Password cracking e malware

In questo report si presenteranno i passaggi effettuati per il cracking di password in hash MD5, nella seconda parte si vedrà una simulazione di attacco DOS.

- Preparazione file da dare in pasto a John the Ripper:
  in questo file ogni riga conterrà *username:hash*, dove gli hash sono le password estrapolate con la SQLi dell'esercizio precedente.

```
admin:5f4dcc3b5aa765d61d8327deb882cf99
gordonb:e99a18c428cb38d5f260853678922e03
1337:8d3533d75ae2c3966d7e0d4fcc69216b
pablo:0d107d09f5bbe40cade3de5c71e9e9b7
smithy:5f4dcc3b5aa765d61d8327deb882cf99
```

- Una volta preparato il file *hash.txt* si andrà ad unzippare la *wordlist* già presente su kali, la *rockyou.txt,* la raccolta di password più comuni degli ultimi 10 anni.

```
┌──(root㉿kali)-[/home/kali]
└─# gunzip /usr/share/wordlists/rockyou.txt.gz
```

- Ora che la wordlist è unzippata si può dire a john di utilizzarla per crackare le password hashate:

```
┌──(root㉿kali)-[/home/kali]
└─# john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt /hom
e/kali/Desktop/hash.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX
2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (admin)
abc123           (gordonb)
letmein          (pablo)
charley          (1337)
4g 0:00:00:00 DONE (2026-01-07 14:10) 133.3g/s 102400p/s 102400c/s 153600C
/s my3kids..dangerous
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked pa
sswords reliably
Session completed.
```

Conclusione

Sono stato in grado di ottenere le password in chiaro tramite il cracking offline con l'utilizzo di John the Ripper, il processo ha impiegato solo pochi secondi ma in casi con password più complesse il processo potrebbe impiegarci ore, giorni o settimane.

DOS Attack

In questa seconda parte del report si mostreranno i passaggi per simulare un attacco DOS contro la vm Metasploitable, tramite l'utilizzo del software *Slowloris*. Di seguito riporto le descrizioni di DOS, DDOS e Slowloris:

- **DOS (Denial Of Service)** si verifica quando un **singolo attaccante** (una sola macchina/IP) inonda un server bersaglio di traffico (pacchetti TCP, UDP, richieste HTTP) o sfrutta una vulnerabilità software per esaurirne le risorse (CPU, RAM o banda).
- **DDOS (Distributed Denial of Service)** è l'evoluzione del DoS, l'attacco proviene da **molteplici fonti** distribuite (migliaia o milioni), solitamente compromesse (dispositivi IoT zombie) che formano una **Botnet**.
- **Slowloris** è un tipo specifico di DoS che opera al Livello 7 (Applicazione) del modello ISO/OSI, specificamente contro server web che gestiscono le connessioni tramite thread (come Apache). È un software intelligente perché Invia richieste HTTP parziali e le mantiene aperte il più a lungo possibile, inviando piccoli pacchetti di dati (header fake) ogni tanto per impedire al server di chiudere la connessione per timeout.

Dopo aver installato Slowloris sulla Kali Linux si potrà lanciare il comando per il DOS

```
┌──(root㉿kali)-[/home/kali/slowloris]
└─# python3 slowloris.py 192.168.51.101 -s 350
[07-01-2026 14:40:22] Attacking 192.168.51.101 with 350 sockets.
[07-01-2026 14:40:22] Creating sockets...
[07-01-2026 14:40:37] Sending keep-alive headers...
```

Di default Sowloris crea 150 sockets ma qui si ha specificato di crearne 350.
Per monitorare la connettività tcp alla porta 80 di Meta si andrà ad utilizzare il tool tcping

```
┌──(root㉿kali)-[/home/kali]
└─# tcping 192.168.51.101 80
/usr/bin/tcping: 1: bc: not found
seq 0: tcp response from 192.168.51.101 [open]  36.342 ms
seq 1: tcp response from 192.168.51.101 [open]  13.204 ms
```

Ci si può accorgere di come le response arrivino con un po' di delay, dato per lo stress che Slowloris sta causando alla macchina target.

Conclusione
Alzando il numero di Sockets si può stressare ulteriormente il target fino a saturarne le risorse, l'evidenza di ciò si potrebbe vedere utilizzando tcping dato che alcune response andrebbero in timeout.

Valutazione di Sicurezza e Piano di Intervento: Malware WannaCry

In questa terza parte si descriverà come isolare e mettere in sicurezza un ipotetico host Windows infetto dal malware WannaCry per evitare che infetti tutta una rete aziendale.

Analisi della Minaccia - Ransomware WannaCry

WannaCry è classificato come *Ransomware Worm*, possiede un meccanismo di auto propagazione che non richiede interazione umana per diffondersi, una volta infettato un host questo cifra i dati presenti sulla macchina infetta appendendo l'estensione ".wncry". Il vettore di attacco principale sfrutta l'exploit *EternalBlue* che colpisce una vulnerabilità critica nell'implementazione del protocollo *SMBv1* sui sistemi operativi Windows (pre-patch di Marzo 2017), per questo motivo può scansionare attivamente la rete locale e internet sulla porta TCP 445, cercando altri host vulnerabili a EternalBlue per replicarsi istantaneamente.

Fase 1: Contenimento Immediato

Sarebbe di immediata importanza bloccare il *Lateral Movement* del worm disabilitando l'accesso dell'host alla rete aziendale, scollegando eventuale cavo ethernet, disattivando le schede WiFi / disabilitando interfacce di rete o agendo direttamente sullo switch di accesso (il traffico viene bloccato dalla porta dello switch).

Fase 2: Blocco della porta TCP 445

Nello spiacevole caso in cui il worm si sia diffuso sarebbe importante ridurne la propagazione, data la sua propagazione tramite protocollo SMB sulla porta 445 sarebbe opportuno bloccare questa porta sui firewall perimetrali e sui client tramite group policy. Nel caso di propagazione individuata si potrebbe segmentare la rete in modo da isolare la VLAN infetta.

Fase 3: Remediation sull'host Windows

Tornando sullo scenario in cui l'host infetto è 1 si dovrebbe scegliere tra possibili remediation:
Formattazione e Ripristino → Si cancella interamente il disco rigido, si reinstalla il sistema operativo da un'immagine sicura e si ripristinano i dati dall'ultimo backup pulito.

PRO	**Eliminazione garantita** del malware e di eventuali Backdoor	**Tempistica certa**
CONTRO	**Data Loss:** I dati creati tra l'ultimo backup e l'infezione sono persi	**Downtime:** Il sistema è inutilizzabile finché il restore non è completo

Rimozione e Tentativo di Decrittazione → Si tenta di rimuovere il malware usando antivirus/antimalware e si cerca di decriptare i file usando tool specifici.

PRO	**Dati preservati**	**Analisi:** Permette di studiare il malware
CONTRO	**Rischio Residuo:** Difficile garantire che il sistema sia pulito al 100%	**Inefficacia:** Per WannaCry, la decrittazione è matematicamente impossibile senza chiave

Negoziazione → Si paga l'attaccante sperando di ricevere la chiave privata per decriptare i dati (sconsigliato).

Personalmente l'opzione di formattazione e ripristino parrebbe la più indicata.

Fase 4: Hardening Post-Incidente

La messa in sicurezza non è finita col ripristino. L'host windows sarebbe pulito ma potenzialmente vulnerabile (se l'immagine ISO è antecedente a Marzo 2017).
Prima di rimettere in comunicazione l'host con la rete sarebbe imperativo installare l'aggiornamento di sicurezza **MS17-010.**
Per ridurre la superficie d'attacco si consiglierebbe di disabilitare definitivamente il protocollo obsoleto SMBv1, vettore dell'exploit EternalBlue.