La seguente tabella riporta le vulnerabilità della Top 10 OWASP 2017[30] riconducibili alle minacce di elevation of privilege, e per ciascuna vulnerabilità indicata, le relative pratiche[31] e requisiti[32] di sicurezza consigliati da OWASP:

OWASP TOP-10 2017 (Rischi di sicurezza delle applicazioni)	**OWASP Proactive Controls 2018 v 3.0** (Pratiche di sicurezza proattive)	**OWASP ASVS 3.0** (Requisiti di sicurezza applicative)
A5 - Broken Access Control	C7 - Enforce Access Controls	V4 - Access Control
A6 - Security Misconfiguration	C7 - Enforce Access Controls	V19 - Configuration
A9 - Using Components with Known Vulnerabilities	C7 - Enforce Access Controls	V13 - Malicious Controls

Tabella 20 - Rischi di sicurezza OWASP relativi all'Elevation Of Privilege

Alcuni esempi di minacce di elevation of privilege:

- Tasti permanenti in Windows: Questo attacco è abbastanza facile da eseguire e non richiede alcun tipo di conoscenza avanzata per poterlo portare. Per eseguire questo attacco è necessario un accesso fisico alla macchina e la possibilità di poterla avviare da un disco di ripristino. Una volta eseguito l'avvio, sarà necessario modificare il file di sistema associato alla funzione del tasto permanente (Sticky Key) (toccando cinque volte il tasto shift). Da prompt dei comandi, si fa una copia del file "sethc.exe" che si trova nella directory "%systemroot%\system32". Dopodiché, tutto ciò che bisogna fare è copiare il file "cmd.exe" nella cartella "%systemroot%\system32" rinominando il file come "sethc.exe". Dopo che l'eseguibile del file "cmd" è stato copiato nella corretta posizione, la macchina viene riavviata. Quando si presenta la schermata di accesso, toccando il tasto shift per cinque volte consecutive i "tasti permanenti" vengono attivati rendendo disponibile una command shell con accesso a livello di sistema. Da questo livello di accesso, un attaccante può creare una backdoor nel sistema e creare un account di amministratore locale.
- Suite Sysinternals su Windows: Un altro modo comune di eseguire escalation dei privilegi in Windows è attraverso l'uso della suite di strumenti Sysinternals. Dopo che un aggressore ottiene una backdoor nel sistema usando il metodo "Sticky Keys" sopra descritto, può aumentare ulteriormente i propri privilegi di accesso al sistema. Questo metodo di attacco richiede l'uso del comando "Psexec" e dei diritti amministrativi locali alla macchina. Dopo aver eseguito il login con l'account di backdoor, attraverso il semplice uso dello strumento "psexec.exe" è possibile aumentare i permessi di accesso al sistema. Ciò lo si può fare utilizzando il comando "psexec.exe -s cmd".
- Process Injection: Lo sfruttamento delle debolezze presenti nei processi è un altro modo per eseguire l'escalation dei privilegi. Ad esempio uno strumento usato per i test di penetrazione come "Process Injector" ha la capacità di enumerare tutti i processi in esecuzione su un sistema e nel contempo di rilevare il relativo account di esecuzione. Per sferrare questo tipo di attacco, è necessario accedere con un account con maggior livello di autorizzazione. Dopo aver identificato il processo che si desidera iniettare, ad esempio, "cmd.exe", è possibile procedere con l'injection eseguendo il comando "pinjector.exe -p [PID] cmd.exe [port]", dove PID rappresenta l'identificativo del processo dal quale si intende copiare i permessi.
- Enumerazione delle Password degli utenti su Linux: Un attacco base di escalation dei privilegi, comune in ambiente Linux, viene condotto attraverso l'enumerazione degli account utente configurati sulla macchina. Questo tipo di attacco richiede che l'attaccante acceda alla shell dei comandi di sistema. Ciò, normalmente lo si può fare attraverso lo sfruttamento di server ftp non

30 https://www.owasp.org/index.php/Category:OWASP_Top_Ten_2017_Project

31 https://www.owasp.org/index.php/OWASP_Proactive_Controls

32 https://github.com/OWASP/ASVS

correttamente configurati. Una volta che l'attaccante ha ottenuto l'accesso alla shell, eseguendo il comando "cat /etc/passwd | cut -d: -f1" potrà visionare l'elenco di tutti gli utenti della macchina.

- Metasploit su Android: Metasploit è uno strumento ben noto alla maggior parte degli hacker e contiene una libreria di exploit noti. Nel caso di dispositivi Android, Metasploit può essere utilizzato per attaccare i dispositivi Android rooted. Una volta che un dispositivo Android è rooted, su questo viene reso disponibile un file binario "SU" che consente di eseguire comandi come root.
- Utilizzo di file dannosi: Un attacco di questo tipo sfrutta una configurazione di sistema che consente all'attaccante di accedere direttamente a un file eseguibile, ad esempio attraverso l'accesso alla command shell; oppure, nel peggiore dei casi, permette all'attaccante di caricare un file per poi eseguirlo. I server web, i server ftp e i sistemi middleware message oriented che presentano numerosi punti di integrazione possono essere considerati particolarmente vulnerabili, in quanto sia chi sviluppa che gli amministratori devono essere costantemente allineati riguardo le interfacce e i relativi opportuni privilegi.
- Dirottamento dell'esecuzione di un thread privilegiato: Un attaccante può a volte dirottare un thread privilegiato dal sistema sottostante utilizzando metodi sincroni (chiamando una funzione privilegiata che fallisce a seguito di un input non previsto) o asincroni (modificando variabili di ambiente utilizzate dal processo che in qualche modo ne determinano il flusso di esecuzione). Ciò può consentire all'avversario di accedere a funzionalità che il progettista del sistema non aveva previsto, ma può anche consentire all'attaccante di passare inosservato o di negare ad altri utenti servizi essenziali causando seri problemi.
- Elevazione dei privilegi in ambito HTTP: L'utilizzo di metodi standard HTTP (Get, Put, Delete) potrebbero essere esposti verso l'esterno. Un'interpretazione rigorosa del metodo HTTP Get indica che quei servizi che espongono una interfaccia tramite HTTP Get non devono essere usati per cancellare informazioni sul server, ma non esiste alcun meccanismo di controllo degli accessi che garantisce tale logica. Ciò significa che a meno che i servizi non siano correttamente configurati con le opportune ACL e l'implementazione del servizio dell'applicazione segua tale principio, allora una qualsiasi richiesta HTTP può facilmente eseguire una cancellazione o aggiornamento lato server. L'aggressore identifica un URL HTTP Get come http://sitovittima/aggiornamentoOrdine, che a sua volta chiama un altro processo per aggiornare l'ordine presente su un database o per aggiornare un'altra risorsa. Non essendo il metodo Get idempotent (ovvero può essere chiamato più volte ottenendo sempre lo stesso risultato) la richiesta può essere presentata più volte dall'attaccante, inoltre, l'attaccante può essere in grado di sfruttare l'URL pubblicato ed accessibile attraverso il metodo Get per eseguire effettivamente aggiornamenti (invece di recuperare semplicemente dati). Ciò può comportare una modifica dolosa o involontaria dei dati lato server.
- Sovvertimento delle funzionalità di firma del codice: Numerosi linguaggi utilizzano la firma del codice per garantirne l'identità e quindi legare il codice ai privilegi assegnatigli all'interno di un ambiente. Sovvertire tale meccanismo può essere strumentale in un attacco di escalation dei privilegi da parte di un aggressore. Qualsiasi mezzo capace di sovvertire il modo in cui una macchina virtuale impone la firma del codice può essere associato a questo tipo di attacco.
- Programmi target con privilegi elevati: Questo tipo di attacco ha come obiettivo quei programmi che funzionano con privilegi elevati. L'attaccante potrebbe tentare di sfruttare un bug presente nel programma in esecuzione e di ottenere del codice arbitrario da eseguire con privilegi elevati. Per esempio l'attaccante potrebbe individuare delle vulnerabilità in quei programmi che scrivono nelle directory di sistema o nelle chiavi di registro (come la posizione di registro "HKEY_LOCAL_MACHINE", dove vengono memorizzate una serie di variabili critiche dell'ambiente Windows). Questi programmi vengono tipicamente eseguiti con privilegi elevati e di solito non sono stati progettati pensando agli aspetti di sicurezza. Tali programmi sono gli obiettivi perfetti per uno sfruttamento in quanto forniscono notevoli vantaggi all'attaccante quando vengono compromessi. L'utente malintenzionato cerca di eseguire del codice arbitrario con lo stesso livello di autorizzazione di una chiamata di sistema privilegiata.