ServerBee
...turning iron into honey

Analýza konfigurace linuxového serveru

pro společnost
Běžná firma s.r.o.

vypracoval
Root Sudovič

dne
19.1.2038

Požadavky klienta

- Zjistit verzi OS
- IP adresy na rozhraní
- Firewallová pravidla
- Služby na serveru
- HW parametry serveru (CPU, počet CPU, RAM, velikost HDD)

Konfigurace a základní informace o systému

Hardware

- HP ProLiant DL20 Gen9 (s/n XXXXXXXXXX, SKU XXXXXX-XXX)
- 1x Xeon(R) CPU E3-1230 v5 @ 3.40GHz, 4 jádra, 8 threadů
- 1x 8GB RAM (p/n XXXXXX-XXX)
- 2x 1TB HDD ST1000DM010-2EP102 (s/n XXXXXXXX, XXXXXXXX)

Operační systém

- Debian 8.11
- Softwarový RAID – mirror
- 909GB místa celkem, 83GB obsazeno
- 31GB dat v e-mailech (/var/mail)
- 25GB dat v uživatelských home adresářích

Konfigurace sítě

- eth0 WAN interface, eth1 LAN interface
- eth0 IP: X.X.X.X/29, Y.Y.Y.Y/28
- eth1 IP: 192.168.1.1/24
- Povolen IPv4 forwarding

Firewall

- Odchozí provoz z vnitřní sítě bez omezení
- Odchozí provoz ze serveru bez omezení
- Příchozí provoz do vnitřní sítě povolen pouze pro:

Zdrojová IP	Port	Protokol	Cílová IP
1.2.3.4, 5.6.7.8	3389	tcp	192.168.1.252
	888	tcp	192.168.1.10
	80	tcp	192.168.1.40

- Příchozí provoz na server povolen povolen pro:

Služba	Rozhraní	Protokol	Porty
FTP	WAN/LAN	tcp	21
SSH	WAN/LAN	tcp	22
SMTP	WAN/LAN	tcp	25,587
Dovecot (IMAP/POP3)	WAN/LAN	tcp	993,995
HTTP	WAN/LAN	tcp	80,443
Dovecot (IMAP/POP3)	LAN	tcp	110,143
DNS resolver	LAN	udp	53

- NAT pravidla:

Zdrojový port	Rozhraní	Protokol	Cílový port	Cílová adresa
888	WAN	tcp	888	192.168.1.10
777	WAN	tcp	80	192.168.1.140
3389	WAN	tcp	3389	192.168.1.252

Zálohování

- Nepovedlo se zjistit způsob zálohování serveru

Monitoring

- Nenalezen žádný běžný monitorovací agent (Zabbix/Nagios/Munin)
- Z logu služeb není patrný externí monitorovací systém

Běžící služby

DHCP server

- DHCP pool 192.168.1.101 - 192.168.1.200

DNS Bind

- Rekurzivní DNS server pro LAN

MySQL server

- Pro potřeby webmailu

Apache

- HTTP server pro Roundcube Webmail, PHPMyAdmin

Dovecot

- IMAP/POP3 server
- Sieve server pro aplikaci pravidel pro zprávy

Sendmail MTA

- SMTP server
- Žádný antispam, zprávy jsou pravděpodobně filtrovány na primárním MX mx.domain.tld.

Proftpd

- FTP server pro uživatelské účty

SSHD

- SSH přístup pro všechny uživatele bez omezení
- Přihlašování heslem

Zjištěné problémy

- Přihlašování heslem na SSH
- Malware maskovaný jako atd daemon, spuštěný pod uživatelem apache
- Cronem spouštěný bitcoin miner
- Chybí ochrana proti pokusům o násilné zjištění hesla k IMAP/POP3 účtům
- Neaktualizovaný PHPMyAdmin – může dojít ke zneužití serveru
- Poslední aktualizace systému před více než jedním rokem
- DNS resolver neověřuje DNSSEC

Urgentní zásahy

- Nastavit přihlašování SSH klíčem pro všechny uživatele
- Analyzovat možný způsob instalace malwaru a následně jej odstranit
- Aktualizovat webmail a phpmyadmin