**Report di Analisi Nmap per l'Host 192.168.50.101**

**Informazioni Generali:**

* Data e ora dell'analisi: 2023-08-19 11:26 EDT
* Latenza dell'host: 0.00023s

**Porte Aperte e Servizi:**

1. Porta 21/tcp - FTP
   * Servizio: vsftpd 2.3.4
   * Stato: Aperta
   * Accesso FTP anonimo: Consentito
2. Porta 22/tcp - SSH
   * Servizio: OpenSSH 4.7p1 Debian 8ubuntu1 (protocollo 2.0)
   * Stato: Aperta
   * Hostkey: DSA, RSA
3. Porta 23/tcp - Telnet
   * Stato: Aperta (possibile servizio Telnet)
4. Porta 25/tcp - SMTP
   * Stato: Aperta (possibile servizio SMTP)
5. Porta 53/tcp - DNS
   * Servizio: ISC BIND 9.4.2
   * Stato: Aperta

...

**Servizi Specifici:**

* Servizio FTP (Porta 21/tcp):
  + Server FTP: vsFTPd 2.3.4
  + Accesso anonimo: Consentito
* Servizio SSH (Porta 22/tcp):
  + Server SSH: OpenSSH 4.7p1 Debian 8ubuntu1
  + Hostkey: DSA, RSA
* Servizio DNS (Porta 53/tcp):
  + Server DNS: ISC BIND 9.4.2

...

**Altre Informazioni:**

* Sistema Operativo: Linux 2.6.X
* Dettagli OS: Linux 2.6.9 - 2.6.33
* Dispositivo: Oracle VirtualBox virtual NIC
* Indirizzo MAC: 08:00:27:D0:2D:2F

**Riepilogo delle Vulnerabilità Potenziali:**

* Accesso FTP anonimo abilitato (Porta 21)
* Versioni obsolete dei servizi SSH e Samba
* Possibili servizi non sicuri come Telnet e Telnet

**Conclusioni:** L'host 192.168.50.101 presenta diverse porte aperte con servizi in esecuzione. Alcuni di questi servizi potrebbero rappresentare potenziali rischi di sicurezza a causa di versioni obsolete o configurazioni non sicure. È consigliabile effettuare ulteriori valutazioni e test per garantire la sicurezza dell'host.