Internal Penetration Testing: Methodology and Findings

-- T Sreenivasulu

Objectives and Methodology

Simulate Internal Threat

Perform reconnaissance and enumeration from an insider perspective to identify potential attack vectors

Identify Vulnerabilities

Discover exposed services and security weaknesses that could be exploited by malicious actors

Fortify Network Security

Provide actionable insights to strengthen defenses against internal threats

Utilize Standard Tools

Employ industry-standard tools like ARP-Scan, Ping, and Nmap to simulate real-world attack scenarios

Network Discovery Phase

Tool Used

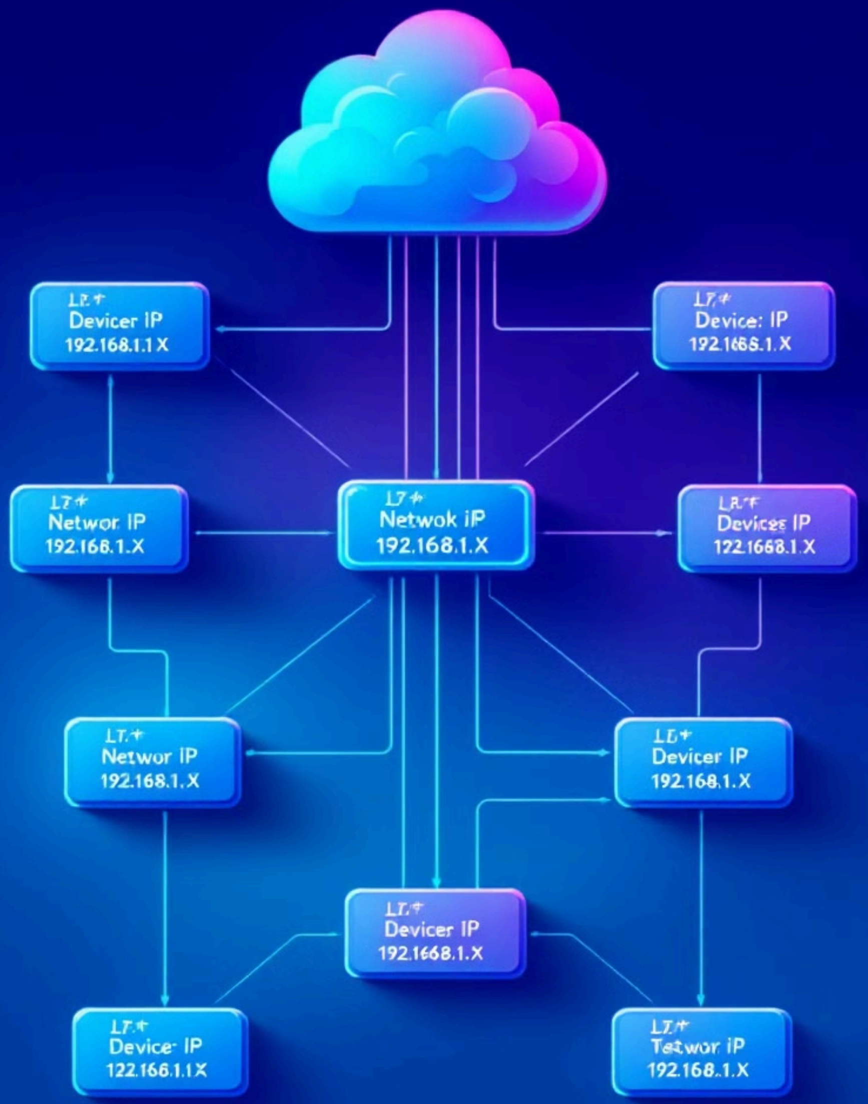
Netdiscover - A simple but powerful tool for identifying live hosts in the local subnet through ARP requests

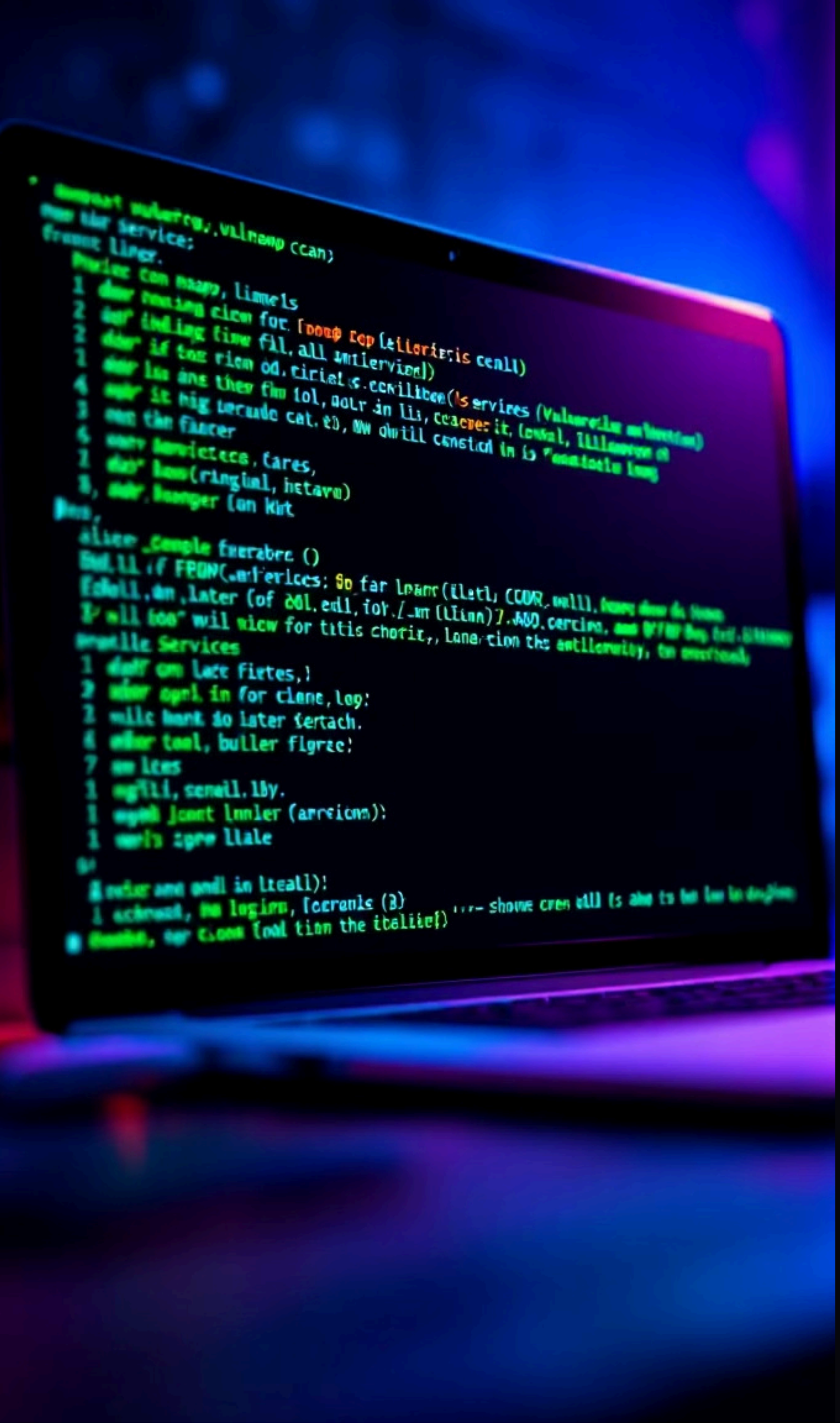
Command Executed

sudo netdiscover - This command sends ARP requests to discover devices on the local network without prior knowledge of the network range

Key Findings

Identified 4 live hosts on the network, including the target machine at 192.168.73.133 with MAC address 00:0c:29:35:db:d0 (VMware)





Port Scanning & Service Enumeration

Tool Used	Nmap - Network Mapper
Command	nmap -sV -sC -Pn -p- 192.168.73.133

3

Open Ports

21

FTP Port

Running vulnerable ProFTPD 1.3.3c

80

HTTP Port

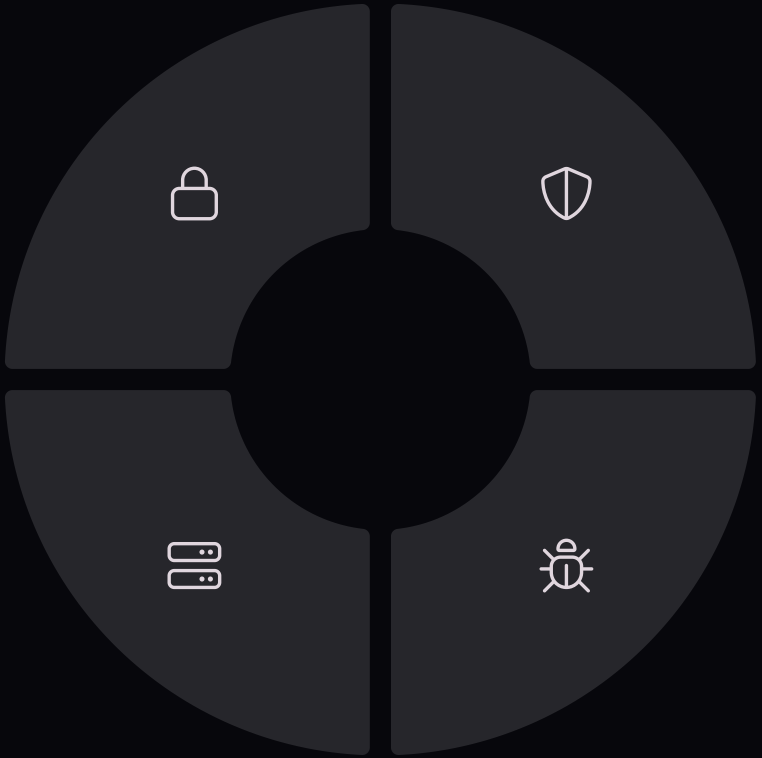
Apache 2.4.18 web server

22

SSH Port

OPENSSH 7.2p2

Vulnerability Assessment



OpenSSH 7.2p2

Older version with outdated crypto settings

Potential for credential-based attacks

FTP Security

Anonymous login disabled

Still vulnerable to backdoor exploit

Apache 2.4.18

Older version with potential vulnerabilities

Secondary attack surface

ProFTPD 1.3.3c

Known backdoor vulnerability (CVE-2010-4221)

Primary entry point for exploitation

Exploitation Process

Identify Vulnerable Service

ProFTPD 1.3.3c identified as vulnerable to backdoor exploit

Launch Metasploit Framework

Use msfconsole to search for and select appropriate exploit module

Configure Exploit Parameters

Set target IP, local host, and payload options for reverse shell

Execute Exploit

Run exploit/unix/ftp/proftpd_133c_backdoor with cmd/unix/reverse payload

Gain Root Access

Successfully obtain full privileged access to the target system

Post-Exploitation Findings

Access Level Verification

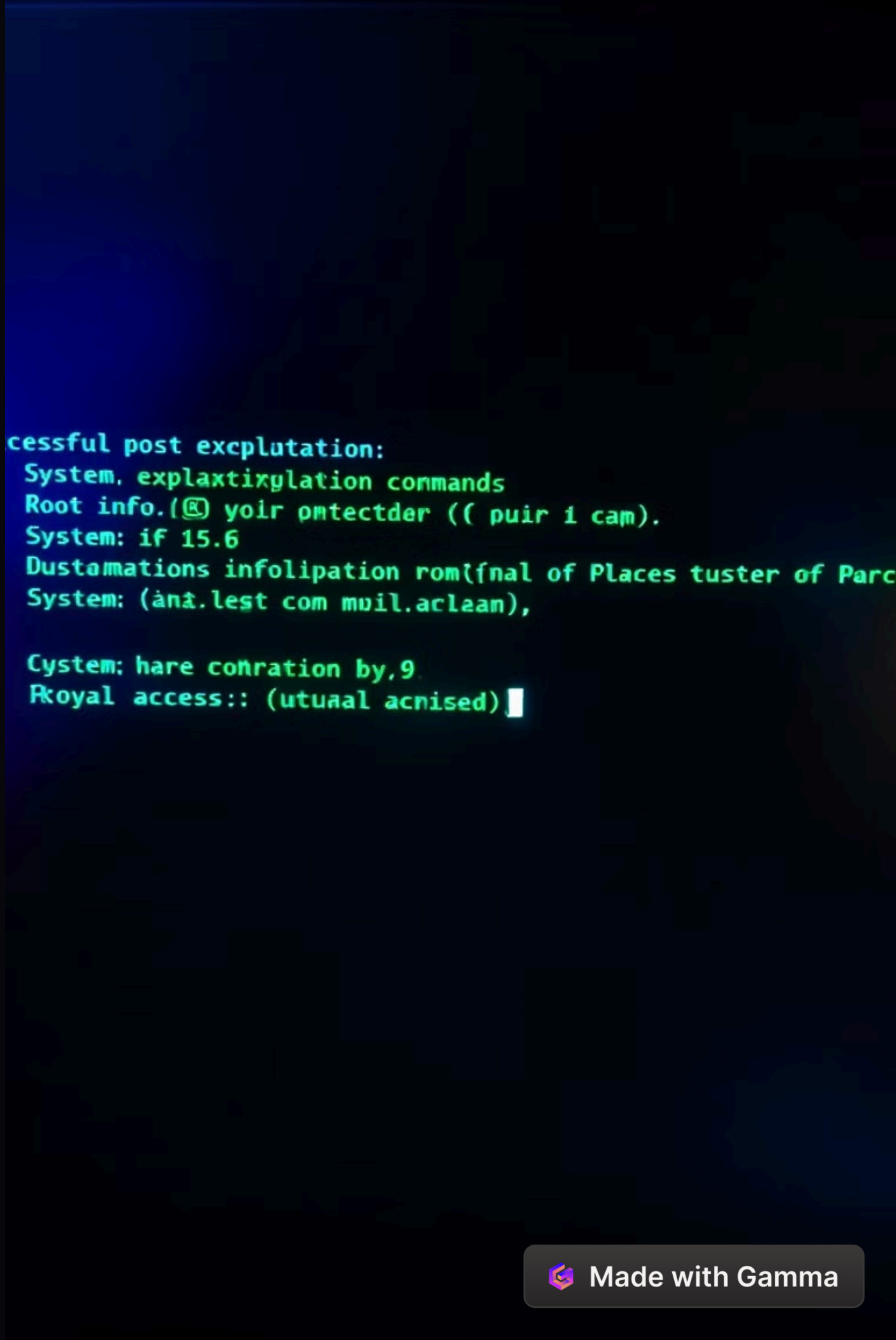
Commands like "whoami" confirmed root access, providing complete system control with no privilege escalation required

System Information Gathering

Hostname identified as "vtsec" with Linux kernel version 4.10.0-28-generic running on Ubuntu 16.04.2 x86_64 architecture

File System Exploration

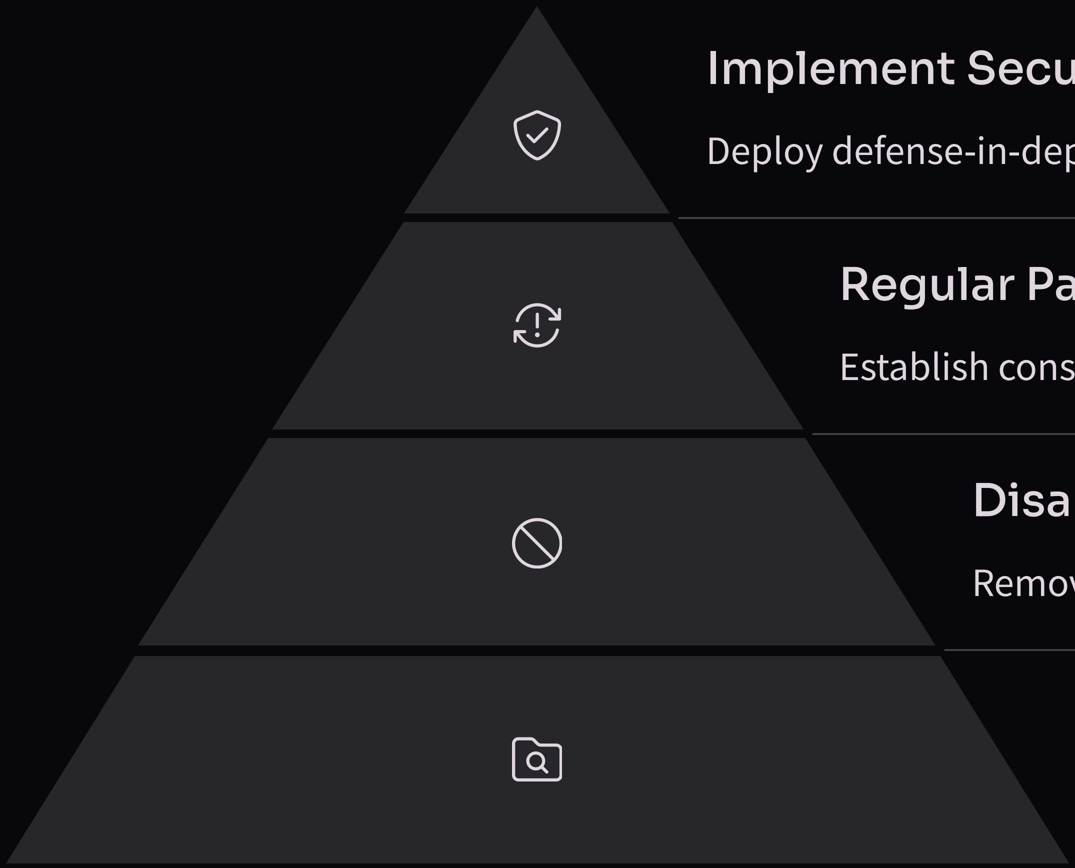
Complete access to all system directories including sensitive areas like /etc, /root, and user home directories, allowing for data exfiltration or further lateral movement



```
cessful post excplutation:
 System, explaxtixglation conmands
 Root info.(Ⓡ yoir pmtectder (( puir i cam).
 System: if 15.6
 Dustamations infolipation rom(fnal of Places tuster of Parc
 System: (ànȧ.lest com mvil.aclaan),

 Cystem: hare conration by,9
 Rkoyal access:: (utuaal acnised)█
```

Conclusions and Recommendations



Implement Security Controls

Deploy defense-in-depth strategies

Regular Patching

Establish consistent update protocols

Disable Unnecessary Services

Remove or secure FTP and other vulnerable services

Continuous Monitoring

Implement intrusion detection systems

Thank You

Made with Gamma