**Vulnerabilità analizzate:**

**1. Bash Remote Code Execution (Shellshock) - CVE-2014-6271**

**Descrizione:**  
La vulnerabilità Shellshock permette l'esecuzione remota di comandi arbitrari su sistemi con versioni di Bash non aggiornate. Il problema deriva dalla gestione impropria delle variabili d'ambiente, che consente agli attaccanti di iniettare codice dannoso. Questa vulnerabilità è critica, soprattutto se Bash viene invocato da servizi come CGI o SSH.

**Sfruttamento:**  
Un attaccante può inviare richieste HTTP con intestazioni modificate o utilizzare comandi SSH per eseguire codice sul sistema vulnerabile. Esempio:

curl -H 'User-Agent: () { :; }; echo; /bin/bash -c "echo Exploit!"' http://<target>/cgi-bin/script.cgi

**2. Apache Tomcat End-of-Life (<= 5.5.x)**

**Descrizione:**  
Le versioni Apache Tomcat fino alla 5.5.x non sono più supportate e non ricevono aggiornamenti di sicurezza. Questo le rende vulnerabili a una serie di attacchi, come esecuzione di codice remoto, disclosure di informazioni e vulnerabilità note non mitigate. L'accesso al gestore Tomcat può consentire l'upload di file dannosi.

**Sfruttamento:**  
Un attaccante può accedere al **Manager App** utilizzando credenziali deboli o di default (admin:admin) per caricare file .war malevoli e ottenere il controllo del server.

**3. Ubuntu Kernel Vulnerabilities (USN-625-1)**

**Descrizione:**  
Questa vulnerabilità riguarda versioni obsolete di Ubuntu (6.06, 7.04, 7.10, 8.04) con kernel 2.6.15/20/22. Problemi nella gestione della memoria e dei moduli kernel possono portare a escalation dei privilegi o Denial of Service (DoS). Questi sistemi non ricevono più patch di sicurezza.

**Sfruttamento:**  
Un attaccante locale può sfruttare bug del kernel per ottenere privilegi di root o causare il crash del sistema. Esempio: eseguendo codice che sfrutta buffer overflow o errori di puntatori.

**4. VNC Server 'password' Password**

**Descrizione:**  
Il VNC server configurato con la password predefinita password espone il sistema a un accesso remoto non autorizzato. Una configurazione del genere permette ad attaccanti di prendere il controllo completo della macchina senza necessità di brute force.

**Sfruttamento:**  
Un attaccante può collegarsi facilmente al server VNC:

nc <target\_ip> 5900

Inserendo password come credenziale, ottiene l'accesso al desktop remoto.

**5. Ubuntu Perl Vulnerability (USN-1770-1)**

**Descrizione:**  
Le versioni di Perl su Ubuntu 8.04, 10.04, 11.10, 12.04 e 12.10 contengono vulnerabilità che possono causare Denial of Service (DoS) o comportamenti imprevisti nei processi. Questo è particolarmente pericoloso per applicazioni che processano input non affidabili.

**Sfruttamento:**  
L'attaccante invia input appositamente costruiti per sfruttare errori nei meccanismi di parsing o di gestione delle espressioni regolari. Ad esempio, input malformati possono esaurire risorse o bloccare i servizi.

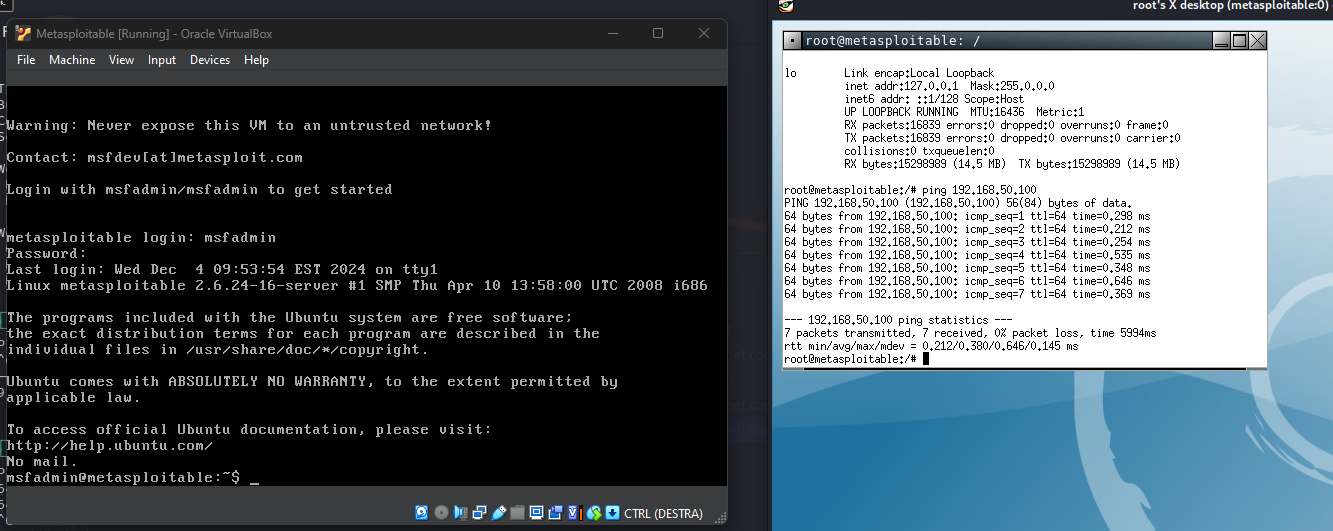
**6. Bind Shell Backdoor Detection**

**Descrizione:**  
Il report indica la presenza di una backdoor "bind shell", un programma malevolo che ascolta su una porta specifica per fornire accesso remoto al sistema compromesso. Questo è un chiaro segno di compromissione del sistema.

**Sfruttamento:**  
Un attaccante si connette alla porta aperta dalla backdoor utilizzando strumenti come nc:

nc <target\_ip> <port>

Una volta connesso, ottiene l'accesso alla shell del sistema.



Sfruttando la vulnerabilità della porta 5900 lasciata aperta e della password del VNC server “Password”, attraverso vncviewer ho potuto accedere remotamente alla Meta