- Cross Zone Scripting: Un aggressore è in grado di indurre una vittima designata a caricare contenuti nel proprio browser web che bypassa i controlli delle zone di sicurezza ottenendo così l'accesso per l'esecuzione con maggiori privilegi del codice di scripting o di altri oggetti web come i controlli ActiveX non firmati o gli applet. Si tratta di un attacco di elevazione dei privilegi mirato alla sicurezza dei browser web la cui sicurezza è basata su zone. In un modello basato su zone, le pagine appartengono a una delle zone corrispondenti al livello di privilegio assegnato a quella pagina. Le pagine in una zona non attendibile avrebbero un livello inferiore di accesso al sistema e/o sarebbero limitate nelle tipologie di contenuto eseguibile che queste sono autorizzate ad invocare. In un attacco di questo tipo, ad una pagina che dovrebbe essere assegnata ad una zona meno privilegiata vengono concessi i privilegi di una zona ritenuta maggiormente affidabile. Questo lo si può fare, sfruttando i bug presenti nel browser web o una configurazione errata nei controlli di zona, attraverso un attacco di cross-site scripting che fa sì che il contenuto dell'aggressore venga trattato come proveniente da una pagina attendibile. Questo attacco si differenzia dal "Restful Privilege Escalation" in quanto quest'ultimo minaccia lato server, l'inadeguata sicurezza dei metodi di accesso RESTful (come HTTP DELETE), mentre il "cross zone scripting" minaccia lato client, il concetto di "zone di sicurezza" implementato dal browser.
- Dirottamento di un processo privilegiato: Un aggressore ottiene il controllo di un processo a cui sono assegnati privilegi elevati per eseguire del codice arbitrario. Solitamente sul sistema operativo, ad alcuni processi vengono assegnati privilegi elevati tramite l'associazione ad un particolare utente, gruppo o ruolo. Se un aggressore è in grado di dirottare il processo, questo a sua volta sarà in grado di assumerne il livello di privilegi per eseguire il codice a sua scelta. I processi possono essere dirottati attraverso una gestione impropria dell'input da parte dell'utente (ad esempio, un buffer overflow o alcuni tipi di attacchi di iniezione) o utilizzando utility di sistema non adeguatamente protette che supportano il controllo del processo.

5.5.4.2 Attack tree

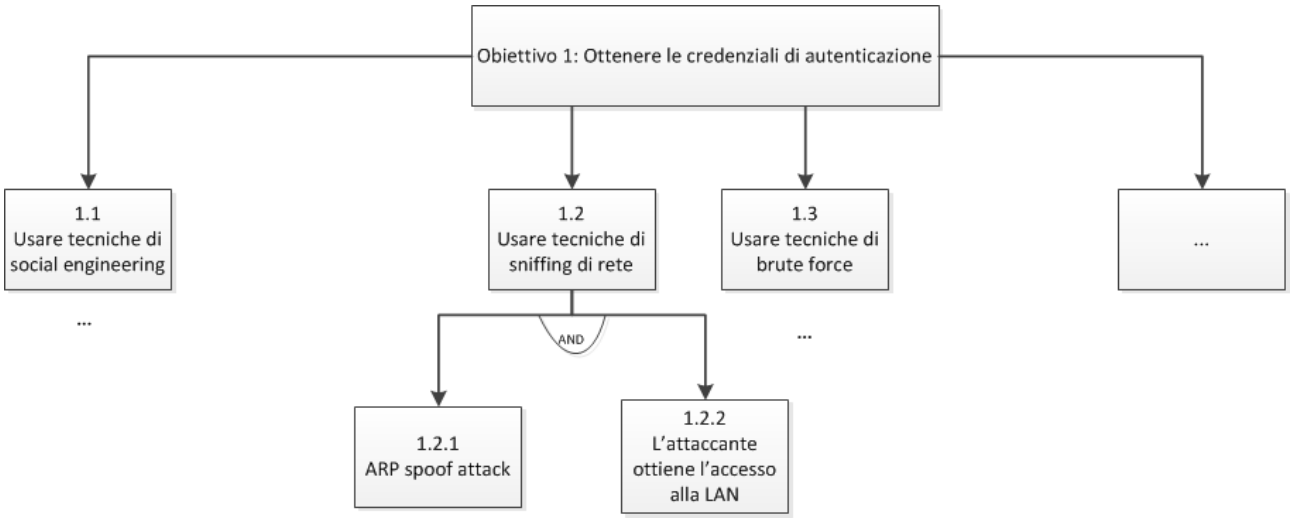
L'attack tree rappresenta un'ulteriore metodologia per raccogliere e documentare i potenziali attacchi in modo strutturato e gerarchico.
Un attack tree è modellato attraverso una struttura ad albero i cui elementi base sono:

- Il nodo radice che rappresenta *l'obiettivo finale* dell'attaccante,
- I nodi figli che rappresentano i *sotto-goals* che concorrono al raggiungimento dell'*obiettivo finale*,
- Le foglie che rappresentano gli *attacchi*.

La modellazione segue la seguente logica di base:

- I "nodi OR" indicano le alternative, ossia modi indipendenti, per raggiungere un goal/sotto-goal.
- I "nodi AND" indicano i passi che concorrono al raggiungimento dello stesso goal/sotto-goal.

PASSO 1 – Modellazione degli attacchi
Si modellano quindi, tanti attack tree quanti sono gli obiettivi di un attaccante. In questa fase l'analista deve identificare i possibili obiettivi di attacco e, per ciascuno di essi, i passi attraverso cui realizzarli (la capacità di identificazione degli obiettivi e dei passi è quindi assolutamente soggettiva).
Si riporta di seguito, un esempio di modellazione di attack tree:



Nell'esempio in figura:

- Il nodo radice rappresenta l'obiettivo finale dell'attaccante che consiste nell' "Ottenere le credenziali di autenticazione",
- L'obiettivo finale può essere raggiunto in vari modi ("OR"):

  1.1 - "Usare tecniche di social engineering",
  1.2 - "Usare tecniche di sniffing di rete",
  1.3 - "Usare tecniche di brute force", ecc.
- Sulla base della modalità di Livello-1 scelta, saranno diversi gli elementi (nodi foglie) che concorreranno al raggiungimento dell'obiettivo radice. Ad esempio, nel caso si scelga il percorso 1.2 - "Usare tecniche di sniffing di rete" l'obiettivo si raggiunge (sub-goal) attraverso 2 step correlati ("AND"):

  1.2.1 - "ARP spoof attack";
  1.2.2 - "L'attaccante ottiene l'accesso alla LAN".

Lo stesso attack tree può anche essere rappresentato in forma testuale:

Obiettivo 1 - Ottenere le credenziali di autenticazione
1.1 - Usare tecniche di social engineering OR
...
1.2 - Usare tecniche di sniffing di rete OR
1.2.1 - ARP spoof attack AND
1.2.2 - L'attaccante ottiene l'accesso alla LAN
1.3 - Usare tecniche di brute force OR
...
...

PASSO 2 – Analisi degli attributi di sicurezza

Dopo aver modellato i possibili attacchi al sistema, è necessario analizzare gli attributi di sicurezza del sistema quali, ad esempio:

1. la possibilità o l'impossibilità dell'attacco (P=Possibile, I=Impossibile)
2. il costo dell'attacco (valore in euro, es. 10K)
3. gli strumenti necessari per realizzare l'attacco (AS=Attrezzature Specifiche, SAS=Senza Attrezzature Specifiche)

Per determinare il costo di un attacco:

1. si determina il valore per ciascun nodo foglia.