Skupljanje promjenjivih podataka

Case Logbook

Profil incidenta

1. Ime klijenta.
2. Kako je incident otkriven?
3. Što klijent misli da se dogodilo?
4. Kad klijent misli da se incident dogodio?
5. Tko ili što je prijavilo incident?
6. Koji hardware/software je u igri?
7. Tko su kontakti klijenta?
8. Koliko je sustav u pitanju kritičan?

Dokumentiranje koraka

1. Tko izvodi forenzičko prikupljanje podataka?
2. Povijest korištenih alata i naredbi.
3. Ispisi (eng. *output*) alata i naredbi.
4. Datum i vrijeme pojedinih akcija.

Promjenjivi podaci

1. Tip i verzija operacijskog sustava.
2. Datum instaliranja sustava.
3. Registrirani vlasnik.
4. Sistemski direktorij.
5. Ukupna količina fizičke memorije.
6. Instalirani fizički hardware i lokacija.
7. Instalirane software aplikacije.

Postupci za skupljanje promjenjivih podataka

- Čupanje kabla iz struje može spasiti neke podatke koji su bili predbilježeni za brisanje ili na kojima su se radile izmjene u trenutku nestanka napajanja. Ako je napadač promijenio rutinu gašenja računala dodatkom ili micanjem nekih datoteka, neće se pokrenuti jer je zaobiđena procedura gašenja. Doduše, gube se podaci o procesima, mrežnim vezama i ulogiranim korisnicima. U idealnoj situaciji će se iščupati mrežni kabel prije skupljanja bilo kakvih podataka.
    - `uptime` - vrijeme posljednjeg reboota
    - `who` - trenutno ulogirani korisnici
    - `last` - kratka povijest nedavno ulogiranih korisnika

Skupljanje podataka

	Naredba	Opis

1	`uname -a;`
	`cat /proc/meminfo,`
	`free`
		Ime računala, mrežni čvor, tip procesora, OS i verziju jezgre. “How do we know that this information really came from the computer system in question?”
		Podaci o slobodnoj i iskorištenoj memoriji računala - korisno kod udaljenog pristupa računalu.

2	`date`	Trenutno vrijeme i datum na sustavu. Važno zbog određivanja neusklađenosti između lokalnog vremena i vremena na sustavu.
3	`netstat`	Koje veze dolaze od i prema host računalu. Da bi ovi podaci imali smisla, klijent mora istražitelju dati uvid u normalne operacijske parametre. Tako će istražitelj moći eliminirati dozvoljene veze i fokusirati se na nedozvoljene.
4	`history`	Shell history, daje popis naredbi upisivanih u shell od zadnjeg paljenja.
5	`ps axu`	Koji procesi se vrte. Potrebno usporediti s popisom dozvoljenih procesa dobivenog od klijenta.
6	`w`	Procesi od svakog korisnika. Vrijednost **TTY** polja znači: - `tty#` - korisnik je ulogiran u konzolu. - `ttyp#` ili `pts#` - korisnik je ulogiran s udaljenosti. U tom slučaju polje **From** sadrži IP adresu korisnika.
7	`top`	Koji procesi koriste najviše memorije.
8	`lsof`	Podaci o otvorenim datotekama i o procesima koji su ih otvorili.
9	`chkconfig -list`	Koji procesi se pokreću prilikom paljenja pojedinih RC razina (*Run Control Levels*). Linux standardno ima 5 načina bootanja koje se naziva RC razinama. To su: 0 Halt 1 Single-user mode 2 Basic multi-user mode (without networking) 3 Full multi-user mode (text-based only) 4 not used 5 Full multi-user mode (GUI based) 6 Reboot Na ovaj način se može otkriti postoji li podmetnuta aplikacija ili malware koji su dodani RC skriptama.
10	`cat /etc/crontab`	Pregled kronoloških dnevnika, zapisuju zadatke koji se po izvode po rasporedu. Ovi se podaci razlikuju od podataka u RC skriptama jer se ovi zadaci pokreću neovisno o RC razini u kojoj se sustav pokrene. Također, zadaci se mogu dodavati i izvršavati bez potrebe za rebootom sustava. Podatke iz `crontab` zapisa treba pažljivo usporediti s podacima dobivenima od klijenta.

11	`/etc/passwd,`
	`/etc/shadow,`
	`/etc/groups`
		Podaci o korisnicima, njihovim grupama i korisnicima.
		Može pokazati da li je nešto izmijenjeno ili je dodan neautorizirani korisnički ID. Ovi podaci mogu pomoći u povezivanju zabilježenih aktivnosti i pripadnih ID brojeva. Ne valja srljati u zaključke da ID korisnika nepobitno znači da je baš taj korisnik koristio svoj ID.

	Naredba	Opis
12	`/etc/hosts`, `/etc/hosts.equiv`, `~/.rhosts`, `/etc/hosts.allow`, `/etc/hosts.deny`, `/etc/syslog.conf`, `/etc/rc`, `/etc/inetd.conf`	Lokacije podataka o sustavima kojima host računalo ima pristup, računala koja su se nedavno spojila na metu i lokacije raznih dnevničkih datoteka.
13	`arp -a`	Ispisuje usmjeriteljsku tablicu koja povezuje IP s MAC adresama računala. Može se odrediti da li postoje trajni ARP zapisi te da li su kreirani ARP posrednici što može dobro doći u slučaju Man-in-the-Middle (MITM) napada. U tom napadu, napadač bi u ARP tablici ciljanog računala <Y> zamijenio svoju MAC adresu s psotojećom IP adresom <IP-X>. Nakon toga bi u ARP tablici računala <X> zamijenio IP adresu računala <Y> sa svojom. Sva komunikacija između 2 zatrovana sustava sad ide preko napadača.
14	`ifconfig`	Pomaže u detekciji *sniffera*. U ispisu naredbe treba potražiti pojam PROMISC. To označava mrežnu karticu koja radi u promiskuitetnom načinu rada odnosno koja prima i pakete koji nisu naslovljeni na MAC adresu njenog računala.
15	`nmap -sP <subnet-255>`	Šalje paket svima u podmreži kako bi se otkrilo koja računala su dostupna odnosno koja su odgovorila na ICMP Echo zahjev. Umjesto ICMP paketa (ukoliko su računala podešena da ne odgovaraju na njih), može se poslati i TCP ping. U tom slučaju je potrebno od klijenta doznati koji port koriste sva računala i kojeg ne filtrira vatrozid.
16	`/etc/resolv.conf`, `host <IP-address>`	`resolv.conf` sadži popis *nameservera*, a `host` otkriva *hostname*.
17	`nmap -vv -sV -P0 -O <IP-adresa>`	Otkriva otvorene portove, dostupne servise te traži podatke o operacijskom sustavu računala.