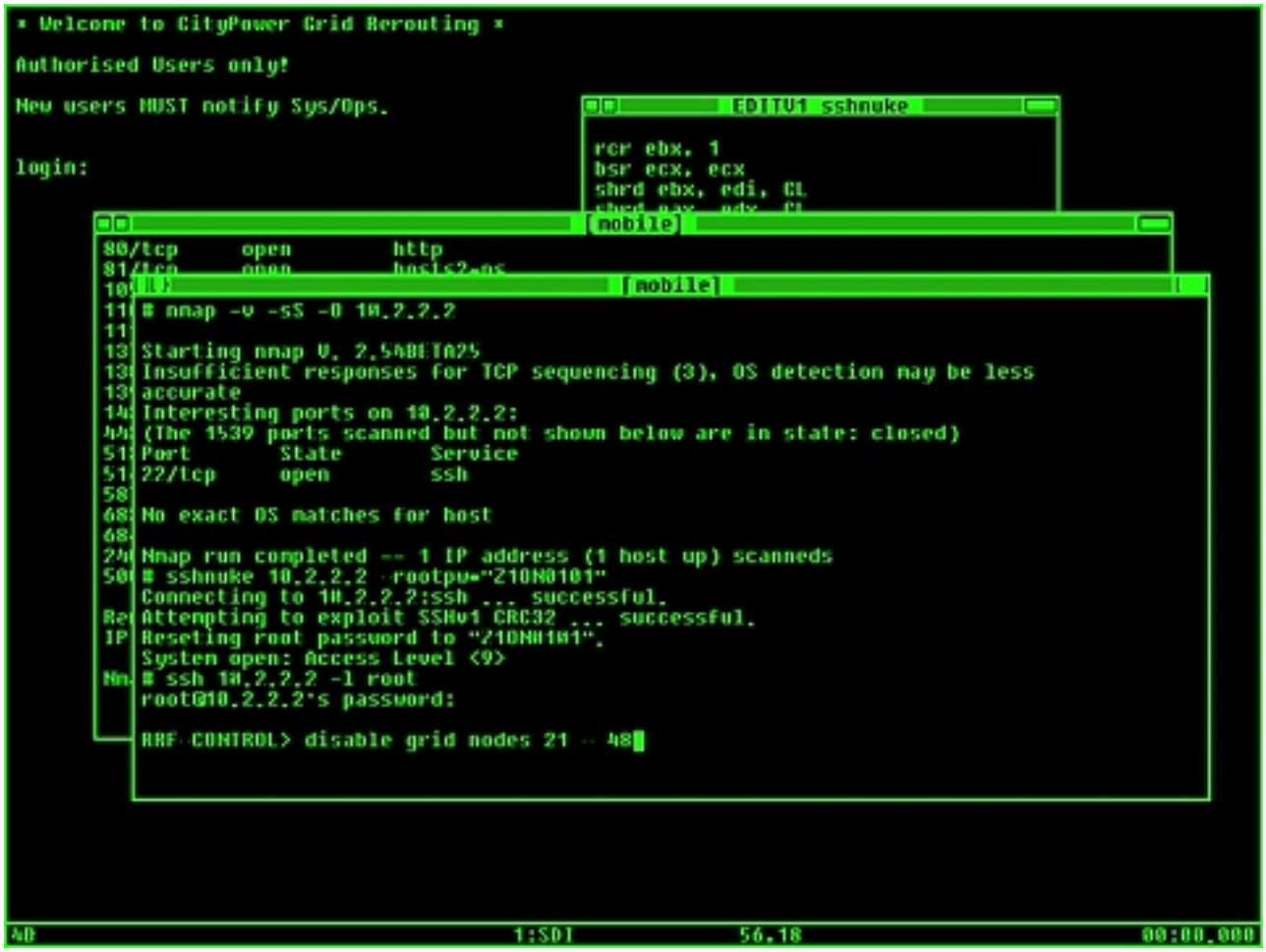

Dalla letteratura cyberpunk abbiamo imparato a conoscere gli ICE che sarebbe l'acronimo di Intrusion Countermeasures Electronics (Contromisure elettroniche anti-intrusione).

La Classificazione:

- **White ICE** - Avverte e semplicemente annota (logga) le intrusioni.

- **Gray ICE** - Oltre ad annotare le intrusioni si difende dagli attacchi in maniera autonoma.

- **Black ICE** - Lo stadio evolutivo finale, non solo si difende ma risponde agli attacchi cercando di danneggiare l'intrusore.

Dopo aver rispolverato i significati, passiamo ad analizzare se nella realtà siamo riusciti a implementare con successo, negli anni, i rispettivi livelli di ICE.

White ICE nella realtà

Si può dire con certezza assoluta che esistono.
Tutti i sistemi che in qualche modo effettuano logs sono dei White ICE. Se pensiamo a un sistema *nix like, quasi tutti i daemons e i processi importanti effettuano in qualche modo il logging di tutto quello che accade e di cui fruisce del servizio. Anche gli [**honey pot**] sono un esempio "passivo" di difesa.

- howto sull'uso delle honey pot
- howto sull'uso di syslog

Gray ICE nella realtà

Possiamo dire con certezza che esistono.
TUtti i sistemi che effettuano delle operazioni dopo aver letto e/o confrontato i logs precedentemente accumulati sono dei Gray ICE. Basta pensare a fail2ban, snort ed altri sistemi che permettono di effettuare delle operazioni (in genere una sorta di banning temporaneo) al raggiungimento di un "punteggio". Portiamo un esempio esemplificativo prendendo come spunto fail2ban.
[**fail2ban**] non fa altro che guardare con molta attenzione i logs che noi gli diciamo di guardare.

Ad esempio possiamo dirgli che dopo un certo numero di tentativi falliti (letti dal log del server ssh) quell'ip va posto in quarantena per un certo periodo temporale.
Questo approccio, nei contesti in cui la sicurezza è una cosa abbastanza importante, viene utilizzato praticamente quasi sempre. Ci sono sofisticati sistemi IDS che possono attivare vari triggers e varie operazioni di chiusura. Uno dei più emblematici è [**knocks**] una sorta di apriti-sesamo che permette, mediante una opportuna combinazione di pacchetti inviati a una opportuna "distanza" temporale di aprirci le porte necessarie. Possiamo asserire che si tratta con certezza di sistemi Gray ICE perchè non si limitano ad ascoltare passivamente ma interagiscono grazie alle regole che gli abbiamo impostato noi amministratori.

- howto sull'uso di fail2ban
- howto sull'uso di knockd

Black ICE nella realtà

Possiamo ipotizzare che esistano, perchè non possiamo provarlo.
Mi prendo la responsabilità di queste parole, pesanti. Ma in piena onestà, io che ho effettuato degli esperimenti in merito, sono assolutamente convinto che esistano dei server che se attaccati reagiscono a loro volta.
La legislatura in merito è abbastanza carente e come sappiamo spesso i buchi vengono riempiti da chi è felice di fare il pioniere. Io stesso ho effettuato dei banali esperimenti in cui istruivo il mio server (con fail2ban) ad effettuare una scansione [**nmap**] dell'attaccante e a provare dei banali attacchi (come l'ssh bruteforce).
Un server che attaccato reagisce non è fantasia o fantascienza, oggi è realtà. Avendo a disposizione interi framework di exploit (qualcuno ha deto [**Metaexploit**]?) ipotizzare la scelta e l'avvio automatico di un attacco non è tanto dissimile dalla realtà.
Ovviamente ci troviamo nella situazione che una opportuna difesa di base e le comuni regole di sicurezza neutralizzano completamente questi attacchi blandi. Questo avviene perchè il sistema di reazione non è raffinato ma basato solo ed esclusivamente su un set di regole causa effetto. Se l'ip 10.10.10.10 mi attacca ed è basato su un sistema windows allora automaticamente posso provare un set di attacchi base. Ma se l'attacker è già un sistema *nix con un sistema default di difesa e con tutte le signature opportunamente eliminate/offuscate, il nostro contro-attacco è destinato miseramente a fallire.
Quando e se metteremo molta più intelligenza (reti neurali, ai, etc) allora avremo semplicemente dei sistemi molto più flessibili e raffinati che riescono a utilizzare meglio gli strumenti a disposizione scegliendoli in maniera accurata in base allo spettro di variabili relative alle difese del nemico.

- howto sull'uso di metaexploit
- howto sull'uso di nmap