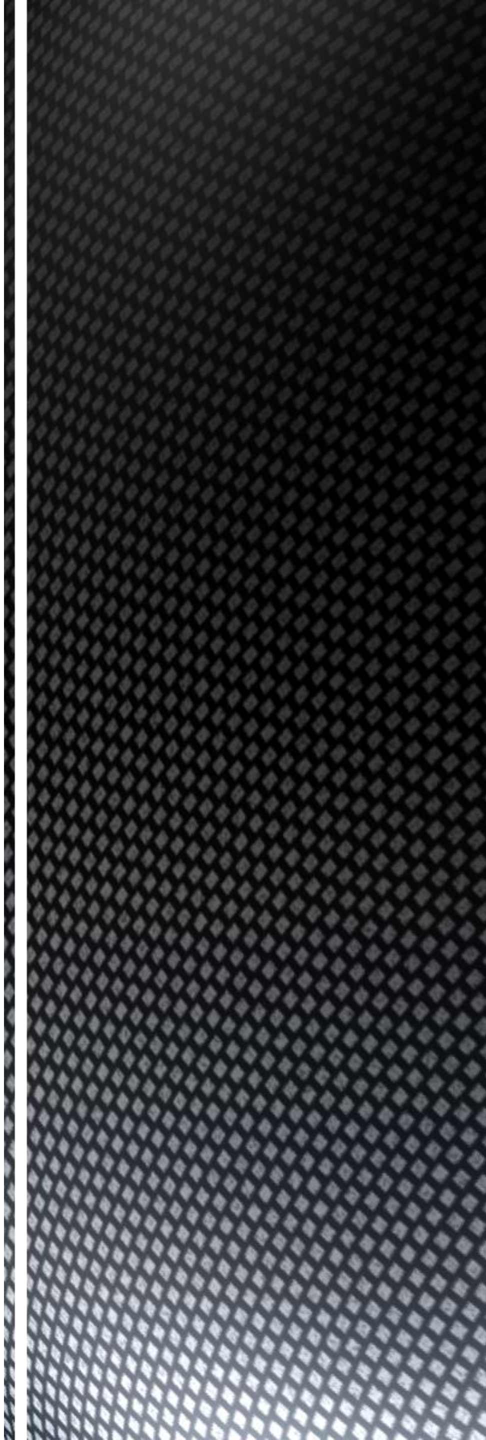
ETHICAL HACKING

Ravindra Singh



Executive Summary

This report presents the results of the vulnerability assessment and penetration test of Marvel corporation and underlying internet and network infrastructure. The purpose of this assessment is to identify application and network –level security issues that could affect Marvel's network infrastructure.

The scope of this exercise includes evaluating the security of the network and application, perform unauthorized attempts into system, obtain confidential information, and determine the overall security of the application by performing a wide variety of vulnerability checks. The testing included servers, operating systems and network devices associated with Marvlels virtual network.

In conclusion,   I have identified areas where security policy is not being adhered to, this introduces a risk to the organization and therefore I must declare the system as insecure.

Problems Identified

After completing vulnerability analysis and penetration testing it was determined that the network configuration was flawed. The Backdoor were extremely vulnerable to data theft, server hijacking, DDOS attacks and injections. In addition usernames and passwords were brute forced rather easily.

Solutions

System hardening - Minimize a catastrophe

- disable built in accounts
- determine necessary protocols
- use of service packs
- patch management
- group and user policies
- protect bios
- identify and remove unnecessary applications
- configuration of baselines.
- educate employees on the dangers of unsecured networks
  - shoulder surfing
  - password complexity

Closing Remarks

Recommendation

- Harden the system.
  - greatly reduce a cyber attack
- Employee awareness
- Closing unnecessary services
- Patch management
- Update firewalls
- Intrusion detection and prevention systems, etc.
- Backup and recovery
  - Securing data - valuable data should never be wiped away but protected.

Proof of Concept

I was able to use accessible programs to:

- create a remote session
- obtain access credentials
- inject faulty scripts
- gain access to restricted files.

IT infrastructure

- vulnerable
- exploitable
- cause massive financial and data loss.

Questions & Answers

Q: Name an exploit found on webserver that would be considered critical or high?
A: FTP was open and subject to backdoor exploits

Q: Name an exploit found on the DNS server that would be considered critical or high?
A: SSH was open and subject to brute force vulnerabilities.

Q: Can you remotely connect to the webserver outside of the network?
A: Yes with Metasploit by setting the RHOSTS and LHOSTS

Q: Can you remotely connect to the CEO outside of the network? A: Yes. I used the internal kali server and connected with
Metasploit by setting the RHOSTS and LHOSTS.

Q&A: Not present

Q: What tools Did I use to conduct the vulnerability assessment and why?
A: NMAP. NMAP is an open source network scanner that identifies what devices are running on the system, discovers hosts that are available and services, finding open ports and detecting security risks. Zenmap is a GUI version that can be used.

Q: What tools did you use to conduct the exploit and why?
A: Metasploit. It develops, tests and executes exploits. It can be used to create security testing tools and exploit modules and also as a penetration testing system. Searchsploit is another one and Hydra is another one.

Q: What users are located on the webserver machine?
A: Use cat /etc/passwd and it provides the list of all users .

Q: What exploit was successful on the Webserver?
A: FTP. The backdoor exploit was vulnerable.

Q: Were you able to exploit a Linux machine and which one worked?
A: SSH was exploitable on the DNS server by Brute force.