MONARCH NETWORKS

3/12 INTERNAL SECURITY ASSESSMENT RESULTS

CLASSIFIED

2023-03-12 14:00:00 PST

This document details the results of the internal security assessment completed just two hours before the events of Operation Titan Shield. This security assessment was prompted by a previous cyber attack that left Monarch's systems crippled and incredibly vulnerable to further attack. The attackers established various forms of persistence within Monarch's network, including backdoors, web shells, broken authentication mechanisms, and much more. The assessment revealed multiple critical vulnerabilities that can be exploited to cause significant damage to Monarch's operations.

Network Summary

monarch.lan

Name	IP	OS	Role	Scored SRV
bravo	**x.3**	**Windows Server 2016**	**ADDC + DNS**	**DNS**
skullisland	**x.4**	**Windows Server 2019**	**FTP + HTTP WIKI (IIS)**	**FTP, HTTP**
atoll	**x.5**	**Windows Server 2019**	**RCUBE SQL + HTTP E-COM (XAMPP)**	**HTTP**
sedona	**x.7**	**Ubuntu 22.04 Desktop**	**HTTP BLOG**	**HTTP**
janjira	**x.8**	**Ubuntu 20.04 Desktop**	**BLOG + WIKI + E-COM SQL**	**-**
yunnan	**x.9**	**Fedora 36 Desktop**	**SMTP + HTTP Webmail [RCUBE]**	**SMTP, HTTP**

Administrators:

madmin (main user)
- Password: Password1!

iserizawa
- Password: Password1!

vgraham
- Password: Password1!

ichen
- Password: Password1!

Users:

branda
hbrooks
lsan
jconrad
abrooks
wriccio
singh
erussell
mrussell
scoleman
rstanton
nlind
iandrews

Vulnerability Report

1. **bravo [172.16.x.3]**: Windows Server 2016
   a. **Anonymous RCE with Psexec**
      i. **Can literally use any credentials**
   b. Vulnerable to Eternal Blue
   c. RDP enabled
      i. CMD accessible through lock screen via sticky keys
   d. Webshells [Password: ghost287]
      i. dashboard/wso.phtml
      ii. dashboard/images/images.bmp
   e. Everyone and Authenticed Users have Generic All on Domain Admins
2. **skullisland [172.16.x.4]**: Windows Server 2019
   a. RDP enabled
   b. Powershell Constrained Language
   c. SMB 1.0 enabled
   d. FTP anonymous access. Everyone has write access
   e. Mediawiki cred
      i. Username: madmin
      ii. Password: Password1!
   f. Press shift 5 times in user login page to open cmd
      i. REG ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe" /v Debugger /t REG_SZ /d "C:\windows\system32\cmd.exe"
      ii. You can add users, delete, change password, etc
   g. Defender screwed up
   h. P0wny shell at http://172.16.x.4/phplog.php
   i. Microsoft IIS FTP Server NLST Response Overflow
3. **atoll [172.16.x.5]**: Windows Server 2019
   a. Administrator account is enabled
   b. All users have password of Password1!
   c. Go to /admin797vqu490, credentials are in readme
   d. Php shell at /js/bozo.php and at /error.php
   e. SMB 1.0 enabled
   f. RDP enabled
   g. Remote MySQL access
      i. mysql -u roundcubeuser -p -h 172.16.x.5
      Password: Password1!
   h. C:\Windows\System32\windows.bat is scheduled to execute every 5 minutes
      i. Opens a youtube video *delay*
      ii. Turns off firewall *delay*
      iii. Starts a tcp listener on port 4311
4. **sedona [172.16.x.7]**: Ubuntu 22.04
   a. Tcp listener (gives root) listening on port 6556 spawned after user clicks on malicious Ghidra desktop file AND initiated from /etc/crontab file

b. php webshell at /var/www/html/wordpress/setup/wp-config-1.php
c. Tcp listener (gives root) disguised as wordpress binary initiated by false service wordpress.service. Listener is listening on port 8080

5. **janjira [172.16.x.8]**: Ubuntu 20.04
   a. BASH is SUID
   b. PAM is broken, pam_deny replaced with pam_permit
   c. Web server (80) displaying passwords entered by the blue team
      i. http://172.16.x.8/data.txt
   d. Web server (443) with PHP shell:
      i. http://172.16.x.8:443/index.php
   e. Web server (8080) with PHP shell
      i. http://172.16.x.8:8080/index.php
   f. SQL user remote password: Password1!
      i. $ mysql -u remote -p -h 172.16.x.8
   g. xRDP is installed and running, auth is broken so login as literally any user
   h. startup application that starts a python bind shell on port 4444
   i. Cronjob starting netcat bind shell on port 1200 every minute
   j. INIT service that reverts sshd_config to insecure version every 240 seconds, restarts SSHD, and allows SSH through firewall {ufw and iptables}.
   k. SYSTEMD service that starts a netcat bindshell every 600 seconds and allows it through UFW and IPTABLES firewall (port 3000)
   l. /etc/bash.bashrc reverts vgraham password to Password1!
6. **yunnan [172.16.x.9]**: Fedora 36
   a. BPFdoor via crontab
   b. Cockpit
   c. SSH
   d. pam_deny replaced with pam_permit
      i. You can basically do any of the persistent techniques, because passwords will work
   e. PHP shell at e.php
      i. p0wny shell
   f. ip/config/config_webmail.php
      i. Also p0wny shell
   g. xRDP is installed and running
   h. VNC is running for main user
   i.
   j.