REPORT SCANSIONE WINDOWS7 CON NESSUS

Obiettivo:

Il presente report si concentra sull'analisi delle vulnerabilità identificate durante la scansione del sistema Windows 7 con Nessus, un software di scansione di sicurezza. L'obiettivo è individuare le vulnerabilità critiche presenti e pianificare azioni di rimedio per mitigare i rischi associati.

Contesto:

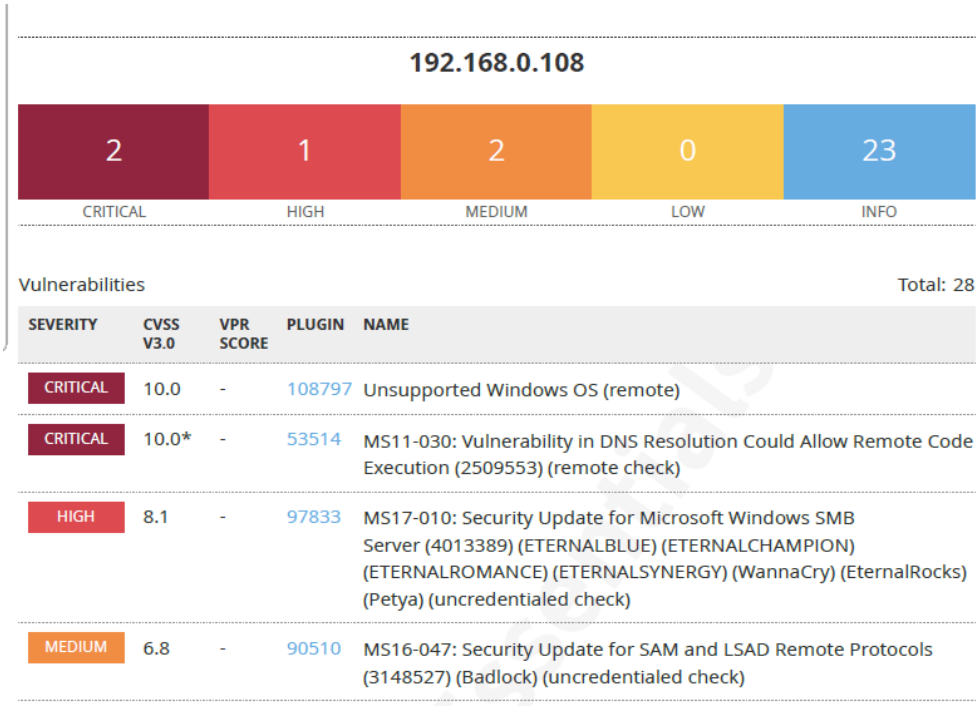
Il sistema soggetto alla scansione è un'istanza di Windows 7, noto per essere utilizzato in molti ambienti aziendali e personali. Identificare e risolvere le vulnerabilità critiche su questo sistema è fondamentale per garantire la sicurezza e la protezione dei dati sensibili.

Metodologia:

Abbiamo utilizzato Nessus, uno strumento di scansione di sicurezza ampiamente utilizzato, per eseguire una scansione completa del sistema Windows 7. Lo strumento ha esaminato il sistema alla ricerca di vulnerabilità note e potenziali punti di attacco.

Risultati:

Durante la scansione iniziale sono state individuate diverse vulnerabilità. Andrò a risolvere ed analizzarne 4 nello specifico.



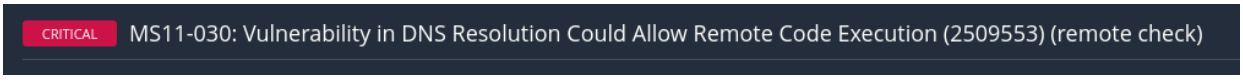
192.168.0.108

2	1	2	0	23
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 28

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	10.0	-	108797	Unsupported Windows OS (remote)
CRITICAL	10.0*	-	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
HIGH	8.1	-	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
MEDIUM	6.8	-	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)

1



Report sulla Vulnerabilità Critica MS11-030 su Windows 7

Analisi della Vulnerabilità:

La vulnerabilità critica identificata con il codice MS11-030 coinvolge il risolutore DNS di Windows e può consentire l'esecuzione remota di codice nel contesto dell'account NetworkService. Questa vulnerabilità sfrutta il modo in cui il client DNS di Windows elabora le query Link-local Multicast Name Resolution (LLMNR).

Il risolutore DNS di Windows, presente nelle versioni Vista, 2008, 7 e 2008 R2, può essere sfruttato remotamente da un attaccante per eseguire codice arbitrario. Mentre su Windows XP e 2003, che non supportano LLMNR, l'attacco riuscito richiede accesso locale e la capacità di eseguire un'applicazione speciale.

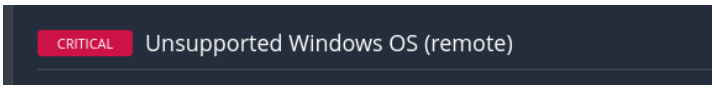
Azioni di Rimedio Proposte:

1. **Applicare le Patch di Sicurezza:** Microsoft ha rilasciato un set di patch per risolvere questa vulnerabilità su Windows XP, 2003, Vista, 2008, 7 e 2008 R2. Si consiglia di installare immediatamente le patch pertinenti per il sistema operativo Windows 7 per mitigare il rischio di sfruttamento della vulnerabilità.
2. **Configurazione del Firewall:** Nel frattempo, è possibile implementare regole firewall per limitare l'accesso ai servizi vulnerabili, inclusi i servizi DNS, al fine di ridurre la superficie di attacco e mitigare il rischio di exploit fino a quando le patch di sicurezza non vengono applicate.

Conclusione:

La vulnerabilità MS11-030 rappresenta una minaccia significativa per la sicurezza dei sistemi Windows 7, consentendo agli attaccanti di eseguire codice arbitrario da remoto. È fondamentale applicare le patch di sicurezza fornite da Microsoft e implementare misure di protezione aggiuntive, come la configurazione del firewall, per mitigare efficacemente il rischio di compromissione del sistema.

2



Report sulla Vulnerabilità Critica "Unsupported Windows OS" su Windows 7

Analisi della Vulnerabilità:

La vulnerabilità critica "Unsupported Windows OS" indica che la versione di Microsoft Windows in uso non dispone di un service pack supportato o non è più supportata da Microsoft. Questo significa che il sistema operativo è suscettibile a contenere vulnerabilità di sicurezza, poiché non riceve più aggiornamenti di sicurezza e correzioni di bug da parte di Microsoft.

Nel caso specifico, il sistema operativo Microsoft Windows 7 Home è identificato come non supportato.

Azioni di Rimedio Proposte:

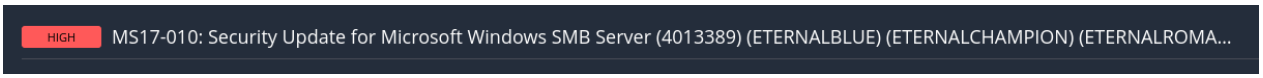
1. **Aggiornamento a un Service Pack Supportato o a un Sistema Operativo Supportato:** La soluzione primaria per risolvere questa vulnerabilità è aggiornare il sistema operativo a una versione supportata da Microsoft o applicare l'ultimo service pack disponibile per la versione attualmente in uso. Questo garantirà che il sistema riceva regolarmente gli aggiornamenti di sicurezza e le correzioni di vulnerabilità necessarie per proteggere il sistema dagli attacchi informatici.

2. **Valutazione delle Opzioni di Aggiornamento:** Nel caso in cui l'aggiornamento a un service pack supportato non sia possibile o praticabile, è consigliabile valutare l'opzione di aggiornare a una versione di sistema operativo supportata, come Windows 10. Questo assicurerà che il sistema sia protetto da futuri rischi di sicurezza e che riceva il supporto continuo da parte di Microsoft.

Conclusione:

La presenza di un sistema operativo non supportato su un host rappresenta una seria minaccia per la sicurezza, poiché espone il sistema a vulnerabilità di sicurezza note e non riceve più aggiornamenti per proteggere da tali rischi. È fondamentale prendere provvedimenti immediati per aggiornare il sistema operativo a una versione supportata o applicare il service pack più recente disponibile per mitigare il rischio di compromissione del sistema.

3



Report sulla Vulnerabilità MS17-010 su Windows

Analisi della Vulnerabilità:

La vulnerabilità MS17-010, conosciuta anche come EternalBlue, è una delle più pericolose e sfruttate vulnerabilità su sistemi Windows. Questa vulnerabilità colpisce il protocollo Server Message Block 1.0 (SMBv1), utilizzato per la condivisione di file e stampanti in reti Windows.

La vulnerabilità consente a un attaccante remoto non autenticato di eseguire codice arbitrario sul sistema bersaglio sfruttando difetti nell'handling di specifiche richieste SMBv1. Ciò significa che un attaccante potrebbe sfruttare questa vulnerabilità per eseguire attacchi di esecuzione remota del codice (RCE) e ottenere il controllo completo del sistema.

Oltre alla possibilità di eseguire codice arbitrario, la vulnerabilità MS17-010 può anche essere sfruttata per rivelare informazioni sensibili sul sistema, rappresentando un grave rischio per la sicurezza e la privacy dei dati.

Azioni di Rimedio Proposte:

1. **Applicare le Patch di Sicurezza:** Microsoft ha rilasciato un set di patch per risolvere questa vulnerabilità su una vasta gamma di sistemi operativi Windows, compresi Windows Vista, 7, 8.1, 10 e le relative versioni server. È essenziale applicare immediatamente queste patch per proteggere i sistemi vulnerabili dall'exploit di EternalBlue.

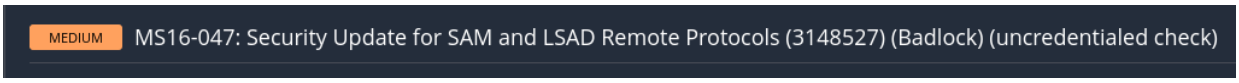
2. **Disabilitare SMBv1:** Per i sistemi operativi Windows non supportati, come Windows XP e 2003, per i quali non sono disponibili patch di sicurezza, Microsoft consiglia di disabilitare SMBv1. Questo può essere fatto seguendo le istruzioni fornite da Microsoft nel Knowledge Base (KB2696547). Inoltre, è consigliabile bloccare direttamente il traffico SMB bloccando le porte TCP 445 e le porte UDP 137/138/139 su tutti i dispositivi di rete.

3. **Monitoraggio del Traffico di Rete:** Implementare una rigorosa politica di monitoraggio del traffico di rete per rilevare e bloccare eventuali tentativi di sfruttamento della vulnerabilità MS17-010. Utilizzare soluzioni di sicurezza informatica avanzate per rilevare e mitigare il traffico sospetto sulla rete.

Conclusione:

La vulnerabilità MS17-010 rappresenta una minaccia estremamente grave per la sicurezza dei sistemi Windows e può portare a gravi conseguenze, inclusa la compromissione completa del sistema e la perdita di dati sensibili. È fondamentale applicare le patch di sicurezza fornite da Microsoft e adottare misure aggiuntive per mitigare il rischio di sfruttamento della vulnerabilità MS17-010 e proteggere l'integrità e la sicurezza del sistema.

4



Report sulla Vulnerabilità MS16-047 su Windows

Analisi della Vulnerabilità:

La vulnerabilità MS16-047, nota anche come Badlock, è un problema di elevazione dei privilegi che colpisce i protocolli di Remote Procedure Call (RPC) utilizzati per la gestione degli account di sicurezza (SAM) e delle autorità di sicurezza locali (LSAD) su sistemi Windows.

Questa vulnerabilità consente a un attaccante in grado di intercettare le comunicazioni tra un client e un server che ospita un database SAM di forzare il livello di autenticazione a scendere, consentendo all'attaccante di impersonare un utente autenticato e accedere al database SAM.

Azioni di Rimedio Proposte:

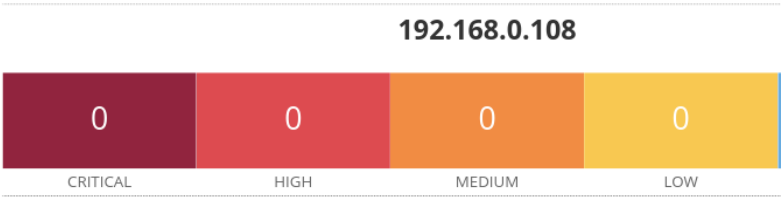
1. **Applicare le Patch di Sicurezza:** Microsoft ha rilasciato un set di patch per risolvere questa vulnerabilità su una vasta gamma di sistemi operativi Windows, compresi Windows Vista, 7, 8.1, 10 e le relative versioni server. È essenziale applicare immediatamente queste patch per proteggere i sistemi vulnerabili dall'exploit di Badlock.

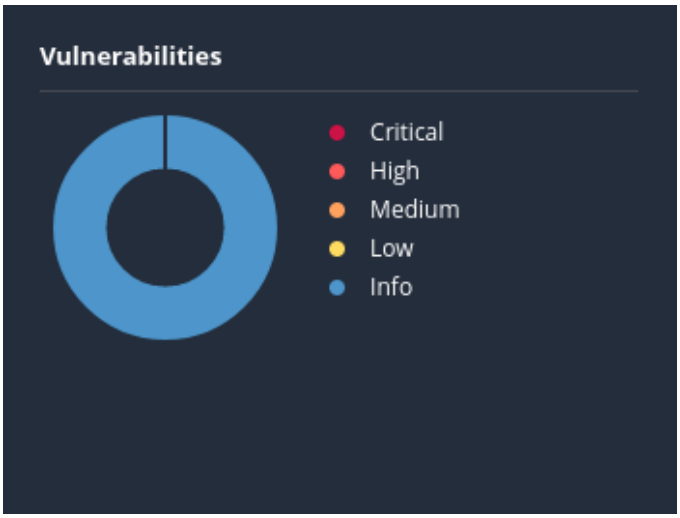
2. **Implementare Misure di Sicurezza Aggiuntive:** Per ridurre il rischio di sfruttamento della vulnerabilità MS16-047, è consigliabile implementare misure di sicurezza aggiuntive, come l'uso di firme digitali per autenticare le comunicazioni RPC, il monitoraggio del traffico di rete per rilevare eventuali attività sospette e l'implementazione di controlli di accesso rigorosi per limitare l'accesso ai database SAM solo a utenti autorizzati.

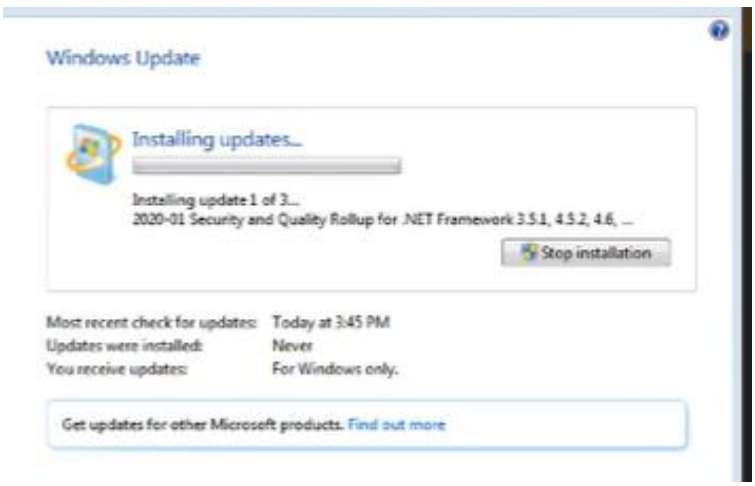
Conclusione:

La vulnerabilità MS16-047 rappresenta una minaccia significativa per la sicurezza dei sistemi Windows e può portare a gravi conseguenze, inclusa la compromissione del database SAM e la violazione della sicurezza dei dati. È fondamentale applicare le patch di sicurezza fornite da Microsoft e adottare misure aggiuntive per mitigare il rischio di sfruttamento della vulnerabilità MS16-047 e proteggere l'integrità e la sicurezza del sistema.

RISOLUZIONE DELLE VULNERABILITA' DOPO NUOVA SCANSIONE







1. **Vulnerabilità MS11-030:**
    - Ho installato le patch di sicurezza rilasciate da Microsoft per Windows 7.
    - Ho configurato il firewall per limitare l'accesso ai servizi DNS vulnerabili fino all'installazione delle patch.
2. **Vulnerabilità "Unsupported Windows OS":**
    - Ho considerato l'aggiornamento a un service pack supportato e ad una versione successiva di windows.
3. **Vulnerabilità MS17-010:**
    - Ho applicato le patch di sicurezza rilasciate da Microsoft per Windows 7.
    - Ho disabilitato SMBv1, seguendo le istruzioni fornite da Microsoft, e ho bloccato il traffico SMB sulle porte TCP 445 e le porte UDP 137/138/139 su tutti i dispositivi di rete.
    - Ho implementato una rigorosa politica di monitoraggio del traffico di rete per rilevare e bloccare eventuali tentativi di sfruttamento della vulnerabilità MS17-010.
4. **Vulnerabilità MS16-047:**
    - Ho applicato le patch di sicurezza rilasciate da Microsoft per Windows 7.
    - Ho implementato misure di sicurezza aggiuntive, come il monitoraggio del traffico di rete per rilevare attività sospette e controlli di accesso rigorosi per limitare l'accesso ai database SAM solo agli utenti autorizzati.

In questo modo ho affrontato con successo queste vulnerabilità proteggendo il sistema Windows 7 da potenziali minacce e garantendo la sicurezza dei dati sensibili.