Õppevideo: kuidas häkkida elektrivõrku

10 years ago- 29.04.2016 By Kaido Einama

Üks meie mugava tsivilisatsiooni alustalasid on eluliselt tähtsad võrgud - elektrivõrgud, veevarustus, kommunikatsioon... kõiki neid süsteeme juhivad arvutid. Neisse aga on ikka aeg-ajalt sisse häkitud. Häkkerite grupp RedTeam sai loa kolme päeva jooksul sisse murda elutähtsasse elektrivõrku. See õnnestus kui mitte just mängleva kergusega, siis ootamatult lihtsalt kindlasti.

Testi viis läbi Midwesti elektrikompanii USA-s ja üles filmis Business Insider. Häkkeriteks olid RedTeami nn valgemütsid ehk heatahtlikud häkkerid, kes oma tööga näitavad pigem kätte nõrku kohti kui hakkavad kuritahtlikult neid turvaauke ära kasutama.

> **Vaata siit BUSINESS INSIDERI videot kolmepäevasest *whitehat*´ide häkkimisest elektrivõrkudesse**

Grupp sissemurdjaid tegutses kolme päeva jooksul ja sai oma ülesande täidetud. Business Insideri võttegrupp tõdes kolmandal päeval, et kui elektriettevõtted kohe midagi ette ei võta, siis on häkkerite lihtsamat sorti rünnakutega võimalik suurtel aladel "tuled ära kustutada".

Alajaama ja serveriruumi ligipääsud saavutati aga tõesti üsna kergesti. Sealt edasi oli tee valla kuni regionaalse juhtimise ülevõtmiseni. Kasutati ka *Social Engineering*ut ehk psühholoogilist rünnet oluliste ligipääsude väljapetmiseks - teeseldi kohaliku internetiteenuse pakkuja tehnikuid, et pääseda elektrivõrgu haldaja kontorisse ja kuna väljanägemine oli vastav, siis antigi häkkeritele valvuri poolt külalise pääse isikutunnistust küsimata. Suurem ülemus siiski lõpuks sekkus ja niisama *social engineering*uga sisse ei saanud. Nüüd jäi üle sisse murda.

Öösel tuldi tagasi tõsisema varustusega. Mingisse kõrvalisse laoruumi muugiti sisse mõne sekundiga. Alarmi seal ei olnud. Edasi tuli kontoriruumide poole pääseda. Natuke aega hiljem olidki häkkerid sellesama valvurilaua ääres, kust neid päeval edasi ei lastud. Pisut uurimist ja leiti arvutivõrgu (LAN) pesa, kuhu sai sokutada *Plug Bot*i - kavala lutika, mis jälgib sisevõrgu liiklust ja saadab selle info välja jälgijatele. Plug Bot sokutati varjulisse kohta ja ühendati vargapesasse elektritoiteks. Kuna elektrifirma kontoris on niikuinii igasuguseid kaableid ja karpe, siis üks lisakarp ilmselt kellegi tähelepanu ei ärata.

Natukese aja pärast olid tegelased serveriruumis. Lõpuks, kui tundus, et sissetung oli avastatud, lahkuti mõõdetud sammul. "Kõnni, aga ära jookse!" tähendas, et rahulikult jalutavat kampa keegi ei kahtlusta.



Alajaama kaitsesid liikumisandurid ja panoraamkaamera. Droon saadeti neid uurima. Üks sensor kasutas mikrolaineandurit, teine infrapunakiirgust, et avastada soojasid kehasid (nagu inimene). Panoraamkaamerat uurides leiti lõpuks ka pime nurk, mida kaamera ei katnud.

Peale drooniluuret mindi minema ja saabuti ööpimeduses juba kindla plaaniga tagasi.

Kuna kaamera vaatenurk oli välja selgitatud - 270 kraadi, siis oli teada ka lähenemisnurk, kust kaamerasse veel ei jää. Okastraataiast roniti pimedas nurgas üle tavalist tekki kasutades. Vaikselt andureid blokeerides roniti sisse ja avati seadmekapp, kus juhtmed ja pistikupesad on häkkeri jaoks juba sama hea kui sissepääs võrku. Installiti pealtkuulamisseadmed ja asuti sisevõrku jälgima.

Kokku murti niimoodi sisse kaheksasse alajaama ja süsteemi. Mõnesse siseneti tudengitena (ja hiljem RFID pääsukaarte salaja kopeerides), kättesaadavatesse USB pesadesse sokutati USB pulkasid, mis arvuti juhtimise üle võtsid, lõpuks oleks olnud võimalik kõik need alajaamad ka pimedaks lülitada. Elektrifirma

teatas pärast testi, et näidatud turvaaugud kõrvaldati kohe ja enam samamoodi sisse murda ei saa.

Aga mujal ilmselt saab? Seega kui vähegi viitsimist, on tõsisematel häkkeritel võimalik praegu suure tõenäosusega meie heaolu tagavad võrgud välja lülitada ilma mingite pommivõõde ja rakettideta. Varuge küünlaid ja konserve, kui see oht liiga tõsine tundub.

FOTOD: KAADRID VIDEOST

- Uudised
- Turvalisus

Pilt

