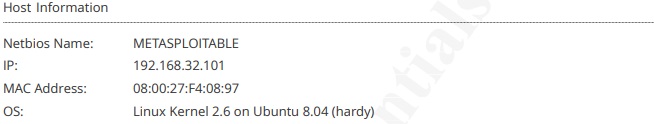
# Vulnerabilità Host



A seguito della scansione effettuata sull’host in questione, sono state rilevate: 44 vulnerabilità, suddivise in:

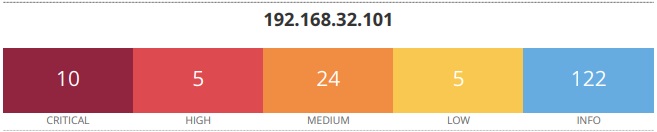
Critica

Alta

Media

Bassa

e 122 Informazioni di applicazioni e servizi.



Orlando Tangari

Per le vulnerabilità di livello critico, è necessario:

un riavvio,

un aggiornamento,

una reinstallazione,

riconfigurazione,

disabilitazione di SSL 2.0 e 3.0 a favore di TLS 1.2

un cambio password con una più sicura,

dei servizi e dei protocolli, con minaccia critica, presenti sull’host.

Per le vulnerabilità di livello alto, è necessario:

un aggiornamento,

appropriate restrizioni,

una riconfigurazione,

dei servizi e delle applicazioni, con minaccia alta, presenti sull’host.

Per le vulnerabilità di livello medio, è necessario:

una disattivazione di un metodo HTTP,

un aggiornamento,

un’applicazione di firma dei messaggi,

rimozione di codici deboli,

una riconfigurazione,

una generazione di un certificato SSL,

abilitazione del supporta TLS 1.2 e 1.3,

dei servizi, delle patches e delle applicazioni, con minaccia media, presenti sull’host.

Per le vulnerabilità di livello basso, è necessario:

una disabilitazione di una crittografia in modalità CTB per abilitazione di cifratura CTR o GCM,

una disabilitazione degli algoritmi MD5 e MAC a 96 bit,

una rimozione del supporto EXPORT\_DHE,

una limitazione di accesso alla porta di X11,

dei servizi e delle applicazioni, con minaccia bassa, presenti sull’host.