Tel. 1843
El. p. cert@nksc.lt
https://www.nksc.lt

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS
PRIE KRAŠTO APSAUGOS MINISTERIJOS

INFORMACINIS BIULETENIS

KIBERNETINIO INCIDENTO TYRIMUI BŪTINOS INFORMACIJOS SURINKIMAS IR IŠSAUGOJIMAS „LINUX“ OPERACINĖSE SISTEMOSE

2024 m. liepos 1 d.
Vilnius

Nacionalinis kibernetinio saugumo centras (toliau – NKSC) jau rašė apie tyrimams būtinų įrodymų ***„Windows“*** šeimos operacinėse sistemose išsaugojimo svarbą, įrankius, komandas ir metodus. Daugiau informacijos rasite - https://www.nksc.lt/doc/biuleteniai/2024_01_29_irodymu%20issaugojimas.pdf.

Tiek ***„Windows“***, tiek ir ***„Linux“*** šeimos operacinėse sistemose **neatlikus** išsamaus kibernetinio incidento **tyrimo** ir neišsiaiškinus incidento atsiradimo priežasčių bei pasekmių, išlieka didelė tikimybė, kad: **incidentas pasikartos**, **nebus identifikuotos visos pažeistos sistemos/įrenginiai, nenustatyti piktavalių atlikti veiksmai** ir pan.

Šiame informaciniame biuletenyje priminsime kokius veiksmus reikėtų atlikti siekiant maksimaliai sumažinti informacijos, reikalingos kibernetinio incidento tyrimui, praradimo tikimybę. Pateiksime įrankius ir komandas, kurių pagalba galima greitai ir paprastai surinkti pirminę informaciją apie ***„Linux“*** šeimos operacinėse sistemose vykstančius procesus, naudotojus/grupes, tinklo sujungimus ir pan. Pažymime, kad atsižvelgiant į kibernetinio incidento tipą ir poveikį, visada reikia įvertinti, kokius veiksmus reikėtų atlikti pirmiausiai: sustabdyti failus šifruojančio žalingo programinio kodo veikimą ar sukurti operatyviosios atminties atvaizdą.

Operatyviosios atminties atvaizdo sukūrimas

Operatyviosios atminties analizė užima svarbią vietą kibernetinio incidento tyrime. Siekiant apeiti kibernetinio saugumo priemones, pasislėpti ar paslėpti įkalčius, piktavaliai stengiasi žalingą programinį kodą įdiegti tiesiai į įrenginio operatyviąją atmintį. Dažniausiai operatyviojoje atmintyje žalingas programinis kodas saugomas neužkoduotas ar neužšifruotas. Aptikus žalingą programinį kodą ir jį išanalizavus pavyksta nustatyti kokius veiksmus atliko piktavaliai ar kokį užsibrėžtą tikslą jie norėjo įvykdyti.

Siekiant neprarasti kibernetinio incidento tyrimui svarbios informacijos, kuri gali būti išlikusi įrenginio operatyviojoje atmintyje, rekomenduojame pirmiausiai, **neatliekant jokių kitų veiksmų**, sukurti ir išsaugoti operatyviosios atminties atvaizdą. Operatyviosios atminties atvaizdas priklausomai nuo naudojamos programinės įrangos gali būti išsaugotas skirtingais formatais: ***„raw“***, ***„lime“*** ar ***„padded“***. Rekomenduojame naudoti ***„raw“*** formatą.

Tel. 1843
El. p. cert@nksc.lt
https://www.nksc.lt

Operatyviosios atminties atvaizdą galima sukurti pasinaudojus nemokama trečiųjų šalių programine įranga, pavyzdžiui:

- ***„LiME“***, https://github.com/504ensicsLabs/LiME;
- ***„Fmem“***, https://github.com/NateBrune/fmem;
- ***„Avml“***, https://github.com/microsoft/avml.

Naudojantis virtualizacijos platformomis, operatyviosios atminties atvaizdą galima sukurti pačių platformų priemonėmis. Detalesnės informacijos reikėtų ieškoti virtualizacijos platformos gamintojo oficialioje dokumentacijoje, pavyzdžiui:

- https://kb.vmware.com/s/article/2003941.

Disko atvaizdo sukūrimas

Norint išsaugoti kuo daugiau informacijos, susijusios su kibernetiniu incidentu, visada rekomenduojame sukurti ir išsaugoti įrenginio „kietojo“ disko atvaizdą (angl. *image*). Toks būdas laiko atžvilgiu nėra efektyvus, tačiau minimizuoja informacijos (įkalčių/artefaktų) praradimą ar sugadinimą. Reikėtų pažymėti, kad disko atvaizdai užima daug vietos, tad reikėtų pasirūpinti vieta/disku, kur bus saugomas disko atvaizdas. Disko atvaizdas gali būti išsaugotas skirtingais formatais priklausomai nuo naudojamos programinės įrangos. Dažniausiai ***„Linux“*** operacinėse sistemose naudojama ***„dd“*** komanda, kurios pagalba ir sukuriamas disko atvaizdas, pavyzdžiui:
„sudo dd if=/dev/sda of=/path/to/file/atvaizdas.img bs=4M conv=sync,noerror status=progress“

„if=/dev/sda“ – įvesties failas, nurodomas diskas (***„sda“***, ***„sdb“***, ***„sdd“*** ir pan.) kurio atvaizdas bus sukurtas;
„of=/path/to/file/atvaizdas.img“ – išvesties failas, nurodoma direktorija ir failo pavadinimas;
„bs=4M“ – bloko dydis (gali būti keičiamas);
„conv=sync,noerror“ – nurodoma tęsti veikimą nepriklausomai nuo klaidų ir sinchronizuoti duomenis;
„status=progress“ – atvaizduojama komandos (vykdomos operacijos) būsena.

Daugiau informacijos apie ***„dd“*** komandą galima sužinoti surinkus komandą ***„man dd“***.

Naudojantis virtualizacijos platformomis, daugeliu atveju, atskirai disko atvaizdo kurti nereikia, kadangi virtualus diskas saugomas kaip failas. Virtualaus disko formatas priklauso nuo virtualizacijos platformos gamintojo. Dažniausiai naudojamų virtualių diskų formatai: ***„vmdk“***, ***„vhd“***, ***„vhdx“*** ar ***„vdi“***.

Pirminės informacijos surinkimas

Kaip jau buvo minėta, įvykus kibernetiniam incidentui, labai svarbu surinkti, išsaugoti ir nesunaikinti informacijos, reikalingos kibernetinio incidento tyrimui. Kartais sukūrus ir išsaugojus įrenginio operatyviosios atminties atvaizdą, kibernetinio incidento tyrimui ar situacijos suvaldymui kyla būtinybė surinkti pirminę informaciją veikiančioje (angl. *live*) sistemoje.

Pirmiausiai rekomenduojame patikrinti:

- vykdytų komandų įstoriją (***„.bash_history“***, ***„.zsh_history“***);

Tel. 1843
El. p. cert@nksc.lt
https://www.nksc.lt

- naudotojus, jų teises ir grupes;
- tinklo sujungimus (angl. *network connections*), tinklo prievadus;
- įdiegtą programinę įrangą (paketus);
- sisteminius uždavinius (***„cron“***);
- įdiegtus servisus;
- tinklo parametrus ir konfigūraciją;
- ***„kernel“*** modulius;
- programinę įrangą, kuri sukonfigūruota startuoti operacinės sistemos startavimo metu arba (naudotojo) prisijungimo metu;
- ***„SSH“*** autorizacijos raktus ir žinomas ***„SSH“*** stotis;
- veikiančius procesus;
- ***„arp“*** lentelę ir ***„dns“*** nustatymus;
- direktorijas: ***„/tmp/“***, ***„/var/tmp/“*** ir ***„/dev/shm/“***
- įvykių žurnalus (angl. *logs*).

1 lentelė. Komandų pavyzdžiai

Komanda	Komentaras
cat	Komandos pagalba galima tikrinti failo turinį (išspausdinti į ekraną (konsolę)), pavyzdžiui, peržiūrėti ***„root“*** naudotojo vykdytų komandų įstoriją ***„cat /root/.bash_history“***
cat /etc/passwd	Gaunama informacija apie operacinėje sistemoje veikiančius/sukurtus naudotojus (angl. *users*)
cat /etc/group	Gaunama informacija apie operacinėje sistemoje veikiančių/sukurtų naudotojų (angl. *users*) grupes
cat /etc/shadow	Gaunama informacija apie operacinėje sistemoje veikiančių/sukurtų naudotojų (angl. *users*) slaptažodžius, jų galiojimą laiką ir pan.
cat /etc/sudoers	Gaunama informacija apie naudotojų, turinčių *„sudo“* teises, konfigūraciją
whoami, ***id***, ***who***, ***logname***	Gaunama informacija apie šiuo metu prisijungusius naudotojus, jų ***„id“***, grupės ***„id“*** ir pan.
netstat	Gaunama informacija apie tinklo sujungimus, maršrutizavimo lentelės, tinklo prievadus ir pan, pavyzdžiui, ***„netstat –atupen“***. Priklausomai nuo ***„Linux“*** distribucijos ar versijos gali prireikti papildomai įdiegti ***„net-tools“*** programinės įrangos paketus
cat /var/lib/dpkg/status ***cat /var/log/dpkg.log*** ***rpm -qa --root=/mntpath/var/lib/rpm*** ***ls -la /usr/sbin/***	Gaunama informacija apie įdiegtą programinę įrangą (paketus). Rekomenduojame peržiūrėti visas direktorijas, failus ar įvykių žurnalus

Tel. 1843
El. p. cert@nksc.lt
https://www.nksc.lt

ls -la /usr/bin/ ***ls -la /bin /sbin/*** ***find / -type f -executable***	
cat (ls -la) /var/spool/cron/crontabs/* ***cat (ls -la) /var/spool/cron/atjobs*** ***cat (ls -la) /var/spool/anacron*** ***cat (ls -la) /etc/cron**** ***cat (ls -la) /etc/at**** ***cat (ls -la) /etc/anacrontab*** ***cat (ls -la) /etc/incron.d/**** ***cat (ls -la) /var/spool/incron/****	Gaunama informacija apie sisteminius uždavinius. Rekomenduojame peržiūrėti visas direktorijas ar failus
cat /etc/inittab ***ls –la /etc/rc.d/*** ***ls –la /etc/rc.boot/*** ***ls –la /etc/init.d/*** ***cat /etc/inetd.conf*** ***ls –la /etc/xinetd/*** ***ls –la /etc/systemd/system*** ***ls –la /etc/systemd/system/multi-user.target.wants/*** ***ls –la /usr/local/etc/rc.d/***	Gaunama informacija apie įdiegtus servisus. Rekomenduojame peržiūrėti visas direktorijas ar failus

Tel. 1843
El. p. cert@nksc.lt
https://www.nksc.lt

ls –la ~/.config/autostart/ ***ls –la /lib/systemd/system/***	
cat /etc/hosts ***ls –la /etc/networks/*** ***ls –la /etc/netplan/*** ***cat /etc/resolv.conf*** ***cat /etc/nsswitch.conf***	Gaunama informacija apie tinklo parametrus ir konfigūraciją. Rekomenduojame peržiūrėti visas direktorijas ar failus
ls –la /lib/modules/$(uname -r) ***ls –la /etc/modprobe.d*** ***ls –la /etc/modprobe*** ***cat /etc/modprobe.conf***	Gaunama informacija apie ***„Linux“ „kernel“*** modulius. Rekomenduojame peržiūrėti visas direktorijas ar failus
ls –la /etc/profile.d/* ***cat /etc/profile*** ***cat /etc/bash.bashrc*** ***cat ~/.bashrc*** ***cat ~/.bash_profile*** ***cat ~/.profile*** ***cat ~/.config/autostart*** ***cat /etc/rc.local***	Gaunama informacija apie programinę įrangą, kuri sukonfigūruota startuoti operacinės sistemos startavimo metu arba (naudotojo) prisijungimo metu. Rekomenduojame peržiūrėti visas direktorijas ar failus
cat ~/.ssh/authorized_keys ***cat ~/.ssh/known_hosts***	Gaunama informacija apie ***„SSH“*** autorizacijos raktus ir žinomas ***„SSH“*** stotis (raktus)
ps, htop	Gaunama informacija, apie veikiančius procesus, pavyzdžiui, ***„ps –aux“***
arp –a	Gaunama ***„arp“*** lentelės (angl. *ARP table*) informacija
ls –la /var/log/*	Gaunama informacija apie ***„Linux“*** operacinėje sistemoje saugomus įvykių žurnalus

Įvykių žurnalų surinkimas ir išsaugojimas

Tel. 1843
El. p. cert@nksc.lt
https://www.nksc.lt

Viename iš informacinių biuletenių jau rašėme, kad labai svarbu tinkamai sukonfigūruoti auditavimo, įvykių žurnalų registravimo ir saugojimo funkcionalumą. Suprantama, kad tai reikėtų atlikti nelaukiant kada įvyks kibernetinis incidentas. Daugiau informacijos kaip tai atlikti rasite - https://www.nksc.lt/doc/biuleteniai/2021-12-01-Linux.pdf.

„Linux“ šeimos operacinėse sistemose (***„Debian-based“ ar „RPM-based“***) įvykių žurnalai saugomi kataloge (direktorijoje) ***„/var/log/“***. Reikėtų paminėti, kad darbo ar tarnybinėse stotyse įdiegta papildoma programinė įranga, įskaitant ir saugumo priemones, gali kaupti atskirus įvykių žurnalus. Jų saugojimo vieta priklauso nuo konkrečios programinės įrangos, todėl reikėtų nepamiršti išsaugoti ir šių įvykių žurnalų.

Įsilaužus į įstaigos vidinį tinklą, piktavaliai stengiasi pasiekti kuo daugiau resursų, atlieka žvalgybą, pavyzdžiui skenuoja tinklo prievadus ar ieško pažeidžiamumų, kuriuos galėtų vėliau išnaudoti tolimesnėms atakoms. Svetainių/informacinių sistemų prieigos, el. pašto, tinklo įrangos (pavyzdžiui ***„NetFlow“***), ugniasienių ar saugumo priemonių įvykių žurnalai neretai leidžia gauti svarbios ir naudingos informacijos apie kibernetinį incidentą bei padeda identifikuoti pažeistas sistemas ar įrenginius.

Surinktos informacijos saugojimas ir perdavimas

Surinkus kibernetinio incidento tyrimui reikalingą informaciją, būtina užtikrinti jos integralumą. Vienas iš paprasčiausių būdų – apskaičiuoti perduodamos informacijos (failo) kontrolinę sumą. ***„Linux“*** operacinėse sistemose komandų: ***„md5sum“***, ***„sha1sum“***, ***„sha224sum“***, ***„sha256sum“***, ***„sha384sum“*** ar ***„sha512sum“*** pagalba galima apskaičiuoti failo ***„md5“***, ***„sha-1“***, ***„sha-224“, „sha-256“***, ***„sha-384“*** ar ***„sha-512“*** kontrolines sumas. Skaičiuojant failų kontrolines sumas rekomenduojame naudoti neprastesnį kaip ***„sha-256“*** algoritmą. Pavyzdžiui, ***„sha256sum /home/nksc/memory_dump.img“***.

Būtina užtikrinti, kad kibernetinio incidento tyrimui reikalinga informacija būtų **saugoma atskirai** nuo paveiktų sistemų ar įrenginių. Informacijos perdavimą tretiesiems asmenims ar organizacijoms (paslaugų teikėjams) būtina dokumentuoti, pavyzdžiui, pasirašant priėmimo/perdavimo aktą.