

# Cyber Security & Ethical Hacking

## Attacchi alle reti

## Agenda

- DOS-DDOS
- Buffer overflow
- NetBios/Share di Windows e le NULL Session

## Understanding DOS - DDOS ATTACKS

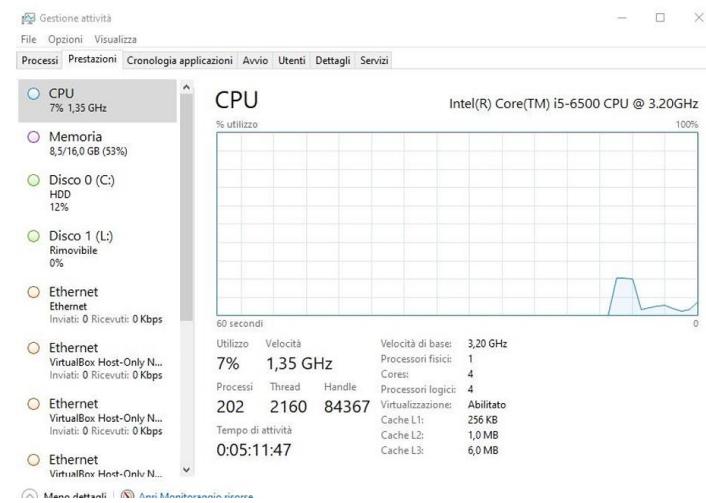
Oggi è comune aprire un giornale o guardare un telegiornale e trovarsi di fronte a notizie riguardanti attacchi DOS-DDOS.



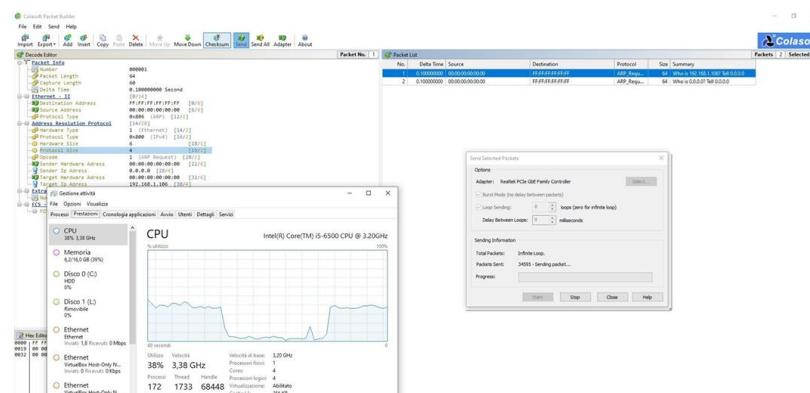
Ma cosa sono questi DOS e DDOS?

- DoS (Denial of Service) si riferisce a un tipo di attacco informatico in cui un aggressore mira a interrompere l'accesso legittimo a un servizio, rendendolo non disponibile agli utenti autorizzati. Questo può essere fatto inviando una grande quantità di traffico al server di destinazione, sovraccaricandolo e impedendogli di gestire ulteriori richieste.
- DDoS (Distributed Denial of Service) è una variante avanzata degli attacchi DoS in cui gli aggressori utilizzano più sistemi compromessi, noti come botnet, per inviare simultaneamente traffico dannoso al servizio di destinazione da diverse posizioni geografiche. Questo rende l'attacco più difficile da contrastare, poiché proviene da diverse fonti simultaneamente.

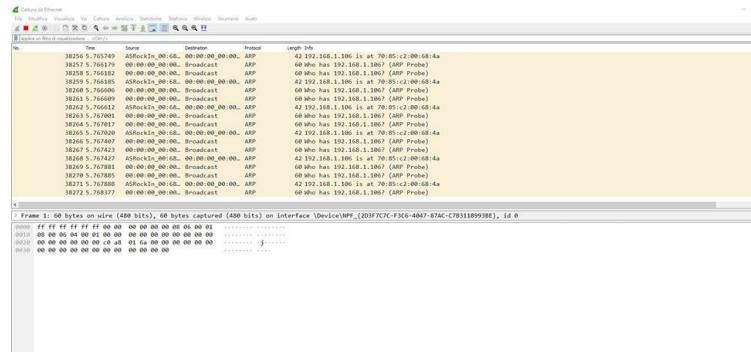
In breve un attacco dos-ddos mira a saturare la cpu di un dispositivo, creando latenza e nei peggiori dei casi il down del sistema.



Abbiamo simulato un attacco DOS usando COLASOFT.  
Notate come il grafico della cpu si è alzato.

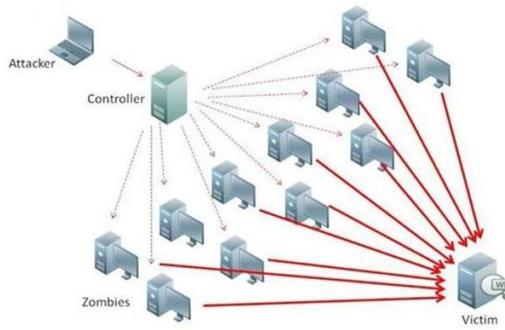


Abbiamo attivato  
WIRESHARK e abbiamo  
intercettato l'attacco,  
questo è una simulazione di  
quello che accadde in un  
vero attacco dos.



## ATTACCO DDOS.

Nella attacco DDOS abbiamo un elemento nuovo e importante che lo va a differenziare dal DOS. Lo scopo dell'attacco ddos è sempre quello di mandare in down o creare un'enorme latenza su un dispositivo ma in questo caso andiamo ad usare una botnet.

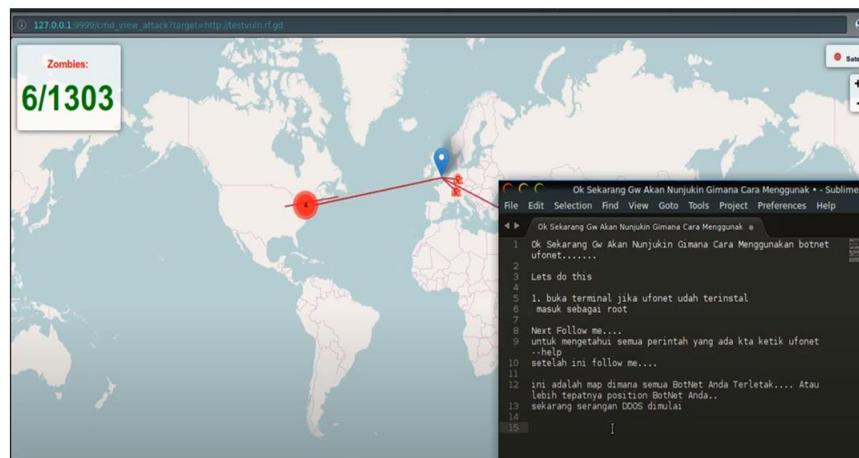


Cos'è una botnet:

- Una botnet è una rete di dispositivi infettati da malware e controllati da un'entità remota, spesso senza il consenso dei proprietari dei dispositivi. Questi dispositivi possono includere computer, server, dispositivi IoT e persino smartphone. Gli attaccanti utilizzano botnet per eseguire attacchi distribuiti, come attacchi DDoS (Distributed Denial of Service), spamming di email, furto di informazioni personali e finanziarie, e per l'attuazione di altri tipi di attività malevole.  
I dispositivi infetti all'interno di una botnet, noti come "bot" o "zombie", sono spesso manipolati per eseguire attività dannose senza che i proprietari ne siano consapevoli. Questi dispositivi possono essere reclutati nella botnet attraverso l'installazione di malware, come virus, worm o trojan, che consente a un attaccante di assumere il controllo remoto. Le botnet possono essere usate per scopi illeciti, tra cui l'estorsione, il furto di informazioni, la spionaggio e l'attacco di altri sistemi informatici.

Ecco un esempio di un attacco DDoS: abbiamo impiegato UFONet per simulare l'attacco.

UFONet è un'applicazione gratuita che ci permette di comprendere e simulare un attacco DDoS.



## I buffer overflow & lo stack

La vulnerabilità buffer overflow vengono sfruttate da vari attacchi che ottengono il controllo sul flusso di esecuzione di un programma o una routine del sistema operativo. Controllare l'esecuzione di un programma significa essere in grado di fargli fare qualcosa di differente rispetto alla logica stabilita dal programmatore.

Un attacco che sfrutta un buffer overflow può:

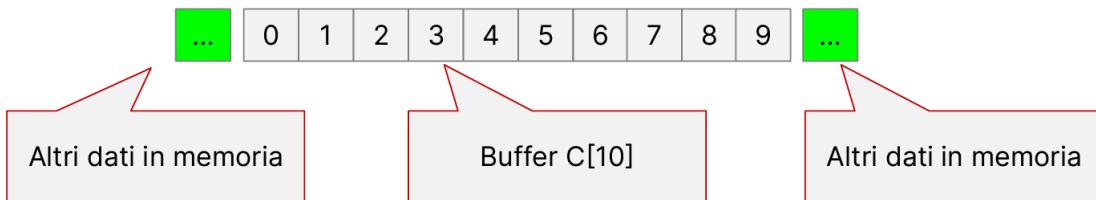
- **Causare il crash di un programma** o dell'intero sistema operativo.
- **Scatenare un secondo attacco di tipo privilege escalation.**
- Ottenere la possibilità di **eseguire codice malevolo direttamente sulla macchina vittima.**
- **Aggirare le funzionalità di sicurezza** di un sistema operativo.

Per capire cos'è una vulnerabilità di tipo buffer overflow, ricordiamo cos'è un buffer.

Un buffer è un'area di memoria che risiede in RAM riservata per contenere dei dati temporanei come:

- Un **input utente**.
- Una parte di un **file video**.
- Il **banner dei server** ricevuti da una web app.
- Altro.

I buffer hanno una dimensione finita, ossia possono contenere un certo quantitativo di dati. Per farvi un esempio pratico, vi ricordate la dichiarazione di un vettore in C ? Ai vettori viene associata una grandezza tra parentesi quadre che indica la dimensione del vettore. Ad esempio: INT C[10], definisce un vettore di 10 interi.



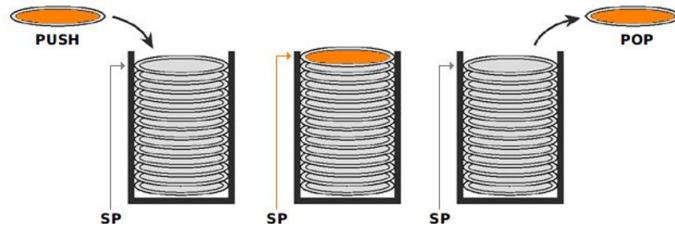
Se lo sviluppatore di un'applicazione non impone strettamente dei limiti ai buffer, un attaccante potrebbe trovare un modo per scrivere dei dati oltre questi limiti, scrivendo codice arbitrario nella memoria del computer. **Con un codice arbitrario particolare un attaccante potrebbe arrivare a controllare il flusso di esecuzione del programma.**

Come vedremo a breve, una vulnerabilità buffer overflow sfrutta proprio la mancanza di controllo dell'input in una determinata porzione di memoria. Di conseguenza, un potenziale attaccante potrebbe inserire 100 interi all'interno di un buffer di dimensione 10, di fatto andando a sovrascrivere i dati contigui al buffer in memoria.

Durante l'esecuzione di un programma i dati e le variabili, così come i buffer, vengono salvati **in una struttura chiamata stack**.

Lo stack può essere immaginato come una pila di piatti, dove si può solo aggiungere e rimuovere un piatto alla volta dalla cima.

L'azione per **aggiungere** un piatto sulla cima della pila, viene chiamata «**PUSH**» mentre l'azione che **rimuove** un piatto dalla cima viene detta «**POP**». Questo approccio prende il nome di LIFO (last in first out), ovvero l'ultimo piatto inserito sulla cima è il primo ad essere rimosso.



Facciamo un esempio pratico, immaginiamo di avere i due vettori A e B definiti come segue:

```
int A [2] = {21,35}
int B [3] = {11,22,33}
```

B[0]	11
B[1]	22
B[2]	33
A[0]	21
A[1]	35

E supponiamo che venga chiesto all'utente di inserire 3 numeri nel vettore B. L'utente ne inserisce per sbaglio 4: 1,2,3,4

```
int A [2] = {4,35}
int B [3] = {1,2,3}
```

B[0]	441
B[1]	222
B[2]	333
A[0]	214
A[1]	35

L'elemento 0,1,2 del vettore B viene correttamente sovrascritto con il nuovo valore.

Venne sovrascritto per errore anche l'elemento 0 del vettore A, in quanto l'utente ha erroneamente inserito più valori di quanti ammessi.

**Un utente lecito che vorrà leggere il valore A, troverà un valore diverso da quello reale, in quanto A[0] è stato modificato a causa dell'overflow di B.**

# NetBios/Share di Windows e le NULL Session

Microsoft Windows è uno dei sistemi operativi più utilizzati in ambito enterprise. Si impiega soprattutto su client e server per fornire autenticazione, condivisione file, gestione stampanti e tante altre funzionalità del mondo IT di una compagnia.

Nelle diapositive che seguono, vedremo come funziona il file sharing di Windows e come si possono sfruttare alcune delle funzionalità fornite se non configurate correttamente.

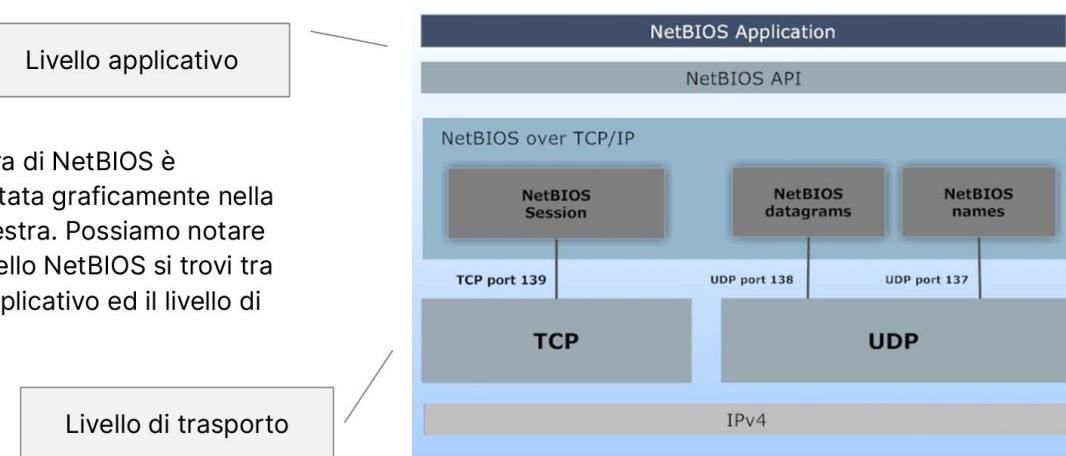
Per capire come funzionano gli attacchi alla condivisione file in rete, dobbiamo prima capire come funzionano le share di rete.

NetBIOS, network basic input / output system, ovvero sistema base di input ed output di rete è un protocollo di livello di sessione (con riferimento al sistema ISO/OSI), utilizzato da client e server quando sfogliano gli share su una rete locale, come potrebbe essere una cartella che è stata condivisa da un determinato utente.

NetBIOS è in grado di fornire determinati servizi, quali:

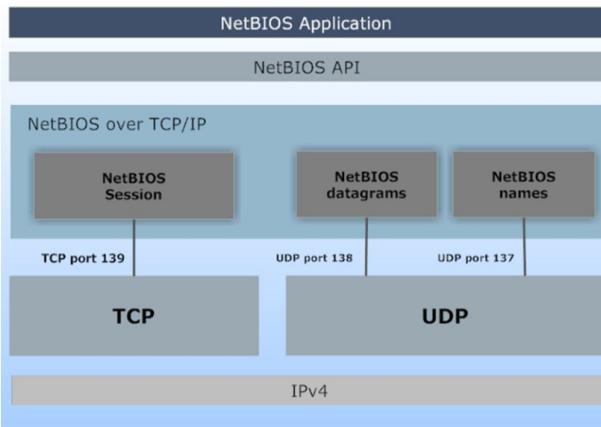
- **Name service:** NetBIOS offre la registrazione e la risoluzione dei nomi NetBIOS.
- **Session service:** garantisce l'affidabilità della comunicazione orientata alla connessione.
- **Datagram service:** offre anche la comunicazione non fidata (senza connessione).

La struttura di NetBIOS è rappresentata graficamente nella figura a destra. Possiamo notare come il livello NetBIOS si trovi tra il livello applicativo ed il livello di trasporto.



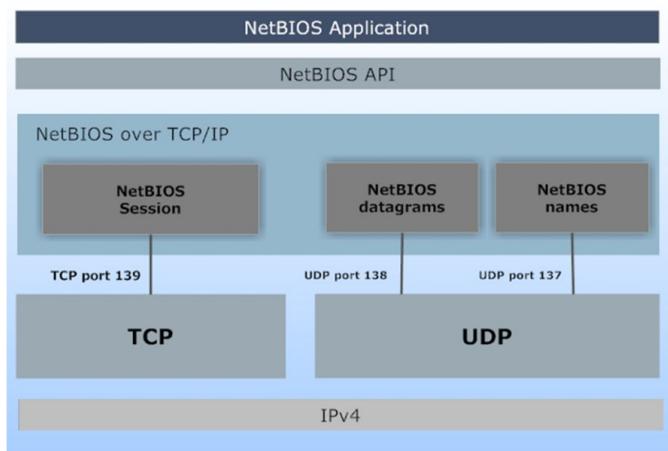
Come potete notare dalla figura, NetBIOS utilizza:

- **UDP** per la risoluzione dei nomi NetBIOS e per gestire la comunicazione uno a molti connectionless (senza connessione).
- Utilizzando i datagrammi NetBIOS, un host può spedire messaggi di dimensioni ridotta a molti altri computer.



Come potete notare dalla figura, NetBIOS utilizza:

- **TCP**: per la gestione del traffico che ha necessità di girare su un canale cifrato, come ad esempio la copia di un file, o qualsiasi altra trasmissione di dati da e per una share di Windows.



Nella pratica, quando una macchina Microsoft Windows sfoglia una rete, utilizza le diverse componenti di NetBIOS:

- **Datagrammi**: per ottenere una lista delle share e delle macchine attive sulla rete.
- **Nomi**: per identificare i gruppi di lavoro (workgroup).
- **Sessioni**: per trasmettere dati da e per una share Windows.

Una macchina Windows può condividere un file o una directory sulla rete, in modo tale che altri utenti sia locali che remoti possano accedere alla risorsa e modificarla se autorizzati.

Condividere risorse e file ha molti vantaggi, quali:

- Riduce la ridondanza.
- Migliora l'efficienza delle reti aziendali.
- Velocizzano la cooperazione su file e deliverable progettuali.
- Permettono di distribuire l'utilizzo di oggetti remoti (ad esempio stampanti, fax).
- E molte altre features.

Condividere in rete, o creare una share di rete in ambiente Windows è piuttosto semplice. Solitamente l'utente deve abilitare il servizio «condivisione file e stampanti» e decidere quali file o directory condividere.

**L'utente che condivide una risorsa può impostare dei permessi su una share di rete, decidendo chi può eseguire quali operazioni tra lettura, scrittura e modifica dei permessi.**

Un utente autorizzato ad una determinata risorsa può accedervi utilizzando i percorsi **Universal Naming Convention Paths (UNC)**.

Il formato di un percorso UNC è come segue:

```
\NomeServer\NomeShare\file.txt
```

Esistono share dedicate che vengono utilizzate dagli amministratori di sistema e da Windows stesso, come:

- [\\NomeComputer\C\\$](\\NomeComputer\C$), che fornisce ad un amministratore accesso ad un volume sulla macchina locale.
- [\\NomeComputer\admin\\$](\\NomeComputer\admin$), che punta alla directory di installazione di Windows.
- [\\NomeComputer\ipc\\$](\\NomeComputer\ipc$), che si usa per le comunicazioni tra i processi.

Potete provare ad accedere alle share admin del vostro pc scrivendo:

```
\localhost\admin$
```

Sulla barra degli indirizzi del vostro browser preferito oppure nell'explorer di Windows.

Accedere ad una share significa avere accesso alle risorse del computer che sta condividendo le informazioni. Viene da sé che se una share non è propriamente configurato, può aprire la strada ad un malintenzionato che potrebbe così ottenere:

- Informazioni riservate.
- Accesso non autorizzato a file contenenti informazioni riservate.
- Accesso ad informazioni che potrebbero essere utilizzate per costruire un attacco personalizzato.



---

Una delle vulnerabilità storiche delle share di Windows sono le **NULL session**.

**N.B. Solo per conoscenza storica.**

Gli attacchi «**null session**» si possono utilizzare per recuperare dalla macchina target molte informazioni. Un attaccante infatti può riuscire a recuperare informazioni quali:

- **Password**.
- **Utenti di un sistema**.
- **Gruppi** di un sistema.
- **Processi** in esecuzione.
- **Programmi** aperti.
- E molto altro.

Le «null session» si possono sfruttare da remoto, questo significa che un attaccante può utilizzare il proprio PC per attaccare una macchina Windows vulnerabile.

Inoltre si può utilizzare questo tipo di attacco per eseguire azioni sulla macchina vittima tramite API o RPC.

Negli anni scorsi, la maggior parte dei sistemi Windows era vulnerabile alle «null session» e gli attacchi di questo tipo hanno avuto un impatto enorme su tutto l'ecosistema Windows.

**Ad oggi, sono ancora veramente pochi i sistemi vulnerabili, perlomeno sono sistemi legacy.**

Di per sé gli attacchi null session si basano su una vulnerabilità dell'autenticazione delle share amministrative di Windows, che permettevano ad un attaccante di collegarsi ad una share locale o remote **senza autenticazione**.

Vediamo nei prossimi esempi come enumerare le share.

**Nbtstat:** è un tool da riga di comando per Windows per enumerare le share dato un determinato obiettivo. Con il comando **nbtstat /?**, possiamo vedere come si utilizza il tool. Riportiamo l'output nella figura qui a destra. L'utilizzo più comune è con lo switch **-A** seguito dall'IP che visualizza le informazioni su un determinato target. Ad esempio:

```
:/|>
>nbtstat -A 10.130.40.80

Local Area Connection:
Node Padres: [10.0.2.15] Scope Id: []

NetBIOS Remote Machine Name Table

Name          Type        Status
-----        -----
ELS-WINXP    <00>      UNIQUE      Registered
WORKGROUP    <00>      GROUP       Registered
ELS-WINXP    <20>      UNIQUE      Registered
WORKGROUP    <1E>      GROUP       Registered

MAC Address = 00-0C-29-BF-98-BD
```

Visualizza le statistiche di protocollo e le connessioni TCP/IP correnti mediante NBT (NetBIOS su TCP/IP).  
NBTSTAT [ [-a NomeRemoto] [-A Indirizzo IP] [-c] [-n]  
[-r] [-R] [-s] [-S] [Intervallo] ]  
  
-a (stato scheda) In base al nome specificato il nome, elenca la tabella dei nomi del computer remoto.  
-A (Stato scheda) In base all'indirizzo IP specificato elenca la tabella dei nomi del computer remoto.  
-c (cache) Elenca la memoria cache di NBT dei nomi remoti [computer] e dei relativi indirizzi IP.  
-n (npms) Elenca i nomi NetBIOS locali.  
-o (risolti) Elenca la tabella delle risoluzioni broadcast e WINS.  
-R (Ricaricamento) Ripulisce la tabella del nome cache remota e la ricalca.  
-S (Sessioni) Elenca la tabella delle sessioni con gli indirizzi IP di destinazione.  
-s (sessioni) Elenca la tabella delle sessioni che converte gli indirizzi IP di destinazione in nomi computer NETBIOS.  
-RR (Agg.Rilascio) Invia pacchetti di rilascio nome a WINS, quindi avvia l'aggiornamento.  
  
Nome Remoto Nome del computer host remoto.  
Indirizzo IP Indirizzo IP del computer host remoto all'indirizzo IP.  
Intervallo Rivede le statistiche selezionate, interrompendo per un numero di secondi pari all'intervallo tra ogni visualizzazione. Premere Ctrl+C per interrompere la visualizzazione delle statistiche.

Vediamo da vicino l'output del comando.

La prima riga della tabella di suggerisce che il nome del PC con indirizzo 10.130.40.80 è «ELS-WINXP»

Il record type **<00>** indica che il PC è una workstation, mentre il tipo «**UNIQUE**» ci dice che questo computer ha solo un indirizzo IP assegnato.

```
:/|>
>nbtstat -A 10.130.40.80

Local Area Connection:
Node Padres: [10.0.2.15] Scope Id: []

NetBIOS Remote Machine Name Table

Name          Type        Status
-----        -----
ELS-WINXP    <00>      UNIQUE      Registered
WORKGROUP    <00>      GROUP       Registered
ELS-WINXP    <20>      UNIQUE      Registered
WORKGROUP    <1E>      GROUP       Registered

MAC Address = 00-0C-29-BF-98-BD
```

La seconda linea, inclusa nel rettangolo in rosso in figura contiene il gruppo di lavoro oppure il dominio al quale appartiene il computer.

La terza riga, evidenziata dal rettangolo in blu, è una riga particolarmente interessante.

Il record di tipo <20> ci informa che il servizio di condivisione su quella data macchina è attivo, e che quindi possiamo provare a recuperare qualche informazione utile sul computer.

```
:> >nbtstat -A 10.130.40.80

Local Area Connection:
Node Padres: [10.0.2.15] Scope Id: []

NetBIOS Remote Machine Name Table

Name          Type      Status
-----
ELS-WINXP    <00>    UNIQUE   Registered
WORKGROUP    <00>    GROUP    Registered
ELS-WINXP    <20>    UNIQUE   Registered
WORKGROUP    <1E>    GROUP    Registered

MAC Address = 00-0C-29-BF-98-BD
```

Quando un attaccante sa che una macchina ha il servizio di file Server attivo, può enumerare gli share utilizzando il comando NET VIEW. La figura sotto riporta il comando net view verso il target 10.130.40.80

Queste due righe rappresentano due directory condivise dalla macchina in esame.

```
:> >NET VIEW 10.130.40.80
Shared resources at 10.130.40.80

Share name      Type      Used as   Comment
-----
eLS             Disk
WIA_RIS_SHARE  Disk
The command completed successfully.
```

I tool che abbiamo visto finora sono tool per Windows. E' possibile fare enumerazione delle share anche da un computer con Linux, utilizzando i tool forniti dalla suite Samba.

Gli strumenti della suite Samba sono preinstallati su Kali Linux, ma sono anche disponibili praticamente per tutte le altre distribuzioni Linux.

Per lanciare le stesse operazioni che abbiamo visto con nbtstat, si può utilizzare **nmblookup**. Al netto del comando stesso, la sintassi è molto simile a quella già vista per nbtstat.

```
:> # nmblookup -A <target ip address>
```

Come di consueto per studiare lo strumento e capirne il funzionamento, potete utilizzare il manuale di nmblookup, oppure l'help rapido con lo switch --help, come in figura a destra.

Nell'immagine in basso abbiamo riportato l'output del comando nmblookup sul target 10.130.40.80 analizzato in precedenza. Notata come i risultato sono gli stessi:

```
$ nmblookup -A 10.130.40.80
Looking up status of 10.130.40.80
    ELS-WINXP      <00> -          M <ACTIVE>
    WORKGROUP     <00> - <GROUP> M <ACTIVE>
    ELS-WINXP      <20> -          M <ACTIVE>
    WORKGROUP     <1e> - <GROUP> M <ACTIVE>

MAC Address = 00-0C-29-BF-98-BD
```

The screenshot shows the man page for nmblookup(1). It includes sections for NAME, SYNOPSIS, DESCRIPTION, and OPTIONS. The SYNOPSIS section shows the command usage: nmblookup [-M|-master-browser] [-R|-recursion] [-S|-status] [-r|-root-port] [-A|-lookup-by-ip] [-b|-broadcast <broadcast address>] [-U|-unicast <unicast address>] [-d|-debug level>] [-s|-smb config file] [-l|-NetBIOS scope] [-t|-translate] [-f|-flags] [name]. The DESCRIPTION section states that this tool is part of the samba(7) suite. The OPTIONS section details various flags: -M/-master-browser, -R/-recursion, -S/-status, -r/-root-port, -A/-lookup-by-ip, -n/-netbiosname <primary NetBIOS name>, -i/-scope <scope>, and -W/-workgroup<domain>. It also mentions the -l parameter for specifying a NetBIOS scope.

La suite Samba fornisce un ulteriore tool **smbclient**.

**Smbclient** è un client tipo ftp per accedere alle share di Windows. Questo tool è in grado, tra le altre cose, di fare enumerazione delle share di un host con riferimento alla figura in basso a destra:

- **-L**, permette di visualizzare quali servizi sono disponibili sul target.
- **//**, l'indirizzo IP deve essere preceduto da due slash.
- **-N**, fa in modo che il tool non chieda una password.

```
$ smbclient -L //10.130.40.80 -N
Domain=[ELS-WINXP] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]

Sharename      Type      Comment
-----        ----      -----
eLS            Disk
IPC$          IPC       Remote IPC
WIA_RIS_SHARE Disk
ADMIN$         Disk       Remote Admin
C$             Disk       Default share
```

Come potete vedere dalla figura qui a destra, smbclient non solo riporta tutte le share identificate dai tool che abbiamo visto in precedenza.

Ma **mostra anche le share amministrative** che vengono nascoste dagli strumenti standard di Windows per ragioni di sicurezza.

```
$ smbclient -L //10.130.40.80 -N
Domain=[ELS-WINXP] OS=[Windows 5.1] Server=[Windows 2000 LAN Manager]

Sharename      Type      Comment
-----        ----      -----
eLS            Disk
IPC$          IPC       Remote IPC
WIA_RIS_SHARE Disk
ADMIN$         Disk       Remote Admin
C$             Disk       Default share
```

Dopo aver stabilito che il servizio condivisione file è attivo ed aver enumerato gli share disponibili su un dato target, è il momento di capire se l'attacco basato sulle **null session** sia possibile.

Per verificarlo, possiamo provare a sfruttare la share amministrativa **IPC\$**, cercando di avviare una connessione senza credenziali valide.

La prima cosa che dobbiamo fare è collegarci alla share **IPC\$**, utilizzando un nome utente ed una password vuoti. Possiamo farlo in diversi modi:

- Con il comando **NET USE**.

```
> NET USE \\<target IP address>\IPC$ '' /u:''
```

- Con il comando **smbclient**.

```
# smbclient //10.130.40.80/IPC$ -N
```

Un altro tool per Linux per sfruttare vulnerabilità del tipo «null session» è **Enum4Linux**. Come di consueto possiamo consultare l'help del comando per capire il suo utilizzo. Tra gli switch più significativi troviamo sicuramente:

- **«-S»** che permette di enumerare le share di una macchina, compresi le share amministrative.
- **«-U»** che permette di estrarre i nomi utente.
- **«-P»** che permette di controllare le password policy. Può essere poi utilizzato per configurare un attacco all'autenticazione su rete.

```
(kali㉿kali)-[~]
└─$ enum4linux
enum4linux v0.9.1 (http://labs.portcullis.co.uk/application/enum4linux/)
Copyright (C) 2011 Mark Lowe (mrl@portcullis-security.com)

Simple wrapper around the tools in the samba package to provide similar
functionality to enum.exe (formerly from www.bindview.com). Some additional
features such as RID cycling have also been added for convenience.

Usage: ./enum4linux [options] ip

Options are like "enum":
  -U      get userlist
  -M      get machine list*
  -S      get sharelist
  -P      get printer policy information
  -G      get group and member list
  -d      be detailed, applies to -U and -S
  -u user  specify username to use (default '')
  -p pass  specify password to use (default '')

The following options from enum.exe aren't implemented: -L, -N, -D, -F

Additional options:
  -a      Do all simple enumeration (-U -S -G -P -r --n -i).
          This option is enabled when you don't provide any other options.
  -h      Displays this message and exits
  -r      enumerate users via RID cycling
  -R range RID ranges to enumerate (default: 500-550,1000-1050, implies -r)
  -K n    Keep searching RIDs until n consecutive RIDs don't correspond to
          a username. Implies RID range ends at 999999. Useful
          against DCs
  -l      Get some (limited) info via LDAP 389/TCP (for DCs only)
  -s file  brute force guessing for share names
  -K user User(s) that exists on remote system (default: administrator,guest,krbtgt,d
          )
  -x      Used to get sid with "lookupsid known_username"
          Use commas to try several users: "-k admin,user1,user2"
  -o      Get OS information
  -i      Get printer information
  -w wrkg Specify workgroup manually (usually found automatically)
  -n      Do not mangle output to stdout
  -v      Verbose. Shows full commands being run (net, rpcclient, etc.)
  -A      Aggressive. Do write checks on shares etc

RID cycling should extract a list of users from Windows (or Samba) hosts
which have RestrictAnonymous set to 1 (Windows NT and 2000), or "Network
access: Allow anonymous SID/Name translation" enabled (XP, 2003).

NB: Samba servers often seem to have RIDs in the range 3000-3050.

Detailed help: http://www.labs.portcullis.co.uk/application/enum4linux/
```

**GRAZIE**  
Episode