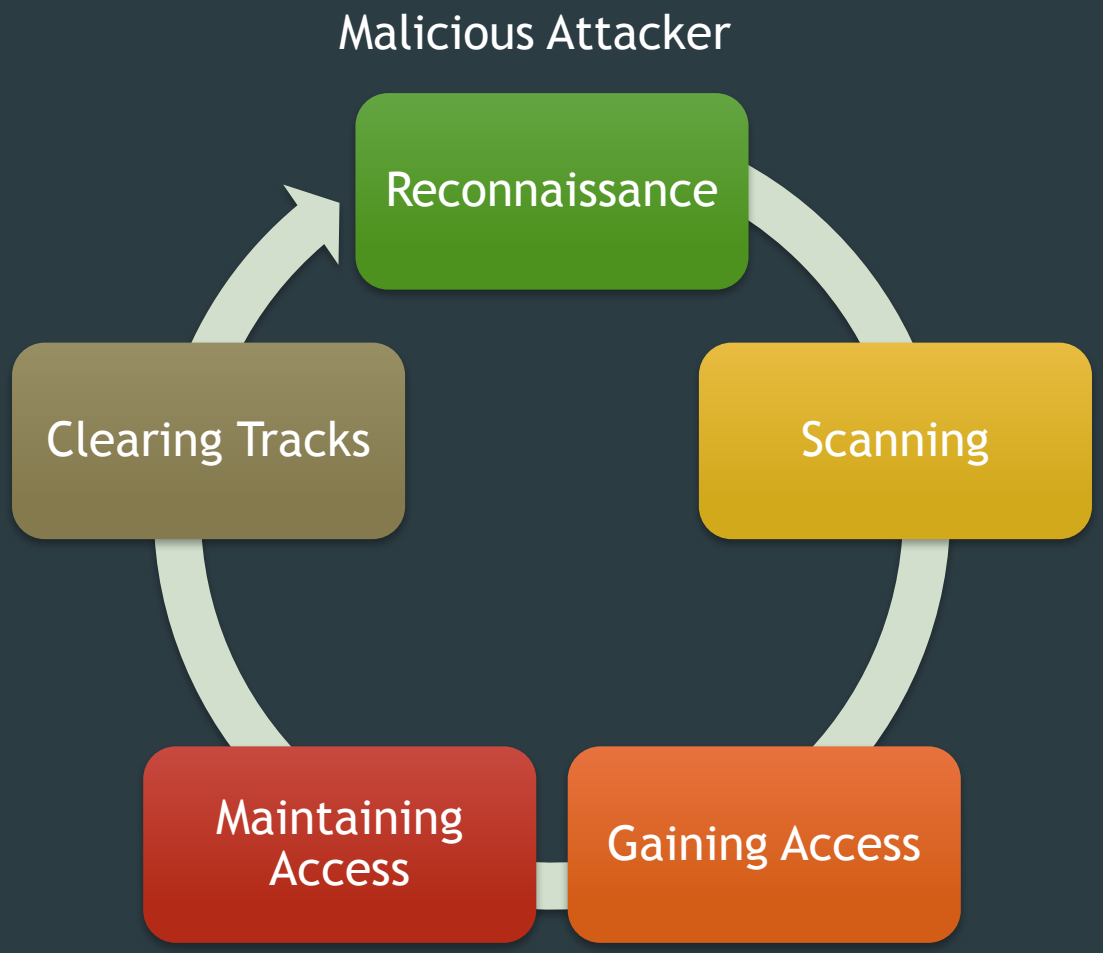
$Che cos’è un Penetration Testing

- Il Penetration Tester ha lo scopo di trovare TUTTE le vulnerabilità del suo target
- Questa attività richiede molto **metodo, abilità** ma soprattutto **predisposizione alla sofferenza e al dolore!!!**
- Differisce da un cracker poiché quest’ultimo cerca solamente una qualsiasi strada che gli permetta di avere un accesso privilegiato al sistema
- Richiede una consocienza approfondita dei vettori di attacco e del loro potenziale

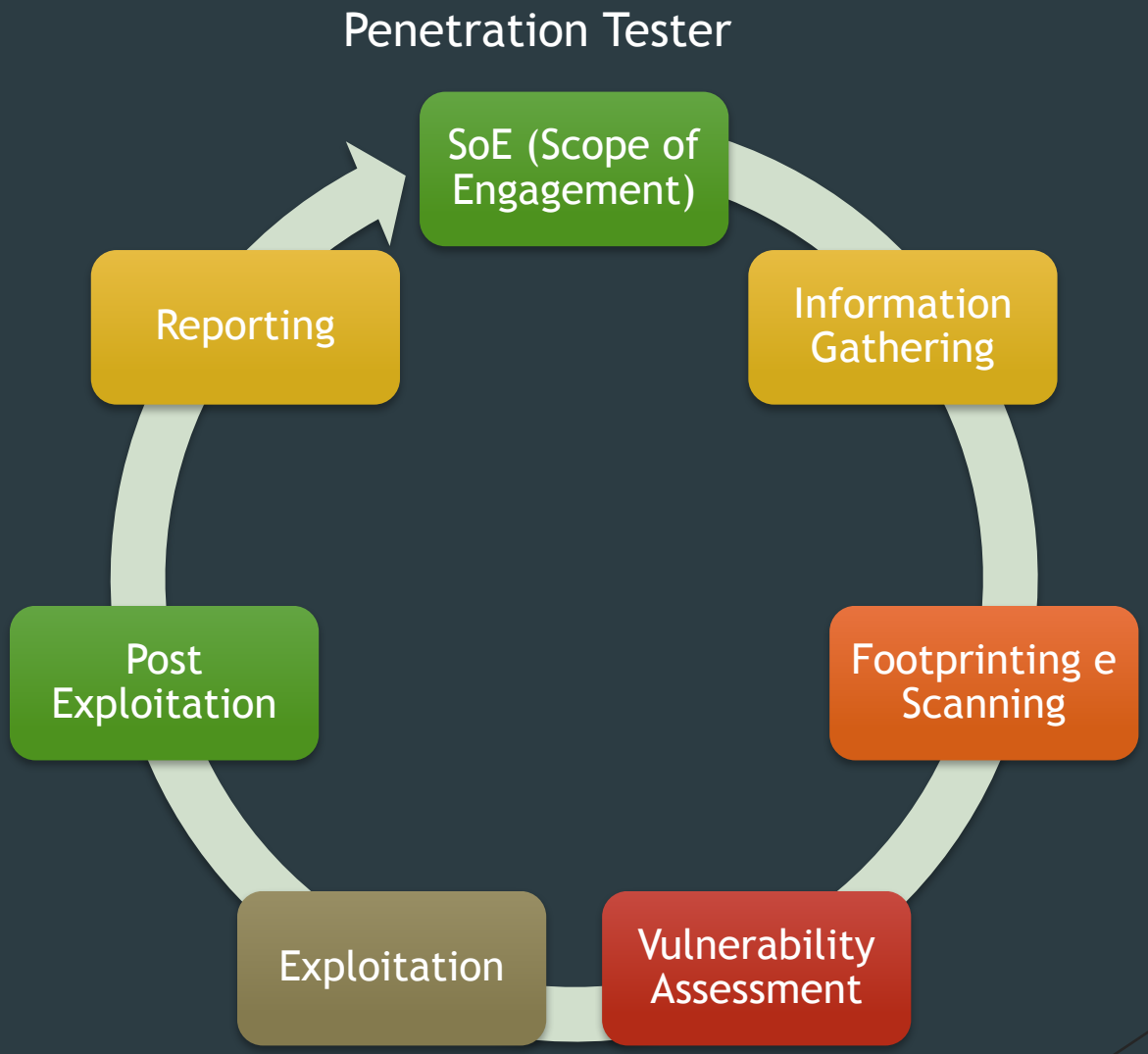
$Aspetti legali

- Le aziende pretendono informazioni riguardanti la disponibilità, la riservatezza e l'integrità dei propri dati
- Stipulazione di un NDA (Non Disclosure Agreement)
- La confidenzialità è solo una degli aspetti legali di un pentesting. Bisogna poi stabilire cosa **poter fare e cosa non poter fare**
- Regole di ingaggio:
  - Una lista di cosa è permesso fare al penetration tester
  - La finestra temporale in cui avverranno i test
  - I contatti all'interno dell'azienda con cui il penetration tester si interfaccerà

$Fasi di un Penetration Testing



$Fasi di un Penetration Testing



$Information Gathering

- Molti principianti tendono a saltare questa fase – SBAGLIATO!!
- Importante eseguirla DOPO aver stipulato lo SoE
- Da eseguire su più livelli
  - Infrastrutturale
  - Gerarchia aziendale
- Cercare di collezionare il più alto numero di informazioni
- Solida base per futuri attacchi di **Social Engineering**

$Information Gathering - Infrastruttura

- Lo scopo è quello di dare un significato ad ogni indirizzo IP del nostro scope
  - C'è un host attivo?
  - C'è un server in uso?
  - Quale sistema operativo si trova sull'host e sul server?
  - Quali porte sono esposte?
  - Qual è la versione dei servizi esposti?

- Queste domande ci aiutano a
  - Concentrarsi solo su server ed host attivi
  - Costruire attacchi mirati
  - Preparare la superifice per la fase di **Exploitation**

$Information Gathering – Web App

- In caso di Web App le informazioni da raccogliere sono
  - Domini
  - Sottodomini
  - Pagine
  - Tecnologie in uso (PHP, .NET, etc.)
  - Framework e CMS in uso (Wordpress, Drupal, Joomla, etc.)

- Nel caso delle Web App uno degli strumenti più utilizzati in tutte le fasi di un Penetration Testing è sicuramente **Burp Suite**

$Footprinting e Scanning

- Identificare il giusto sistema operativo di una macchina consente di risparmiare molto tempo
- Non ha senso cercare vulnerabilità di Microsoft su sistemi Linux
- Più si è precisi in questa fase, più si sarà agevolati durante la fase di Vulnerability Assessment
- Ci sono degli strumenti che cercano di identificare il sistema operativo, la versione e il livello di patching

$Footprinting e Scanning

- Il passo successivo è la **scansione delle porte**
- Fase cruciale
- Ogni errore fatto qui si ripercuote sulle fasi successive
- Lo strumento più utilizzato in questa fase è **NMAP**

$Footprinting e Scanning

- Conoscere che una porta è aperta è solo metà del lavoro
- Occorre necessariamente sapere quale servizio è in esecuzione su quella determinata porta
- Conoscendo i servizi si può
  - Dedurre il sistema operativo
  - Dedurre il ruolo e l'importanza dell'host per il cliente

$Vulnerability Assessment

- Lista di vulnerabilità
- Nella prossima fase, si utilizzeranno concretamente queste liste
- Più grande e dettagliata sarà la lista, più si avrà possibilità di exploitare il target
- Può essere fatto manualmente o con strumenti automatizzati
- I principali sono **Nessus - Nexpose - OpenVAS**

$Vulnerability Assessment

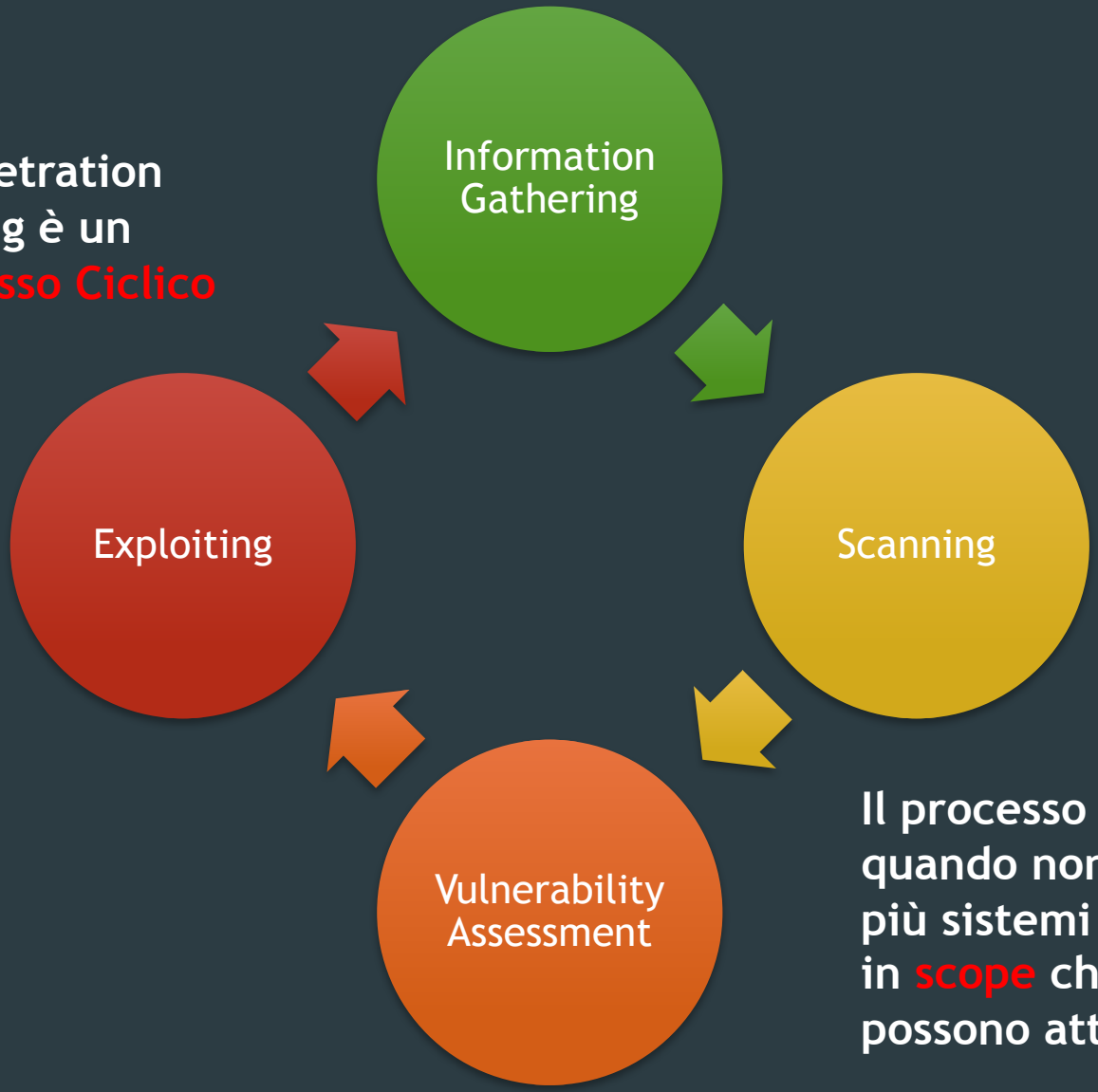
- Generazione di report al termine dello scan
- Fondamentale per la fase successiva
- Fare moltissima attenzione alla configurazione di questi scanner
- Se mal configurati potrebbero avere effetti indesiderati
- **Gli scanner (strumenti in generale) automatici aiutano il pentester, ma non sono in grado di fare un Penetration Testing da soli!!!**

$Exploitation

- Verifica dell'esistenza delle vulnerabilità scovate in precedenza
- Si testano **TUTTE** le vulnerabilità
- Si tentano 'priviledge escalation' sui sistemi
- Si cerca di espandere i propri orizzonti (pivoting)
- Si tenta di collezionare il maggior numero di informazioni

$Exploitation

Il Penetration Testing è un Processo Ciclico



Il processo termina quando non ci sono più sistemi e servizi in scope che si possono attaccare

$Reporting

- Fase importantissima
- Verrà letto da
  - Dirigenti
  - Sviluppatori
  - Personale IT
- È il vero prodotto del nostro lavoro
- Deve essere il più chiaro ed esaustivo possibile

$Reporting

- Deve contenere
  - Tecniche utilizzate
  - Vulnerabilità trovate
  - Exploit utilizzati
  - Analisi di rischio e di impatto per ogni singola vulnerabilità
  - Suggerimenti per risolvere il problema
- Cosa guarderà il cliente???
- Ovviamente i suggerimenti per risolvere i problemi!

$Reporting

- Oltre che un bravo attaccante, un pentester deve essere anche un ottimo comunicatore
- Molto spesso si chiedono ore aggiuntive di consulenza post-report
- Alla fine della consulenza, il report deve
  - Essere crittografato ed archiviato – se pattuito
  - Essere distrutto – se pattuito

$Conclusioni

- Seguire in maniera rigida le varie fasi!
- I migliori attaccanti spendono giorni/settimane/mesi solo sulla fase di Information Gathering
- Più è ampia la superficie d'attacco, più possibilità si ha di riuscire nell'intento

$Conclusioni #2

- L’importanza del

RED TEAM!

- L’importanza del

BLU TEAM!

DEMO

Grazie per l’attenzione